European Payment Institutions Federation aisbl

12 October 2016

EPIF RESPONSE TO THE EBA CONSULTATION ON THE RTS ON SCA

ABOUT EPIF (EUROPEAN PAYMENT INSTITUTIONS FEDERATION)

EPIF, founded in 2011, represents the interests of the non-bank payment sector at the European level. We currently have over 190 authorised payment institutions and other non-bank payment providers as our members offering services in every part of Europe. EPIF thus represents roughly one third of all authorized Payment Institutions in Europe. Our diverse membership includes a broad range of business models, including:

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

EPIF seeks to represent the voice of the PI industry and the non-bank payment sector with EU institutions, policy-makers and stakeholders. We aim to play a constructive role in shaping and developing market conditions for payments in a modern and constantly evolving environment. It is our desire to promote a single EU payments market via the removal of excessive regulatory obstacles.

We wish to be seen as a provider for efficient payments in that single market and it is our aim to increase payment product diversification and innovation tailored to the needs of payment users (e.g. via mobile and internet).

GENERAL OBSERVATIONS

EPIF is supportive of initiatives that introduce more choice to innovation in the European payments sector and believes that we should adapt to customer needs and the rapid pace of change in the market.

EPIF believes that Strong Authentication requirements should carefully balance security and user friendliness, taking into account payment service users' desire for convenience

EPIF is strong supporter of the risk based approach. We believe the RTS should be less prescriptive and more business-model and technology neutral in order not to hamper innovation and the development of the EU Digital Single Market.

Moreover, the RTS should be fully consistent with the provisions and spirit of the revised Payment Services Directive (PSD2) and its implied mandates given to the EBA.

RESPONSE TO GENERAL QUESTIONS

1. **Do you agree with the EBA's reasoning on the requirements of the strong customer authentication, and the resultant provisions proposed in Chapter 1 of the draft RTS?**

No, we do not agree.

1. **Application of the provisions to card payments**

Before responding more specifically to the question, EPIF would like to propose some clarifications in relation to card payments.

We are requesting clarification on the applicability of the RTS to card payments, specifically in the section of the clarification on PSD2 provisions (17) on page 9.

Our understanding[1] is that card payments are initiated through the payee and therefore would fall within scope of Article 97(1)(c) of PSD2 and not Article 97(1)(b), which applies to electronic payment transactions initiated by the payer.

This would lead to the different application of certain PSD2 provisions, i.e. Article 74(2). Also, this would allow the EBA RTS to be clearer and more focused on remote card transactions.

EPIF also suggests leaving card present transactions out of scope; fraud risks are well covered by existing card member verification methods such as chip and PIN.

2. So called transitional arrangements: Legal and political consistency with the Level 1 text

The EBA interprets that Article 74(2) of PSD2, which allows the payee or the payee's PSP the option not to accept SCA, only applies during the short-time transitional period between the application date of PSD2 (13 January 2018) and the application date of the RTS under consultation (in October 2018 at the earliest).

EPIF believes the proposed provisions supersede the PSD2 Level 1 text and the wider objectives of the European Union under the Digital Single Market initiative. We call on the EBA to reassess this provision. The impact of such a change would have a devastating effect on e-commerce inside and outside Europe. It would require PSPs to enforce SCA at the detriment of their business and would lead to a rise in the number of declined transactions.

3. The level of detail of the rules

We note that the EBA rightly explained on pages 47-48 of the consultation that, in connection with SCA, it had weighed up two approaches (principle-based requirements and detailed requirements). It nonetheless concludes that "authentication requirements should be developed in the form of high-level principles, to facilitate adaptability to emerging security threats and implementation of innovative security solutions".

We believe that the SCA regime is too prescriptive and narrow in its design. As we have already stated, this will otherwise hamper the development of e-commerce in Europe. Moreover, as drafted the RTS are not technological neutral.

