EMA Response to the EBA Discussion Paper on future draft RTS on Strong Customer Authentication and Secure Communication under the revised PSD2

The Electronic Money Association is the trade body for electronic money issuers and innovative payment service providers, and our members include leading payments and e-commerce businesses worldwide, representing online payments, card-based products, vouchers, and those employing mobile channels of payment. A list of EMA members is given in the Appendix of this document. The EMA has participated in the evolution of innovative payments from small niche offerings to a growing sector that is offering alternatives for payments to consumers and businesses alike, and we develop industry good practice in areas of compliance, customer service and enable the sharing of know-how.

Our members are regulated electronic money institutions, payment institutions and some are credit institutions. They are all subject to the provisions of the PSD and will be subject to the provisions of the proposed PSD2.

The opinions expressed are those of the EMA as a whole and may not represent the view of individual members.

1. Background

The EBA published a Discussion Paper (**DP**) seeking feedback on issues related to strong customer authentication (**SCA**), the protection of personalized security credentials (PSC) and the requirements for common and secure open standard of intra-PSP communication on 8 December 2015. Responses to the EBA DP can be submitted until **8 February 2016**.

EMA members have reviewed the DP and are providing the feedback listed below to the 20 Questions detailed in the Paper.

General comments on the Discussion Paper are provided first; these are followed by feedback to each of Questions in the Paper.
General comments include:

- A Reference (**Ref**): This is the Paragraph number of the DP that gives rise to a Comment.
- **Comment**: Detailed feedback, including justification/rationale for any points raised; where applicable, alternative controls/methods that are proposed.

FEEDBACK

Organisation Name	**Electronic Money Association ("EMA")**
Name of individual (*providing feedback on behalf of the organisation***)**	Dr. Thaer Sabri, Chief Executive
Date of Submission:	8th February 2016

2 Overall Comments

2.1 Background and rationale (Section 3)

Discussion Paper Reference	***Comment***
Par.6, 15, 61, 62	Based on the timeline stated in the referenced Discussion Paper Articles, we understand that it is likely that the EBA RTS will specify the requirements for common and secure open standards of intra-PSP communication rather than develop or maintain such standards. Additionally, we understand that the earliest possible application date of these EBA RTS is October 2018; that is, at least 10 months after the deadline for the transposition of PSD2 in national legislation across the EEA. Given the key role of the RTS in PSPs' ability to implement PSD2 requirements on SCA and intra-PSP communication, it would be helpful if it was made clear that compliance would not be enforced in the interim period. It would be helpful if the EBA would, in the meantime, provide guidance on this issue in its forthcoming Consultation Paper.
General	Many of our members are PSPs that are regulated in an EEA territory and offer payment services around the world. The development of customer authentication and communication solutions specifically for EEA users would lead to an inconsistent customer experience, customer confusion and may even increase the scope of some social engineering/phishing attacks. Additionally, the introduction of over-engineered, prescriptive, customer authentication & intra-PSP communication protocols could disadvantage our Members in their efforts to compete with other global payment industry players.

