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

EPC RESPONSE TO THE EBA CONSULTATION ON THE DRAFT REGULATORY TECHNICAL STANDARDS SPECIFYING THE REQUIREMENT ON STRONG CUSTOMER AUTHENTICATION AND COMMON AND SECURE COMMUNICATION UNDER PSD2

1. Background

The EBA published the above consultation paper on 12 August 2016. Responses could be submitted until 12 October 2016.

The EBA invited comments on all proposals put forward in this consultation paper and in particular on the specific questions detailed below.

This response template was only created for internal use and for publication on the EPC website. The finalised responses were copied directly into the dedicated form on the EBA website as no attachments could be submitted.

2. List of Questions

Question 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?

The EPC welcomes the EBA reasoning but would like to offer the following comments:

Rationale 19: For recurrent card transactions, the SCA of the payer should be required for the first transaction only, if it follows the same logic as the exemption for recurring credit transfers in Art. 8 of the RTS. The EPC suggests reflecting this in the RTS.

Rationale 19.a): The EPC suggests to reflect this Rationale in the RTS.

Rationale 19.b): We do not perceive the legal basis authorising the EBA to state that Article 74(2) of the PSD2 would only apply during a transitional period. Art. 74(2) is in no way time bound, or limited, as suggested by EBA in Rationale 19(b). There is no language within PSD2 to support this proposition that Art.74 (2) is made redundant by EBA excluding any risk elements from the draft RTS. As we believe that such risk based analysis and exclusions are clearly contemplated, and required, under the mandate provided at Art.98, by failing, or refusing, to cater for risk, we believe the EBA has exceeded that mandate.

Art.1.: Is it correct to derive from this article that hereby mag-stripe card transactions will be no longer allowed including the fallback from chip. In any event any such prohibition should not apply to transactions with a non-EEA card within the EEA or with an EEA card at a non-EEA POS terminal as this would only leave cash as a possible means of payment, could create hardship or inconvenience for consumers and would hamper international commerce.

Art.1.2.: Suggest to update as follows**:** **“**security features**,** ~~including, but not limited to algorithm~~, …… ~~expiration time~~, ensuring that:**……”** This would specify the requirements while being technically neutral.

Art.1.2.(b): The EPC suggest to delete “generated for the same payer”.

Art.1.3.(b): Although the EPC agrees with this principle in general, there are situations where a feedback to the payer about what went wrong during authentication may prove helpful. As an example, with card payments it is currently common practice that a message ‘wrong PIN’ is given on the terminal display. The EPC therefore suggests to revise Art. 1.3.(b).

Art.1.3.(c): The EPC seeks clarification on the fact that the party who can block is the party who issued the personalised credentials for the authentication.

Art.1.3.(d): As the EPC agrees that HTTP over TLS is a minimum requirement, the EPC acknowledges that this requirement may need to evolve rather quickly in the near future, depending on the creativity of fraudsters, and therefore the EPC would prefer to have “by relying where applicable on standardised state-of-the-art secure communication protocols, ~~including but~~ ….. ~~HTTP over TLS~~.”

Art.1.3.(e): This article is beyond the mandate given by the PSD2. The EPC suggest to limit the article to mechanisms that prevent, detect or block authentication fraud. Furthermore it is not technology neutral and does not provide flexibility to the ASPSPs and therefore 'shall' should be replaced by 'may'. Therefore, the EPC proposes the following modification to the article:

"…….prevent, detect and block, to the extent possible, transactions based on compromised PSCs or authentication codes. These mechanisms ~~shall~~ **may** take into account, but are not limited to: i. …… v."

Art.2.2(b): The EPC seeks further clarification on what is meant by independence and segregation. The EPC understands that a logical separation would meet the requirements as stated in this Article.

In addition, the EPC seeks clarification if for instance the current practice (for e.g. mobile contactless payments) whereby a dedicated mobile payment app which is present on the mobile device performs an electronic signature subsequent to the verification of a mobile code within the mobile payment app would meet the requirements stated.

