European Association
Of Payment Service Providers
For Merchants

EPSM

EPSM e.V., Ludwigstr. 8, D-80539 München

Mr Vadis Dombrovskis
Vice-President for the Euro and Social Dialogue
European Commission
Rue de la Loi / Wetstraat 200
1049 Brussels
Belgium

EPSM e.V.
Ludwigstr. 8
D – 80539 München

Tel.: +49 - 89 - 6 14 45 - 412
Fax: +49 - 89 - 6 14 45 - 3412
E-mail: board@epsm.eu

8 May 2017

EBA Final Report, Draft Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication

Dear Mr Dombrovskis,

Thank you very much of your kind response to our letter dated 23 March 2017. We understand that at this point in time no further formal consultation on the Final Report of the Draft Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication under Article 98 of Directive 2015/2366 (PSD2) is scheduled.

Therefore, EPSM would like to submit herewith some uncertainties and obstacles of the Regulatory Technical Standards (RTS) that should be considered in the adoption process by the European Commission.

Our letter addresses the following topics:

1. Authentication Code, Art. 4 RTS
2. Contactless Payments, Art. 11 RTS
3. Trusted Beneficiaries, Art. 13 RTS
4. Recurring Payments, Art. 13 RTS
5. Business to Business Transactions, Art. 4 and 5 RTS
6. Transaction Risk Analysis, Art. 16 RTS
7. Liability Shift, new chapter RTS
8. Prepaid E-Money Transactions, Recital 8 RTS
9. Magnetic Stripe and Signature Transactions, Analysis 272 RTS

From the perspective of EPSM, the topics summarised below are of particular importance. Nevertheless, many of them suggest only minor amendments or clarifications.

- The requirement of Article 4 should only apply to remote payment transactions, as there is still uncertainty as to whether card transactions initiated with presently issued EMV cards are always capable of fulfilling the requirements for authentication codes. This change would not result in additional security risks, but would prevent the necessity of the reissuance of millions of chip cards.

- Present chip cards are not capable of adding up consecutive payment amounts for contactless transactions, potentially in different currencies. Therefore, the cumulative amount should be deleted in Article 11, which would imply only a minor and acceptable increase of risk.

- The managing organisations of communication standards for batch payments (e.g. SWIFT and EBICS) should be asked whether their standards can accommodate with the requirements of authentication code and dynamic linking. If there is any uncertainty, then these requirements should not apply to batch payments.

- The exemption of Article 16 should also apply to card present transactions. Furthermore, additional guidance regarding the calculation of fraud levels is suggested, and clarification that only the payment service provider of the payer is responsible for monitoring the transactions and calculating the respective fraud level.

- The interpretation of EBA and the draft RTS do not match the text of PSD2 regarding the option for payment service providers of the payees to abstain from requiring strong customer authentication. A respective change is recommended.

- A clarification that strong customer authentication shall not apply to prepaid payment instruments subject to Article 63 (1) point (b) is suggested, in order to avoid misinterpretations when the RTS are made applicable in the Member States.

- In contrast to transactions initiated electronically, transactions that are initiated by handwritten signatures – regardless if on paper or on sign-pads – do not fall under Article 97 1 (b) PSD2. As a section of the Analysis in the RTS could be misinterpreted, clarification is recommended.

Please refer to the following pages for more information.

1. Authentication Code, Art. 4 RTS

a. Content of Draft Regulation Text

The present formulation of the draft RTS stipulates in Article 4 that the authentication of transactions, which qualify for strong customer authentication, need to result in the generation of an authentication code.

EBA analyses (in response to comment number 272 (4) on page 143) that the EMV chip cards are in the scope of PSD2 and the RTS. Furthermore, the EBA is of the view that chip and PIN transactions are not non-compliant with SCA provided that they are DDA or higher. It is, however, up to the providers and issuers to assess whether or not their systems comply with PSD2 as well as the RTS requirements.

b. Implementation Obstacles

On 28 February 2017, immediately after the issuance of the final draft of the RTS from EBA, EPSM had addressed EMVCo with the question as to whether present DDA EMV Chip cards fully comply with the drafted requirements from EBA, in particular with regard to the requirement of an authentication code. Unfortunately, EPSM has not received a formal answer on this question, up to now.

