EBA-CP-2016-11

12 August 2016

Consultation Paper

On the draft Regulatory Technical Standards specifying the requirements on strong customer authentication and common and secure communication under PSD2

Contents

1. Responding to this consultation 3

2. Executive Summary 4

3. Background and rationale 5

4. Draft regulatory technical standards on strong customer authentication and common and secure communication under PSD2 (Directive 2015/2366) 25

5. Accompanying documents 45

1. Responding to this consultation

The EBA invites comments on all proposals put forward in this paper and in particular on the specific questions summarised in 5.2.

Comments are most helpful if they:

- respond to the question stated;
- indicate the specific point to which a comment relates;
- contain a clear rationale;
- provide evidence to support the views expressed/ rationale proposed; and
- describe any alternative regulatory choices the EBA should consider.

Submission of responses

To submit your comments, click on the 'send your comments' button on the consultation page by 12 October 2016. Please note that comments submitted after this deadline, or submitted via other means may not be processed.

Publication of responses

Please clearly indicate in the consultation form if you wish your comments to be disclosed or to be treated as confidential. A confidential response may be requested from us in accordance with the EBA's rules on public access to documents. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by the EBA's Board of Appeal and the European Ombudsman.

Data protection

The protection of individuals with regard to the processing of personal data by the EBA is based on Regulation (EC) N° 45/2001 of the European Parliament and of the Council of 18 December 2000 as implemented by the EBA in its implementing rules adopted by its Management Board. Further information on data protection can be found under the Legal notice section of the EBA website.

2. Executive Summary

On 12 January 2016, the revised Payment Services Directive (EU) 2015/2366 entered into force in the European Union, and will apply from 13 January 2018.

The PSD2 aims in particular at ensuring that all payment services offered electronically are carried out in a secure manner, adopting technologies able to guarantee the safe authentication of the user and to reduce, to the maximum extent possible, the risk of fraud.

To that end, Article 98 foresees that EBA shall develop, in close cooperation with the ECB, draft Regulatory Technical Standards specifying the requirements of the strong customer authentication (SCA), the exemptions from the application of strong customer authentication, the requirements with which security measures have to comply in order to protect the confidentiality and the integrity of the payment service users' (PSU) personalised security credentials, and the requirements for common and secure open standards of communication between account servicing payment service providers (ASPSP), Payment Initiation Services (PIS) providers, Account Information Services (AIS) providers, payers, payees and other payment service providers.

The draft RTS proposed in this consultation paper, together with the provisions already stated in the PSD2 itself, set out a harmonized framework that is aimed at ensuring an appropriate level of security for consumers and Payment Service Providers, through the adoption of effective and risk-based requirements, securing and maintaining fair competition among all PSPs and allowing for the development of user-friendly, accessible and innovative means of payment.

The draft RTS proposed in this Consultation Paper has benefitted from an assessment of the 118 submissions that the EBA received in response to the Discussion Paper it had published on the same topic in December 2015. The resultant draft RTS that is being proposed in this Consultation Paper covers a similar ground as the Discussion Paper, i.e. it starts with the requirements on strong customer authentication, which is followed by a definition of the exemptions to these requirements. The draft RTS then proceeds to requirements related to the protection of the personalised security credentials, followed by common and secure open standards of communication. The Consultation Paper ends with clarifications related to the implementation of this RTS.

Next steps

The consultation period will run from 12 August 2016 to 12 October 2016. The final RTS will be published after consultation.

3. Background and rationale

3.1 Background

1. On 12 January 2016, the Directive (EU) 2015/2366 on payment services in the internal market, (thereafter referred as PSD2) entered into force in the European Union, and will apply from 13 January 2018. PSD2 confers 11 mandates on the EBA, three of which relate to the development, in close cooperation with the European Central Bank (ECB), of draft Regulatory Technical Standards and Guidelines to ensure the establishment of adequate security measures for electronic payments. The mandates include:

    - Guidelines on the establishment, implementation and monitoring of the security measures, including certification processes where relevant (in relation to the management of operational and security risks) (Article 95);

    - Guidelines, addressed to (a) payment service providers, on the classification of major incidents, and on the content, the format, including standard notification templates, and the procedures for notifying such incidents; and addressed to (b) competent authorities, on the criteria on how to assess the relevance of the incident and the details of the incident reports to be shared with other domestic authorities (Article 96); and

    - Regulatory Technical Standards on authentication and communication (Article 98).

2. The last mandate (Article 98) foresees that EBA shall develop, in close cooperation with the ECB, draft Regulatory Technical Standards addressed to payment service providers (PSP) specifying:

    a) the requirements of the strong customer authentication (SCA) when the payer accesses his payment account online; initiates an electronic payment transaction or carries out any action, through a remote channel, which may imply a risk of payment fraud or other abuses;

    b) the exemptions from the application of Article 97 on strong customer authentication and adequate security measures to protect the confidentiality and integrity of PSCs, based on the level of risk involved in the service provided; the amount, the recurrence of the transaction, or both ; or the payment channel used for the execution of the transaction;

    c) the requirements with which security measures have to comply in order to protect the confidentiality and the integrity of the payment service users' (PSU) personalised security credentials, and

    d) the requirements for common and secure open standards of communication for the purpose of identification, authentication, notification, and information, as well as for

the implementation of security measures, between ASPSP[1], PIS providers, AIS providers, payers, payees and other payment service providers.

3. PSD2 provides that these draft RTS shall be developed by EBA in accordance with the following objectives:

   a) ensuring an appropriate level of security for PSUs and PSPs, through the adoption of effective and risk-based requirements;

   b) ensuring the safety of PSUs' funds and personal data;

   c) securing and maintaining fair competition among all PSPs;

   d) ensuring technology and business-model neutrality; and

   e) allowing for the development of user-friendly, accessible and innovative means of payment.

4. When developing these particular RTS, the EBA has to make difficult trade-offs between competing demands. For example, the objective of ensuring a high degree of security would suggest that the EBA should develop the Technical Standards at a very detailed and technological level. By contrast, the objective to facilitate innovative means of payment would suggest that the EBA should do the opposite and pitch the Technical Standards at a less detailed and higher level, so as to allow room for the industry to develop industry solutions that are compliant with the EBA's Technical Standards but that also allow for innovation over time, so as to exploit technological advancements and to respond to future security threats.

5. Similarly, while Technical Standards that are pitched at a high level may facilitate innovation, it is also likely that this would result in many different industry solutions to emerge across the EU, in particular for the communication between ASPSPs, PIS providers, AIS providers, payers, payees and other payment service providers. This, in turn, could lead to a fragmentation that will undermine the objective of the PSD2 of integrating retail payments in the EU and facilitating competition across the EU.

6. Finally, the objective of ensuring a high degree of security and safety would suggest that the EBA's Technical Standards should be onerous in terms of authentication, whereas the objective of user-friendliness would suggest that the RTS should rather promote the competing aim of customer convenience, such as one-click payments.

7. Against this background, and prior to starting to develop the substance of the RTS, the EBA sought input from interested parties on where the ideal balance should lie via the publication of a Discussion Paper (DP). Unlike a Consultation Paper, a DP does not contain any specific regulatory proposals. Instead, it identifies and characterizes the problems or issues that the

[1] PSD2 article 4 (17) "Account servicing payment service provider" means a payment service provider providing and maintaining payment accounts for a payer.

future regulatory approach is meant to mitigate, and asks respondents to express their views on the way the EBA has identified and characterized the problem. Given the wide and heterogeneous nature of the audience from which input was sought, the EBA requested respondents to qualify the category of activities that best described their organisation, so that EBA could identify potential diverging views between different types of respondents.

8. The Discussion Paper was organised in five sub-chapters, the sequence of which followed the structure of the mandate conferred on the EBA in Article 98 PSD2 and the last one of which related to possible synergies with the Electronic Identification and Trust Services for Electronic Transactions Regulation (eIDAS).

9. The Discussion Paper was published on 8 December 2015 and the consultation period closed on 8 February 2016. The EBA received 118 responses to the DP, among which 82 gave permission for the EBA to publish them on the EBA website. This represents the second highest number of responses ever received by the EBA to a discussion or consultation paper.

10. While a majority of these responses were received from institutions that categorised themselves as credit institutions, the EBA also received responses from individual payment institutions and electronic money institutions, national and European trade associations representing these institutions, IT service providers, retailers, small and medium size enterprises, consumers or consumers associations, as well as academics.

11. In parallel, the EBA participated in the EU Commission PSD2 transposition workshop where further clarifications were provided to Member States in order to ensure a harmonised implementation of the PSD2 at the EU level. Where relevant, the EBA has relied on these clarifications to develop the substance of the RTS under consultation.

12. The EBA will assess the responses it will receive to the Consultation Paper, will make changes where appropriate, and plans to publish the final draft RTS, as provided by the PSD2, within 12 months of entry into force of the Directive, i.e. by 12 January 2017. However, the PSD2 also provides that the RTS will only be applicable 18 months after the adoption by the EU Commission, which would suggest an application date of the RTS of October 2018[2] at the very earliest. The intervening period provides the industry with sufficient time to develop industry standards and/or technological solutions that are compliant with the EBA's RTS.