Art.2.3.: For clarification reasons the EPC suggests an amendment of the end of this article as follows ''… the authentication code generated in accordance with Article 1 shall be specific to the maximum amount that the payer has given consent to be blocked ~~and the payee~~ **as** agreed to by the payer when initiating the transaction''.

Art.3.1.: A clarification would be needed as to what "an unauthorised party" is meant to be. The EPC suggests taking into account the long-standing security awareness efforts made towards educating users not to share their personal security credentials, under any circumstance, with third parties. If customers get used to sharing credentials, it could create a harmful precedent that could end up increasing risk and fraud."

In general, articles 3, 4 and 5 should avoid imposing a minimum set of characteristics to knowledge, possession and inherence elements that could hinder user experience or future innovation.

Art.6.2. & 6.3.: These articles cover requirements which address the exposure of single authentication elements through the usage of a multi-purpose device. As such it mitigates a threat to authentication elements, irrespective of the independence topic which is meant to be covered by Art.6. Therefore the EPC suggests to make 6.2 and 6.3 a separate article.

Art.6.2.: Following a risk-based approach, the EPC believes that an ASPSP can not only rely on mitigating "the risk of the multi-purpose device being compromised". Consumer multi-purpose devices should be considered largely outside the scope of control of a bank. Therefore the EPC suggests to adapt this sentence to "…shall provide measures to mitigate the consequences of the multi-purpose device being compromised."

Art.6.3.: In relation to the mitigating measures, as stated before, the EPC considers that it is better to list some examples that may be used, instead of the mechanism that shall be used. Therefore, the following changes to the RTS are proposed:

"For the purposes of paragraph 2, the mitigating measures ~~shall~~ **may** include, but are not limited to….."

Art.6.3.(a): We suggest not to use the term 'trusted execution environment', since this is a specific defined term (with capital letters: Trusted Execution Environment) in the Global Platform standard. This reference is too specific; the EPC suggests replacing this term by "a segregated secure environment".

General comments:

1. There is no clear differentiation between authentication and authorisation in the document. It is suggested that the Recitals specify different definitions for:

- Authentication code without linking, according to Rationale 22(b). This is important to clarify Art.1.

- Authentication code with dynamic linking to the transaction amount and payee (for remote electronic payments). This is important to clarify Art.2.

2. In Recital 14 on page 27 the real phishing risk is missing. Phishing occurs at the payer's side and if payers get used to enter their authentication codes into non-ASPSP interfaces, they may increasingly also be subject to phishing attacks by fraudsters.

3. The RTS could gain in clarity by adding a few additional definitions, applying a more consistent wording and a proper coverage of essential facts currently only reflected in the rationales.

Question 2: 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.

General comments:

The EPC welcomes the reasoning about the flexibility offered on where and when the dynamic linking can take place.

For dynamic linking the EPC believes 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 one.

Rationale 26: In relation to this rationale, the EPC is convinced that other techniques than the ones mentioned in this Rationale are available to 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 smart phone with a single online banking 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)

Art.2.2(b): The EPC seeks further clarification on what is meant by independence and segregation. The EPC understands that a logical separation would meet the requirements as stated in this Article.

In addition, the EPC seeks clarification if for instance the current practice (for e.g. mobile contactless payments) whereby a dedicated mobile payment app which is present on the mobile device performs an electronic signature subsequent to the verification of a mobile code within the mobile payment app would meet the requirements stated.

Art.2.3.: For clarification reasons the EPC suggests an amendment of the end of this article as follows ''… the authentication code generated in accordance with Article 1 shall be specific to the maximum amount that the payer has given consent to be blocked ~~and the payee~~ **as** agreed to by the payer when initiating the transaction''.

Art.2.4.: The EPC proposes to make the text of this Article unambiguous on the concept of “batch” and required procedure for authorisation. In case of a “batch”, the customer should not be required to check every individual transaction in the online environment before authorisation. Furthermore, the EPC would like to ask for clarification which part of the text is being specified by the words “considered collectively”. How to dynamically link the authentication code to multiple payments involving multiple payees?