Below we look in turn at how the proposed rules might impact different market participants:

[1] Supported by the European Commission answer on question 135 at http://ec.europa.eu/finance/payments/docs/framework/transposition/faq_en.pdf

A. Impact on merchants and the payments industry

Clarity on authentication vs. authorisation

For instance, the terminology used in the Articles (particularly in Chapter 1) seems to confuse "authentication" (the process of proving the identity of the payment service user) with "authorisation" (the process of approving the execution of a payment or specific action). The requirements for strong customer authentication as currently drafted mix up elements of what the industry considers to be part of the authorisation process and those associated with the authentication process. The PSD2 definition of "authentication" (PSD2 Article 4 (29)) makes it clear that authentication is limited to a "procedure which allows the PSP to verify the identity of a Payment Service User (PSU) or the validity of the use of a specific payment instrument, including the use of the user's personalised security credentials".

Costs and timeframe for implementation

Turning more specifically to card payments, the authentication step results in the generation of a code that reflects the results/strength of the authentication process. This is then included in a subsequent authorisation of the payment, which results in the generation of an authorisation code that completes the payment process for that transaction. The two steps, whilst carried out in real time, are distinct and separate. To re-engineer the card processes to comply with requirements as stated in the RTS will result in significant effort and cost and is likely to require that merchants and payment gateway services re-engineer their websites to include a new step that allows an authentication code (as described in the RTS) to be entered or captured during customer authentication. It may also require a more fundamental change to card transaction processes to bring together authentication and authorisation steps to minimise the impacts on transaction processes.

Taking 3D Secure as an example, the implementation took the industry seven to ten years to develop and implement: re-engineering today's systems to implement the RTS will surely take as long, and incur significant costs, diverting merchants and PI's investments away from the development of new products and services, which is likely to impact negatively the development of Europe's digital economy.

B. Impact on the customer experience

Balancing security and convenience – the future of One-Click

The RTS's prescriptive approach to SCA is likely to have a negative impact on the customer experience, and hence on e-commerce activity. Different use cases and payment products might require differing approaches to SCA. The success of products such as One-Click online payments (PayPal and Amazon) or mobile wallets (Apple and Samsung) demonstrate that consumers seek convenience as well as security.

The RTS should therefore accommodate innovation and convenience, in addition to security, and be principle-based and focused on openness, transparency, accessibility and user friendliness. As currently drafted the RTS seem to give preference to particular detailed processes and techniques, rendering the application of SCA inflexible and prescriptive. A flexible application of SCA would benefit consumers and merchants and help achieve a Digital Single Market in the EU.

Differentiating between different categories of customers

More careful consideration should also be given to the nature of the customer. Companies might have different requirements to the consumer. The SCA regime should take this into consideration Indeed, both PSD and PSD2 recognize the need to apply different levels of protection between consumers and legal persons, as emphasized in recital 53: “As consumers and undertakings are not in the same position, they do not need the same level of protection. While it is important to guarantee consumer rights by provisions from which it is not possible to derogate by contract, it is reasonable to let undertakings and organisations agree otherwise when they are not dealing with consumers.” Specifically, Articles 38 and 61 permit contractual derogations to respectively all of Title III and most of Title IV for payment services provided to persons other than consumers, hence covering:

- legal persons, and
- natural persons acting for the purpose of their profession or business (which, by extension, appeals to the notion of commercial card defined in the Regulation (EU) 2015/751 on interchange fees for card-based payment transactions

Legal persons usually use internal control mechanisms allowing them to authenticate the person initiating the payment order in his/her capacity to act on behalf of the company. Such controls prove particularly robust through processes to follow, third-party signature requirements and independent controlling bodies. Furthermore, both undertakings and individuals acting on their behalf using payment instruments such as commercial cards usually also benefit from much better protection than consumers through their insurance policies.

The burden of one-time authentication codes

For instance, Article 1(1) of the RTS mentions the use of an authentication code that is accepted only once: this requirement is likely to have a negative impact on consumer experience (and therefore e-commerce activity), and it may limit PI’s opportunities to develop innovative solutions to authenticate payers.

This is very prescriptive and does not appear to be aligned with the PSD2 text. While PSD2 Recital 96 - which provides the underlying context for the security measures - indicates that such measures "may result in authentication codes **such as** one-time passwords", neither it nor PSD2 Article 97 and Article 98 state that such measures must involve single use authentication codes. In fact, PSD2 Article 98(2)(d) indicates that the draft RTS are required to "ensure technology and business model neutrality".

