EBF response to the EBA Consultation Paper on the draft RTS on strong customer authentication and common and secure communication under PSD2

The European Banking Federation wishes to thank the EBA for consulting market participants on its draft RTS and for hosting a hearing on 23rd September, as it has allowed us to clarify some provisions that we initially could have misunderstood. As a result, we wish to propose amendments aimed at clarifying and simplifying specific provisions.

Q1: 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?

The EBF proposed amendments will hopefully clarify some issues, notably on card based transactions, whilst making the RTS future proof in an ever changing environment where both innovation and the fight against fraud require flexibility and adaptability to market constraints and technical opportunities. Such flexibility is vital, especially as it is unclear when the RTS will be reviewed or how quickly changes can be introduced. Equally, we propose to insert some clarification currently provided in the rationale into the RTS itself as we understand the rationale will eventually not be part of the final legally binding text.

For example, the interaction between AS PSPs and TPPs (as described in Rationale point 19a) on the use of credentials should be clearly explained in a recital as follows:

> **(7 bis) In accordance with Article 97(5), PISPs have the right to rely on the authentication procedures provided by the account servicing payment service provider (AS PSP) to the user. In such cases, the authentication procedure will remain fully in the sphere of competence of the AS PSP. The only situation when the transaction would be authenticated within the sphere of competence of the PISP is when a PISP issues its own personalised security credentials for the user, in place of the credentials issued by the AS PSP. This would however require a prior contractual agreement between the PISP and the AS PSP on the acceptance of such credentials by AS PSP. Such agreement would also be outside of the scope of PSD2.**

Generally speaking and as the EBA appeared to acknowledge at the public hearing, the focus of the draft RTS to date has been on consumer interacting with merchants in an e-commerce environment but we believe the EBA should give further consideration to applying the draft RTS in a corporate or business environment, taking equally financial inclusion into account.

Turning to the articles proposed in Chapters 1, 2 and 3, we concur with the EBA's reasoning to opt for high level principles rather than detailed prescriptive requirements, as it is certainly the best approach; technology and fraud evolve at an extremely rapid pace and any regulatory standard will need to be future proof. Option 1.1 mentioned on page 47[1], confirmed in rationale 22[2] is fully in line with the mandate given to the EBA in PSD2 to develop standards that are deemed to be based on "effective and risk based requirements" (article 98.2.a), whilst ensuring "technology and business model neutrality" (article 98.2.d) and "allow for the development of user-friendly, accessible and innovative means of payments" (article 98.2.e).

Unfortunately, we fail to identify the same approach in the articles proposed in the consultation paper. For example, a very prescriptive list of exemptions to Strong Customer Authentication is at odds with option 1.1 retained as the best option by the EBA itself, even more because AS PSPs are ultimately liable for any unauthorised transactions, whether they have been initiated by the PSU or via a PISP. It should therefore be the AS PSP's ultimate responsibility to assess its risks on an on-going basis, based on its own internal processes and industry protocols. Therefore, AS PSPs should be given the ability to decide whether to establish a specific tool based on its own risk policy. Market reality shows that authentication methods for purchasing on-line can differ from one transaction to another, depending on the security protocols implemented by e-retailers, the amount of the transaction or the environment within which this transaction takes place. Risk profiling based on device, IP recognition and behavioural analytics becomes more sophisticated by the day. The European Union cannot deprive itself of this myriad of methods as they offer the right balance between security and convenience, provided of course, users are protected as rightly stated in PSD2.

The draft RTS appears to be too prescriptive to allow AS PSPs to rapidly adapt to any new security threat or innovation. The wording throughout the draft RTS seems indeed to imply that it sets mandatory security features ("included but not limited to", see article 1.2, 1.3.d, 3.1,…). We would therefore retain them as mere illustrations, rather than prescriptive minima, as fraud and technology evolution could render some of this mechanism redundant in the future.