If EMVCo should conclude, after the in-depth analysis, that the requirements for the generation of an authentication code in Article 4 cannot be met with the presently issued EMV Chip cards, this would result in the re-issuance of millions of debit and credit cards which will not be feasible in the anticipated time frames.

c. Proposed Solution

The regulator should consider that the European card payment industry has invested millions of Euros in the recent years to have with the EMV Chip and PIN technology the highest security level possible. Consequently, there is basically no fraud that uses vulnerabilities of this security standard. This needs to be recognised. Requirements drafted for online payments shall not apply to POS card payments, where sufficient security measures are in place already.

EPSM believes that neither the thousands of European payment service providers (PSPs) nor the regulator will get clarification on this question other than from EMVCo. Until this question is solved, the applicability of Article 4 should not apply to transactions other than transactions initiated remotely.

d. Suggested Wording

EPSM suggests including an extra paragraph in Article 4 that clarifies:

‘This requirement applies to ***remote*** *payments only.’*

2. Contactless Payments, Art. 11 RTS

a. Content of Draft Regulation Text

The RTS foresee in Article 11 that PSPs are exempt from the application of strong customer authentication where the transaction amount does not exceed EUR 50 (paragraph (a)) and the cumulative amount, or the number of previous contactless electronic payment transactions initiated via the payment instrument offering a contactless functionality since the last application of strong customer authentication, does not respectively, exceed EUR 150 or 5 consecutive individual payment transactions (paragraph (b)).

b. Implementation Obstacles

The present wording of Article 11 cannot be implemented in present contactless card payment transactions of the major international card schemes. There are two counters available in the present EMV Chip cards of the international card schemes for two different purposes. Unfortunately, they are not fully interfacing with each other. This leads to a situation whereby the cumulative amount cannot be calculated.

c. Proposed Solution

As the condition ‘the cumulative amount since the last application of strong customer authentication does not exceed EUR 150’ of Article 11 (b) cannot be implemented at present, it is suggested to delete this condition for the time being.

EPSM believes that the resulting increased risk of a total maximum of EUR 250 – in case a fraudster initiates five payments with a maximum amount of EUR 50 every time – is acceptable.

The regulator together with the experts from the payments industry should review this Article at the next review circle of the RTS and decide then if a maximum cumulative amount is necessary and feasible.

d. Suggested Wording

EPSM suggests deleting the words struck out below in Article 11 (b):

... ~~the cumulative amount, or~~ the number~~,~~ of previous contactless electronic payment transactions initiated via the payment instrument offering a contactless functionality since the last application of strong customer authentication does not, respectively, exceed ~~EUR 150 or~~ 5 consecutive individual payment transactions.

3. Trusted Beneficiaries, Art. 13 RTS

a. Content of Draft Regulation Text

Article 13 1. (a) of the RTS exempts PSPs from the application of strong customer authentication where the payee is included in a previously created list of trusted beneficiaries. According to Article 13 2. (a), strong customer authentication is required for the creation and the amendment of this list. This may be done by either the payer or the PSP of the payer, provided that the payer gave its consent.

b. Implementation Obstacles

The option to allow the PSPs of the payers to create the list of trusted beneficiaries could lead to a situation where the PSPs of the consumers sell the inclusion in a white list to merchants. White-listing on the initiative of the PSP of the payer would very much disadvantage small and medium size merchants who would have a much smaller business benefit than large ones to get listed as a trusted beneficiary.

These large merchants, who often practice the so-called ‘card-on-file card transactions’ could be willing to purchase the right to be put on a list, in case this should be offered from the PSP of the payer. This possibility contradicts the objectives of PSD2 and the RTS where security concerns should dominate the development, not market domination.