It is therefore unclear why authentication must always result in the generation of a code, let alone with single use. It is also unclear how future proof such a solution would be when new technologies and innovations are introduced.

If it is the payer, and especially a consumer who has to input the one-time authentication code during the purchase, this would surely disregard finding the right balance between convenience and security.

C. Promoting the growth of e-commerce

Allowing for the use behavioral and transaction-based data

EPIF notes that, according to Article 1(3)(e) of the draft RTS, the SCA procedure shall include mechanisms to "prevent, detect and block fraudulent payment transactions before the PSP's final authorization". In the context of such mechanisms, Article 1(3)(e)(iii) makes explicit reference to "spending behavioral patterns". Article 1 (3)(e) also implies that points (i) to (v) of this article do not constitute an exhaustive list.

A PSP should therefore have the choice whether to use behavioral and transaction-based data prior to a formal SCA process as part of a sophisticated fraud prevention process or alternatively use it as part of the actual SCA process.

Transaction risk analysis is a tool currently being used by the industry to great effect. We would argue in particular that more prominence should be given to the use of behavioral data. This is an essential tool being used by the payment industry in the application of a risk based approach. We propose to allow behaviour of the payer (e.g. consumer device characteristics, communication session characteristics, payment application settings, payer/payee risk profile data, threat environment data, industry blacklists, location, etc.), as well as spending patterns to be included in a transaction risk analysis approach.

Specifically, EPIF strongly believes that the RTS should (i) allow for behavioural and transaction-based data to be an integral part of the SCA process, and (ii) foresee that where a PSP uses behavioural and transaction-based data effectively an exemption from the SCA should be introduced. We will elaborate on these two points in turn:

First, we strongly disagree that behavioural data are just an "additional tool for fraud prevention" (point 29 of the rationale). They can be used for authentication purposes and are a crucial tool if the EBA's aim is to allow for "the development of user-friendly, accessible and innovative means of payment" (point 28 of the rationale). Several payment providers have developed sophisticated risk management systems that analyse specific behavioural patterns, as well as transaction data and other information, to both authenticate users and to detect fraud. Behaviour-based characteristics can be used to analyse – for example - the physical behaviour of the payer (e.g. consumer device characteristics, communication session characteristics, payment application settings, payer/payee risk profile data, threat environment data, industry blacklists, location, etc.), as well as spending patterns.

By being able to assess, for instance, whether a payer is at home, on their home computer, making the same payment amount to the same payee as last month, a PSP will be in better position to assess the risk and the level of authentication required. Such analysis can act as a kind of 'invisible' strong customer authentication, reinforced by the fact that customers (and criminals) are not aware of what aspects of behaviour are being utilised. Because behavioural attributes can be collected and assessed over a period of time, they are less susceptible to theft, malware, spoofing, or malicious replication.

Second, we are concerned that the RTS do not foresee an exemption for a transaction risk analysis for any PSP. We believe this runs counter to Article 98 (2)(a) of the PSD2 which provides that the RTS shall "ensure an appropriate level of security for payment service users and payment service providers, through the adoption of effective risk based requirements" and Section 22 on page 10 of the RTS, which stipulates that the strong customer authentication procedure shall include mechanisms to prevent, detect and block fraudulent payment transactions before the PSP's final authorization. It is these mechanisms that would enable PSPs to perform a transaction risk analysis.

We therefore strongly urge the EBA to reconsider this aspect of the RTS and introduce an exemption based on a transaction risk analysis. We believe this would improve the customer experience without compromising security. It would provide a boost to the growth of the EU's Digital Single Market.

EPIF could support an approach which is based on defined outcomes (for example, a maximum level of fraud for a particular payment method or service provider) rather than on specific methods.

2. **Based on your knowledge, what types of consumer data do financial institutions use most? In particular, in relation to the "dynamic linking" procedure, do you agree with the EBA's reasoning that the requirements should remain neutral as to when the "dynamic linking" should take place, under the conditions that the channel, mobile application, or device where the information about the amount and the payee of the transaction is displayed is independent or segregated from the channel, mobile application or device used for initiating the payment, as foreseen in Article 2.2 of the draft RTS.**

Yes, we agree.