Article 1.1 does not seem to include card transactions that are not supported by a chip, such as magnetic stripe payment cards, because this type of cards does not generate an authentication code[3]. As this type of card is still in distribution in Europe and used as a fall-back solution, we would propose amending article 1.1 as follows:

1. For the purposes of the application of strong customer authentication in accordance with Article 97(1) of Directive (EU) 2015/2366, **and with the exception of magnetic stripe based card transactions,** the authentication procedure shall result in the generation of an authentication code that is accepted only once by the payment services provider each time that the payer, making use of the authentication code accesses its payment account online, initiates an electronic transaction or carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.

[1] "Develop principle-based requirements for the authentication of a payment service user"
[2] "The draft RTS should be developed at a higher rather than granular level of detail"
[3] The same would go for fall-back from chip to magnetic stripe in case of chip failure.

We also understand from rationale 18 that direct debit transactions given in the form of an electronic mandate require strong customer authentication as they are considered as implying a “risk or payment fraud or other abuses” (article 1.1). As a consequence, mandates that do not qualify under the standard definition would not require any SCA. In order to clarify this specific issue, we would propose to introduce a clear definition of e-mandates (see our proposed drafting at the end of the document).

Article 1.2: Technical neutrality of security features is of the essence if the RTS are to be future proof and adapted to allow PSPs, merchants and PSUs to prevent, detect and tackle cybercrime. The wording appears nevertheless quite prescriptive as the security features proposed are set as a minimum “<u>including but not limited to</u>”. We would propose to mention these security features, with the exception of the expiration time of the authentication code, as mere <u>illustrations</u> of possible security features AS PSPs can adopt.

Article 1.2 should therefore be amended as follows:

2. The authentication code shall be characterized by security features **such as** ~~including, but not limited to~~, algorithm specifications, length, information entropy ~~and expiration time~~, ensuring that:

The reason why we propose to delete any reference to expiration time is because the authentication code generated by Chip Authentication Program (CAP) protocols based solutions do not have an expiration time feature, given that neither chip cards nor CAP readers have clocks. The CAP protocol is event based, i.e. a generated code is valid until it is used or a subsequent CAP code is used. It is also worth mentioning that CAP is, at present, the most secure authentication mechanism and one of the most used hardware based generators of authentication codes.

Article 1.3 (a) should be understood as a time-out in case of inactivity of the PSU as a general time-out is neither appropriate nor proportionate. We would therefore propose to amend article 1.3.a as follows:

3. The strong customer authentication procedure shall include mechanisms to:

   (a) limit the maximum time allowed to the payer to access its payment account **online in case of inactivity on his/her part**, where the access has been performed through strong customer authentication (“time out”);

Article 1.3 (b) should take stock of the fact that, in a payment card environment, the PSU is immediately informed whenever he or she has entered a wrong password. Informing the PSU that the authentication procedure has failed in the end with no recourse for the PSU to enter the right password will prove to be very inconvenient to him or her.

We would therefore propose to amend article 1.3.b as follows:

3. The strong customer authentication procedure shall include mechanisms to:

   (a) limit the maximum time allowed to the payer to access its payment account online, where the access has been performed through strong customer authentication (“time out”);

   (b) **with the exception of static passwords**, exclude that any of the elements of strong customer authentication can be identified as incorrect, where the authentication procedure has failed to generate an authentication code for the purposes of paragraph 1;

Article 1.3 (d): Today, HTTP over TLS is currently being upgraded and represents as such, a minimum requirement. Nevertheless, industry should stay ahead of cybercrime and be able to adopt state of the art technologies in a rapid and flexible manner. In these circumstances, considering that HTTP over TLS should be included in the Regulatory Technical Standard will certainly not be future proof. We would therefore advocate state of the art protocols to allow the EBA RTS to be future proof.

Amendment to article 1.3.d:

> (d) protect communication sessions against the capture of data transmitted during the authentication procedure or manipulation by unauthorised parties, ~~including but not limited to~~ by relying, where applicable on **protocols such as** HTTP over TLS

Article 1.3.(e): AS PSPs have a long experience in protecting their clients' assets, both for accessing their accounts or initiating payments (credentials) and prevent/fight fraudulent activities. Agility, innovative technologies and flexibility is of the essence in this respect.