3.2 Rationale

13. In order to explain how the EBA arrived at the provisions in the draft RTS that are proposed in the consultation paper on hand, this section summarises the EBA's understanding of some of the PSD2 provisions where relevant for the development of the EBA mandates, the responses received to the Discussion Paper and elaborates on the options and policy choices that were made when developing the provisions. In so doing, the structure of the rationale section mirrors the structure of the RTS set out in chapter 3, i.e. it starts with SCA, followed by exemptions, personalised security credentials, and common and secure open standards of communication. This is followed by the EBA's feedback to comments received regarding the application of the RTS requirements to third parties that PSPs may rely on for the provision of payment services. When this Consultation Paper uses technical terms that are defined in PSD2, the definitions of the PSD2 apply.

3.2.1 The requirements of the strong customer authentication

14. This section of the draft RTS specifies the requirements of strong customer authentication, which, according to Article 4(30) PSD2, is an authentication that

    a) is based on the use of two or more elements categorised as

        i. knowledge (something only the user knows),

        ii. possession (something only the user possesses), and

        iii. inherence (something the user is),

    b) ensures the elements are independent from one another, in that the breach of one does not compromise the reliability of the others, and

    c) is designed in such a way as to protect the confidentiality of the authentication data.

Clarification on PSD2 provisions

15. Article 97(1) of PSD2 requires that "Member States shall ensure that a payment service provider applies strong customer authentication where the payer:

    a) accesses its payment account online;

    b) initiates an electronic payment transaction;

    c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses."

16. The EBA has identified several questions related to the implementation of Article 97(1)b, in particular on the scope of the payment instruments to which this requirement should apply as well as how it should be applied by PSPs for a card payment transaction or the provision of PIS.

17. In relation to the scope of payment instruments, the EBA understands that Article 97(1)b applies to electronic payments initiated by the payer, such as credit transfers or card payments, but does not apply to electronic payments initiated by the payee only, such as direct debits.

18. However, if the payer's consent for a direct debit transaction is given in the form of an electronic mandate, it qualifies as falling under the category of "any action through a remote channel which may imply a risk of payment fraud or other abuses" as defined in Article 97(1)(c) of PSD2 wherever PSPs are involved in the signature of the e-mandate, either through direct communication with the payer or via the payee's PSP.

19. In relation to how Article 97(1)b should be applied by PSPs for a card payment transaction or the provision of PIS, the EBA understands that:

    a) in accordance with Article 97(5), PISPs have the right to rely on the authentication procedures provided by the account servicing payment service provider (ASPSP) to the user. In such cases, the authentication procedure will remain fully in the sphere of competence of the ASPSP. 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 ASPSP. This would however require a prior contractual agreement between the PIS and the ASPSP on the acceptance of such credentials by ASPSP. Such agreement would also be outside of the scope of PSD2.

    b) when considering remote card payment transactions, card acquiring PSPs should require payees to support strong customer authentication for all payment transactions, in order to allow the payer's PSP to perform SCA in compliance with PSD2. The EBA understands that Article 74(2) of PSD2, which allows the payee or the payee's PSP the option not to accept SCA, only applies during the short-time transitional period between the application date of PSD2 (13 January 2018) and the application date of the RTS under consultation (in October 2018 the earliest). During this transitional period, "where the payee or the payment service provider of the payee fails to accept strong customer authentication, it shall refund the financial damage caused to the payer's payment service provider".

Assessment of the responses to the EBA Discussion Paper, as input to the EBA's draft RTS

20. A majority of the responses received to the Discussion Paper on this topic requested the EBA to define the requirements of strong customer authentication in a way that would facilitate the development of innovative security solutions in years to come, as well as to facilitate an utmost of consumer convenience.

21. Against this background, the majority of respondent were of the view that the requirements should be as much as possible principle-based, i.e. developed at a high level, and should not prescribe specific technical solutions. However, several respondents requested further

clarification on the relationship between the authentication elements, the personalised security credentials (PSCs), and the strong customer authentication (SCA) procedure.

22. The EBA concurs with the view of the participants that, in order to ensure technology and business-model neutrality and to allow for PSPs to be able continuously to adapt to evolving fraud scenarios, the draft RTS should be developed at a higher rather than granular level of detail. With regards to SCA, the principles underlying the provisions in the draft RTS proposed by EBA, which have to be read in conjunction with the provisions of the PSD2 itself, can be summarised as follows:

    a) Authentication elements include the Personalised Security Credentials (PSCs), i.e. the personalised features provided by the payment service provider to the PSU for the purposes of authentication, as well as devices and software used to generate or receive authentication codes that may either be provided by the payment service provider to the payment service user or possessed by the payment service user without being provided by the payment service provider. In that respect, PSPs should ensure the protection of the confidentiality and integrity of PSCs, authentication devices and software, in compliance with the requirements included in Chapter 3 of these RTS.

    b) For strong customer authentication, PSPs have to ensure that a valid combination of authentication elements, i.e. based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, results in the generation of an authentication code that is only accepted once by the PSP for the same PSU. For electronic remote payment transactions, PSPs have to ensure that a valid combination of authentication elements, as described above, results in the generation of an authentication code to the payer's PSP, which is only accepted once for the same PSU and which is specific to the amount and payee agreed to by the payer when initiating the electronic remote payment transaction.

    c) Additionally, the strong customer authentication procedure shall include mechanisms to prevent, detect and block fraudulent payment transactions before the PSP's final authorisation. These mechanisms, which are described in article 1.3(e) of these RTS, shall take into account, but are not limited to, parameterised rules, signs of malware infection in the session and known fraud scenarios, an adequate transaction history of the payer to evaluate its typical spending behavioral patterns, information about the customer device used and a detailed risk profile of the payee and/or the payees device.

23. In relation to the "dynamic linking" to the amount and payee for electronic remote payment transactions, several respondents pointed out that EBA should remain neutral as to when the "dynamic linking" should take place. In particular, these respondents were of the view that EBA should not require that the authentication code in the form of a one-time password sent to the

payer is generated based on algorithms that take into account the amount of the transaction and the payee. Indeed, such requirement could in their view prevent PSPs from adapting the SCA solutions currently implemented in compliance with the EBA GL on the security of internet payments[3], in order to make them compliant with the requirements of dynamic linking.

24. Having assessed these responses, the EBA believes that the suggested draft RTS offers the flexibility for PSPs to adapt their current SCA solutions in order to make them compliant with the requirements of dynamic linking contained in these RTS, and for industry to complete this adaptation within the 18-month period foreseen by PSD2. Indeed, according to the requirements for SCA proposed in this CP, the authentication code can be either a single piece of data that is being input by the payer on the interface of the relevant PSP or can be generated from several pieces of data, such as a one-time password that is being input by the payer on the interface of the relevant PSP, the amount, and the payee of the transaction. Alternatively, the authentication code can take the form of digital signatures of such data using keys stored in the authentication elements.

25. This clarification means, for example, that the one-time password (OTP) linked to the amount and payee may be alternatively generated by the payer's PSPs with or without any action required by the payer itself, according to the technological solution adopted. In any case, the authentication procedure should ensure that the payer is always made aware of the amount and payee of the transaction he is authorising and should be tamper-resistant to prevent any manipulation of the amount and of the payee during the initiation of the payment transaction so that any change to the amount or payee shall result in a change of the authentication code.

26. Furthermore, the authentication procedure should ensure 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. To that end, the channel, device or mobile application where the information about the amount and the payee of the transaction is displayed should be independent or segregated from the channel, device or mobile application used for initiating the payment. This can be done, for example, via an independent channel to prevent any manipulation of the transaction details through the initiation process of the payment transaction.

27. Many responses received to the DP also underlined a number of cases where, for electronic remote payment transactions, the "dynamic linking" might be difficult to implement, such as for payment transactions where the amount of the transaction might not be known or for bulk payments where several payment orders are agreed by the PSU in one "transaction". The EBA took into account this feedback and included in Articles 3(3) and 3(4) of the draft RTS, a precise description of the "dynamic linking" procedure to cater for these special situations.

28. With regards to the definition of authentication elements categorised as knowledge (something only the user knows), possession (something only the user possesses), and inherence

[3] https://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-the-security-of-internet-payments

(something the user is), the majority of respondents was of the view that, in order to ensure technology neutrality and allow for the development of user-friendly, accessible and innovative means of payment, the EBA should refrain from further defining the nature of these elements. Given the definition of strong customer authentication provided in Article 4(30) PSD2, the EBA is of the view that there is no need to further define these authentication elements.

29. However, with regards to the inherence element, the EBA concurs with the view of the majority of respondents that behavioural data cannot be considered as a standalone inherence element, but rather as an additional tool for fraud prevention.

30. With regards to the use of mobile devices (e.g. mobile phone or tablet) as authentication element as well as a device allowing the reading or storage of another authentication element, the majority of respondents were of the view that this should be possible as long as the strong customer authentication procedure mitigates the inherent risks of the mobile device being compromised.

31. The EBA concurs with the views expressed by the respondents and recognises that, depending on how the strong customer authentication procedure is designed, several technical solutions might be used to mitigate such risks. In order to ensure technology and business-model neutrality, the EBA proposes in the draft RTS a principles-based approach that requires PSPs to ensure independence of the elements used for the strong customer authentication procedures in terms of the technology, algorithms and parameters used, in order to prevent that the breach of one element may compromise the reliability of another, in particular when a multi-purpose device such as a mobile phone or tablet is used within the strong customer authentication procedure.