As EPSM expects severe market distortions, if PSPs of the payers are entitled to create the lists of trusted beneficiaries and sell this white listing to large merchants, the respective European merchant organisations as well as the competition authorities should be consulted.

c. Proposed Solution

Only the payer should be allowed to create, confirm or amend the list of trusted beneficiaries.

d. Suggested Wording

EPSM suggests deleting the words struck out below in Article 13. 2 (a):

... In relation to point (a) of paragraph 1, the payer ~~or the payer’s payment service provider, provided that the payer gave its consent,~~ creates, confirms or subsequently amends, the list of trusted beneficiaries.

4. Recurring Payments, Art. 13 RTS

a. Content of Draft Regulation Text

Article 13 1. (b) of the draft RTS exempts PSPs from the application of strong customer authentication where the payer initiates a series of payment transactions with the same amount and the same payee.

b. Implementation Obstacles

Many consumers in Europe do not only use direct debits for periodic payments, like utility bills, but also use their payment cards. As the amounts of these bills change from time to time, it seems to be inconsistent exempting only recurring payments with the same amount.

Furthermore, the payee already has the required payment and authentication data of the payee available for these recurring payments. Consequently, EPSM believes that the consecutive payments do not get initiated by the payer, but by the payee. As such, these transactions are not in the scope of Article 97 1 b) PSD2 and the respective RTS.

c. Proposed Solution

To avoid any doubts on this question, EPSM proposes to have a respective clarification inserted into the Recitals of the RTS.

d. Suggested Wording

EPSM suggests deleting Article 13. 1 (b) and 13. 2 (b):

~~*... the payer initiates a series of payment transactions with the same amount and the same payee.*~~

~~*In relation to point (b) of paragraph 1, the payer initiates the series of payment transactions for the first time, or subsequently amends, the series of payments.*~~

Instead, EPSM suggests including a clarification in the Recitals of the RTS:

Payments which are initiated by the payee alone rather than by the payer through the payee are excluded from the scope of PSD2 and from the application of strong customer authentication, regardless of whether the amount is the same or different.

5. Business to Business Transactions, Art. 4 and 5

a. Content of Draft Regulation Text

EPSM understands that the current draft RTS applies to all transactions, regardless of whether the payer and payee are consumers or business entities. EBA clarifies in its Analysis (see answer to question [272] 7)) that corporate transactions (including via SWIFT and EBICS) are within the scope of strong customer authentication.

b. Implementation Obstacles

There is a large number of corporate batch payment transactions using SWIFT or EBICS (used in France and Germany) that do not have fraud issues related to authentication. These internet banking standards have been successfully designed in order to implement a very high level of security.

c. Proposed Solution

EPSM strongly suggests seeking input from the organisations that manage the communication standards such as SWIFT and EBICS to make sure these standards comply with the requirements of the RTS.

Until a respective confirmation is provided, strong customer authentication and dynamic linking shall not apply to credit transfers transmitted in a batch format to the payers' PSP.

The regulator, together with the experts responsible for the standards should review this topic at the next review circle of the RTS and decide then if the requirements of a authentication code and the dynamic linking is necessary and feasible.

d. Suggested Wording

For the time being, EPSM suggests deleting paragraph Article 5 4. and adding new Article 19 that should be formulated as follows:
Subject to compliance with the requirements laid down in paragraphs 1, 2 and 3 of Article 2, payment service providers are exempted from the application of strong customer authentication and the dynamic linking, where the payer transmits a batch of credit transfers to the payer's payment service provider.

6. Transaction Risk Analysis, Art. 16 RTS

a. Content of Draft Regulation Text

Article 16 of the draft RTS exempts PSPs from the application of customer authentication, where the payer initiates a remote electronic payment transaction that has been identified as posing a low level of risk.

b. Implementation Obstacles

ESPM sees some challenges with Article 16 RTS.