Article 98.1 (c) aims at protecting "the confidentiality and the integrity of the PSU's personalised security credentials". Article 1.3.e imposes mechanisms to "prevent, detect and block fraudulent payment transactions before the PSU's final authorisation" that go beyond the mere protection of credentials, may not be future proof and deprive AS PSPs of the ability to rapidly adapt to yet unknown fraud trends pending the update of the RTS.

We would therefore kindly suggest either to delete paragraph e) or, alternatively, amend it as follows:

> (e) prevent, detect and block fraudulent payment transactions before the PSP's final authorisation. These mechanisms ~~shall~~ **may** take into account, but not be limited to:

Would paragraph (e) be maintained, it is unclear at this point in time whether AS PSPs will be able to fulfil these requirements in case the payment transaction has been initiated by a PISP. In this very particular circumstance, AS PSPs may lose access to critical data that will prevent them to properly manage the transaction cycle. We would therefore suggest to add a paragraph aimed at ensuring that AS PSPs receive equivalent information, whether the payment is initiated by the user or by a PISP as follows:

> **(f) AS PSPs must receive the same kind of information generally collected from the PSU, whether the payment was initiated by the PSU or by its PISP.**

It should also be noted that mandating requirements based on "complexity" and "expiration time is increasingly out of step with advice from several national expert bodies.

Article 3.1: Static passwords used in electronic payment environments can be repeatable (card static password for example). It should therefore be clarified that static password used to authenticate electronic payment transactions do not fall under the required criteria of length (static passwords are 4/5 digits), complexity, expiration time[4] and non-repeatability. More generally, static passwords are processed in a very secure environment that prevents their detection by non-authorised third parties. Equally, frequent password changes do little to improve security and very possibly make security worse by encouraging

[4] Although payment cards do have an expiration date, static passwords usually do not.

the use of passwords that are more susceptible to cracking. Flexibility is, again, of the essence, when managing strong customer authentication.

Article 3.1 should be amended as follows:

1. **With the exception of static passwords in remote environments,** the elements of strong customer authentication, categorised as knowledge **may** ~~shall~~ be characterized by security features ~~including~~ **such as** ~~but not limited to~~, length, complexity, expiration time and the use of non-repeatable characters ensuring resistance against the risk of the elements being uncovered or disclosed to unauthorised parties.

AS PSPs can only mitigate risks for the products and services they offer to their clients (home banking, payment applications,…, payment cards), multi-purpose devices are largely out of their control. As a result, we would propose that article 6.2 is rephrased as follows:

2. Where any of the elements of strong customer authentication or the authentication code, is used through a multi-purpose device including, but not limited to, mobiles phones and tablets, the authentication procedure shall provide measures to mitigate the **consequences** ~~risk~~ of the multi-purpose device being compromised **for the part under its control.**

In order to take account of the variety of business models in the various Member States, the mitigation measures cannot be prescriptive as stated under article 6.3, in line with our comment under 2.2.b. Besides, article 6.3.a should refer to "secure, segregated environment" in order to provide enough flexibility for future market innovations.

Article 6.3 should therefore read as follows:

Article 6.3: For the purposes of paragraph 2, the mitigating measures **may** ~~shall~~ include, but not be limited to:

a. the implementation of **secure, segregated** ~~separated Trusted Execution~~ **e**~~E~~nvironments inside the multi- purpose device;

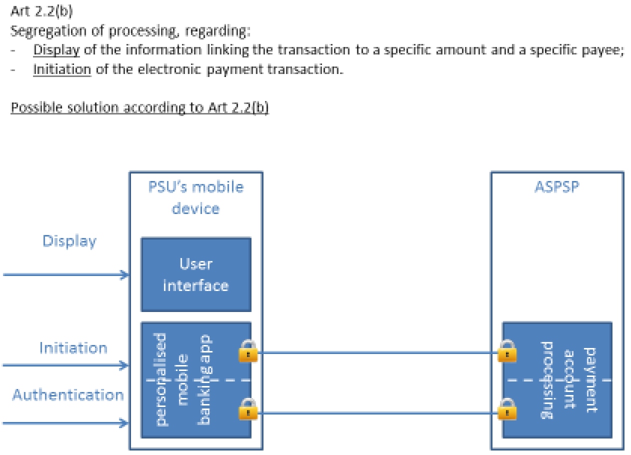
b. mechanisms to ensure that the software or device have not been altered by the payer or by a third party or mechanisms to mitigate the risks related to such alteration where this has taken place.

