EBA/DP/2015/03

8 December 2015

Discussion Paper

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

Contents

1. Responding to this Discussion Paper 3

2. Executive Summary 4

3. Background and rationale 5

Background 5

Rationale 7

4. Discussion 11

4.1 Considerations prior to developing the requirements on strong customer authentication 11

4.2 The exemptions to the application of strong customer authentication 15

4.3 The protection of the payment service users' personalised security credentials 18

4.4 Considerations prior to developing the requirements on common and secure open standards of communication 21

4.5 Possible synergies with the regulation on electronic identification and trust services for electronic transactions in the internal market (e-IDAS) 26

Annex - Summary of questions 29

1. Responding to this Discussion Paper

The EBA invites comments on all proposals put forward in this paper and in particular on the specific questions stated in the boxes below (and in the Annex of this paper).

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 view expressed;
- describe any alternatives the EBA should consider; and
- provide where possible data for a cost and benefit analysis.

Submission of responses

To submit your comments, click on the 'send your comments' button on the consultation page by 08.02.2016. 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.

Disclaimer

The views expressed in this discussion paper are preliminary and will not bind in any way the EBA in the future development of the draft Regulatory Technical Standards. They are aimed at eliciting discussion and gathering the stakeholders' opinion at an early stage of the process.

2. Executive Summary

Reasons for publication

The European Banking Authority (EBA) was established in 2011 with the objective of protecting the public interest by contributing to the short, medium and long-term stability and effectiveness of the financial system, for the Union economy, its citizens and businesses.

One of the many areas in which the EBA has more recently been pursuing these objectives is the market for payment services. Establishing a single and efficient market for payments is essential to enabling consumers, retailers and other market participants to enjoy the full benefits of the EU internal market and to stimulate overall economic growth, consumption and trade. The year 2015 has then seen a further step up for the role of the EBA in the regulation of this area, including through the revised Payment Services Directive (PSD2), which is due to enter into force at the beginning of 2016 and is expected to confer on the EBA the mandate to develop six Technical Standards and five sets of Guidelines.

One particular Technical Standard, on strong customer authentication and secure communication, is key to achieving the objective of the PSD2 of enhancing consumer protection, promoting innovation and improving the security of payment services across the European Union. The EBA will be developing this mandate in close cooperation with the European Central Bank.

Prior to the publication of the consultation paper with the draft technical standards, which is currently foreseen for the second quarter of 2016, the EBA and ECB have decided to issue a discussion paper, so as to benefit from input by market participants on a number of issues that are key to the development of the technical standard. The EBA invites respondents to share their views on the identified issues and on the potential clarifications suggested.

Contents

The discussion paper invites views on issues related to strong customer authentication; the exemptions to the application of strong customer authentication; the protection of the personalised security credentials of the payment service users; the requirements for common and secure open standards of communication; and possible synergies with e-IDAs Regulation on electronic identities.

Next steps

The period to provide responses to this discussion paper will run from 8 December 2015 to 8 February 2016. The publication of the subsequent consultation paper with the draft technical standard is foreseen for the second quarter of 2016.

3. Background and rationale

Background

1. The European Banking Authority (EBA) was established in 2011 with the objective of protecting the public interest by contributing to the short, medium and long-term stability and effectiveness of the financial system, for the Union economy, its citizens and businesses.[1] According to its founding regulation, the EBA is to pursue this objective by contributing to

    - improving the functioning of the internal market, including, in particular, a sound, effective and consistent level of regulation and supervision;

    - ensuring the integrity, transparency, efficiency and orderly functioning of financial markets;

    - strengthening international supervisory coordination;

    - preventing regulatory arbitrage and promoting equal conditions of competition;

    - ensuring the taking of credit and other risks are appropriately regulated and supervised; and

    - enhancing customer protection.

2. In addition, the EBA is mandated to monitor new and existing financial activities and adopt guidelines and recommendations,[2] with a view to

    - promoting the safety and soundness of markets and convergence of regulatory practice,

    - achieving a coordinated approach to the regulatory and supervisory treatment of new or innovative financial activities, and

    - ensuring that market participants engaging with innovations can have confidence in doing so.

3. One of the many areas in which the EBA has more recently been pursuing these objectives is the market for payment services. Establishing a single and efficient market for payments is essential to enabling consumers, retailers and other market participants to enjoy the full

[1] See Article 1(5) of the EBA's founding regulation at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32010R1093

[2] Ibid, Article 9

benefits of the EU internal market and to stimulate overall economic growth, consumption and trade.

