To the European Banking Authority

Consultation Reply

on the draft Regulatory Technical Standards specifying the requirements on strong customer authentication and common and secure communication under PSD2 of 12 August 2016 (EBA-CP-2016-11)

10 October 2016

Contact:

EPSM e.V.
board@epsm.eu

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

About the EPSM

The "European Association of Payment Service Providers for Merchants (EPSM)” is an interest representation and information platform of 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, UK).

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 scope of the Regulatory Technical Standards (RTS) is unclear to EPSM. In order to avoid different interpretations in the Member States, EBA should provide definitions and clarifications in the RTS. EPSM believes that a more thorough differentiation of the different payment types is strongly required in order to make this regulation a success.

General:
The wording in Art. 1 RTS does not to fit to the present global EMV standard practice for POS-terminal transactions. The wording was formulated with 'online-banking credit transfers' in mind. The established and secure EMV standard that is applied for the vast majority of European card payment transactions would have to be changed. If EBA persists in the present draft wording and scope of the RTS, the creation and implementation for an extra EU EMV dialect would require a time period of 5 to 10 years (if the security relevant software of POS devices needs to be changed).

EBA should also consider that a layered security level is inherent to card payments. Merchants, acquirers and issuers each employ their own risk prevention systems and balance risk versus convenience. In contrast thereto, security of online banking payment methods mainly focus on the accurate authentication of the payer by the ASPSP, or PISP respectively. Therefore, we are concerned that due to the obligation to support SCA in every card transaction, the well established multi layer security of card payments will be replaced through SCA as sole risk prevention method.

Authentication Code:
It is unclear what an 'authentication code' is and what qualifies for it. The wording 'authentication code' is used in a different context in PSD2 (Recital 96) and the accompanying FAQ document. It seems that the idea of an authentication code fits to online remote payments, but is not feasible for card payments at POS.

Technically speaking, it is indistinct if the EBA required 'authentication code' can be realised by any of the EMV standardised data like the Message Authentication Code (MAC) or the ARQC (Authorization Request Cryptogram).

Consequently, the RTS should stick to the wording of PSD2 and the requirement of an authentication code only being applicable for 'remote electronic payment transactions'. In case EBA maintains the requirement of authentication codes for all transaction types, EBA should at least consult with EMV technical specialists to evaluate the best, feasible, secure and efficient way forward – instead of a burdensome, lengthy, expensive and unnecessary process.

Clarification Requirements:
If EBA will stick to the current wording, the following questions should be clarified to avoid different interpretations in the EU member states.

1. Is an 'EMV Chip & Signature' transaction at a POS terminal considered to be a strong authentication?
   a) in case the signature is provided on a paper slip
   b) in case the signature is provided on a signature pad"?

2. Is an 'EMV based, offline authorized' transaction compliant with the EBA requirements?
   EPSM believes offline authorised transactions should remain an option, especially as these transactions types are important for the handling of emergency transactions, when no connection between the POS terminal and a host is available.

3. Is an "EMV based, offline-PIN authenticated" transaction compliant with the EBA SCA requirements?

Definitions:
It is unclear what qualifies as 'an electronic payment initiated by the payer' under PSD2 and the RTS. From the few definitions and recitals at hand it has to be considered that debit and credit card payment methods, no matter if swiped, waved, authorised offline, online, using PIN or signature on paper or sign-pads, are covered from the draft Regulatory Technical Standards (RTS), despite all the remote payments. Considering Recitals 95 and 96 of PSD2, stating that not the same level of protection is needed for all different types of transactions, EBA should clarify which transaction types do and which transaction types do not fall under the scope of Article 97 (1) PSD2.

In this respect, EBA should provide clear definitions that help to understand if the following ways to initiate a card payment transaction qualify for strong customer authentication:

- Handing over a payment card to the merchant?
- Inserting a card into a POS terminal by the card holder?
- Inserting a card into a POS terminal by the merchant?
- Signing a printed "card payment slip"?
- Entering a PIN at successfully at a POS terminal?
- Entering a PIN at non-successfully at a POS terminal?
- Sending successfully the daily "cutover" order from the POS terminal to the acquirer?

Recurring Payments:
Recurring payment transactions should either be excluded from the scope or exempt from the applicability of strong customer authentication. The principle that is established for credit transfers (Art. 8 (2) (b) RTS) should also be available for other transaction types, e.g. recurring credit card transactions initiated by the payee.

One-Leg-Transactions:
Last but not least, PSD2, Art. 97 covers ‘one-leg transactions’. Up to now, not all markets outside the EEA support strong customer authentication. EPSM believes tourists visiting Europe should not be excluded from using their payment cards. Therefore, EBA should clarify that the scope of Art 97 (1) does not cover:

- International card payment transactions where the issuer residing outside the EEA does not support SCA,
- International card payment transactions where the acquirer residing outside the EEA does not support SCA.

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.

EBA shall remain neutral on this question as to when the ‘dynamic linking’ should take place.

Q3: 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?

EPSM does not see other significant threats.

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?

While in PSD2 the concept of risk considerations (‘risk based approach’) is recognized, the draft RTS list a limited number of scenarios when transactions are exempt from strong customer authentication. In this regard, EPSM does not agree with EBA. EPSM believes it should be to the discretion of the PSPs to decide which transactions qualify as low risk transactions.

Payments market participants, including acquirers, issuers, merchants and many specialised service providers, have developed very specific risk based approaches considering a whole set of criteria to qualify the risk of a given transaction for years. By applying sophisticated techniques it has always been the highest principle to find the best balance between the security needs of all parties involved and the convenience for the user.