Q2: 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?

We support an approach that allows the PSP to decide how to implement dynamic linking and the extent to which such dynamic linking is visible to the user. However, the EBA request for segregation is rather confusing as one single application and different channels could be used in the same device. We are very concerned about the impact that the independence requirement could have on the user experience. PSUs are used to both initiate and authenticate payments through the same device in an easy way.

The additional security benefit of segregation still needs to be demonstrated in relation to the existing technical infrastructure set up by the market to offer secure products and services to their clients.

Market practice shows indeed that very secure mobile banking environments have not all been built around segregation/independence of channels, devices or applications. For example, segregation is not needed when the entire transaction process is encrypted end-to-end, with a two factor authentication and a dynamic linking between the transaction amount and the payee*, as illustrated in the diagram below*.



Art 2.2(b)

Segregation of processing, regarding:

- Display of the information linking the transaction to a specific amount and a specific payee;
- Initiation of the electronic payment transaction.

Possible solution according to Art 2.2(b)

In very concrete terms, the diversity of technical solutions on the market improves resilience and decreases exposure to criminals.

Besides, a blunt segregation of applications within the same device would introduce an over complicated process for users, forcing them to go from one application to the other, eventually discouraging them to ever use their mobile phone for payment applications.

Independence of channel, application or device can therefore be an option, quod non, but cannot be imposed as the only solution. We would therefore prefer that, instead of an obligation, this independence requirement be a recommendation. This would give AS PSPs the ability to decide whether to require the use of a second authentication device or not.

Additionally, we need further clarification on what is expected when requiring that "the authentication code [..] shall be specific to [..] the payees of the batch of transactions considered collectively" as stated in Article 2.4.

Would segregation be nevertheless maintained, it should be organised in a way that can be understood and implemented by market operators by adding a "logical" separation of channel, application or device in article 2.2.b.

Article 2.2 (b) should therefore be amended as follows:

(b) the confidentiality, authenticity and integrity of the information displayed to the payer through all phases of the authentication procedure including generation, transmission and use of the authentication code.

Alternatively, article 2.2 (b) should be amended as follows:

(b) the confidentiality, authenticity and integrity of the information displayed to the payer through all phases of the authentication procedure including generation, transmission and use of the authentication code. The channel, device or mobile application through which the information linking the transaction to a specific amount and a specific payee is displayed shall **logically** be independent or segregated from the channel, device or mobile application used for initiating the electronic payment transaction.

Article 2.1 (b): Based on the definition provided by the PSD2 under article 4 (29), a clear difference must be established between the authentication code that identifies the PSU based on something he or she knows, possesses or is inherent to him or her and the authorisation code that is specific to a specific transaction with a designated payee.

We would therefore propose to replace "authentication code" with "authorisation code" in article 2.1 (b) as follows:

1. For the purposes of the application of strong customer authentication in accordance with Article 97 (2) Directive (EU) 2015/2366, the authentication procedure shall also provide that:

   (a) The payer is made aware at all times of the amount of the transaction and of the payee;

   (b) The **authorisation** ~~authentication~~ code generated in accordance with Article 1 shall be specific to the amount of the transaction and the payee agreed to by the payer when initiating the transaction.