	Therefore, we would urge the EBA to take into account the impact of the RTS that will be drafted on the operations of global PSPs that are registered in an EEA territory. Some flexibility in the implementation of the RTS should therefore be afforded to PSPs with a global footprint.
General	We are strong advocates of a risk-based approach in the design of security controls or of a security requirements framework. Our Members employ a range of risk management processes to monitor/track a range of risks on an ongoing basis and deploy remediation measures if certain risks exceed agreed thresholds. A Cost-Benefit Analysis is often employed to assess the viability of proposed remediation measures and their contribution to lowering a PSP's risk exposure. EMA Members would also highlight that payment fraud typically migrates to target the weakest links in the global payment industry security chain. Currently, payment card credential databases that can be used to create counterfeit cards (or carry out remote purchases) in territories/merchants outside the EEA are a favourite target of organised security attacks. The fraud impact of these attacks (to PSPs and to individual customers) will not likely be lowered even after the adoption of the RTS that the EBA is developing. Thus, we would urge the EBA to adopt a risk-based approach in the design of the RTS that it is developing to address Strong Customer Authentication (SCA) and secure intra-PSP communication. In our view, an analysis of the expected benefits (in lowering fraud levels) against the "cost" (to customer experiences and PSP operations) should be employed in the design of the proposed RTS.
General	The EMA believes that the RTS that will be drafted by the EBA should: ➢ Identify a set of principles/requirements to be met by APIs/authentication solutions that will be developed by independent 3rd parties. These requirements should be detailed enough to allow a multi-stakeholder Governance Body (*see separate comment below*) to assess the compliance of independent solutions; however, they should not be so detailed (e.g. exhaustive lists) that they inhibit the development of innovative solutions or become rapidly outdated as new types of attacks appear.
General	PSD2 is set to facilitate the deployment of new payment interactions including those a Payment Service User (PSU) initiates through a Third Party Provider (TPP) such as PI-PSP or AI-PSP. The scope of sharing of users' Payment Security Credentials (PSCs) across PSPs in such interactions is left unclear in the PSD2 text. Currently, a number of such interactions are already supported employing solutions that do not involve the sharing of PSCs outside the PSU and the issuer of the PSCs. It is our view that the EBA RTS should seek to: ➢ Define PSC assurance thresholds and confirm how these may be impacted by sharing of PSCs beyond the PSU and the issuer of these credentials and, ➢ Explore the fraud/liability risk "ownership" implications when such PSCs are shared across different entities in a multi-party

	payment service delivery chain.
General	The EMA believes that the EBA should seek to define an RTS Governance Framework that will be employed to assess compliance of independent SCA & communication solutions with the RTS. This may involve a central EEA body or relevant teams established within each national competent authority. This should have meaningful industry representation to enable the provision of practitioner expertise and the inclusion of new and innovative developments. It would also enhance industry support and adoption.

3 Questions

3.1 Considerations prior to developing the requirements on strong customer authentication (Section 4.1)

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:	The RTS should seek to provide a tighter identification of the types of customer online account interactions that require PSPs to apply SCA. The existing PSD2 text references to: • "*Accesses its payment account online*" [Article 97(1)a] and, • "*Any action, through a remote channel, which may imply a risk of payment fraud or other abuses*" [Article 97(1)c] provide a very loose characterisation of payer online account interactions that can be interpeted to encompass the majority of such interactions even when no sensitive payment data or PSC are exposed. Interactions between AI-PSPs and AS-PSPs that involve the exposure and re-use of payment service user PSCs (originally established & delivered by the AS-PSP to the PSU) can give rise to risk of compromise of such credentials if the communication channel is not secure. These credentials may subsequently be used to obtain unauthorised access to the AS-PSP account. Additionally, interactions between TPPs and AS-PSPs that impede the ability of the latter to perform their standard Fraud Monitoring (for example, due to the lack of payee information) may give rise to increased risks of fraud. Changes to some payment account settings (e.g. account thresholds, contact details, payee whitelists) can give rise to additional fraud risk and should be covered by the requirement to complete SCA.
Rationale:	Many online account access interactions (i) do not expose sensitive payment data/ PSC and (ii) cannot be used to alter existing account settings; thus, they do not give rise to payment fraud risks. They should be excluded from the requirement to carry out SCA and listed as an example in the low-risk transaction SCA exemption category (*see Comment under Question 7, below*).
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"-based authentication elements that can only be used/accessed under the control of the legitimate PSU should be eligible for use to complete SCA. Such elements may be **physical** (PIN Pad, mobile device, chip card, Secure Element in a mobile device) or **virtual/data** (device digital certificate, electronic payment credentials provisioned to a customer device, device/application Token etc.).

