To the European Banking Authority

Consultation Reply by EPSM

on the Discussion Paper on future Draft Regulatory Technical Standards on strong customer authentication and secure communication under the revised Payment Service Directive (PSD2)

8th February 2016

Contact:

EPSM e.V.
board@epsm.eu

EU Transparency Register Number of the
European Association of Payment Service Providers for Merchants:
75870078560-90

1. Preface

The EPSM appreciates to be given the opportunity to provide comments and recognises the work already undertaken from the European Banking Authority (EBA). Given the complementary membership of the European Association of Payment Service Providers for Merchants it becomes obvious that the topics tabled from EBA can be viewed from different perspectives.

During the preparation of the feedback reply, the statements of the participants were in some respects quite heterogeneous – very much dependent on the services the respective companies provide. Consequently, EPSM suggests for the development process of the Regulatory Technical Standards (RTS) to assess the reasonability of each security measure for every category of services provided according to Article 4 of PSD2.

Consequently, it should be recognised that the payment service providers involved and addressed by the RTS have different roles and capabilities to fulfil the envisaged requirements. An account servicing payment service provider (ASPSP) for example fully controls the online banking account and has a contract directly with the payment service user (PSU). As such an ASPSP may use various methods to follow the requirements of strong customer authentication when a direct debit transaction is initiated. On the other hand, a Payment Initiation Service (PIS) provider must be able to rely on the methods provided by the ASPSP.

Thirdly, in case a remote payment is initiated with a credit card, all involved payment service providers (PSP) typically only utilize technologies offered by the card schemes. Therefore, it needs to be recognised in the development process that the card schemes are presently not directly addressed by PSD2 and the envisaged RTS. Possibly, a close dialogue between EBA and the card schemes during the process can help to minimise market disruption.

About the EPSM

The "European Association of Payment Service Providers for Merchants (EPSM)" is an interest representation and information platform of currently 67 European payment network operators, acquirers and other payment service providers for merchants. Among the non-voting members are terminal manufacturers, processing and acquiring providers as well as payment schemes. It is based in Munich, Germany.

The 67 EPSM members have their headquarters in 15 European countries (AU, BE, CH, CZ, DE, DK, FR, GR, IR, LU, LV, NL, SE, SK and UK).

For more information about EPSM and its members, please visit the EPSM website.

2. Questions tabled from EBA

Chapter 4.1: Requirements on strong customer authentication

1. *With respect to Article 97(1) (c), are there any additional examples of transactions or actions implying a risk of payment fraud or other abuses that would need to be considered for the RTS? If so, please give details and explain the risks involved.*

EPSM very much supports the list provided in PSD2 and further defined from EBA.

Nevertheless, in regard to Article 97 (1) b) of PSD2 and the considerations from EBA (i. on page 12 of the Discussion Paper) it should be noted that the market has developed a long set of different scenarios and solutions for the payment initiation and authentication. The considerations provided from EBA are a good first step to understand which exceptions will be allowed. Unfortunately, there remains uncertainty which payment initiation scenarios are exactly covered.

From the text provided, one could understand that paper-signature based direct debit transactions and paper-signature based debit- or credit card transactions are excluded. But in regard to signature based transactions, it is believed that it should not make a difference if a signature is provided on a piece of paper or on a signature pad. Acquirers and merchants have invested significantly in signature-pads. Consequently, it should be clarified that a signature provided on a piece of paper or on a signature-pad will be treated equally.

These considerations show the risk to unintentionally block innovative solutions with the regulation. To minimise these risks and to ensure that consumers coming from abroad, potentially not having devices capable to comply with the requirements of PSD2, EPSM stipulates EPA to consult closely with the involved market players like the major card schemes.

In regard to iii. (page 12 of the Discussion Paper), EPSM would like to draw the attention to an additional fraud scenario acquirers experience, the so-called ‘merchant identity fraud’. In this scenario, a fraudster takes over a legitimate business but has no intention to deliver the goods or provide the services purchased from the consumers who have entered the respective authorisation data on the payment platform of the fraudster. At the time the acquirers intend to recover the funds, they have to find out that fraudster is gone and they are liable for the loss and the respective fees.

Regrettably, this kind of fraud is difficult to tackle with the RTS developed at present. Nevertheless, it should be kept in mind that with even the most sophisticated mechanisms, fraud can hardly be stopped completely.

2. *Which examples of possession elements do you consider as appropriate to be used in the context of strong customer authentication, must these have a physical form or can they be*

data? If so, can you provide details on how it can be ensured that these data can only be controlled by the PSU?

The RTS should not be too prescriptive. Future innovations for strong customer authentication should not be hindered by inflexible RTS.

3. *Do you consider that in the context of "inherence" elements, behaviour-based characteristics are appropriate to be used in the context of strong customer authentication? If so, can you specify under which conditions?*

Again, the RTS should not be too prescriptive. Future innovations for strong customer authentication should not be hindered by inflexible RTS.

4. *Which challenges do you identify for fulfilling the objectives of strong customer authentication with respect to the independence of the authentication elements used (e.g. for mobile devices)?*

As far as mobile devices are concerned, EPSM believes that mobile devices are principally capable of providing independent authentication elements. The following characteristics of a mobile phone could be used: Unlock mobile by PIN or fingerprint, unique number of hardware, combination of hardware/software, SMS, entering PIN or password when initiating a payment.

Irrespectively of the channel an ASPSP offers and which strong customer authentication methods an ASPSP accepts, the very same channels and methods shall be open if a PSU initiates a transaction via the services of a PIS. Therefore, it should be clarified that ASPSP shall provide a level playing field to PIS and may not block communication channels or authentication methods for PIS when these channels and methods are accepted in case the PSU would be allowed using them.