The same goes for **article 2.3** where the code linked to the transaction amount and the payee should be referred to as an "authorisation code", not an authentication code as follows (a typo is being corrected at the same time):

> **Article 2.3**: For the purposes of the application of strong customer authentication in accordance with Article 97(2) of Directive (EU) 2015/2366 to a card-based payment transaction for which the payer has given consent to the exact amount of the funds to be blocked pursuant to 75(1) of that Directive, the **authorisation** ~~authentication~~ code generated in accordance with Article 1 shall be specific to the maximum amount that the payer has given consent to be blocked as ~~and the payee~~ agreed ~~to~~ by the payer when initiating the transaction.

As the concept of "authentication" is already defined in PSD2, we would suggest adding a definition of "authorisation".

Article 2.4: A "batch" of payments is to be understood as multiple payments mostly used in corporate environments for which the PSU is not required to check each and every individual transaction. At first sight, it seems rather difficult, if not impossible, to generate a code that would be specific to each payee within one single file. This provision requires clarification from the EBA.

Q3: In particular, in relation to the protection of authentication elements, are you aware of other threats than the one identified in articles 3, 4 and 5 of the draft RTS against which authentication element should be resistant?

For more than 30 years, close cooperation with law enforcement agencies has allowed the banking industry to stay ahead of cybercrime to detect trends and upgrade their security measures and products on an on-going basis. Flexibility and adaptability is of the essence and should be maintained. We would therefore strongly support a risk based approach that allows PSPs to protect their clients' assets (clients and corporates alike) by giving them the agility needed to immediately react to new fraud trends and work closely with law enforcement agencies to share data intelligence.

With regard to article 7, further information on the audit/review of SCA procedures would be welcomed so as to understand what kind of controls would be required to comply with this obligation.

Q4: 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?

As stated earlier, PSD2 is very clear on the way exemptions to strong customer authentication should be drafted. Exemptions should indeed be based on "the level of risk involved in the service provided" (article 98.3.a), allowing, for example, AS PSPs to continue their current processes for managing transactions. To the contrary, the list of exemptions proposed under article 8 is too prescriptive and detailed to give AS PSPs the necessary flexibility to manage their risks in an appropriate way, given that they are ultimately liable for any unauthorised transaction. This would decrease the ability of PSPs to react to unforeseen fraud attempts. Besides, a detailed list of exemptions would immediately become the target of fraudsters and organised crime.

We would therefore propose to set high level standards that AS PSPs can adapt to in a flexible manner, depending on the environment or specific cyber threats at a given moment in time. These standards could relate to the PSU's device, the communication, application, payer and payee profiling, transaction level (to go on-line or not), Interpol warnings…, merchants' own authentication processes, in line with option 1.1 referred to earlier. For a long time now, merchants have been closely associated with the fight against fraud and some e-merchants have adopted very sophisticated tools to identify their clients and do a risk assessment on the case by case basis. Some have elected not to apply strong customer authentication and agreed to be fully liable in case of an unauthorised transaction.

Article 8.1: We understand from article 8.1 and rationale 19.b that all payees will have to apply strong customer authentication as from October 2018 at the earliest. We have not identified any reference to such transitional period in Article 74.2 or Article 115. Indeed, Article 74.2 clearly allows PSPs (and payees) not to require SCA provided any "financial damage" resulting unauthorised transaction is refunded to the payer. This shift of liability has been in place for more than 20 years as part of the EMV standard and has allowed merchants to adopt their own risk management processes that have proved to be quite effective over time and a useful complement to the processes put in place by PSPs.

We would therefore suggest to add this provision to article 8.1 (a) as follows:

1. The application of strong customer authentication in accordance with Article 97(1) **and article 74.2** of Directive (EU) 2015/ 2366 is exempted where:

    (a) the payer accesses exclusively the information of its payment account online, or the consolidated information on other payment accounts held, without disclosure of sensitive payment data.

    (b) The payment service provider has elected not to apply strong customer authentication and agreed to bear any resulting financial loss, unless the payer has acted fraudulently

    (c) The payee has elected not to apply strong customer authentication for given transactions and has agreed to refund the payer for any financial damage caused.

We see no justification to the fact that article 8.1 (b) i) and ii) seems to restrict the exemption to SCA to contactless payments only. There are indeed many environments in which cards are currently used without SCA. Should the EBA select to maintain a restrictive list of exemptions, we would propose to include "contact" transactions in the list of exemptions for transactions below 50€ and in environments where SCA is not technically feasible (parkings, tollways,…).