4. In fulfilment of its innovation mandate, for example, the EBA issued, in July 2014, an *Opinion on Virtual Currencies*, setting out a short term and long term regulatory approach towards this particular innovation.[3] And in December that same year the EBA published final *Guidelines on the Security of Internet Payments*, which are aimed at promoting the safety of markets, protecting consumers, and contributing to an effective and consistent level of regulation.[4]

5. The year 2015 has then seen a further step up for the role of the EBA in the regulation of payments across the EU, with several EU Directives and Regulations conferring mandates on the EBA. This includes:

   - the Regulation on Interchanges Fees for Card-based Transactions (IFR), which requires the EBA to develop draft Regulatory Technical Standards (RTS) to define how to separate payment card schemes and processing entities so that they are independent from one another, and

   - the revised and pending Payment Services Directive (PSD2), which is expected to enter into force in January 2016 and expected to confer on the EBA the development of six Technical Standards and five sets of Guidelines.

6. With regard to the PSD2, the EBA will have to develop some of the mandates within 12 months of entry into force of the Directive (which is estimated to occur in January 2016), while others are due within 18 or 24 months.

7. In terms of interaction with stakeholders, the EBA will develop these mandates in the same way as it has done for the other 100+ Technical Standards and 30+ Guidelines it has issued since its inception in 2011.[5] Half way through the development process, the EBA will publish a Consultation Paper (CP) with *draft* requirements, and will usually do so for a period of 3 months. The EBA takes the responses to these consultations seriously, assesses them thoroughly and therefore provides, when later publishing the *final* requirements, an extensive feedback statement, or 'Final Report', that sets out whether or not, and if so how and why, the consultation responses have or have not resulted in changes between the draft and the final requirements.

[3] See http://www.eba.europa.eu/-/eba-proposes-potential-regulatory-regime-for-virtual-currencies-but-also-advises-that-financial-institutions-should-not-buy-hold-or-sell-them-whilst-n

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

[5] In addition, the EBA has also published during that period 20+ Opinions, 60+ Reports, and more than a dozen other deliverables. For details, see http://www.eba.europa.eu/regulation-and-policy. For the period 2015-17, and across all the EU Directives and Regulations that fall into its remit, the EBA will develop another 50+ technical standards and 55+ sets of Guidelines.

8. Depending on the nature of the topic, the EBA may additionally invite stakeholders to a Public Hearing during the consultation period, with a view to answer questions that will allow stakeholders better to devise their pending responses. The date for any Public Hearing will be published on the EBA website at the moment when the related Consultation Paper is published.

9. Depending on the complexity of the mandate at hand, the EBA may also decide to seek additional input from stakeholders already at the beginning of the policy development process. It may do so by requesting input bilaterally from particular firms, trade associations or other stakeholders, or it may issue a Discussion Paper (DP).

10. Unlike a Consultation Paper, a DP does not suggest any specific regulatory solutions. Instead, it identifies and characterizes the problems or issues that the 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. A DP is usually chosen if the audience from which input is sought is so wide and heterogeneous that more targeted forms of interaction, such as bilateral meetings or workshops, would not allow the EBA to obtain the breadth of views required. The approach summarized above will be followed for all Technical Standards and Guidelines that are conferred on the EBA in the PSD2.

11. One particular Technical Standard, on strong customer authentication and secure communication provided in Article 98 PSD2, recommends itself for using a DP, so as to seek early input into the policy development process, and it is this technical standard that is the subject of the Discussion Paper on hand. Akin to all security-related mandates in the PSD2, the EBA has developed this DP in close cooperation with the European Central Bank (ECB).

Rationale

12. The overall objective of the security-related mandates conferred on the EBA is set out in recital 95 of the Directive, which states that “the security of electronic payments is fundamental in order to ensure 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.”

13. Thus it brings a number of new and important elements and improvements to the EU electronic payments market, which are aimed at:

    a) improving consumer protection against fraud, possible abuses and payment incidents through enhanced security requirements for electronic payments, such as making strong customer authentication for electronic payments compulsory; and

    b) promoting competition through a regulatory framework conducive to guaranteeing equivalent operating conditions to existing and new market players, enabling new services, so called Payment Initiation Services (PIS) and Account Information

Services (AIS), and the development of innovative mobile and internet payments in Europe.