It is understandable that 'EBA was not able to identify which minimum set of information the RTS should require for such transaction risk analysis to ... allow a specific exemption from the application of SCA' (see No 54, page 16). This being said, EPSM strongly believes that it is the wrong way to exclude the option of risk evaluation for PSPs altogether.

EPSM considers the attempt of the regulator trying to override the efficient work of all the risk and fraud experts in a few articles inappropriate. In order to avoid significant changes in the payments market to the dissatisfaction of all participants, including the consumers, EBA is asked to leave the decision which transaction qualify as a low risk transaction to the PSPs. EPSM believes that EBA has better ways and means at hand to achieve the same or even a better result (to safeguard the consumer). One option would be to introduce liability shifts between the PSPs and to exclude liability for the consumer.

In this context, a Super-Complaint from Which, a consumer protection organisation in the UK, to the Payment System Regulator issued on 23 September 2016 provides compelling evidence that the strict obligation to support SCA in all transactions which the EBA is going to impose must be considered as an inappropriate and a misguided over-interpretation of Art. 97 (1) and Art. 74 (2) PSD2.

Consequently, only the payments which cause difficulties for the consumers should be in the scope of Art. 97 PSD2. In contrary to EBA's view as set out in No's 19b and 41 of the Consultation Paper, EPSM does not support an understanding that card acquiring PSPs 'should require payees to support SCA for all payment transactions'.

EBA should rather continue following the principles EBA has established in No. 7.5 of the EBA Guidelines issued on 19 December 2014 which are applicable at present:

> *(quote:) 7.5*
> *[cards] PSPs offering acquiring services should require their e-merchant to support solutions allowing the issuer to perform strong authentication of the cardholder for card transactions via the internet. The use of alternative authentication measures could be considered for pre-identified categories of low-risk transactions, e.g. based on a transaction risk analysis, or involving low-value payments, as referred to in the PSD.*

From a security and risk perspective, it is not understandable why contactless transactions should be favoured over contact-based payments. E.g. toll booths on motorways or parking meters usually do not require a PIN entry for low value payments with contact-based cards. EPSM believes EBA should abstain from interfering with the marked developments by favouring contactless transactions over contact transactions. Furthermore, this seems to contradict with the mandate laid out in Art. 98 (2) (d) PSD. The RTS shall be developed from EBA in order to ‘ensure technology and business-model neutrality’.

It is therefore suggested to delete the words ‘contactless’ in Art. 8 (1) b) i. RTS. Additionally, EPSM is of the opinion to put the maximum amount to 100 EUR, instead of 50 EUR as many relevant payment transactions are above 50 EUR, e.g. payment at motorways.

In addition, EPSM considers the application of a cumulative threshold not to be feasible in environments where access or pass through is controlled by card payment such as toll stations or parking meters. Typically in these low value acceptance environments with cardholder activated terminals, payment devices are not regularly equipped with PIN pads or signature pads. Also, the payer would not be prepared to enter a PIN. We are concerned about scenarios where pass through is massively hindered due to delay or even abort of payment transactions.

Accordingly, we suggest deleting clause of Art. 8 (2) b ii RTS, or at least provide a five to ten years period to allow the instalment of the respective terminals.

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?

EBA should clarify that the list of exemptions is only optional and not mandatory. As fraud patterns change, PSPs should be given the opportunity to apply strong customer authentication if they deem appropriate, also for low value payments. For example, it should be possible for to set the maximum threshold for transactions in gaming or gambling to 5 EUR.

Therefore, EPSM suggests changing Art. 8 (1) and Article 8 (2) RTS in the following way: The word ‘is’ should be replaced by the words ‘may be’.

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?

In principle EPSM agrees with EBA’s reasoning on the protection of the confidentiality and the integrity of the security credentials. Nevertheless, EBA should note that there are alternative, indirect identity payment instrument verification and authentication processes from global companies available which have the advantage that they avoid man in the middle, boy in the browser, or security breach attacks.

Therefore, EBA should further consult with security experts to avoid exclusions of solutions that can establish a high level of security.

Q7: 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?

The use of open standards is generally a good concept for creating an effective market with many players. Nevertheless, PSD2 states in Recital 32 that ASPSPs are required to provide also 'direct access' to payment initiation service providers. It is the understanding of EPSM members that for this direct access no separated communication infrastructure should be required.

Furthermore, article 19 of the draft RTS provides ASPSPs with the opportunity to develop a 'dedicated' communication interface which than would be mandatory for TPPs to use in order to access the customer's bank account. The dependency from the ASPSP's developments seems to be in contrast with the intention of PSD2.

Q8: 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?

ISO 20022 was originally designed for bank to bank messages. As such, ISO 20022 is only a messaging standard and not a communication standard. Since APSPs do not use this standard for their communication with their customers, it is likely that ISO 20022 will result in being an obstacle for TPPs direct access to the customers' payment account. It should be avoided that the obligation to use ISO 20022 elements indirectly leads to the foreclosure of TPPs direct access.

Q9: 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 ?

As the knowledge about the availability and the functionality of website certificates issued under an e-IDAS policy is not very widely spread, the process of securing the payments functionalities should not solely rely on these certificates.

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 ASPSP's communication interface? If not, please indicate what would be in your view the appropriate frequency and rationale for such frequency.

Considering the availability of different future payment means, e.g. 'instant payments', we would like to refer to the market specialists (like account servicing payment service providers), with consideration of the views of the competition authorities.

Summary:
The present RTS were written mainly looking towards online credit transfers and the corresponding ASPSP services. Other payment methods, like payment cards, seem to have played a much lower priority. EPSM believes that the present draft lacks clarity, provides too much room for interpretation which will lead to significant uncertainties.

The major threat of the RTS is seen in an unbalanced overregulation in areas in which no regulation is needed – or a much lighter regulation would be sufficient.