32. In addition, in order to ensure that the strong customer authentication procedure remains resilient over time, the draft RTS proposes that PSPs periodically test, evaluate and audit the security of the overall strong customer authentication procedure. The conduct of such evaluation, which should rely on openly and publicly available state-of-the-art methods, must be organisationally independent from the units involved in the design, development and maintenance of the strong customer authentication procedure.

33. Finally, in relation to the possible synergies with the regulation on electronic identification and trust services for electronic transactions in the internal market (e-IDAS) as detailed in Chapter 4.5 of the DP, a majority of respondents was of the view that e-IDAS regulation might offer one of many suitable solutions on which PSPs could rely for ensuring the strong customer authentication procedure, but should not be considered as the only solution.

34. The EBA concurs with the views expressed by the respondents and believe that the proposed draft RTS do not prevent the possibility to adopt strong customer authentication procedures based on the services of a public e-identity scheme under the e-IDAS regulation framework, as long as these public e-identity schemes comply with the draft RTS.

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?

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.

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?

3.2.2 Exemptions

35. This section of the draft RTS has to specify the exemptions from the application of Article 97(1), (2) and (3) on strong customer authentication and security measures to protect the confidentiality and integrity of payment service users' personalised security credentials.

36. According to PSD2, the exemptions should be based on the following criteria:

    a) the level of risk involved in the service provided;

    b) the amount, the recurrence of the transaction, or both;

    c) the payment channel used for the execution of the transaction.

Clarification on PSD2 provisions

37. Recital 95 of PSD2 provides that the "security of electronic payments is fundamental for ensuring the protection of users and the development of a sound environment for e-commerce. All payment services offered electronically should be carried out in a secure manner, adopting technologies able to guarantee the safe authentication of the user and to reduce, to the maximum extent possible, the risk of fraud."

38. The same recital continues to provide that "a solid growth of internet payments and mobile payments should be accompanied by a generalised enhancement of security measures. Payment services offered via internet or via other at-distance channels, the functioning of which does not depend on where the device used to initiate the payment transaction or the payment instrument used are physically located, should therefore include the authentication of transactions through dynamic codes, in order to make the user aware, at all times, of the amount and the payee of the transaction that the user is authorising."

39. Recital 96 of PSD2 then adds that "the security measures should be compatible with the level of risk involved in the payment service. In order to allow the development of user-friendly and accessible means of payment for low-risk payments, such as low value contactless payments at

the point of sale, whether or not they are based on mobile phone, the exemptions to the application of security requirements should be specified in regulatory technical standards (…)."

40. Against this background, while PSD2 introduces the obligation for payment services providers to apply strong customer authentication for electronic payments, it also acknowledges the benefit to allow the development for user-friendly and accessible means of payments for low-risk payments. Taking into account this innovation rationale and in accordance with the criteria and the mandate provided in PSD2, the draft RTS under consultation specifies the cases (the exemptions) in which payment services providers are not obliged to apply strong customer authentication.

41. Finally, the EBA understands that the exemptions to SCA as defined in the RTS under consultation constitute a part of the authentication procedures performed by the payer's PSP (also referred as ASPSP) and should therefore be applied by the ASPSP only. The EBA underlines that this understanding is therefore a change compared to the exemptions to SCA specified in Guideline 7.5 of the EBA Guidelines on the security of internet payments (EBA GL/2014/12). The Guidelines apply since August 2015 until the application date of the EBA's RTS in October2018 the earliest and allow PSPs offering acquiring services for card-based remote payment transactions to use alternative authentication measures for pre-identified categories of low-risk transactions.[4]

Assessment of the responses to the EBA Discussion Paper, as input to the EBA's draft RTS

42. A vast majority of respondents to the DP supported the need to allow for exemptions in order to ensure that the payment is user-friendly, avoid "apathy" on the customer side due to excessive use of the SCA, and avoid an increase in transaction costs due to the implementation of SCA. Most respondents also underlined that these exemptions should not be mandatory for the PSP, so that the PSPs are always in a position to apply strong customer authentication in case of risk of fraud, even on transactions that would meet the criteria for exemption.

43. However, with regards to the scope of the exemption, divergent views were expressed depending on the category of the respondent. A vast majority of banks and banking associations were of the opinion that the list of exemptions should not be an exhaustive list, so as to leave the PSP the ability to apply exemptions based on its own transaction risk analysis. In the view of these respondents, an exhaustive list of possible exemptions or criteria to be considered by the PSPs for the transaction risk analysis may not be future proof and prevent future innovations in fraud prevention analysis.

44. By contrast, several other respondents, in particular payment initiation services providers, expressed a strong support for a clear and limited list of exemptions, in order to ensure a high level of security, transparency, a level-playing between PSPs, and to expose the payer to SCA on a regular basis, so that the application of SCA no longer creates a significant inconvenience for

[4] See http://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-the-security-of-internet-payments#

the payer. These respondents underlined the need that any exemptions to the application of strong customer authentication should equally apply to PIS and AIS, without any discrimination from the ASPSPs other than for the objective reasons provided in Articles 66 and 67 of PSD2.

45. Furthermore, in relation to the exemption for low-value payments, many respondents requested that the EBA better specify the threshold for such transactions. Finally, several respondents, and in particular Account Information Services Providers, supported an exemption for purely consultative services with no display of sensitive payment data.

46. Having assessed these responses, the EBA came to the view that, in order to ensure that all payment services offered electronically are carried out in a secure manner while ensuring user convenience and a level playing between PSPs, the draft RTS under consultation should contain a list of specific exemptions defined in Chapter 2 of the draft RTS, in which PSPs are not obliged to apply strong customer authentication.

47. In that respect, the EBA concluded that a distinction should be made between the exemptions to the application of SCA according to Article 97(1) and the exemptions to the application of SCA according to Article 97(2). Furthermore, the EBA has not been able to identify any rationale for exempting the application of security measures to protect the confidentiality and integrity of payment service users' personalised security credentials according to Article 97(3), which the RTS proposes shall therefore always be ensured, without exemption.

48. On the particular issue of exemptions for exclusively "consultative" services with no display of sensitive payment data, the draft RTS proposes to define the exemption so that PSPs are not required to apply SCA every time the user is accessing its account data, including when the user is accessing these data via an AIS provider. This exemption applies only if the two following conditions are met:

    a) the "consultative" service provided does not go beyond access to non-sensitive payment data, and

    b) ASPSPs apply strong customer authentication:

        i. for the first time the PSU accesses the information of its account online, and
        ii. when the PSU accesses the information of its payment account online, or the consolidated information on other payment accounts held, later than one month after the last day in which strong customer authentication was applied.

49. With regards to the definition of sensitive payment data, Article 4 (32) of PSD2 defines them as "data, including personalised security credentials which can be used to carry out fraud. For the activities of payment initiation service providers and account information service providers, the name of the account owner and the account number do not constitute sensitive payment data". Several respondents to the DP indicated that, given this definition, market participants may still have divergent views on what should make the list of sensitive payment data. This diversity can

probably be explained by the fact that sensitive payment data may differ from one payment instrument to another.

50. Having assessed these responses, the EBA has come to the view that, on balance of the arguments and in order to ensure technology neutrality and allow for the development of innovation, the EBA shall not further define a list of sensitive payment data falling under the scope of these RTS.

51. In relation to the exemption for point of sale electronic payment transactions, EBA acknowledges that, in order to allow the development of user-friendly and accessible means of payment for low-risk payments, an exemption for low-value contactless payments at the point of sale, whether or not they are based on mobile phone, should indeed be granted and is therefore being proposed in the draft RTS.

52. The conditions for exempting such contactless payment transactions include that the individual contactless payment transaction does not exceed 50 euros and that the cumulative amount of previous consecutive contactless electronic payment transactions below 50 euros without strong customer authentication does not exceed 150 euros. EBA decided not to extend this exemption beyond contactless payments at point of sale, so as to preserve the safe authentication of the user and the high level of security currently achieved for cards payment transactions at point of sale by the EMV Chip & Pin technology.

53. In relation to exemptions based on a transaction risk-based analysis, the EBA understands that the provision in the PSD2 requires a consistent application of SCA by all PSPs, in line with the overall objective of the PSD2 to ensure a fair competition and to safeguard against possible discrimination between PSPs. This is in compliance with Article 97(4) of PSD2, which specifies that any exemptions to the application of strong customer authentication equally apply to PIS and AIS, without any discrimination from the ASPSP other than for objective reasons as set out in Article 66(4)c and 67(3)b of PSD2.

54. In that respect, the EBA recognises there is merit in implementing a transaction risk-analysis as part of the strong customer authentication procedure proposed in Chapter 1 of the draft RTS. However, the EBA was not able to identify which minimum set of information the RTS should require for such transaction risk analysis to be sufficiently reliable to allow a specific exemption from the application of SCA, while also ensuring a fair competition among all payment service providers. Against this background, the EBA has concluded for the Consultation Paper not to propose exemptions based on a transaction-risk analysis performed by the PSP.