14. PSD2 (chapter 5) requires in particular for the EBA to issue Guidelines and draft Regulatory Technical Standards 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, for the management of operational and security risks (article 95);

    - Guidelines with regard 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 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).

15. The last mandate (in Article 98) is one of those that will benefit from input at the beginning of the policy development process through a DP. The EBA is required to publish the RTS by 12 months after the date of entry into force of the Directive. The Commission would then adopt the RTS, after which the PSD2 provides that another 18 months pass until the RTS applies. The exact date of said application is unknown as it depends, inter alia, on the extent to which the EU Parliament and EU Council exercise their scrutiny rights during the adoption process. However, given the timelines set out in PSD2 as per above, the very earliest application date is October 2018[6].

16. 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 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 strong customer authentication, 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;

[6] This is based on the assumption that EBA delivers the final draft RTS by December 2016 and EU Commission adopts it within 3 months so April 2017.

(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 account servicing payment service providers (ASPSP)[7], PIS providers, AIS providers, payers, payees and other payment service providers.

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

- ensuring an appropriate level of security for PSUs and PSPs, through the adoption of effective and risk-based requirements;
- ensuring the safety of PSUs' funds and personal data;
- securing and maintaining fair competition among all PSPs;
- ensuring technology and business-model neutrality; and
- allowing for the development of user-friendly, accessible and innovative means of payment.

18. When developing this particular RTS, the EBA will have to make difficult trade-offs between competing demands such as :

i. High security requirements (which may suggest a high degree of prescription in the requirements as to avoid circumvention of rules) versus facilitation of the development of innovative security solutions in years to come (which may suggest the opposite, i.e. high level requirements that provide certain flexibility);

ii. High security requirements (which may suggest that the payment user will be subject to a set of security and authentication steps) versus customer convenience (which may suggest the exact opposite, i.e. one-click payments); and

iii. Very detailed requirements for common and open standards of communication to be implemented by all account servicing payment service providers to avoid a scenario where in practice the solutions implemented by APSPs are so divergent that these become a barrier for AIS and PIS to provide payment account access services but may limit future innovations in communication standards versus less detailed requirements which could allow the exact opposite (i.e. allow for future innovations

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

in communication standards but establish a barrier for AIS and PIS to provide their services).

19. In that respect, the EBA has identified several issues that would benefit from views by market participants before the EBA starts developing the draft RTS. The EBA invites respondents to share their views on the identified issues and on the potential clarifications suggested in this Discussion Paper.

20. To that end, the Discussion Paper is organised in five sub-chapters, the sequence of which follows the structure of the mandate conferred on EBA by Article 98 PSD2 and ending with a specific chapter related to possible synergies with the electronic identification and trust services for electronic transactions regulation (e-IDAS). Chapter 4.1 invites views on the issues related to strong customer authentication. This is followed by chapter 4.2, which considers issues related to the exemptions to the application of strong customer authentication. Chapter 4.3, in turn, addresses issues related to the protection of the PSUs' personalised security credentials. Chapter 4.4 aims at investigating the requirements for common and secure open standards of communication. Finally, Chapter 4.5 outlines possible synergies with e-IDAs Regulation.

21. Technical terms used in this Discussion Paper are based on the definitions of the PSD2. The EBA will use the responses to the DP as one of the inputs for the development of draft RTS, on which it will publicly consult in Q2 or Q3 of 2016.

4. Discussion

4.1 Considerations prior to developing the requirements on strong customer authentication

Background on PSD2 provisions

22. Article 97(1) and (3) PSD2 requires PSPs to apply strong customer authentication and have in place adequate security measures to protect the confidentiality and the integrity of the PSUs' personalised security credentials when the payer

    a) accesses its payment account online;

    b) initiates an electronic payment transaction; or

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

23. Article 97(2) provides that, with regard to the initiation of electronic remote payment transactions, payment service providers shall apply strong customer authentication, which includes elements that dynamically link the transaction to a specific amount and a specific payee.

24. Article 4(29) PSD2 defines authentication as any procedure which allows the PSPs to verify the identity of a PSU or the validity of the use of a specific payment instrument, including the use of the user's personalised security credentials (PSC).

25. Article 4(30) provides that "strong customer authentication means an authentication 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, and is designed in such a way as to protect the confidentiality of the authentication data."

26. Article 4(31) reads that "personalised security credentials means personalised features provided by the payment service provider to a payment service user for the purposes of authentication".