	Ensuring that physical possession-based authentication elements can only be controlled by the PSU will typically leverage (a) A secure customer registration process, (b) A secure distribution process that leverages previously-registered/verified contact details, (c) A separate "activation" process and (d) Guidance provided to PSUs on the need to keep such elements under their control at all times and report lost/stolen/compromised physical elements or mobile devices. Limiting access to virtual possession-based authentication elements to the legitimate PSU usually leverages secure distribution/provisioning processes to previously-registered target customer devices. Using these processes, the virtual authentication element is typically cryptographically bound to some unique/persistent characteristic of the target device that is difficult to alter or manipulate. A separate "activation" step may follow that involves extended PSU authentication; typically, this leverages existing customer account information. The process of limiting the use of data-based authentication elements to a specific physical device (or a set of devices) limits the risk of exposure/re-use of these elements by an unauthorised party and supports a PSP's efforts to build up a Customer Profile. Additional authentication element access controls may be incorporated: ➢ In the design of a user interface/application client that needs to be used to access data-based possession authentication elements, ➢ Through the use of the target device's customer access interface if this interface is open for use by 3rd party application developers; this may leverage independent inherence or knowledge-based authentication elements. It is worth noting that possession-based authentication elements are mostly used alongside other independent authentication elements (e.g. knowledge-based) to provide increased confidence that a payment interaction is initiated by a legitimate PSU.
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:	Inherence authentication elements should be uniquely associated with a payment service user. Typically, biometrics (fingerprint, iris scan, facial scan, voiceprint etc.) are used to complete user authentication using inherence-based authentication elements. Since behaviour-based transaction characteristics cannot be uniquely attributed to a payment service user, they are not appropriate to use to complete SCA. Instead, such characteristics are typically used – as part of a transaction risk assessment process – to identify low risk transactions that are exempted from the need to complete SCA. The use of behaviour-based characteristics, as part of a transaction risk analysis process, is dependent on the existence of an established Customer Profile, for the PSU attempting to initiate a payment account interaction.

	While drafting the RTS, we feel it is also important for the EBA to evaluate the impact of existing data protection requirements on processes that can facilitate the sharing of customer behaviour-based characteristics. PSPs may find it difficult to demonstrate to external parties that they have complied with SCA requirements by using certain inherence elements, if they are prevented from sharing such elements with external parties due to applicable data protection regulations.
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 growing use of mobile devices to initiate remote payment transactions limits the independence/"separation" of authentication elements used in multi-factor user authentication processes. The compromise of a customer's mobile device may allow an attacker to gain access to multiple authentication elements (inherence or possession-based) stored in/delivered to or accessed through that device. The use of Trusted Execution Modules/Secure elements to store authentication elements in an increasing number of mobile devices can minimise the risk of such elements being compromised if the device falls outside the control of the legitimate user. Increasingly, PSPs are required to design customer registration processes that leverage multiple communication channels (fixed line, mobile, wireless, VoIP, e-mail) and secure communication protocols (using end-to-end encryption) or 3rd party communication platforms (use of social media accounts etc.) to deliver independent authentication elements to the legitimate PSU. A number of additional risk-based factors (behavioural, device-based etc.) are used to flag mobile payment interactions where additional customer authentication should take place. When drafting the RTS, we would encourage the EBA to: ➢ Acknowledge the operational difficulties that the growing use of the mobile channel introduces in this respect and, ➢ Ensure that a risk-based, flexible approach is applied to the requirement to ensure authentication element "independence".
5. Which challenges do you identify for fulfilling the objectives of strong customer authentication with respect to dynamic linking?	
Response:	The lack of a definition for "dynamic linking" in PSD2 makes it difficult to fully assess the challenges involved in completing SCA that comprises elements "*dynamically*" linked to particular amount/payee transaction information. The RTS that are drafted by the EBA should seek to provide additional clarity on this point by providing examples (not an exhaustive list!) of mechanisms that can be used to deliver such linking in the context of a customer authentication. In any case, a significant challenge to the proposed linking of SCA with "dynamic" transaction information is that it will add very significant friction to existing customer online payment interaction flows for certain types of PSPs (*e.g. wallet providers, merchant payment processors for merchants that use direct-debit/standing order/recurring transaction payment arrangements*). These typically comprise an initial customer authentication session followed by a series of payment transactions that may be authorised individually without the