55. With regard to the question raised by some respondents to the DP as to whether the PSPs should always be in a position to apply strong customer authentication in case of risk of fraud, even on transactions that would meet the criteria for exemption, the EBA emphasises that this issue falls outside the scope of the mandate conferred on the EBA in Article 98 of PSD2 and that this is more to do with the interpretation of the PSD2 itself. However, the EBA understands that the EU Commission may provide further guidance to EU Member States in relation to the implementation of the PSD2 in that respect. Pending the availability of such clarification, the

EBA is seeking views from respondents to the CP as to whether the proposed list of exemptions would also be compatible with a potential scenario whereby exemptions would be mandatory for the ASPSPs, meaning that ASPSPs would be prevented from implementing SCA on transactions that meet the criteria for exemption.

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?

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?

3.2.3 Protection of the confidentiality and the integrity of the payment service users' personalised security credentials (PSCs)

56. This section of the draft RTS defines the requirements with which security measures implemented by PSPs have to comply in order to protect the confidentiality and the integrity of the payment service users' personalised security credentials (PSCs).

57. The vast majority of responses to the Discussion Paper focused their comments on the access to the PSCs by AIS and PIS providers, which is addressed by the EBA in the next section below.

58. Several respondents suggested that the EBA includes in the draft RTS specific requirements about PSU awareness programs related to the protection of PSCs, especially against social engineering attacks. Having assessed this suggestion, the EBA considers such requirements to be more suitably included in the EBA mandate under Article 95 PSD2 in relation to Guidelines on Management of Operational and Security Risks, or as part of the user-friendly electronic leaflet to be developed by the EU Commission under Article 106 PSD2, which is required to listing in a clear and easily comprehensible manner the rights of consumers.

59. In order to ensure technology and business-model neutrality, the EBA proposes a principle-based approach that requires PSPs to implement measures to protect the creation, association with payment service users, delivery, renewal and destruction of the credentials. These requirements should guarantee (a) the confidentiality, and the integrity of the enrolled personalised security credentials and (b) their delivery to, or possession by, the intended PSU.

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?

3.2.4 Common and secure open standards of communication for the purpose of identification, authentication, notification, and information

60. This section of the draft RTS defines the requirements for common and secure open standards of communication for the purpose of identification, authentication, notification, and information, as well as for the implementation of security measures, between account servicing payment service providers, payment initiation service providers, account information service providers, payers, payees and other payment service providers.

61. This section is composed of two subsections:

    a) A sub-section that defines principle-based requirements in relation to standards of communication in general. These requirements will be further complemented by the future Guidelines on Management of Operational and Security Risks that the EBA is mandated to issue under Article 95 PSD2.

    b) A second subsection that is dedicated to the requirements for common and secure open standards of communication, which focuses on the communication exchanges between AIS/PIS providers and ASPSPs, as well as for communication between PSPs in relation the confirmation on the availability of funds (Article 65).

62. The majority of answers received to the Discussion Paper on this topic focused on the communication exchanges between AISPs, PISPs, PSPs issuing card-based payment instruments providers, and ASPSPs.

63. In that respect, the responses to the DP appear to suggest that ASPSPs generally favour communication via a dedicated interface, i.e. not via the online banking interface made available to the account holder. In addition, ASPSPs are of the view that the RTS should require that such a dedicated interface is managed by a "governing entity" that would oversee the design, development and maintenance of the interface standard of communication. The same ASPSPs are of the view that such governing body should in particular determine the features of the interface, such as the verification of compliance of accessing parties with the interface access requirements, including the security requirements of the AISP/PISP/Payment service providers issuing card-based payment instruments and ASPSPs; the maximum frequency of request by AIS

providers to limit the Denial of Services; the interoperability of the interface with other interfaces; the information to be exchanged, and the minimum technical and message formats requirements.

64. In the view of ASPSPs, the main advantage of a dedicated interface is that it would be easier for competent authorities and ASPSPs to control and track the access by AIS and PIS providers. Furthermore, a common interface would facilitate the faster, easier and less costly introduction of future AIS and PIS into the market (and possible other types of services), since AISP, PISP and PSPs issuing card-based payment instruments providers would not have to discover on their own how each ASPSP's online banking platform works (a process that is required with the current access for each ASPSP a TPP wishes to connect to).

65. The responses from AIS/PIS providers, in turn, suggest that they are generally not against communication via a dedicated interface but want to remain free to access the payment account in the event that the dedicated interface is not working properly. The main concern of AIS/PIS providers in relation to an access via a dedicated interface is the availability of such dedicated interface, as they fear that APSPs do not invest enough resources to maintain these infrastructures and/or to provide technical support for access to the interface.

66. Furthermore, in the view of the AIS/PIS providers, communication compliant with the PSD2 should mainly cover requirements in relation to:

    a) Secure communication via encryption;

    b) Identification between AISP/PISP/ASPSPs, such as a valid extended certificate for mutual authentication issued by a trust provider (e.g. e-IDAS) or equivalent. However, not all responses provided by PIS/AIS providers convey this particular preference.

67. Some AIS/PIS providers indicated that this could consist, for example, of the combination of the use of HTTPS with certificates. TPPs will then have the same access as the user, even though it would be clear for the ASPSP that the account is being accessed by an AIS/PIS provider. The main advantage of this solution in the view of the PIS/AIS providers is it is a re-use of standards that already exist, and that are open and universal; the limited costs that would accrue for the banks; and that it would ensure the same level of availability and functionalities as for ASPSPs' online banking website. The main downsides in the view of the ASPSPs would be the impossibility to restrict access to specific data in compliance with data protection requirements, as AIS/PIS providers will have full access to information with no possibility to control what information is being accessed.

68. In order to fulfil the mandate conferred on EBA by PSD2, which is to specify the requirement for secure communication between the relevant actors while remaining technologically neutral, the EBA has arrived at the view that the future RTS must not prescribe the use of a specific industry standard of internet communication. Instead, EBA proposes in the draft RTS the requirements with which every communication solution used for secure communication between ASPSPs,

PISPs, AISPs, and PSPs issuing card-based payment instruments will have to comply for the provision of a payment service.

69. These requirements can be summarised as follows:

a) Each ASPSP shall offer at least one communication interface enabling secure communication with AISPs, PISPs, and PSPs issuing card-based payment instruments which shall be documented and freely available on the ASPSP's website. AISPs, PISPs, and PSPs issuing card-based payment instruments shall use this communication interface for payment initiation or any exchange of information related to the access to payment accounts under the conditions as referred to in articles 65, 66 and 67 of PSD2;

b) ASPSPs shall ensure that their communication interface allow PISP or AISP to rely on the authentication procedures provided by the ASPSP to the payment service user, in compliance with Articles 97(5), 66(3)b and 67(2)b of PSD2;

c) ASPSPs shall ensure that their communication interface uses common and open standards which are developed by international or European standardisation organisations. In particular, as suggested by several respondents to the DP, the draft RTS propose that, when transmitting payment and information messages between each other, ASPSPs, AISPs, PISPs and PSPs issuing card-based payment instruments shall use ISO 20022 elements, components or approved message definitions, if available. The EBA considered that requiring the use of ISO 20022 standards was appropriate since these standards are already widely used in the payment sector, between and within Member States, and should ensure an appropriate level of interoperability of different technological communication solutions, in line with the objective stated in Recital 93 of PSD2. The EBA discarded reference to generic internet communications standards (such as HTTP, HTTPS, TLS, and SSL) suggested by some respondents to the DP, as the EBA judged them as already of general use and too unspecific for communication standards under the mandate conferred on EBA by PSD2.

d) ASPSPs shall ensure that their communication interface is offering the same functionalities and the same level of availability, including support, as the online platform made available to the payment service user when directly initiating the payment transaction or directly accessing the information online. The EBA is indeed of the view that in order to remain technology neutral, ASPSPs should remain free to decide whether the communication interface they offer should be dedicated or not to the communication with AISPs, PISPs, and PSPs issuing card-based payment instruments. However, the EBA requires that, if the access is offered via a dedicated interface, this dedicated interface would offer the same service level as the online banking platform of the ASPSP, addressing the concerns that AIS/PIS providers have raised in their response to the DP in relation to the potential lack of availability or the

lack of resources invested by ASPSPs to maintain and/or to provide technical support for accessing such dedicated interface;

e) ASPSPs, PSPs issuing card-based payment instruments, AISPs and PISPs shall ensure that, when exchanging data via the internet, secure encryption is applied between the communicating parties throughout the respective communication session, in order to safeguard the confidentiality and the integrity of the data, using strong and widely recognised encryption techniques;

f) The data elements made available by the ASPSP shall consist of the same information as the information made available to the payment service user when directly accessing the information of a designated payment account online or when directly initiating a payment transaction. The EBA is proposing this requirement to ensure that, if the access is offered via a dedicated interface, this dedicated interface will offer the same level of data as the online banking platform of the ASPSP, addressing the concern that AIS/PIS providers have raised in their response to the DP. For PSPs issuing card-based payment instruments, the data elements made available by the ASPSP shall consist of a simple 'yes' or 'no' answer in relation to the availability of funds, as foreseen by the PSD2;

g) AIS providers shall request information from designated payment accounts and associated payment transactions each time the payment service user is requesting such information or, where the payment service user is not actively requesting such information by connecting to the AIS, no more than two times a day. The EBA is proposing this requirement to address the concern raised by some ASPSPs that AIS providers may make continuous and possibly automated account information requests, which could impact negatively the availability of the ASPSP's online platform.