- Firstly, it is unclear why this exemption only applies to remote transactions. Card payment transactions at the point of sale should be included.

- Furthermore, EPSM understands by interpreting the text of the Article 16 2 (a) to (g) that the payers' PSP should monitor and calculate the fraud rate. This would be reasonable as only the PSP of the payer has the required data listed in paragraph 2. (b). In contrast hereto, the payees' PSP does not have the respective data.

- Additionally, it should be clarified that one-leg-transactions where strong customer authentication has not been applied should be excluded from the calculation of the fraud rates.

- Finally, EPSM believes that the regulator should provide more guidance on how the respective fraud rates can be calculated. As there are significant differences between various products, e.g. for payment cards, it should be clarified that the PSP may differentiate between the different schemes and debit- versus credit cards and consumer-versus corporate cards etc.

c. Proposed Solution

The exemption should apply to all electronic payment transactions and should not be limited to those which are initiated remotely.

It should be clarified that only the PSP of the payer has to monitor and calculate the fraud rates.

More guidance should be provided as to how the fraud rates have to be or may be calculated, regarding one-leg-transactions (see above, third bullet point in 7 b) and possible differentiations (see above fourth bullet point in 7 b).

d. Suggested Wording

- EPSM suggests changing Article 16 1 as follows:
  *Subject to compliance with the requirements laid down in Article 2 and to paragraph 2 of this Article, payment service providers are exempted from the application of strong customer authentication, where the payer initiates a**n** ~~remote~~ electronic payment transaction, identified by the PSP as posing a low level of risk according to the transaction monitoring mechanisms referred to in Article 2(1).*

- EPSM suggests adding in Article 16 2. (a), (b), (d), (f) and (g) the word **payers’** before the words *payment service provider*.

- EPSM suggests adding the following clarification in the Recitals:
The transaction risk analysis shall cover only transactions within the scope of this RTS, therefore one-leg-transactions and transactions authenticated by signature shall be excluded from the calculation of fraud rates.

- EPSM suggests adding the following clarification in the Recitals:
When calculating the fraud rates according to Article 16, the payment service providers may distinguish between various products. For example, they may differentiate between the different schemes and debit- versus credit cards and consumer- versus corporate cards.

7. Liability Shift, new chapter

a. Content of Draft Regulation Text

The RTS do not take into account the option for the payee or the PSP of the payee to accept a transaction without requesting strong customer authentication from the PSP of the payer, if they are willing to accept the associated risk. According to PSD2 Article 74 (2) the PSP of the payee shall refund the financial damage caused to the payers' PSP where the payee or the PSP fails to accept strong customer authentication. In contrast hereto, Art. 97 PSD2 does not explicitly oblige the PSP of the payee to support SCA through the PSP of the payer.

b. Implementation Obstacles

EBA's restriction *'... with the payer's PSP having the final say.'* and the requirements of the text, are forcing the payees' PSP to support the application of SCA through the issuer, even if the PSP of the payee identifies a transaction as low risk by means of transaction risk assessment (TRA). If an acquirer nevertheless fails to require SCA from the issuer, the issuer has no option to accept such transaction relying on the acquirers TRA. The issuer may accept such a transaction only based on its own TRA or would be in violation of Art. 97 PSD2.

The SecurePay Guidelines (EBA/GL/2014/12_Rev1) do, on one side, impose an obligation to the acquirer for a card based payment to support SCA through the issuer, while on the other side, permit an exemption from this obligation based on a TRA (7.5 in the guidelines). We recognize that in this regard the SecurePay Guidelines were drafted to anticipate the PSD2 regulation. Accordingly, the ECB suggested in its report on the SecurePay Guidelines to implement SCA in PSD2 and to complement the SCA provision by a liability shift as set forth in Art. 74 (2) PSD2. We have not been aware that it was intended in the PSD2 legislative procedure to materially shift away from these principles of the SecurePay Guidelines.