Question 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, the EPC is indeed aware of other threats and would like to offer the following comments:

Art.6.2. & 6.3.: As this covers for the exposure of any single authentication element through the usage of a multi-purpose device, it actually also covers for a major threat to single authentication elements not specifically identified in Articles 3, 4 and 5 and as such appears to apply generally and irrespectively of the independence topic assigned to Art. 6.

Art.3.1.: The article is currently too prescriptive and does not respect the principle of technical neutrality in light of the wording used "features including but not limited to". The wording should rather read "features that **may** include but are not limited to"

It is unclear what is meant in this Article by 'non-repeatable characters'. The EPC suggests removing these words, since their most likely meaning is already covered by the term "complexity". The important issue is that the PSP has a password management policy. Beside measures ensuring a certain entropy against guessing attacks, the maximum number of erroneous trials must additionally be limited by the implementation in order to exclude exhaustive trial attacks. The EPC also suggests to remove the reference to "expiration time" since this is less and less considered as a best practice in security policies.

Question 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?

Contrary to EBA's conclusion (in Rationale 54) not to propose exemptions based on a transaction-risk analysis performed by the PSP concerned, they should be maintained, for the reasons illustrated here below and because this is contrary to the risk-based approach of all recent security and supervisory rules. Moreover, it appears to go against the wording of PSD2. Art. 98.3(a): exemptions based on "the level of risk involved in the service provided", since the exemptions in the current draft RTS do not allow for a risk-based assessment / approach by the PSP.

Rationale 53 is unclear in particular as Art. 97 (4) of PSD2 does not refer to exemptions. Also, the EPC disagrees with EBA's reasoning in Rationale 53 where it is stated that the requirement of "a consistent application of SCA by all PSPs" finds its ground in Article 66(4)c and 67(3)b of PSD2. These two Articles only state that an ASPSP is not allowed to discriminate between activities performed through an AISP or PISP and those performed directly by the PSU. Moreover, the exemptions criteria should not be an exhaustive list, so as to leave the PSP concerned the ability to apply exemptions based on its own transaction risk analysis. An exhaustive list of possible exemptions or criteria to be considered by PSPs for the transaction risk analysis may not be future proof and prevent future innovations that are to be expected in this dynamic and changing environment.

Rationale 54: It is clear that risk consideration was intended to be an integral part of the RTS, and, in particular, any exemptions, or situations where PSPs could exclude the use, or application, of the RTS &/or SCA, would incorporate a risk based analysis.

This position is further supported by the provisions of Art.74 (2) PSD2. This provision clearly contemplates situations where the payers, or payees, PSP will dispense with the requirement for SCA, a scenario which sits squarely with the risk based approach as contemplated under Art. 98.

The EPC believes this view is further supported by the references to proportionate, risk based security measures in Recitals 91 & 96, as follows:

- Recital (91): Payment service providers are responsible for security measures. Those measures need to be proportionate to the security risks concerned.
- Recital (96): The security measures should be compatible with the level of risk involved in the payment service.

The EPC would strongly support the specification of a parameter (to be defined by the EBA) dealing with transaction-risk analysis for the exemptions.

At a broad level the following criteria could be considered:

- Consumer device level (device type, OS/browser, malware (not) present, rooted / jailbroken, device identification, etc.).
- Connection level (direct / indirect, IP-address, IP GeoLocation, ISP, etc.).
- Application level (language of the application, etc.).
- Payer level (profiling, user interaction profiling, click-path profiling, etc.).
- Transactional level (history, beneficiary account, amount, country, urgent/non-urgent payment, etc.).
- Payee or beneficiary level (profiling).
- Big data (data related to fraud / threat environment, customer claims).

In addition, the EPC suggests that the criteria for this transaction risk-analysis will be principle-based. It is up to the PSP to decide on the exact capabilities of the fraud detection based on its own risk analysis and appetite.

Art.8. Recurring card-based payments need to be addressed.