70. In relation to the issue of how ASPSPs, PSPs issuing card-based payment instruments, AISPs and PISPs should identify themselves, the feedback received to the DP on the section dedicated to possible synergies with e-IDAS shows that there is a broad consensus for the use of certificates for ensuring identification between these providers. However, many respondents highlighted some potential difficulties as to the use of e-IDAS certificates, in particular due to the liability regime behind the framework that may not be compatible with the liability regime under PSD2.

71. Having assessed the responses on this particular topic, the EBA arrived at the view that further interaction with respondents was necessary so as better to identify the technical feasibility of mutual identification by certifications including the issue of interoperability of different certificate solutions. As a result, the EBA organised a workshop in April in EBA premises a subset of DP respondents representing ASPSP, AISPs and PISPs to discuss this particular issue. During the workshop, two basic approaches for mutual identification of PSPs were discussed:

a) Option 1: website certificates issued by a qualified trust service provider under an eIDAS policy, that would in particular include the name of the institution, its licensing

number, the competent authority that has delivered the license, and the services provided by the PSP (AIS, PIS, both PIS and AIS, PSPs issuing card-based payment instruments or ASPSP).

b) Option 2: website certificates issued by a general Certificate Authority, which would include the same information as above.

72. A third option, i.e. bilaterally agreed certificates, was discussed and discarded. The main advantages and disadvantages identified by participants during the workshops were as follows:

Option 1: Website certificates issued by a qualified trust service provider

73. The advantages include that qualified trust service provider issuing the website certificate would verify for a legal person the name of the legal person to whom the certificate is issued and, where applicable, the registration number as stated in the official records and would take liability in case of oversight. In addition, the certification authority is itself subject to supervision by the supervisory body designated by the relevant Member State under the eIDAS framework to ensure that it performs its verification properly.

74. On the downside, however, it is not yet clear whether any certification authority will have applied to the supervisory body designated by the relevant Member State under the eIDAS framework for the status of qualified trust service provider under eIDAS by the time of implementation of the draft RTS (i.e. October 2018 at the earliest, and certainly not by the delivery deadline of the EBA's RTS in January 2017).

Option 2: Website certificates issued by a general Certificate Authority

75. The advantages of Option 2 include that website certificates issued by a general Certificate Authority are already implemented by all PSPs for communicating with external parties.

76. The downside of Option 2 is that certification authorities do not ensure the verification of the registration number as stated in the official records. In the view of ASPSPs, this would imply that ASPSPs would be required to perform this check, resulting in additional burdensome controls and delays. In addition, even if there are a limited number of providers in EU, there will be a need to define who between the ASPSP and the third party (AISP, PISP or PSPs issuing card-based payment instruments) can decide which certificate can be accepted.

77. Against this background, workshop participants arrived at the view that option 1 should be preferred. The draft RTS submitted for consultation is therefore proposing option 1, under the assumption that there will be qualified trust service providers designated under eIDAS by October 2018. The EBA is however keen to receive the views of respondents on this particular proposal. The responses should include respondents' views on any requirements that the EBA should consider for the scenario that no qualified trust service providers were to be designated under e-IDAS by October 2018.

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?

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?

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 ?

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.

3.2.5 The implementation of the RTS

78. Several respondents to the DP asked clarification on how the draft RTS requirements will apply to third parties on which PSPs may rely for the provision of payment services.

79. By way of response, the EBA underlines that PSD2 specifies requirements applicable to Payment institutions, and by extension to PSPs according to Article 32(3) of PSD2, when relying on third parties, in particular:

    a) Article 19(6) states that "Outsourcing of important operational functions, including IT systems, shall not be undertaken in such way as to impair materially the quality of the payment institution's internal control and the ability of the competent authorities to monitor and retrace the payment institution's compliance with all of the obligations laid down in this Directive."

    b) Article 20(1) specifies that "Member States shall ensure that, where payment institutions rely on third parties for the performance of operational functions, those payment institutions take reasonable steps to ensure that the requirements of this Directive are complied with."

    c) Article 20(2) foresees that "Member States shall require that payment institutions remain fully liable for any acts of their employees, or any agent, branch or entity to which activities are outsourced.

80. Against this background, the EBA understands that this will be the responsibility of each PSP to ensure that when they rely on third parties to provide payment services, including when they outsource operational functions, they remain compliant with the requirements contained in the RTS under consultation.

81. The EBA also clarifies that all the requirements under consultation apply irrespective of the underlying obligations and organisational arrangements between account servicing payment service providers, payment initiation service providers, account information service providers, payers, payees and other payment service providers.

4. Draft regulatory technical standards on strong customer authentication and common and secure communication under PSD2 (Directive 2015/2366)

COMMISSION DELEGATED REGULATION (EU) …/..

of XXX

supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards specifying the requirements on authentication and communication

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,
Having regard to Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, and in particular Article 98(4) thereof,

Whereas:

(1) Payment services offered electronically should be carried out in a secure manner, adopting technologies able to guarantee the safe authentication of the user and to reduce, to the maximum extent possible, the risk of fraud. It is necessary to define the requirements and security features of the strong customer authentication procedure that should be applied each time a payer 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 abuse.

(2) As electronic remote payment transactions are subject to a higher risk of fraud, it is necessary to define additional requirements for the strong customer authentication applied to these transactions, ensuring in particular that the strong customer authentication is specific to the amount of the transaction and the payee agreed to by the payer when initiating the transaction.

(3) When electronic remote payment transactions do not contain a final amount of the transaction or a specific payee, it is necessary to define specific requirements ensuring that the strong customer authentication is specific to the maximum amount that the payer has given consent to be blocked.

(4) It is necessary to define the security features of the elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) for the application of strong customer authentication, as well as requirements ensuring that these elements are independent, so that the breach of one does not compromise the reliability of the others, in particular when any of these elements is used through a multi-purpose device.

(5) As as online frauds are constantly increasing in complexity and reach, the strong customer authentication procedure should be periodically tested by certified auditors.

(6) In order to allow the development of user-friendly and accessible means of payment for low-risk payments, such as low value contactless payments at the point of sale or low value remote payments, as well as access to low-risk services such as online information of payment account without disclosure of sentive payment data, it is necessary to specify the cases in which payment services providers are exempted from the application of strong customer authentication.

(7) To limit the risks relating to fraud and unauthorised access to the payment account, payment services providers should adopt measures that protect the confidentiality and integrity of personalised security credentials as well as authentication devices and software. Given the constant evolution of online frauds, it is necessary that these measures are documented, periodically tested, evaluated and audited by internal or external independent and certified auditorsSuch review should be made available to competent authorities upon their request in order to allow them to ensure enforcement of these requirements.

(8) With a view to ensure that security measures are implemented between account servicing payment service providers, payment initiation service providers, account information service providers, payers, payees and other payment service providers, it is necessary to require proper identification between communicating parties as well as traceability of payment transactions throughout the communication session.

(9) In order to ensure secure communication between the relevant actors in the context of account information, payment initiation and confirmation of availability of funds services, it is necessary to specify the requirements of common and open standards of communication to be implemented by all account servicing payment service providers that allow for the provision of online payment services.

(10) Each account servicing payment service provider should offer at least one communication interface enabling secure communication with account information services providers, payment initiation services providers, and payment services providers issuing card-based payment instruments, which should be documented and freely available on the account servicing payment service provider’s website. This communication interface should allow account information services providers and payment initiation services providers to rely on the authentication procedures

provided by the account servicing payment service provider to the payment service user.

(11) In order to ensure a secure communication for the provision of their services, account information services providers, payment initiation services providers and payment services providers issuing card-based payment instruments should use this communication interface for payment initiation or any exchange of information related to the access to payment accounts.

(12) To ensure the interoperability of different technological communication solutions, is is appropriate to require that account servicing payment service provider's communication interface uses common and open standards which are developed by international or European standardisation organisations as well as ISO 20022 elements, components or approved message definitions, if available, since these standards are already widely used in the payment sector, between and within Member States.

(13) To ensure technology and business-model neutrality, account servicing payment service provider should remain free to decide whether the communication interface they offer should be dedicated or not to the communication with account information services providers, payment initiation services providers, and payment services providers issuing card-based payment instruments. However, to ensure the availability and sufficient technical support for accessing the account servicing payment service provider's communication interface, these requirements specify that if the access is offered via a dedicated interface, this dedicated interface would offer the same service level as the online banking platform of the account servicing payment service provider and should offer a testing facility.

(14) To limit the risks relating to phishing and other fraudulent activities, it is appropriate to ensure that the account servicing payment service provider is aware that he is being contacted by a payment initiation service provider or an account information service provider and not by the client itself.

(15) In order to safeguard the confidentiality and the integrity of the data, it is necessary to ensure the security of communication session between account servicing payment service provider, account information services providers, payment initiation services providers and payment services providers issuing card-based payment instruments. Against this background, it is in particular necessary to require that secure encryption is applied between account information services providers, payment initiation services providers, payment services providers issuing card-based payment instruments and account servicing payment service provider when exchanging data via the internet.

(16) To set out the conditions under which payment initiation service providers and account information service providers can provide their services with the consent of the account holder, it is appropriate to define the data elements to be exchanged between the account servicing payment service providers, account information services providers, payment initiation services providers and payment services providers issuing card-based payment instruments.

(17) This Regulation is based on the draft regulatory technical standards submitted by the European Banking Authority (EBA) to the Commission.