Issues for discussion

27. First, EBA's considerations with respect to these terms and concepts in the context of drafting the RTS under its mandate in Article 98 are summarised below:

i. with regard to (a) above, online access to payment accounts would cover all services where a PSU is using a device (e.g. PC, mobile device[8], chip card, ATM) to log into the payment account for to retrieve information on the payment account. Online in this respect is understood as establishing a connection facilitating the message exchange between the device and the network hosting the payment account information for example via internet or telecommunication.

ii. with regard to (b) above, the initiation of electronic payment transactions would cover all payment transactions within the scope of PSD2 (such as card payments, credit transfers, e-money transactions, direct debits), except where the payment instruction is not electronic (such as physical mail-order, paper based credit transfer or paper based direct debits or telephone orders).

iii. with regard to (c) above, actions carried out via a remote channel that may imply a risk of payment fraud or other abuses could be clarified as covering all actions intrinsically linked to payment services not covered in the categories (a) and (b) above. This could for example include actions related to the activation and deactivations of payment functionalities, the amendment of trusted beneficiaries ("white lists") - or blocked beneficiaries ("black-lists"), the setting of limits or the generation of virtual cards or changing PSU data that may imply a risk of payment fraud or other abuses. It only includes actions that are conducted via the internet or through a device that can be used for distance communication (e.g. mobile devices).

28. Second, in the understanding of the EBA, in case of strong customer authentication PSCs aim at binding the identity of a Payment Service User (i.e. a natural or legal person) to authentication elements. Thus, at the time of registration for a payment service or payment method, the provision of personalised security credentials involves the recording of authentication elements by the PSP.

29. The authentication elements for the purpose of strong customer authentication are categorised as "knowledge", "possession", or "inherence":

i. with regard to "knowledge" elements, these could be described as covering static passwords, codes or a personal identification number known only by the user
ii. with regard to "possession" elements, these could be described as covering the possession of a physical object or potentially data controlled only by the PSU.
iii. with regard to "inherence" elements, these could be clarified as covering biometric characteristics of the PSU such as a fingerprint or an iris scan.

30. At the moment of accessing a payment account or initiating a payment, the use of two elements from the different categories above, serve in a strong customer authentication

[8] In this respect, a "mobile device" is defined as a handheld device which is (i) able to connect to other devices or systems via radio technologies (e.g. GSM/GPRS/UMTS, Wi-Fi, NFC, Bluetooth) and (ii) equipped with a multimedia interface for user interaction (e.g. display, keyboard, loudspeaker).

procedure to demonstrate the identity of a payment service user or the validity of the use of a specific payment instrument.

31. For strong customer authentication the PSCs can be either a valid combination of these elements themselves or something which is only generated when all the elements have been provided (e.g. an algorithm in a chip produces a one-time password or cryptogram, based on a challenge responses where the PSU is asked for a PIN).

32. EBA has identified that a potential complication for compliance with the requirements of Article 97(2) might be related to the independence of the authentication elements, for example when the PSU makes a purchase or accesses his account on a mobile device which at the same time contains the credential (e.g. as part of the hardware and/or software layer) or is used to receive or retrieve the credential (e.g. via SMS or downloading codes from the cloud). Indeed, in that case a potential compromise of the mobile device itself compromises the reliability of the two authentication elements.

33. Third, PSD 2 does not provide details on how the authentication procedure should work for electronic remote payment transactions, where payment service providers apply strong customer authentication that includes elements which dynamically link the transaction to a specific amount and a specific payee.

34. In the understanding of EBA, the purpose of “dynamic linking” and the “dynamic code” mentioned in the recitals is to ensure that the authentication value used for a remote transaction can neither be used for any other purpose than originally intended by the payer nor be re-used if it is disclosed. Thus dynamic linking aims at providing a high assurance that the PSU has been identified and is authorising a specific payment transaction.

35. A complication in that respect is that there are possibly some scenarios in which a requirement for dynamic linking for the initiation of a transaction might be difficult to implement, because of either the characteristics of the channel itself (e.g. authentication given via voice over IP or Interactive voice response systems), or because the transaction amount is unknown (e.g. which amount to specify for recurrent direct debits or recurrent cards transactions).

36. A potentially helpful way to address the latter would be for the EBA to consider under its future regulatory technical standards which exemptions might be necessary (see also chapter 4.2 for further details).