The EPC suggests adding at the end of the article: “The exemptions to SCA being part of the authentication procedure performed by the payer’s PSP (also referred to as ASPSP) should therefore be applied by the ASPSP only”, in accordance with Rationale 41.

Art.8.1.: Why are there no exemptions related to white lists in analogy to Art. 8.2.(a) covered?

Art.8.1.(b): The exemptions from SCA for electronic card payments at a POS shall be the same for contact and contactless transactions. Currently, this Article fails to include existing card payments, such as no-CVM (Card Verification Method) debit- or credit contact card payments for e.g. toll ways, parking, vending machines under EUR 50.

The EPC suggest to cover other proximity payments accordingly.

Art.8.1.(b) and Art.8.2.(d): It is not clear why there is a difference between a contactless payment on a POS terminal and remote payment with respect to the maximum amount. Harmonisation is important for customer education. Moreover, the values should be aligned with Art. 42 of PSD2 defining low-value payments instruments.

Art.8.2.(a): Towards an enhanced user-friendliness, ASPSPs should be allowed to also operate a global white list of generally trustworthy payees for which no whitelisting by the PSU is required (e.g. contractual-based, national tax accounts). Upon need EBA could formulate specific guidance or liabilities in relation with such payees, put by an ASPSP on their global whitelist.

Art.8.2.(b): The EPC suggests to amend the exception as follows*: "the payer initiates on line* ***a pre-agreed series of recurrent credit transfers or standing order, created by the payer,*** *with the same amount…..…."*

Important note: All the comments provided above are made under the assumption that the exemptions remain **optional** for the ASPSPs as mandating the exemptions would be beyond the mandate given by PSD2. Furthermore, mandating the exemptions would not be not technology neutral and would not provide flexibility to the ASPSPs (which are liable) in case of suspected payment fraud or other abuses (Art. 97.1(c) PSD2).

Question 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?

The EPC understands that the application of the exemptions is optional for ASPSPs. Preventing the implementation of stronger security would be against PSD2. ASPSPs take risks through liabilities and may be limited by regulations towards not taking too high risks. But regulations should never refrain ASPSPs from lowering their risks, e.g. through mandating security exemptions. Such an approach would indirectly induce also drastic reactions instead of proper risk-based reactions, should ASPSPs be confronted with new threats specifically targeting any of the exemption scenarios (e.g. massive low amount transaction fraud). Mandating exemptions could also result in unresolved situations that prevent ASPSPs to comply with other regulations (e.g. national) imposing more strict requirements.

Question 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?

The EPC cannot fully agree to the EBA's reasoning as stated in the comments below (see comments on Art 10, 13 and 14):

Rationale 19 a): The EPC welcomes the interpretation. It provides a sensible way for ASPSPs to ensure their responsibilities, namely by either keeping full competence over self-issued authentication procedures, or by entering into a contractual agreement with a third-party, should the ASPSP-issued authentication procedures be substituted by personalised security credentials issued by PIPSPs The EPC also interprets that as a consequence of the above, the PISP / AISP is not allowed to store the credentials issued by an ASPSP without a contract between the PISP / AISP and the ASPSP, since the use of these credentials must be secured with a credential mechanism issued by the PISP / AISP. However, the EPC does not find this adequately reflected in the draft RTS. According to Article 97(5) of PSD2, Rationale 19 a) equally applies for PISPs and AISPs. Consequently, this would have to be reflected by completing the current PISP-only formulation under (19a) to also mention AISPs.

Art.9.1.(a): The EPC suggests to either define "Data on personalised security credentials" or to delete the word "Data". In addition, a risk-based approach should be supported here as well. For example, there are arguments for permitting the user to get a short view of what he/she has keyed into an authentication field.

Art.9.1.(c): The EPC suggests clarifying the word "tamper resistant". Moreover, the cost impact should be evaluated, e.g. is it a realistic requirement that all distributed usage of cryptographic material must take place in tamper resistant environments?