From the hearing, we understand that it is not the EBA's intention to prevent the use of contactless payment instruments over a long period of time. In order to avoid any possible misunderstanding, we would suggest to clarify article 8.1 (b) and make sure that the current customer seamless experience is preserved.

Equally, setting fixed amounts for when a payment requires strong authentication seems at odds with the AS PSP liability in case of unauthorised transactions that should leave it with the choice to strike the right balance between user friendliness and security. Predefined fixed rules weakens the user experience in a considerable way, as they mandate to use strong security measures on transactions that do not need them.

A very good example is a mobile app based PSP payment service where the receiving payment information is linked to a mobile phone number (the so-called "proxy look up" currently developed together with the European Central Bank). Any new user uses strong authentication when registering to the service and then uses lighter authentication methods when transferring money to a friend. Applying strong customer authentication to such services is a kill blow to the use case/service. The AS PSP should have the mandate to self-determine where the limit is for applying strong customer authentication.

Our suggested amendments are summarized below:

(b) the payer initiates a**n** ~~contactless~~ electronic payment transaction at a point of sale within the limits of both the following conditions:

i. the individual amount of ~~contactless~~ electronic payment transaction does not exceed the maximum amount of 50 EUR;

ii. the cumulative amount of contactless transactions without any transaction with strong customer authentication does not exceed 150 EUR

We would also propose to harmonise the limits, independent of the environment, to allow for a consistent customer experience.

In addition, the exemption based on white lists seems to limit its applicability to "where […] the payer initiates online a credit transfer". This exemption should be expanded to other transactions such as, for example, a remote card payment to a customer white listed merchant.

Article 8.2 (d) should therefore read as follows:

(d) the payer initiates a remote electronic payment transaction where all the following conditions are met:

i. the individual amount of the remote electronic payment transaction does not exceed the maximum amount of ~~10~~ **50** Euros; and

ii. the cumulative amount of previous remote electronic payment transactions initiated by the payer without application of strong customer authentication does not exceed **150** ~~100~~ EUR.

Article 8.2: Exemptions to strong customer authentication should not be limited to credit transfers as suggested under article 8.2 (a) and (b) but be extended to all means of payment. The wording should also be coherent with PSD2.

We would therefore suggest to amend article 8.2 (a) as follows:

(a) the payer initiates online a **payment transaction** ~~credit transfer~~ where the payee is included in a list of trusted ~~beneficiaries~~ **payees** previously created by the payer with its account servicing payment services provider.

(b) the payer initiates online a series of credit transfers with the same amount and the same payee.

Q5: 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?

AS PSPs should always have the option of applying more stringent security rules depending on circumstances and fraud attacks since fraudsters are becoming extremely sophisticated over time. Timely and targeted reaction to these threats is of paramount importance. PSPs should be able to adapt their security measures in a way that PSUs are least affected. This difficult equilibrium requires flexibility to apply SCA in certain circumstances, even though the transaction falls under the exemptions, in line with Article 1.3 (e). If the EBA elects to maintain the list of exemption as proposed, none of them should therefore be mandatory. The RTS should foresee a mechanism that allows PSPs to temporarily not apply an exemption should a specific risk be detected.

Q6: 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?

This question should be answered in conjunction with Rationale 19a as the latter seems to restrict measures aimed at protecting credentials to PISPs only. We would also suggest to clarify that these measures apply to all PSPs, i.e. to AISPs alike. Although it is said that the provision of a specific communication interface with a comparable service level to online banking is sufficient to comply with the requirements to communicate with TPPs, access to personalized security credentials by TPPs is not restricted.

This goes against the long-standing Security awareness efforts made by financial sector to educate their customers not to share their credentials with third parties, under any circumstances. If customers get used to sharing credentials for payment initiation or account aggregation services, it could create a harmful precedent that could end up increasing risk and fraud.