5. *Which challenges do you identify for fulfilling the objectives of strong customer authentication with respect to dynamic linking?*

EPSM agrees with EBA (see paragraph 35 of the discussion paper) that the dynamic linking is only feasible for a very limited number of scenarios.

6. *In your view, which solutions for mobile devices fulfil both the objective of independence and dynamic linking already today?*

Please refer to answer to question 4.

Chapter 4.2: The exemptions to the application of strong customer authentication

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

Please see joint answer to 7. - 9. below.

8. Are there any other factors the EBA should consider when deciding on the exemptions applicable to the forthcoming regulatory technical standards?

Please see joint answer to 7. - 9. below.

9. Are there any other criteria or circumstances which the EBA should consider with respect to transaction risks analysis as a complement or alternative to the criteria identified in paragraph 45?

In principle, EPSM supports both, the exemptions and risk based approach. A low value transaction usually indicates a low risk transaction. On the other hand, a low value transaction in the gambling business might be treated differently. Therefore, no final view can be provided on the question which exemptions should be granted and which result from a risk assessment should be required to consider a transaction to be a low-risk transaction.

It is a significant regulatory challenge finding the right balance of consumer convenience and an acceptable low fraud rate. It seems that the market had responded well to this challenge (for example also respecting the business segment of the transaction). Therefore, the regulatory approach should not be too narrow.

When discussion this subject, the opinion was shared that an ASPSP should be liable in case the ASPSP qualifies a fraudulent transaction as a low-risk transaction and the transaction would have been blocked in case strong customer authentication had been applied. Furthermore, that transaction may not be treated differently when initiated via a PIS.

Chapter 4.3: The protection of the payment service users' personalised security credentials

10. Do you consider the clarification suggested regarding the protection of users personalised security credentials to be useful?

Please see joint answer to 10. – 14. below.

11. What other risks with regard to the protection of users' personalised security credentials do you identify?

Please see joint answer to 10. – 14. below.

12. Have you identified innovative solutions for the enrolment process that the EBA should consider which guarantee the confidentiality, integrity and secure transmission (e.g. physical or electronic delivery) of the users' personalised security credentials?

Please see joint answer to 10. – 14. below.

13. Can you identify alternatives to certification or evaluation by third parties of technical components or devices hosting payment solutions, to ensure that communication channels and technical components hosting, providing access to or transmitting the personalised security credential are sufficiently resistant to tampering and unauthorized access?

Please see joint answer to 10. – 14. below.

14. Can you indicate the segment of the payment chain in which risks to the confidentiality, integrity of users' personalised security credentials are most likely to occur at present and in the foreseeable future?

EPSM agrees that the protection of the personalised security credentials is critical. In case the security credential is electronically delivered data, it shall not be transmitted unencrypted from the ASPSP to the PSU. Open, secure and reliable standards should be used for encryption. Users should be educated on how they can validate the certificate of the ASPSP server.

There is a significant benefit of having components or devices certified or evaluated. Nevertheless, it is important not to introduce new or additional certification and evaluation methods. Global standards and innovative developments in other markets, e.g. America (USA) and Asia (Singapore) should be recognised.

Therefore, the regulation must not be too prescriptive in order to avoid costly, unnecessary adoption processes.

Chapter 4.4: Considerations prior to developing the requirements on common and secure open standards of communication

15. For each of the topics identified under paragraph 63 above (a to f), do you consider the clarifications provided to be comprehensive and suitable? If not, why not?

Please see joint answer to 15. – 18. below.

16. For each agreed clarification suggested above on which you agree, what should they contain in your view in order to achieve an appropriate balance between harmonisation, innovation while preventing too divergent practical implementations by ASPSPs of the future requirements?

Please see joint answer to 15. – 18. below.

17. In your opinion, is there any standards (existing or in development) outlining aspects that could be common and open, which would be especially suitable for the purpose of ensuring secure communications as well as for the appropriate identification of PSPs taking into consideration the privacy dimension?

Please see joint answer to 15. – 18. below.

18. How would these requirement for common and open standards need to be designed and maintained to ensure that these are able to securely integrate other innovative business models than the one explicitly mentioned under article 66 and 67 (e.g. issuing of own credentials by the AIS/PIS)?

The use of common, open and secure standards is supported from EPSM. Many communication and certification standards are already available. Furthermore, it is critical, that the access for the PIS and AIS to the respective servers of the ASPSP can be established in a direct, non-discriminatory way. No additional middle-layer shall be required from ASPSP.

Of course, ASPSP shall not be prohibited to develop additional layers for certain applications or services, but the ASPSP shall not require the PIS or AIS to assess the accounts other than via a direct connection using open and existing standards, like 3-way-handshake and HTTPS.

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

19. *Do you agree that the e-IDAS regulation could be considered as a possible solution for facilitating the strong customer authentication, protecting the confidentiality and the integrity of the payment service users' personalised security credentials as well as for common and secure open standards of communication for the purpose of identification, authentication, notification, and information? If yes, please explain how. If no, please explain why.*

Please see joint answer to 19. and 20. below.

20. *Do you think in particular that the use of "qualified trust services" under e-IDAS regulation could address the risks related to the confidentiality, integrity and availability of PSCs between AIS, PIS providers and ASPSPs? If yes, please identify which services and explain how. If no, please explain why.*

EPSM supports the use of open and neutral requirements and certification standards, no matter if developed nationally, European wide or globally. Presently, it is difficult to anticipate the functionality and availability of pan European solutions in the next years.

Consequently, other solutions shall be accepted in addition to the services offered under the e-IDAS regulation.