We agree with the EBA that the dynamic linking requirements should remain neutral as to when it should take place.

EPIF believes, as does the EPC, that the concept of "payee" is not as simple as it can seem. There are examples where the payment is sent to an account which the payer does not know, and the actual sending of funds is performed to an account "behind" that intermediary one. Examples of this are payment facilitators for card payments, credit transfers and direct debits. Many merchants benefit from integrated payment solutions and management of fund flows and reconciliation.

EPIF would like to also see the scope of this provision clarified. It is our reading that the provisions on dynamic linking only apply to Article 97(1)(b) and hence only to remote credit transfers. We would ask the EBA to clarify this point. In relation to Rationale 26 of the draft RTS, we are convinced that techniques other than the ones mentioned in this Rationale are available. These equally create an adequately secured and protected environment to display the amount and the account number of the payee, and assuring the integrity of these data towards the PSU, on a single smartphone with a single app. These techniques include, but are not limited to:

- Secure Element (SIM or dedicated chip) for storage of sensitive data, accessible only by PSU and authorised app
- App-separation / sandboxing
- Remote security updates, to prevent or react on possible weaknesses
- Hardening of an app / secure coding
- White-box cryptography
- Device binding (secure activation of an app for use by only one PSU on only one device), based on continually refreshed data elements or challenge/response
- Detection of mobile malware and fraud on the device
- App-store monitoring (for malicious apps).

We would also welcome further guidance from the EBA on what would represent a valid authentication code. By means of an example, would an SMS be considered as a channel that preserves the confidentiality, authenticity and integrity of the authentication code?

Following the discussion with the EBA during the public hearing, EPIF would also welcome the RTS to clarify that the SCA process can be completed on one device; the same device the customer is using to make the purchase.

3. In particular, in relation to the protection of authentication elements, are you aware of other threats than the ones identified in articles 3, 4 and 5 of the draft RTS against which authentication elements should be resistant?

Yes, we are aware of other threats.

The requirements on knowledge elements do not respect the principle of technical neutrality and are too prescriptive, especially on the use of repeatable characters. A very strong password could contain repeatable characters in capital letters for example. We therefore suggest deleting the reference to non-repeatable characters.

Moreover, we believe that behavioural data should be included within the inherence element. Behavioural and transactional data do not suffer from the vulnerabilities of the other factors (possession and knowledge) because they are recorded by the PSP as events occur, and are stored beyond the reach of the user's ability to manipulate or unintendedly compromise them. Under a number of EU regulations – including the NIS Directive and the General Data Protection Regulation - the PSP is obliged to store such data in a secure way.

The EBA must recognize that even by introducing SCA requirements PSPs can never make a payment transaction 100% secure. There should be no legal requirement to give such a guarantee or near total protection.

The proposed language of the RTS introduces an impossibly high burden upon PSPs to mitigate the risk of fraud. For example Article 1(2) suggests that PSPs must "ensure" that any authentication code used "cannot be forged". Similarly, Article 5(1) states that the security features in devices and software provided to payers in order to read authentication elements "shall also guarantee a sufficiently low likelihood of an unauthorized party being authenticated." These concepts of prevention and guarantee feature in other articles also and we firmly believe these references should be amended so that the Articles do not mandate a specific outcome following the implementation of the SCA.

Furthermore, EPIF questions whether the implementation of SCA as currently proposed will actually solve the fraud problem and may in fact have unintended consequences by pushing remote transactions to other less secured channels, such as cash on delivery, or mail order/telephone order where SCA does not apply. This has the potential impact to increase fraud.

EPIF would therefore like to reiterate once more that it is vital to find the balance between security requirements and usability.

4. Do you agree with the EBA's reasoning on the exemptions from the application of Article 97 on strong customer authentication and on security measures, and the resultant provisions proposed in Chapter 2 of the draft RTS?

No, we do not agree.

EPIF has the following remarks to this question.

As a general rule, the RTS should ensure that ASPSPs cannot use the exemptions to preclude PISPs or other providers from having access to the relevant data.

As EPIF's members represent multiple business models, the general position towards exemptions is undefined. Some members prefer as few exemptions as possible or even none at all where it involves PIS. Other members, most notably the card acquirers, welcome exemptions that benefit the payer's experience without allowing more risk: transaction risk analysis.