EPSM believes that EBA has interpreted the intention of PSD2 differently an in a non-consistent manner.

c. Proposed Solution

EPSM believes that the option foreseen in PSD2 needs to be reflected in the RTS, as this supports developing seamless and fully integrated payments, to facilitate convenient payments to a maximum extent for consumers.

d. Suggested Changes

An additional chapter should be developed to accommodate the principle allowing the payees' PSP to waive the necessity of strong customer authentication and accept the liability, should the transaction prove to be fraudulent.

8. Prepaid E-Money Transactions, Recital 8 RTS

a. Content of Draft Regulation Text

Many of the Articles of the RTS are not suitable for transactions initiated by a prepaid payment instrument, which are qualified as electronic payment transactions and, as such, are in the scope of the RTS.

b. Implementation Obstacles

The majority of presently issued prepaid payment instruments, namely store- and gift cards, are issued anonymously and do not contain PIN technology. The authentication for the use of these payment instruments is either based on the possession of the card or the knowledge of an individual code. Therefore, many of the principles established in the RTS do not fit with these anonymously issued payment instruments.

Article 63 PSD2 allows a number of derogations for low value payments and e-money. Paragraph 1 of this Article clarifies that up to a limit of EUR 150 the issuers may agree with the users that no proof of the authentication is required.

c. Proposed Solution

EPSM believes that no substantial change to the text of the RTS is needed as we believe that the European legislator did not intend to include prepaid payment instruments subject to Article 63 of PSD2 to the scope of the RTS. This was also confirmed in some discussions of EPSM members with individuals from the European Commission. Nevertheless, considering the necessity of a consistent transposition of the RTS in all Member States and the need for legal certainty, a clarification is advised.

d. Suggested Wording

For clarification, EPSM suggests adding the following words at the end of Recital 8 of the RTS:
For the avoidance of doubt, strong customer authentication shall not apply to prepaid payment instruments subject to Article 63 (1) point (b) of the Directive (EU) 2015/2366.

9. Magnetic Stripe and Signature Transactions, Analysis 272 RTS

a. Content of Draft Regulation Analysis

EBA clarifies in its Analysis (answer to comment [272 (2)]) that imprinter card payment transactions are out of scope as they are considered to be paper-based. Additionally, magnetic stripe cards as well as cards with an EMV SDA chip are unlikely to be compliant with the requirements of the RTS, according to [272 (6)].

b. Implementation Obstacles

In the present card payment practice, the fallback to magnetic stripe still plays an important role. Allowing transactions with imprinters while forbidding those with magnetic stripe cards lead to an anachronistic situation that does not reflect the technological developments of the last 30 years with regard to a swift and easy consumer payments experience as well as to the deployment of additional security features.

The following table reflects the understanding of EPSM after having consulted with some of the respective national authorities regarding their interpretation of the PSD2 text. According to them, all transactions that are initiated by a handwritten signature are not in scope – in contrast to those initiated electronically by PIN entry:

	PIN	**Signature**
Imprinter	Not Applicable	Not in scope
Magnetic Stripe	Not RTS Compliant	Not in scope
SDA-Chip	Not RTS Compliant	Not in scope
DDA-Chip	RTS Compliant?	Not in scope
CDA-Chip	RTS Compliant?	Not in scope

Furthermore, in today’s practice, transactions which are initiated with the magnetic stripe are already flagged as a high risk transaction when the card and the POS terminal are chip-ready. In case of doubt, these transactions get declined from either the payers’ or the payees’ PSP.

Therefore, EPSM believes that for better business continuity it should be evaluated if the magnetic stripe and static chip (SDA) card technology should remain as fallback solutions in case severe problems associated with the chip technology should arise. The European payments industry has the role to provide consumers with the possibility to make payments at all times. For this, the magnetic stripe technology could still play an important role.

c. Proposed Solution

Card payment transactions initiated with the magnetic stripe could remain an option as a fall back solution for a limited number of cases and provided that the fraud level remains below a threshold, to be defined. EPSM believes that closing down the option to have cards authorised with the magnetic stripe does have severe implications to consumers and (potentially) in fall back situations.