	need for separate customer authentication until risk/account usage thresholds are reached. A number of mechanisms (timestamps, unique transaction identifiers) can be used to ensure the uniqueness of each transaction; user interface/application design controls can be used to request that an authenticated PSU explicitly authorises every transaction before an attempted transaction can be completed. However, such controls can be compromised by device/OS malware or poor application access controls. This may result in the EBA having to specify User Interface/Application Design criteria that would be needed to facilitate the development of secure User Interfaces. This would not be a desirable approach.
Alternative:	We suggest that a flexible approach to the concept of dynamic linking should be taken by the EBA and EU regulators: whilst every transaction should be authorised separately, users could be periodically prompted to re-authenticate themselves on a risk-based basis rather than for each transaction. This approach would strike a pragmatic balance between PSU authentication, transaction authorisation and a low-friction user experience.
6. In your view, which solutions for mobile devices fulfil both the objective of independence and dynamic linking already today?	
Response:	A number of mobile payment solutions are available in the market that employ SCA and a payment application user interface design that requires the user to authorise every attempted payment transaction. These comprise: ➢ Mobile SMS Tokens that includes transaction information (if the payment interaction is initiated via PC/tablet/mobile browser and the transaction validation/authorisation is provided through a standalone mobile payment application or an e-mail), ➢ A dedicated mobile customer authentication application that can receive secure transaction information (from a PSP) and interact with the PSU to obtain authorisation, ➢ A mobile payment application if it is logically separated from the shopping/order channel (e.g. access to PSCs is only managed by the payment application) and individual transaction data are used to compile payment notification/authorisation messages, ➢ Physical hardware tokens (standalone or securely connected to a customer device) that can be used to generate cryptographic signatures that include individual transaction data or display payment transaction notification messages with individual approval codes forwarded by the PSP that manages the payment account.

3.2 Exemptions to the application of strong customer authentication

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

Response:	The clarifications on the potential exemptions to SCA listed in paragraph 42 are useful. Additional EBA guidance on types of "low-risk" transactions would be welcome; as stated earlier, our Members are looking for examples rather than a definitive list of such transactions! The definition of whitelists in paragraph 42 (Bullet Point B) appears overtly restrictive; the PSP should also be allowed to build up a list of trusted payees that benefit from an exemption to the need to complete SCA (e.g. based on merchant type, a previously-received authorisation as part of a series of recurring transaction/standing order etc). EMA Members that offer Account Information services would also welcome some additional clarity on the scope of the wording in paragraph 42 (Bullet Point E); our assumption is that account balance/status data does not constitute "sensitive payment data" and services that only display these can benefit from this exemption.
8. Are there any other factors the EBA should consider when deciding on the exemptions applicable to the forthcoming regulatory technical standards?	
Response:	When drafting the RTS, we would encourage the adoption of a risk-based approach to identifying SCA exemptions. Such an approach acknowledges wider factors associated with an attempted transaction (e.g. payment channel used, amount, payee, transaction type, recurrence, device profile information, alignment with existing customer profile) to allow PSPs to meet PSD2 security requirements without severely impacting customer experience.
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:	Contextual information about an attempted transaction and customer device status/location information can be combined with customer profile information to identify "low-risk" transactions. Payee information may not always be available to use/accurate enough to support an effective transaction risk analysis. Payment channel criteria may also be leveraged in a transaction risk analysis process. Finally, the overall assessment of the payment threat environment (leveraging security intelligence, data analytics or even law enforcement updates) can be used to support a transaction risk analysis process. Any minimum transaction risk analysis capabilities (and transaction information) the EBA proposes to define in a future RTS should allow the use of alternative risk information to carry out such analysis. This would reflect differences in the availability of such information across different parts of the payment industry.

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

3.3.1 Background on PSD2 provisions

10. Do you consider the clarification suggested regarding the protection of users personalised security credentials to be useful?	
Response:	The clarifications that the EBA proposes to provide in future RTS (on the security afforded to user PSC) as listed in Article 52 are useful. We believe that the clarification provided in the RTS should also address the security principles that apply to the subsequent safe use of delivered PSCs to initiate payment transactions in a range of environments especially when multiple PSPs (AI-PSPs/PI-PSPs and an AS-PSP) are involved.
11. What other risks with regard to the protection of users' personalised security credentials do you identify?	
Response:	Additional payment fraud risks related to the use of PSCs that future EBA RTS should address comprise: ➢ The unintended/unauthorised use of legitimate PSCs (through PSP/payee/transaction spoofing, man-in-the-middle or replay attacks), ➢ Compromise of PSCs shared with rogue 3rd party PSPs/TPPs, ➢ Denial of access/service/availability attacks that impact a PSU's ability to access their online payment account, ➢ PSC lifecycle risks (related to the replacement/withdrawal/suspension of credentials) that may give rise to repudiation of legitimate transactions. In this context, we feel that the issue of secure identification/registration of PSPs in a manner that allows them to be verified by other PSPs should be addressed by the RTS.
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:	PSC issuers use a range of solutions to securely enrol PSUs before delivering payment credentials to the legitimate users. Some of the more innovative solutions comprise: ➢ Leveraging national/industry-wide ID schemes that are widely used in some EEA territories (e.g. Germany, Scandinavia, Baltics etc),