(18) EBA has conducted open public consultations on the draft regulatory technical standards on which this Regulation is based, analysed the potential related costs and benefits and requested the opinion of the banking Stakeholder Group established in accordance with Article 37 of Regulation (EU)) No 1093/2010.

HAS ADOPTED THIS REGULATION:

CHAPTER 1
STRONG CUSTOMER AUTHENTICATION

Article 1
Authentication procedure and authentication code

1. For the purposes of the application of strong customer authentication in accordance with Article 97(1) of Directive (EU) 2015/2366, 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.

2. The authentication code shall be characterized by security features including, but not limited to, algorithm specifications, length, information entropy and expiration time, ensuring that:
   (a) no information on any of the elements of strong customer authentication categorized as knowledge, possession and inherence can be derived from the disclosure of the authentication code;
   (b) it is not possible to generate a new authentication code based on the knowledge of another authentication code generated for the same payer;
   (c) the authentication code cannot be forged.

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) 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;
   (c) determine the maximum number of failed authentication attempts that can take place consecutively within a given period of time and after which the access to an online payment account, the initiation of an electronic payment transaction or the possibility of carrying out any action through a remote channel which may imply a risk of payment fraud or other abuse are temporarily or permanently blocked. Where the block is temporary the number of retries and the time period of the block shall be established taking into account the characteristics of the service provided to the payer and all the relevant risks involved. Where the block is permanent, a secured procedure must be established allowing the payer to regain access to and use the blocked electronic payment services;

(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 HTTP over TLS.

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

i. parameterised rules, including black lists of compromised or stolen card data,
ii. signs of malware infection in the session and known fraud scenarios,
iii. an adequate transaction history of the payer to evaluate its typical spending behavioral patterns,
iv. information about the customer device used,
v. a detailed risk profile of the payer and/or the payer's device,

Article 2

Strong customer authentication procedure with dynamic linking

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 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.

2. For the purposes of paragraph 1, the authentication procedure shall have in place technological solutions ensuring:

(a) the confidentiality, authenticity and integrity of the amount of the transaction and of the payee through all phases of the authentication procedure. Any change to the amount or payee shall result in a change of the authentication code;

(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 be independent or segregated from the channel, device or mobile application used for initiating the electronic payment transaction.

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 Article

75(1) of that Directive, 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 agreed to by the payer when initiating the transaction.

4. For the purposes of the application of strong customer authentication in accordance with Article 97(2) of Directive (EU) 2015/2366 for which the payer has given consent to execute a batch of remote electronic payments to several payees, the authentication code generated in accordance with Article 1 shall be specific to the total amount of the batched electronic payment transactions and to the payees of the batch of transactions considered collectively.

Article 3
Requirements related to elements categorised as knowledge

1. The elements of strong customer authentication categorised as knowledge shall be characterized by security features including, 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.
2. The use of elements of strong customer authentication categorised as knowledge shall be subject to mitigation measures in order to prevent their disclosure to unauthorised parties.

Article 4
Requirements related to elements categorised as possession

1. The elements of strong customer authentication categorised as possession shall be characterised by security features including, but not limited to, algorithm specifications, key length and information entropy ensuring resistance against the risk of the elements being used by, or disclosed to, unauthorised parties.
2. The use of elements categorized as possession shall be subject to measures designed to prevent replication of the elements, including in particular anti-cloning features to offer resistance against the risks of forging and cloning of the elements.

Article 5
Requirements related to devices and software to read authentication elements categorised as inherence

1. Devices and software provided to the payer in order to read authentication elements categorized as inherence shall be characterized by security features including, but not limited to, algorithm specifications, biometric sensor and template protection features ensuring resistance against the risk of sensitive information related to the elements being disclosed to unauthorised parties. These security features shall also guarantee a sufficiently low likelihood of an unauthorised party being authenticated as the legitimate payment service user.

2. The use of elements categorized as inherence shall be subject to measures ensuring that the devices and the software provided to the payer guarantee resistance against unauthorised use of the elements through access to the devices and software.

Article 6
Requirements related to the independence of the elements

1. The use of the elements of strong customer authentication referred to in Article 3, 4 and 5 shall be subject to procedures in terms of the technology, algorithms and parameters, ensuring that the breach of one of the elements does not compromise the reliability of the other elements.
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 risk of the multi-purpose device being compromised.
3. For the purposes of paragraph 2, the mitigating measures shall include, but not be limited to:
    a. the implementation of separated trusted execution environments 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.

Article 7
Review of the strong customer authentication procedure

1. The overall security of the strong customer authentication procedure shall be periodically tested, evaluated and audited by internal or external independent and certified auditors. The periodicity of these audits shall be defined according to the relevant audit framework of the payment services provider.
2. The review referred to in paragraph 1 shall be provided in the form of a report ensuring that the strong customer authentication procedure encompasses measures to comply with this Regulation.
3. The report referred to in paragraph 2 shall be made fully available to competent authorities upon their request.

CHAPTER 2
EXEMPTIONS FROM STRONG CUSTOMER AUTHENTICATION

Article 8
Exemptions to strong customer authentication

1. The application of strong customer authentication in accordance with Article 97(1) 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.

   The application of strong customer authentication shall not be exempted where:

   i. the payer accesses the information of its payment account online, or the consolidated information on other payment accounts held, for the first time,

   ii. the payer accesses the information of its payment account online, or the consolidated information on other payment accounts held, later than one month after the last day in which strong customer authentication was applied.

   (b) the payer initiates a 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 previous non-remote electronic payment transactions initiated via the payment instrument offering a contactless functionality without application of strong customer authentication does not exceed 150 EUR.

2. The application of strong customer authentication in accordance with Article 97(2) of Directive (EU) 2015/ 2366 is exempted where:

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

   The application of strong customer authentication shall not be exempted where the payer creates for the first time or subsequently amends the list of trusted beneficiaries 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.

The application of strong customer authentication shall not be exempted where the payer initiates the series of credit transfers for the first time or amends the series of credit transfers.

(c) the payer initiates online a credit transfer where the payer and the payee are the same natural or legal person and the payee's payment account is held by the payer's account servicing payment services provider;

(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 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 100 EUR.

CHAPTER 3

PROTECTION OF THE CONFIDENTIALITY AND INTEGRITY OF THE PAYMENT SERVICE USERS' PERSONALISED SECURITY CREDENTIALS

Article 9
Requirements for security measures

1. The confidentiality and integrity of personalised security credentials of the payment service user shall be ensured during all phases of the authentication procedure including display, transmission and storage. To that end, the security measures to protect the confidentiality and integrity of payment service users' personalised security credentials shall provide that:

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

   (b) Personalised security credentials data as well as cryptographic material related to the encryption of the personalised security credentials are not stored in plain text.

   (c) Secret cryptographic material related to the encryption of the credentials is stored in secure and tamper resistant devices and environments.

2. The process related to the management of cryptographic material used to encrypt or otherwise render unreadable the personalised security credentials shall be fully documented within the authentication procedure.

Article 10
Security measures for transactions initiated by or through a payee in the context of a card-based payment transaction

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 personalised security credentials.

Article 11
Creation of personalised security credentials

The security measures to protect the confidentiality and integrity of payment service users' personalised security credentials shall ensure the effective and secure creation of such personalised security credentials. To that end, these security measures shall provide that the risks of unauthorised use of the personalised security credentials and of the authentication devices and software due to their loss, theft or copying before their delivery to the payer are effectively addressed.

Article 12
Association of the payer with personalised security credentials, authentication devices and software

The security measures to protect the confidentiality and integrity of payment service users' personalised security credentials shall ensure that the payer is exclusively associated with the personalised security credentials, with the authentication devices and software in a secure manner. To this end these security measures shall ensure that:

(a) The association of payment services user's identity with personalised security credentials, authentication devices and software is carried out in environments where an adequate authentication of the customer and of the PSP offering the service is assured. Against this background, the association shall be carried out in environments under the payment services provider's responsibility and taking into account risks associated with devices and underlying components used during the association process that are not under the responsibility of the payment services provider. The environments under the payment services provider's responsibility include, but are not limited to the payment services provider's premises, the internet environment provided by the payment services provider or in other similar secure websites, automated teller machine (ATM) services;

(b) the association via a remote channel of the payment services user's identity with the personalised security credentials, with a payment instrument and with authentication devices or software shall be performed using the strong customer authentication procedure.

Article 13
Delivery of personalised security credentials, authentication devices and software

The security measures to protect the confidentiality and integrity of payment service users' personalised security credentials shall provide that the delivery of personalised security credentials, authentication devices and software to the payment services user is carried out in a secure manner to address the risks related to their unauthorised use due to their loss, theft or copying. To this end, these measures shall include:

(a) Effective and secure delivery mechanisms ensuring that the personalised security credentials, authentication devices and software are delivered to the legitimate payment services user associated with the credentials, the authentication devices and the software provided by the payment services provider;

(b) Mechanisms ensuring that the authentication software delivered to the payment services user via the internet has been digitally signed by the payment services provider;

(c) Arrangements ensuring that, where the delivery of personalised security credentials is executed outside the premises of the payment services provider or through a remote channel:

   i. No unauthorised party can obtain more than one feature of the personalised security credentials, the authentication devices or software when delivered through the same channel

   ii. The delivered personalised security credentials, authentication devices or software require activation before usage;

(d) Arrangements ensuring that, in cases where the personalised security credentials, the authentication devices or software require to be activated before their use, the activation shall take place in a secure and trusted environment in accordance with the association procedures referred to in Article 12.