Art.10.: This article does not seem to properly reflect the rationale given under Rationale 22b and implemented by Art.1, whereby definitions state a clear segregation between PSCs (incl. single authentication elements) to be kept highly-protected under sole control of the payer and there-off derived one-time authentication codes to be used over the network. Art. 10 notably speaks about payees that store, process or transmit PSCs for payment transactions initiated by or through the payee in the context of a card-based payment transaction, whereby Art.1 mandates that one-time authentication codes be derived from the PSCs for SCA, and Art.1.2.(a) further mandates that no information on any of the elements of SCA can be derived from the disclosure of such one-time authentication codes.

Art.13.(b): "Digitally signed" refers to the usage of one specific technology to ensure the identity of the issuer and the integrity of the software. The market place may evolve and introduce new methods in the future. Hence the EPC suggests using a more technology neutral formulation.

Art.14.: It is suggested to open up to a more risk-based approach here. There is a difference between an ordinary, scheduled renewal of an expired credential, and the replacement of something that has been stolen. It seems too rigorous to require exactly the same procedures for renewal and re-activation of credentials in a trusted setting. Moreover such a practice is time consuming.

Question 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?

Art.17.1.: What is meant by 'secure bilateral identification' between the payer's device and payee's accepting device. Is mutual authentication meant? This would create incompatibility with EMV card based payments where there is no terminal authentication required. The EPC suggests to include a clear definition for "secure bilateral identification" between the TPP and ASPSP to clarify Art.17.

Art.17.2.: Suggest to change to 'adequately protected', because current text is too strictly formulated.

Art.21.5.: Will a PISP or an AISP always have sufficient contact details to inform the payment service user? The EPC is of the opinion that there should also be an obligation for the PISP and AISP to inform the ASPSPs that may be concerned when incidents have occurred. In addition – should the PISPs also have some formal liability to clean up after an incident?

Art.22.1.(a): In relation to the data exchange, the EPC would suggest that EBA would clarify that the ASPSP shall provide the account information service provider **at most** with the same information from designated payment accounts and associated payment transactions made available to the payment services user when directly accessing the information online. Therefore this information may not include display of other types of customer transactions.

Art 22.4: Suggest to change the text to "……with the same information ~~requested~~ **collected** from the payment service user…." (This would include for instance geolocation, IP address, etc. to ensure adequate fraud mitigation).

Question 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?

The RTS should remain agnostic vis-à-vis any particular standard to ensure that the RTS remains future proof.

Question 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 ?

The EPC would like to comment that qualified certificates assure the quality of identification by the CA for the issuing of such a certificate, but not the quality of the technology used to keep the associated private key credentials used for authentication (proof of identity) under sole usage control by its respective owner (a PSP). In order to ensure sole usage control by the respective PSP, the EPC proposes to specify the adequate protection (e.g. crypto smart cards, USB dongles, hardware security modules) for the associated PSP private key credentials, preferably referring to international standards. Based on such an enhanced specification, qualified certificates and associated private key credentials are a common and standard solution for PSP authentication in automated server-server communications.

The EPC agrees with the fact that a Qualified Trust Service Provider (QTSP) could provide the certificates to be used for the identification between PSPs and for website authentication subject to sufficient availability of the appropriate certification authorities on the market. However, in the case of PSP software components installed on any common type device (e.g., tablet, mobile phone), owned by the payer, there is no way to enforce sole usage control over private key credentials by the owning PSP, which renders the certificate based approach completely unsuitable for PSP authentication in such a scenario (no mitigation against PSP impersonation attacks).

Question 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.

The EPC agrees on the frequency of no more than 2 times a day as specified in Art.22.5.(b) (however it should be noted that sometimes it is difficult to distinguish between a real user and a robot). EBA is also advised to also take into account that problems with the communication interface are related not only to the number of times the AISP requests information regarding to the customer, but also to the amount of information/data that could be processed in a single request and the number of requests in a certain time window (possibly from different AISPs).

Art.22.5. (b): The EPC suggests amending the sentence as follows: "…..such information but subject **to prior explicit PSU consent being in place, no more than**….."