It should be clarified in the Recitals that transactions that have been initiated by handwritten signatures, whether on paper or on a sign-pad are out of scope of the RTS.

d. Suggested Wording

EPSM suggests adding the following clarification to the Recitals:

Regarding signatures:
Payment transactions that are initiated with a handwritten signature, regardless of whether the signature is provided on a paper or on a sign-pad, are not in the scope of the RTS, as these transactions are not initiated electronically.

Regarding magnetic stripe and SDA chip card transactions:
EPSM does not propose a particular wording, but refers to the potential unintended consequences if the regulator remains with the view that transaction initiated with magnetic stripes or SDA chips cards are not compliant with the RTS.

This letter is the result of a small working group within the EPSM, coordinated by EPSM’s Lars Tebrügge.

We would appreciate if your organisation would evaluate our analysis and suggestions, and we are happy to answer any further questions.

Yours sincerely,

N. Adolph

Nicolas Adolph	Tony Sillopoulos
Chairman of EPSM	Board Member of EPSM

Annex – Profile of EPSM

EPSM Profile

Homepage: www.epsm.eu

E-Mail: office@epsm.eu

Name: European Association of Payment Service Providers for Merchants (EPSM) e.V.

Purpose: A non-profit trade association for cost-effective interest representation and general information exchange on issues relevant to payment providers for merchants in Europe.

Membership: Members shall have an essential business interest in providing commercially successful payment services to merchants in Europe (but: no issuers, merchants, or consultants). To have the status as a voting member, more than 50% of the sales revenues must result directly from payment- and supporting services for merchants in the EU.

Activities:

- Three meetings per year with external speakers;
- Information exchange by E-Mail;
- Website with members-only 'EPSM Intranet';
- Bimonthly 'EPSM Market Research Newsletter';
- Information exchange with partner organisations, like Concert, EAST, and Vendorcom;
- Consultant to the EPSM for information on current EU affairs.
- Participating Organisation in the global PCI Standards Security Council
- EPSM Chairman is member of the EU Payment Systems Market Experts Group (PSMEG)

Costs: Annual Membership Fees: 1,200 Euros per calendar year, (due in advance, for new members only partially by calendar for each month started).

Duties: Organisation of an informal meeting (sequence according to alphabet, if not otherwise agreed upon), on demand supported by a grant of the association.

Organisation: Board: 5 members, no salary;
Working language: English, on agreement other languages.

Members: The 68 EPSM members have their headquarters in 16 European countries:
(AU, BE, CH, CY, CZ, DE, DK, FR, GB, GR, IE, LU, LV, NL, SE, SK).

- 41 voting (ordinary) members:

  11 payment network operators, 10 acquirers, 6 internet payment providers, and 14 other payment service providers;

- 27 non-voting (extra-ordinary) members:

  7 payment schemes, 5 service providers, 3 terminal manufacturers, and 12 other organisations.

Board: Nicolas Adolph (Chairman, InterCard, Germany);
Iain High (Anderson Zaks, U.K.);
Christian Meyer (Treasurer, epay, Germany);
David Rintel (TrustPay, Slovakia);
Tony Sillopoulos (EDPS, Greece).

In Copy:

Mr Roberto Gualtieri
Chair of ECON Committee
European Parliament
Bât. Altiero Spinelli 15G206
Rue Wiertz / Wiertzstraat 60
1047 Brussels
Belgium

Mr Markus Ferber
Vice-chair of the Committee on Economic and Monetary Affairs
15E242 Rue Wiertz
1047 Brussels
Belgium

Ms Doris Dietze
In her function and activity for the European Council
Bundesminisiterium der Finanzen
Wilhelmstraße 97
10117 Berlin
Germany

Mr Andrea Enria
Chairperson
European Banking Authority
One Canada Square (Floor 46)
Canary Wharf
London E14 5AA
United Kingdom