Article 14
Renewal of personalised security credentials

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

Article 15
Destruction, deactivation and revocation of personalised security credentials, authentication devices and software

The security measures to protect the confidentiality and integrity of payment service users' personalised security credentials shall establish dedicated processes ensuring:

(a) the secure destruction, deactivation or revocation of the personalised security credentials, authentication devices and software;

(b) In case of reusable authentication devices and software distributed by the payment services provider, the secure re-use of such a component is established, documented and implemented before making it available to another payment services user;

(c) the deactivation or revocation of information related to personalised security credentials stored in the payment services provider's systems and databases and, where relevant, in public repositories.

Article 16
Review of the security measures to protect the confidentiality and integrity of payment service users' personalised security credentials

1. The overall security of measures to protect the confidentiality and integrity of payment service users' personalised security credentials, as referred to in articles 9 to 15, shall be documented, periodically tested, evaluated and audited by internal or external independent and certified auditors. The periodicity of these audits shall be defined according to the applicable audit framework of the PSPs.

2. The review referred to in paragraph 1 shall be provided in the form of a report ensuring that the security measures to protect the confidentiality and integrity of payment service users' personalised security credentials encompass measures to comply with this Regulation.

3. The report referred to in paragraph 2 shall be made fully available to competent authorities upon their request.

CHAPTER 4

COMMON AND SECURE OPEN STANDARDS OF COMMUNICATION

Section 1

General requirements for communication

Article 17
Requirements for identification

1. Payment services providers shall ensure secure bilateral identification when communicating between the payer's device and the payee's acceptance devices for electronic payments, including but not limited to payment terminals.

2. Payment services providers shall ensure that mobile applications and other payment services users interfaces offering electronic payment services are protected against misdirection of communication to unauthorised third parties.

Article 18
Traceability

Payment services providers shall have processes in place ensuring that all payment transactions and other interactions with the payment services user, with other payment services providers and with merchants in the context of the provision of the payment service are traceable, ensuring knowledge ex-post of all events relevant to the electronic transaction in all the various stages. In particular payment services providers shall ensure that any communication session established with the payment services user, other payment services providers and other entities including, but not limited to, merchants, relies on:

(a) a unique identifier of the session allowing the identification of the communicating parties.

(b) security mechanisms for the detailed logging of the transaction, including transaction number, timestamps and all relevant transaction data.

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

Section 2: Specific requirements for the common and secure open standards of communication

Article 19
Communication interface

1. Account servicing payment service providers that are offering to a payer a payment account that is accessible online shall offer at least one communication interface enabling :

   (a) Account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments to identify themselves towards the account servicing payment service provider.;

   (b) Account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments to securely communicate with the account servicing payment service provider for requesting payment account information, initiating payments from the payer's payment account and receiving confirmation whether an amount necessary for the execution of a card-based payment transaction is available on the payment account of the payer;

   (c) Account information service providers and payment initiation service providers to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user.

2. For the purposes of authentication of the payment service user, the communication interface provided by the account servicing payment service provider shall allow account information service providers and payment initiation service providers to rely on the authentication procedures of the account servicing payment service provider. In particular the interface shall:

   (a) Enable a payment initiation service provider or an account information service provider to instruct the account servicing payment service provider to start the authentication procedure;

   (b) Enable the establishment and maintenance of communication sessions between the account servicing payment service provider, the account information service provider, the payment initiation service provider and the payment services user throughout the authentication procedures;

   (c) Ensure the protection of the integrity and confidentiality of the personalised security credentials and of the authentication codes when these are transmitted by the payment initiation service provider or the account information service provider.

3. Account servicing payment service providers shall ensure that their communication interface uses ISO 20022 elements, components or approved message definitions, if available, as well as standards of communication which are developed by international or European standardisation organisations.

4. Account servicing payment service providers shall make sure that the technical specification of their communication interface is documented, the documentation made available for free and publicly on their website. This documentation shall specify a set of routines, protocols, and tools needed by payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments for allowing their software and applications to interoperate with the systems of the account servicing payment service providers.

5. Except for legitimate emergency situations, account servicing payment service providers shall make sure that any change to the technical specification of their communication interface is made publicly available in advance as soon as possible and, except in emergency situations, not less than 3 months before the change is implemented. Payment service providers shall document legitimate emergency situations where changes were implemented and make them available to competent authorities on request.

6. Account servicing payment service providers shall ensure that their communication interface is operating on the same level of service, including support, as the online platform made available to the payment service user when directly accessing its accounts online. Account servicing payment service providers shall monitor the availability of this communication interface and make such statistics available on demand to the competent authorities.

7. Account servicing payment service providers shall make available a testing facility, including support, for connection and functional testing by providers to test their software and applications before starting to be used for offering payment services to users.

Article 20
Identification

1. For the purpose of identification, payment service providers shall rely on Qualified certificates for website authentication as per article 3(39) of Regulation (EU) No 910/2014.

2. For the purpose of this Regulation, the registration number as stated in the official records according to in Annex IV (C) of Regulation (EU) No 910/2014 shall be the authorization number of the account servicing payment service provider or the payment service provider issuing card-based payment instruments, and the account information service providers and payment initiation service providers available in the public register of the home Member State defined in Article 14 of Directive (EU) 2015/2366.

3. For the purposes of this Regulation, qualified certificates for website authentication shall include additional specific attributes in relation to :

   (a) the role of the payment service provider , which can be account servicing payment service provider, payment initiation service provider, account information service provider or payment service provider issuing card-based payment instruments, .

   (b) the name of the competent authorities where the payment service provider is registered.

4. The attributes referred to in paragraph 3 shall not affect the interoperability and recognition of qualified certificates for website authentication.

Article 21
Security of communication session

1. Account servicing payment service providers, payment services providers issuing card-based payment instruments, account information service providers and payment initiation service providers shall ensure that when exchanging data via the internet, secure encryption is applied between the communicating parties throughout the respective communication session in order to safeguard the confidentiality and the integrity of the data, using strong and widely recognised encryption techniques.

2. Payment service providers issuing card-based payment instruments, account information service providers and payment initiation service providers shall keep the sessions for payments or related services as short as possible and actively terminate the session with the account servicing payment service provider as soon as the requested action has been completed.

3. When maintaining parallel network sessions with the account servicing payment service provider, account information service providers and payment initiation service providers shall ensure that those sessions are securely linked to relevant sessions established with the payment service user, so that the communication sessions between the account servicing payment service provider, the account information service provider, the payment initiation service provider and the payment service user are maintained consistently in order to prevent that any message or information communicated between them could be misrouted.

4. Information messages exchanged by account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments with the account servicing payment service provider should contain unambiguous reference to :

   (a) the payment service user and the corresponding communication session in order to distinguish several requests from the same payment service user,

   (b) for payment initiation services, the uniquely identified payment transaction initiated,

(c) for confirmation on the availability of funds, the uniquely identified request related to the amount necessary for the execution of the card-based payment transaction.

5. Account information service providers and payment initiation service providers shall make sure that when transmitting personalised security credentials and authentication codes, these are not accessible to any of their staff at any time. In case of loss of confidentiality of personalised security credentials under their sphere of competence, account information service providers and payment initiation service providers have to inform the payment services user associated with and the issuer of the personalised security credentials without undue delay.

6. Account information service providers and payment initiation service providers shall ensure that the processing and routing of personalised security credentials and authentication codes take place in secure environments in accordance with common security standards in compliance with ISO 27001.

Article 22
Data exchanges

1. Account servicing payment service providers shall provide:

(a) Account information service providers with the same information from designated payment accounts and associated payment transactions made available to the payment service user when directly accessing the information online, provided that this information does not include display of sensitive payment data;

(b) Payment initiation service providers with the same information on the initiation and execution of the payment transaction made available to the payment service user when directly initiating the payment transaction,

(c) Payment service providers issuing card-based payment instruments providers with a confirmation of whether the amount necessary for the execution of a card based payment transaction is available on the payment account of the payer. This confirmation shall consist of a simple ‘yes’ or ‘no’ answer.

2. In case of an unexpected event or error occurring during the process of identification, authentication, or the exchange of the data elements, the account servicing payment service provider shall send a notification message to the account information service provider, the payment initiation service provider or the payment services provider issuing card-based payment instruments which explains the reason for the unexpected event or error.

3. Account information service providers shall have in place suitable and effective mechanism to limit the request of information to both designated payment accounts and associated payment transactions, in accordance with the user's explicit consent;

4. Payment initiation service providers shall provide account servicing payment service providers with the same information requested from the payment service user when directly initiating the payment transaction.

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.

CHAPTER 5
FINAL PROVISIONS

Article 23
Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the Commission
The President

[For the Commission
On behalf of the President

[Position]

5. Accompanying documents

5.1 Draft cost-benefit analysis / impact assessment

Article 10(1) of the EBA Regulation provides that when any regulatory technical standards developed by the EBA are submitted to the Commission for adoption, they should be accompanied by an analysis of 'the potential related costs and benefits'. This analysis should provide an overview of the findings regarding the problem to be dealt with, the solutions proposed and the potential impact of these options.'