1. An exemption based on a transaction risk analysis

EPIF is very concerned that the EBA's decision not to include an exemption based on a transaction risk analysis performed by the PSP will have a detrimental impact on existing PSP service delivery models and on the growth of the EU's digital economy. We believe that this decision does not meet the mandate set forth in the PSD2 Article 98, which states that the exemptions should be based on "the level of risk involved in the service provided". In doing so, the EBA goes beyond its mandate.

EPIF would strongly support the inclusion of transaction risk analysis in the exemptions. This would also allow aligning the liability to the PSP or merchant based on their respective transaction risk analysis.

An efficient transaction risk analysis process could consist of:

A PSPs putting in place risk management systems to evaluate the riskiness of transactions, taking into consideration a number of factors such as:

- Consumer device level (device type, OS/browser, malware (not) present, rooted / jailbroken, device identification, etc. All of these subject to availability to the payee PSP.)
- 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)

B Ensuring the criteria for this transaction risk analysis should be principle-based. It is up to the PSP to decide on its exact capabilities, based on its own risk analysis and appetite.

C Based on that analysis, PSPs would then either deploy SCA (if the risk is high) or alternative methods of authentication (for lower risk transactions). Periodic reviews with home state regulator would ensure that the fraud rate remains at acceptable levels in view of the risk. Some of the metrics that PSPs can share with regulators to measure authentication outcomes and the level of risk include:

- Claims for lack of authorization
- Success in refuting such claims
- Authentication leakage (authenticated cases that resulted in loss)
- Financial loss rates.

2. The proposed exemptions

EPIF believes that a list of SCA exemptions triggered by static transaction thresholds will quickly become outdated leading to a poorer payment service user (PSU) experience and decreased transaction security levels. Additionally, it is not clear how the EBA chose the static SCA exemption transaction thresholds listed in Articles 8(1)(b) (contactless transactions) and Article 8(2)(d) (remote transactions).

We do not support the proposed differentiation between two sets of thresholds as set out in Articles 8 (1)(b) and Article 8(2)(d). These run counter to the aspiration of the draft RTS to remain technology neutral and future proof. Taking the UK market as an example, the threshold of permissible transactions has been repeatedly raised in recent years. Considering the rise in contactless card usage in public transport and the systems used, it will be proportionately expensive and intrusive to the cardholders to introduce a mandate to perform SCA once the cumulative limit has been reached.

Regarding remote transactions, EPIF believes that the transaction thresholds for remote transactions are low and have not been made subject to an impact assessment or risk assessment. A limit of EUR 10 per transaction (and EUR 100 cumulatively) would oblige users to go through the unfriendly experience of SCA for almost any digital payment, regardless of the actual risk posed. This approach will have a detrimental impact on e-commerce, which would be at odds with the European Commission's efforts to foster the digital economy's growth in the EU.

In addition, the list of static SCA exemptions in Article 8 appear to apply only to payer ASPSPs. EPIF would like the EBA to comment on the scope of their existing mandate to remove the ability of payee PSP to process a payment transaction without SCA while accepting the liability for any financial loss caused to the payer's PSP as detailed in PSD2 Article 74 section 2. Especially given the fact that card payments should be classified under Article 97(1)(c) of PSD2.

EPIF believes that the list of exemptions provided by the EBA should not be exhaustive and should give the PSP the ability to apply exemptions based on its own transaction risk analysis. Without this, we would also expect an increase in the costs to the payers based on the requirement that they would have to authenticate themselves at every transaction. At a minimum, the list of exemptions should be significantly extended to take into account risk based SCA exemptions to be applied by ASPSPs as well as all other PSPs.

The mandatory nature of the exemption does also not take into account the context of different countries. In the case of a card transaction for example the transaction limits are not controlled by the card but by the terminal. The applicability of PSD2 to one leg transactions will cause interoperability issues, as the provisions of Article 8 cannot be implemented successfully in all countries.

We suggest to the EBA to keep the exemption.