	➢ On-device generation of temporary credentials (to bootstrap the enrolment process) using client devices that have a segregated Trusted OS-controlled Zone or a hardware security module (Secure element), ➢ Leveraging a previously-registered customer device (to push a mobile customer registration/authentication application that is bound to that device); the biometric authentication interface of the device may be leveraged to support this process if is available for use to 3rd parties. ➢ Leveraging a physical payment instrument (e.g. a payment card previously issued to the target PSU) used in a secure interface (e.g. ATM) to kick off the customer enrolment process. ➢ Application Tokens (that are time-limited and device/channel-specific) distributed over secure communication channels to a registered customer device; these often leverage device manufacturer or MNO device management infrastructure.
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?	
Response:	Self-certification (against a defined requirements' evaluation framework) can be an alternative to independent/3rd party security evaluations. Such an approach can be supplemented by periodic 3rd party evaluation assessments depending on a PSP's risk profile. An RTS Governance Body would use parameters such as transaction volumes, levels of fraud, scope of services to build up a PSP risk profile. This hybrid approach is already used successfully by a range of payment industry security standards (e.g. PCI-DSS, PA-DSS). We would also suggest that an EBA proposal - to recommend 3rd party evaluation/certification of PSP systems/technical components- considers the logistics of establishing a transparent evaluation framework that applies to different types of PSPs. The scope of systems that will need to be certified is extremely wide and not all solutions will be suitable for all types of PSPs. Finally, we hope that the EBA RTS will take into account existing market dynamics; historically, the appetite of global customer device/OS manufacturers/MNOs to submit their devices for payment industry-driven standard certification has been limited. Where such certification has happened, it has led to limited device options or higher device costs that have inhibited customer take up or disrupted widespread service deployments.
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:	The risks to PSCs differ in different segments of the payment chain. The devices used by PSUs to access PSP services are a frequent target of attack since individual users often do not deploy/update security software on these devices; this makes them susceptible to virus/malware that seeks to compromise payment credentials.

	Large databases (of AS-PSPs or cloud IT service providers) holding large numbers of PSCs are usually protected by multiple security controls; however, they are targeted by more sophisticated attackers that wish to gain access to multiple credentials that allow them to harvest large numbers of credentials and use them to execute quickly-scalable fraud. PSD2 introduces new types of communication between PSPs that often have no previous commercial relationship; this communication will also likely be targeted by attackers wishing to access PSCs that may be communicated between PSPs. The EBA RTS should provide guidance on how to preserve the confidentiality & integrity of PSCs; such guidance should be applicable to multiple payment industry segments.

3.4 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:	The clarifications provided in paragraph 63 are suitable; they should be expanded to cover: ➢ The identification/authentication of PSPs by PSUs; this may pose a particular challenge for TPPs when there is no prior relationship between the PSU and the TPP that is offering a specific payment service to the user, ➢ The registration/verification of PSPs (as part of an RTS Governance framework), ➢ The process a PSP can use to confirm that a communication API complies with PSD2 requirements and the EBA RTS.
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:	We believe that, as a minimum, the clarifications provided in the RTS should: ➢ Detail the security requirements applicable to the different types of intra-PSP communication, ➢ Specify a compliance assessment/evaluation framework that can be used to assess whether an API developed by a 3rd party complies with the RTS; this may be provided in the context of the definition of a wider RTS Governance Framework ➢ Describe a process for verifying/registering PSPs that wish to communicate in compliance with the RTS; the process should allow PSPs that have no previous relationship to verify the authenticity of each other as well as the scope of payment services they have been authorised to offer.