Despite of that, we would suggest to clarify that these measures apply to all PSPs, i.e. to AISPs alike.

The Title of article 9 should be amended as follows:

Requirements for security measures ***applicable to all PSPs***

The concept of “data” when it comes to security credentials is rather unclear in article 9.1 (a) and might lead to various interpretations. We would therefore suggest to delete it.

> a) ~~Data on~~ personalised security credentials are masked when displayed and not readable in their full extent.

Article 10: Industry standards (PSC DSS requirements) mandate merchants to protect any data related to cardholders’ accounts when they are processed, stored or transmitted for fraud prevention and detection purposes. We would therefore propose to insert a direct reference to the type of data deemed to be protected by payees in article 10 as follows:

> The service agreement between payment services providers offering acquiring services and payees that store, process or transmit personalised security credentials for payment transactions initiated by or through the payee in the context of a card-based payment transaction, shall include contractual provisions ensuring that payees have the security measures referred to in Article 9 in place to protect data related to **user payment account data** ~~personalised security credentials~~.

Article 14: The renewal of credentials is technology dependent. AS PSPs should therefore be allowed to update the procedures of “creation, association and delivery of the credentials” when renewed or replaced.

Article 14 should therefore be amended as follows:

> The renewal or re-activation of personalised security credentials shall be conducted following **up-to-date security** ~~the~~ ~~same~~ procedures of creation, association and delivery of the credentials and of the authentication *devices in accordance with Articles 11, 12 and 13.

Q7: Do you agree with the EBA’s reasoning on the requirement 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?

Article 17: Current card specifications (EMV) for contact and contactless transactions do not provide for “bilateral identification” between a card or mobile device and a payment terminal because the card device does not identify the terminal. To the best of our knowledge, EMV 2025 does not include any “bilateral identification” either. Paragraph 1 of article 17 should therefore be deleted.

The NTP protocol mentioned under Article 18 (c) is not the only protocol that can be used. As such, it may not be future proof and should only be mentioned as an example in the draft RTS as follows:

> (c) timestamps which shall be based on a unified time-reference system, including but not limited to, using **protocols such as** the standard NTP protocol, and which shall be synchronised according to an official time signal.

Article 19: We fully support the recourse to qualified certificates for web authentication as a matter of principle. Nevertheless, high level principles are probably the best approach in this respect as technology evolves at a rapid pace. The eIDAS Regulation should be seen as a possible solution but not necessarily the unique legally enforceable mechanism of mutual identification as one should not underestimate the impact of a (likely) patchy Member States adherence to the eIDAS Regulation within the EU.

In order to allow future security developments or innovations, reference to ISO 27001 as stated under article 21.6 should be replaced by a generic reference to "commonly accepted international standards".

Seamless and secure communication between AS PSPs and PISPs/AISPs and Card Based payment Instrument Issuers will only be possible if the overall framework allows it to be properly established; the very fact that the registration number would depend on each National supervisory authority introduces a fragmentation within the EU that has no room in a digital environment. Besides, AS PSPs would have to rely on Member States' capacity to make their National registers available 24/7, on-line, accessible across borders, with a probable risk of them not being standardised.

An additional constraint would come from the transitional period between the entry into force of the PSD2 (January 2018), the entry into force of the RTS (October 2018 at the earliest) and the designation of a qualified authority in charge of managing the entire process (date yet unknown).

In other words, PSD2 and the RTS require the whole payment industry to create an entirely new landscape but the most basic tools to make it secure, seamless and open are likely to be missing at the time of its implementation.

Q8: In particular, do you agree that the use of ISO 20022 elements, components or approved message definition, 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 constrain that would prevent the use of such industry standard?

There are no technical barrier to the use of ISO 20022. Nevertheless, the use of any type of standard (as a data dictionary) required to ensure interoperability of technical communication solutions between PSPs for the purpose of PIS, AIS and confirmation of availability of funds, but it should not be limited to ISO 20022 in order to include any other syntax such as JSON who's usage of which is expanding lately. Thus, for the sake of interoperability and accessibility, any reference to ISO 20022 or any other particular standards should be avoided.