Moreover, Article 8 Section 1(b) states that the exemptions from SCA for electronic card payments at a POS shall be the same for contact and contactless transactions. Currently, this Article does not include existing card payments, such as no-CVM (Card Verification Method) debit- or credit contact card payments for toll ways and parking, under EUR50. We also believe that other proximity payments should be equally covered.

It is unclear how recurring card payments (such as magazine subscriptions) fit into the scope of the RTS. We believe these should be considered as out of scope as they are payment transactions similar to Direct Debits. We believe they should be added to the list of exemptions.

5. Do you have any concern with the list of exemptions contained in Chapter 2 of the draft RTS for the scenario that PSPs are prevented from implementing SCA on transactions that meet the criteria for exemption?

Yes, we have concerns.

The PSP should have the right and an ability to apply SCA as a step up, even on transactions listed within the exemptions. To support this stance we would draw attention to a notable contradiction in the regulations between the obligations on the PSP in Article 1(3)(e) of the draft RTS and the potentially unintended consequences of a mandatory exemptions list. According to RTS Article 1(3)(e), the PSP is obliged via its SCA procedure to “prevent, detect and block fraudulent payment transactions before the PSP’s final authorisation”. A key tool in the prevent/detect stages are to make use of security “step up” where risk triggers are hit. Where the SCA exemptions list is made mandatory it would limit the ability of a PSP to make use of “step up” escalations to manage risk without going to the extreme of blocking a suspect transaction. A mandatory list of SCA exemptions (as set out in RTS Chapter2, Article 8) therefore appears at odds with the objectives of RTS Article 1(3)(e).

Not withstanding the above, the EBA should work with national competent authorities to ensure the SCA exemptions cannot be used to deliberately discriminate against payment accounts interaction initiated through an AIS/PIS.

6. Do you agree with the EBA's reasoning on the protection of the confidentiality and the integrity of the payment service users' personalised security credentials, and the resultant provisions proposed in Chapter 3 of the draft RTS?

Once more, EPIF supports a risk-based approach in this area. For example, there are arguments that speak in favour of allowing the user to briefly see what he/she has keyed into an authentication field.

More generally, EPIF believes that this area of security should be harmonised by introducing security methodology such as the use of the PCI certification processes.

EPIF members also have one technical comment to make. The term "data on personalised security credentials" should be defined in the RTS. Otherwise the word "data" should be deleted from the draft RTS.

We are also not sure how the EBA aims to define the term 'tamper resistant devices and environments' (Article 9 section 1(c)). Devices can never be 100% safe, and there are questions how this could be measured. It is yet another example why EPIF favours the consistent application of outcomes and risk based approaches.

In relation to the cryptographic life cycle, EPIF believes this should be considered as a separate control that is applied to protect authentication elements, rather than being part of the authentication process.

7. Do you agree with the EBA's reasoning on the requirements for common and secure open standards of communication for the purpose of identification, authentication, notification, and information, and the resultant provisions proposed in Chapter 4 of the draft RTS?

No, we do not fully agree.

EPIF believes that the RTS should not fundamentally alter the principle which currently gives providers of PIS the right to continue to offer services as per their existing business models. While EPIF does not per se reject the idea that ASPSPs can create dedicated interfaces, the RTS should explicitly clarify that providers of PIS and AIS retain the right to provide their services based on direct access via the customer facing interfaces of ASPSPs. The choice whether a PISP or AISP wishes to use dedicated interfaces should rest solely with the PIS or AIS.

The PSD2 guarantees PIS both the indirect and direct access to the payer's account. A "dedicated communication interface" for the communication with PIS as introduced in Article 19 draft RTS provides for the PIS' indirect access. However, this dedicated interface must not be mandatory in order to not foreclose PIS' direct access. It must be up to the ASPSP to decide whether to provide such an interface or not. Where the ASPSP takes the decision to create such dedicated interfaces, the RTS must also take care to ensure that the imposed investment requirements on PSPs remain as limited as possible.

The RTS must further make clear that PISPs and AISPs can rely on all authentication procedures of the ASPSPs in a systematic fashion.

In addition, in Article 19 section 3, the EBA effectively delegates its responsibility to define requirements for common and secure open standards of communication to third parties. If the market is to implement these measures within 18 months, the market needs clarity on this topic now.