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:	API standardisation efforts that are well placed to deliver secure, open intra-PSP communications comprise: ➢ The ongoing work that the Open Banking Working Group (OBWG) is carrying out in the UK on behalf of HM Treasury, ➢ The SEPAmail secure messaging service and the Instant SEPA Transfer initiative run by EPRB, ➢ The FinTS and ZOB open banking data exchange standards in Germany. The work of the cross-industry **FIDO Alliance** < https://fidoalliance.org/> to produce open standards that facilitate secure, interoperable strong user authentication is also worth tracking; a number of global customer device manufacturers have already deployed devices that are compliant with the FIDO specifications. The EMA believes that, where possible, the RTS should facilitate the reuse of existing frameworks (data/metadata reference models, data dictionaries, ISO currency codes etc.) that are already used by the payment services industry to identify and share payment account data. Our concern is that many bank-focused interfaces/standards do not lend themselves well to communication with other PSPs over open TCP/IP networks.
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)?	
Response:	As new payment service business/delivery models continue to be deployed, we feel that EBA can ensure that the RTS remain relevant and compatible with future innovations by: ➢ Focusing on defining security requirements that deliver the required security properties (e.g. confidentiality, integrity, authenticity) for data exchanged in the course of intra-PSP communication rather than attempting to define specific security controls/mechanisms to use, ➢ Defining a flexible RTS Compliance Assessment Framework, ➢ Designing a Governance Framework that affords PSPs and technology vendors an ability to participate in the maintenance/evolution of the RTS.

3.5 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:	We believe that the potential of the e-IDAS regulation to support SCA, protect PSC and support secure intra-PSP communication should be assessed further. The e-IDAS regulation was produced to address the needs of a different user community (public agencies and individual citizens) and support a specific function (secure and interoperable entity identification & authentication). As far, as we know the payment industry has not been involved in the development/assessment of this regulation, so far. The e-IDAS regulation introduces useful concepts including assigning levels of assurance to access controls that limit the use e-IDAS credentials to the legitimate user. Such a concept may also be applied to PSCs. On the other hand, it is not immediately clear how the e-IDAS regulation can support the PSD2 requirement for dynamic linking of individual transaction data within the customer authentication process. The scope and the timeline of adoption of e-IDAS by the private sector (and even by government entities in different EEA countries) are unclear to us. Additionally, no country outside the EEA has indicated they will be adopting e-IDAS identification services; this limits the appeal of this framework for PSPs with a global presence.
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:	We believe that the use of qualified trust services, as defined in the e-IDAS regulation, can support the secure identification & registration of PSPs potentially acting as PSP Certification Authorities (CAs) that distribute digital certificates to verified PSPs. Such activities will likely form part of an overall RTS Governance Framework (*as per our response to Question 18, above*). In turn, this step can be used to bootstrap the secure intra-PSP and PSU-to-PSP communication including the secure exchange of PSPs between the PSU and the PSC Issuer in service delivery scenarios involving TPPs. If used in a PSP CA capacity in the RTS, the commercial liability status of e-IDAS qualified trust services should be clarified in the Standard.

List of EMA members as of February 2016:

Advanced Payment Solutions Ltd
Airbnb Inc
American Express
Azimo Limited
Blackhawk Network Ltd
Boku Inc
Citadel Commerce UK Ltd
ClickandBuy International Ltd
Clydesdale Bank
Corner Banca SA
Ekuantia EDE, S.L.
EMP Systems
Euronet Worldwide Inc
Facebook Payments International Ltd
First Rate Exchange Services
Google Payment Ltd
iCheque Network Limited
IDT Financial Services Limited
Ixaris Systems Ltd
Kalixa Pay Ltd
MarqMillions
One Money Mail Ltd
Optimal Payments
Park Card Services Limited
Payleven Ltd
Payoneer
PayPal Europe Ltd
PayPoint Plc
PPRO Financial Ltd
Prepaid Services Company Ltd
PrePay Technologies Ltd
PSI-Pay Ltd
QMoney
R. Raphael & Sons plc
Securiclick Limited
Skrill Limited
Stripe
Syspay Ltd
Transact Payments Limited
TransferWise Ltd
Valitor
Wave Crest Holdings Ltd
Wirecard AG
Worldpay UK Limited
Yandex.Money