Q9: With regard 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.

Website certificates issued by a qualified trust service providers under an e-IDAS policy would be the right approach, but only if there is a large adherence to it within the EU (see our comments under Q7). However, mutual recognition will take place between PSPs' servers and not at the level of PSU's devices. When it comes to allowing all common types of devices, it is in the participants' best interest to make sure they offer a seamless customer experience to the market through any device they elect to use.

According to the rationale, EBA identified two basic approaches for mutual identification of PSPs: website certificates issued by a qualified trust service provider under an eIDAS policy and website certificates issued by a general Certificate Authority.

Both approaches seem to be based on an internet-like solution, which goes against the objective of technology and business model neutrality.

Similarly, EBA's preference for website certificates issued by a qualified trust service provider under an eIDAS policy implies that, from its point of view, the risk of no Certification Authority being able to offer a solution that ensures the correct verification of registry numbers outweighs the risk of lacking qualified trust service providers designated under eIDAS by October 2018.

On the other hand, a lot of initiatives are being developed for the public sector and not available (yet) for private usage. This will create duplication and confusion for end users that would have to handle different certificates for different services. Without assessing the accuracy of this conclusion, it is clear that leaving the door open to both approaches and other potential technical solution would minimize the risk of not having a solution for communication among PSPs in place by October 2018.

Therefore, the reference to trust service providers under eIDAS should be made as a possible solution and no as the only legally enforced mechanism of mutual identification.
From our point of view, the key element for the development of a reliable communication solution among PSPs is the availability of a trustworthy and constantly updated central registry of authorized PSPs.

Q10: 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 AS PSP's communication interface? If not, please indicate what would be in your view the appropriate frequency and rationale for such frequency?

As stated under Article 1.3 (f), access to complete data is key for AS PSPs to prevent, detect and fight against criminal activities. We would therefore suggest to amend article 22.4 as follows:

> **Article 22.4:** Payment initiation service providers shall provide account servicing payment service providers with the same information **collected** ~~requested~~ from the payment service user when directly initiating the payment transaction.

One of the key issues in account information services, be they initiated by the PSU or an AISP is to make sure that the information request has not been generated by a robot and has been clearly requested by the PSU. The restriction of AISPSP information requests to no more than 2 times a day "where the payment service user is not actively requesting such information" is a positive attempt to safeguard the availability of the AS PSP's communication interface and reduce the risk of denial of service attacks. However, the different interpretation of what "actively requesting" means and the difficulty of identifying which TPP’s requests are originated by a PSU active request and which ones come directly from the TPP without PSU intervention could render this measure ineffective.

Article 22.5: Frequency of consultation should therefore be a matter of negotiation between all parties involved, PSU, AISP and AS PSP. We would therefore suggest the RTS not to set a maximum request per 24h as follows:

> **Article 22.5**: Account information service provider shall request information from designated payment accounts and associated payment transactions:
>
> (a) any time the payment service user is requesting such information,
>
> ~~(b) or, where the payment service user is not actively requesting such information, no more than 2 times a day.~~

Additional suggestions

We would kindly suggest to insert some definitions in the RTS to bring it in line with the PSD2 or market usage:

Definition:

"**Mandate**" should be understood as the expression of consent and authorisation given by the Debtor to the Creditor to allow such Creditor to initiate Collections for debiting the specified Debtor's account and to allow the Debtor Bank to comply with such instructions in accordance with the EPC SDD Rulebooks. **An e-Mandate** is an electronic document which is created and signed in a secure electronic manner."

Suggestions for clarification:

"**Payer**" should be replaced by "PSU" in appropriate areas of the text where it relates to an activity such as accessing an account online or using account information services and does not involve payment initiation (e.g. in Article 8.1 (a) and 17.1).

12/10/2016

About EBF

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

www.ebf.eu @EBFeu

For more information contact:

Pascale-Marie BRIEN
Senior Policy Adviser
p.brien@ebf.eu
+32 2 508 37 24
+32 478 31 68 96