In Relation to Card Payments

In the context of card payments, EPIF agrees with the use of secure and open standards, specifically PCI. However, clarification is needed on what is meant by secure bilateral identification between the payer's device and payee's accepting device. Is mutual authentication meant? The bulk of chip and PIN transactions are made without the identification on the POI. In addition, bilateral authentication between ASPSPs and customers seems excessive: customer devices generally do not have public key certificates ready for use to identify themselves to merchants' servers, and asking them to obtain one would be a complex and burdensome process: Good (EV) certificates are costly, and require a personal appearance by the consumer to the certificate issuer.

In relation to Article 19(4), EPIF agrees that account servicing PSPs should document technical specifications but not make detailed specifications public, as that could make PSPs more vulnerable to compromise.

Whilst EPIF agrees that PSPs should implement measures on payment services user interfaces to protect against misdirection of communications to unauthorized third parties (Article 17(1)), it is noted that this outcome cannot be ensured in all circumstances. PSPs may not have control over such things as DNS poisoning, phishing on the end user device and malware on the end user device. The obligation should therefore be to use efforts rather than to guarantee (ensure) such an outcome.

8. In particular, do you agree that the use of ISO 20022 elements, components or approved message definitions, if available, should be required to ensure the interoperability of different technological communication solutions implemented between PSPs for the provision of AIS, PIS or for the confirmation on the availability of funds? Do you see any particular technical constraint that would prevent the use of such industry standards?

No, we do not agree.

We believe that ISO 20022 is not widely used or deployed by the market at present. Actually, ISO 8583 (or a standard derived from that) is the standard in use with many payment systems. The EBA should stay neutral at the regulatory level and not recommend specific standards.

Moreover, ISO 20022 is a messaging format designed for bank-to-bank communication. It is not used by banks for communication with their payment service users. The request to use ISO 20022 elements should thus not indirectly lead to a foreclosure of PISPs direct access to the payer's account.

In contrast to the EPC's response, we strongly disagree with the suggestion that ISO 20022 elements, components or approved message definitions should be required for technological communication solutions for the provision of AISPs and PISPs.

Recital 93 of the PSD2 makes clear that the RTS "should be compatible with the different technological solutions available." It would be out of scope for the RTS to define or promote a specific communication or messaging standard.

More concretely, ISO 20022 would raise the following issues:

- ISO 20022 is not at all compatible with TPP direct access via the customer facing online interfaces of the ASPSP.
- Imposing the need for ISO 20022 would impose large investment requirements for PSPs without a clear business case.
- In particular, we see a problem when developing new authentication procedures. As this is one of the key competitive differentiators of PSPs. PSPs must be allowed to innovate within this area without having to have such new procedures subject to review and "approval" by a broader group of companies.
- To our knowledge currently there exists no ISO 20022 standard for AISPs or PISPs. It cannot be the meaning of the RTS to impose an unproven such standard on AISPs and PISPs.

9. With regards to identification between PSPs, do you agree that website certificates issued by a qualified trust service provider under an e-IDAS policy would be suitable and allow for the use of all common types of devices (such as computers, tablets and mobile phones) for carrying out different payment services ?

No, we do not agree.

The scope/timeline of adoption of e-IDAS by the private sector and by different EEA countries is unclear.

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.

While we believe the e-IDAS / Qualified Trust Service provider could potentially be used to issue OPSP server certificates, we believe it is too early to say how effective this framework would be to protect the confidentiality of PSC.

We therefore once more advocate the fact that the RTS should remain technology neutral and less prescriptive.

10. With regards to the frequency with which AIS providers can request information from designated payment accounts when the payment service user is not actively requesting such information, do you agree that the proposed limit of no more than two times a day achieve an appropriate balance between allowing AISP to provide updated information to their users while not negatively impacting the availability of the ASPSP's communication interface? If not, please indicate what would be in your view the appropriate frequency and rationale for such frequency.

No, we do not agree.

EPIF would be in favour of increasing the number of automated AISP payment account requests that will be serviced by the ASPSP to one per hour for a given payment account. We feel that this provides appropriate balance between AISP service priorities and the desire of the ASPSP to ensure optimal performance of the communication interface it provides to a payment account management platform.