A. Problem identification

With technical developments and changes in consumer behaviour, economies are becoming more digital and commerce more electronic, including the means of payment. In the Internal Market, the provision of payment services is still rather fragmented along national borders, hampering also the cross-border purchase of goods and services by European consumers. Besides this imperfect competition between payment service providers in Europe, the retail payments market has been found to be lacking an effective, transparent and secure governance framework, to the detriment of consumers. [5]

In particular in the context of remote transactions, e.g. when initiating an online payment or payment via a mobile device, the identification of the payer becomes more challenging and the risk of fraud or theft of confidential information increases significantly[6]. Surveys and statistics show that, in terms of both transactions and value, fraud in the area of retail payments, in particular for remote ("card not present", CNP) transactions[7], has increased significantly in recent years. Also, one out of four European consumers indicate a subdued level of confidence regarding the security of their payment card details when shopping online[8]. Those observations pose a barrier for the European digital economy to flourish.

[5] COM: Green paper on retail financial services (2015), COM: Towards an integrated European market for card, internet and mobile payments (2012).

[6] EBA: Consumer trends report 2016, EBA: Discussion Paper on strong customer authentication and secure communication (2015).

[7] ECB: Fourth report on card fraud (2015)

[8] GfK: Identifying the main cross-border obstacles to the Digital Single Market – final report on behalf of the European Commission (2015)

B. Policy objectives

These draft RTS aim to contribute to the development of the Digital Single Market and fostering of the EU Internal Market more generally[9]. They are developed with a view to increasing the efficiency of financial services and the protection of consumers in the EU[10].

PSD2 provides that these draft RTS shall be developed by EBA in accordance with the following specific objectives:

a) ensuring an appropriate level of security for PSUs and PSPs, through the adoption of effective and risk-based requirements;

b) ensuring the safety of PSUs' funds and personal data;

c) securing and maintaining fair competition among all PSPs;

d) ensuring technology and business-model neutrality; and

e) allowing for the development of user-friendly, accessible and innovative means of payment.

C. Baseline scenario

Payment statistics show a continuous increase in the use of electronic payment instruments in the EU over the last couple of years[11]. With the dynamic technological innovation and the increased usage of mobile and other electronic devices and online channels by European consumers, the risk of detriment and fraud (involving also the stealing or manipulation of confidential customer information) is expected to increase significantly, with possible breakdowns of confidence in case adverse scenarios become material at a larger scale / more frequently.

Competitive distortions and commercial incentives of providers in the European payment service market render it very unlikely for adequate industry solutions to be found to the problems described above. The need for a secure and consumer-oriented regulatory framework, which at the same time facilitates innovation and competition, is expected to increase under the scenario described above. The previous legal framework, consisting basically of the previous Payment Services Directive, is assessed to be insufficient to address the risks and problems identified. This is in particular owed to the innovative dynamic of the market for retail payment services in Europe with new payment solutions introduced continuously, while the existing legal framework by nature focuses on types of payment services formerly known (such as credit transfers, direct debits ans card payments at the physical point of sale). To fill this gap, the EBA decided to address

[9] COM President (2014), *Political Guidelines for the next European Commission*

[10] EBA (2016), *Annual Report 2015*; EBA (2015), *EBA 2016-2018 Multi-annual work programme*

[11] ECB

the security of internet payments which are comprehensively covered by the EBA's Guidelines on the Security of Internet Payments (EBA GL/2014/12)). The PSD2 has mandated the EBA to develop these RTS on authentication and communication between service providers. The existing legal framework, including the EBA guidelines, remains in force until adoption and entering into force of these RTS.

D. Options considered

1. Developing these draft RTS, the EBA has considered a set of technical options, related to Strong customer authentication

   - Develop principle-based requirements for the authentication of a payment service user (Option 1.1)

   - Develop detailed requirements prescribing the concrete authentication procedure (Option 1.2)

2. Scope of exemptions

   - Develop an exhaustive list of scenarios and criteria which would prescribe exemptions (Option 2.1)

   - Develop a non-exhaustive list of scenarios and criteria for exemptions, allowing PSP to apply additional exemptions based on the PSP's own transaction risk analysis (Option 2.2)

3. Protection of the personalised security credentials

   - Develop principle-based requirements for protecting the integrity and confidentiality of PSC (Option 3.1)

   - Develop detailed requirements for the protection of PSC integrity and confidentiality (Option 3.2)

4. Communication between ASPSP, PISP, AISP, payers, payees and other payment service providers

   - Specify a technical solution for the access to payment account (account information services, payment initiation services and confirmation of availability of funds) (Option 4.1.1)

   - Develop principle-based requirements for the access to payment account (Option 4.1.2)

   - Require identification via certificate by eIDAS qualified trust service provider (Option 4.2.1)

   - Allow identification via certificate issued by General Certificate Authority (Option 4.2.2)

E. Assessment and preferred options[12]

The requirements in these draft RTS affect a broad range of stakeholders, such as providers in the payment service market (ASPSP, AISP, PISP, other payment service providers) including credit institutions, e-money institutions and companies active in the area of financial technology, consumers (payers) and other businesses (payees) in the EU. In addition, supervisory authorities and central banks are affected in their respective functions with regard to safety and efficiency of payment systems, monetary policy, banking system stability and consumer protection.

For each of those stakeholders, the requirements contained in these RTS might potentially be associated with incremental costs and benefits, one-off as well as recurring, direct and more indirect / long-term effects. Given the broad range and diverse interests of the stakeholders possibly concerned, the below summary assesses the overall contribution of the requirements contained in these RTS to the objectives specified in PSD2 and other relevant references, in particular regarding the fostering of competition and innovation in the payment services market while at the same time facilitating sufficient protection of consumers in the EU.

Regarding the first consideration, strong customer authentication, the EBA has assessed whether to provide principle-based or more prescriptive requirements. While more detailed requirements could in a stable and mature market sufficiently protect consumers, in such a dynamic segment like the provision of new payments solutions in Europe, authentication requirements should be developed in the form of high-level principles, to facilitate adaptability to emerging security threats and implementation of innovative security solutions. With authentication solutions being developed by the payment service providers (option 1.1), it can also be reasonably expected that consumer convenience is intrinsically taken care of.

Regarding the second consideration, the scope of exemptions, the EBA has duly considered to ensure safety of PSU's funds and fair competition between PSP. Against this background, reliance on PSP transaction risk analysis as a criteria for exempting the application of SCA would likely not sufficiently protect consumers and – absent any reliable criteria for the validation of its results – possibly harm fair competition in the payment service market.

The EBA therefore proposes a harmonised solution (option 2.1) which specifies a list of conditions to apply exemptions from strong customer authentication.

Regarding the third consideration, the protection of confidentiality and integrity of personalised security credentials, the EBA has evaluated whether to provide extensive and prescriptive requirements or to develop a set of high-level principle-based requirements. To facilitate competition and adaptability, these requirements propose a principle-based approach for

[12] As a background, see also COM: Impact assessment accompanying proposal for payment services directive and interchange fees regulation (2013); London economics et al: Study on the impact of the payment services directive on the internal market and on cross-border payments in the Community (2011)

protecting confidentiality and integrity in the creation, association with payment service users, deliver, renewal and destruction of personalised security credentials (option 3.1). Also against the background of the mandates given to the EBA under PSD2 Art. 95 (Development of Guidelines on Management of Operational and Security Risks) and to the COM under Art. 106 (Development of an electronic leaflet), these draft RTS focus on requirements strictly necessary in the context of customer authentication, to avoid risk of regulatory overlaps.

Regarding the fourth consideration, common and secure open standards of communication between relevant parties in the context of payment services, the EBA has assessed whether to develop principles for the access to payment account or to specify a single technical solution. While giving preference to a specific technical solution would counter the objective of promoting competition and innovation, the different interests and incentives of market participants (ASPSP, AISP, PISP) render it necessary for EBA to give sufficiently concrete guidance for the communication between stakeholders involved in the payment service market (option 4.1.2).

It should also be noted, that the PSD2 foresees that, once the Commission has adopted the EBA's RTS, market participants have another 18 months until the RTS applies. As a result, and depending on the speed by which the EBA's RTS is adopted, the RTS will apply from October 2018 onwards at the very earliest. In the time between, the industry will have to develop standards and/or technological solutions that will be compliant with the EBA's RTS. The EBA will assess in close cooperation with the ECB how best this process can be facilitated to ensure that the objectives of the PSD2 can be achieved.

In addition, technical choices need to be made regarding the identification of ASPSP, PSP, AISP and PISP when communicating. That identification could either be conducted based on certificates issued by a qualified trust service provider under eIDAS or based on certificates issued by a general certificate authority. To maximise efficiency and verifiability of the identification requirement, the EBA proposes reliance on certificates used by a provider as stipulated in the eIDAS framework (option 4.2.1), acknowledging that no such provider has applied and been designated so far.

Overall, the requirements contained in these draft RTS are expected to contribute significantly to increased competition, cross-border activities and efficiency in the market for retail payment services while at the same time sufficiently protecting consumers. In particular, the sufficient protection against fraud and theft of confidential customer information has been carefully considered in the development of these draft RTS. Its overall impact is expected to be net beneficial for providers, consumers and businesses.

5.2 Overview of questions for consultation

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?

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.

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?

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?

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?

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?

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?

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?

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 ?

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.