Questions

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

2. Which examples of possession elements do you consider as appropriate to be used in the context of strong customer authentication, must these have a physical form or can they be data? If so, can you provide details on how it can be ensured that these data can only be controlled by the PSU?

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

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

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

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

4.2 The exemptions to the application of strong customer authentication

Background on PSD2 provisions

37. Recital 95 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. There does not seem to be a need to guarantee the same level of protection to payment transactions initiated and executed with modalities other than the use of electronic platforms or devices, such as paper-based payment transactions, mail orders or telephone orders."

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 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. Article 74 (2) provides that "***Where*** the ***payer's*** payment service provider does not require strong customer authentication, the payer shall not bear any financial losses unless the payer has acted fraudulently. 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.

41. Finally, Article 98.3 PSD2 specifies that the exemptions for strong customer authentication shall be based on the following criteria:

    - the level of risk involved in the service provided;
    - the amount and/or the recurrence of the transaction;
    - the payment channel used for the execution of the transaction.

Issues for discussion

42. However, PSD 2 does not provide details on the criteria to be considered by PSPs for future exemptions for strong customer authentication. A potentially helpful way to address this issue would be for the EBA to clarify for example that exemptions could apply for:

    A. low-value payments as defined in the PSD2 provided that the risk for cumulative transaction are monitored;

    B. outgoing payments to trusted beneficiaries included in previously established white lists by a PSU;

    C. transfers between two accounts of the same PSU held at the same PSP;

    D. low-risk transactions based on a transaction risk analysis (taking into account detailed criteria to be defined in the RTS);

    E. purely consultative services, with no display of sensitive payment data, taking into account data privacy laws

43. Considering the scope of Article 97 and the fact that PSD2 excludes paper-based transactions, mail and telephone order, the EBA has so far not identified circumstances that would justify considering exemptions based on the payment channel used for the execution of the transaction. Moreover, the EBA observes that a number of providers can, when receiving an authorisation request, not necessarily identify the payment channel (e.g. mobile versus internet payments).

44. With respect to D above, the EBA currently observes in the market that the reliability of such analysis is closely related to the availability of sufficiently detailed information and history from both, the payer and payee.

45. A potentially helpful way to address this issue would be for the EBA to consider providing clarification in its future regulatory technical standards as to which kind of capabilities and minimum set of information are required for such tools reliably to evaluate the risk of a transaction. Such capability could, for example, be required to be based on comprehensive real-time risk analysis taking into account (a) an adequate transaction history of that customer to evaluate the latter's typical spending and behaviour patterns, (b) information about the customer device used (e.g. IP address, model, operating system, language preferences) and where applicable (c) a detailed risk profile of the payee (e.g. types of service provided, transaction history) and the payees device (where applicable).

Questions

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

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

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

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

Background on PSD2 provisions

46. Article 97(3) of PSD2 states that Member States shall ensure that payment service providers have in place adequate security measures to protect the confidentiality and integrity of payment service users' personalised security credentials

47. Article 98(c) confers on EBA the mandate to develop the draft regulatory technical standards with which PSPs have to comply with, in accordance with Article 97(3), in order to protect the confidentiality and the integrity of the payment service users' personalised security credentials (PSC).

48. Article 4(31) defines "personalised security credentials" as personalised features provided by the PSPs to a PSU for the purpose of authentication.

49. Recital (94) outlines that EBA should in this respect systematically assess and take into account the privacy dimension, identify the associated risks and potential the remedies to minimise such threats to data protection.

50. Recital (96) states that "safe use of personalised security credentials is needed to limit the risks relating to phishing and other fraudulent activities. In that respect, the user should be able to rely on the adoption of measures that protect the confidentiality and integrity of personalised security credentials. Those measures typically include encryption systems based on personal devices of the payer, including card readers or mobile phones, or provided to the payer by its account servicing payment service provider via a different channel, such as by. SMS or email. The measures, typically including encryption systems, which may result in authentication codes such as one-time passwords, are able to enhance the security of payment transactions. The use of such authentication codes by payment service users should be considered to be compatible with their obligations in relation to payment instruments and personalised security credentials also when payment initiation service providers or account information service providers are involved".

Issues for discussion

51. One of the questions arising in this respect is how to ensure, throughout the payment chain, the protection of users' personalised security credentials as well as the privacy of PSU data. Such data might be particularly at risk where the data is:

    A. created, issued and transmitted to the PSU (commonly referred to as "enrolment"), usually when the PSU signs up for a payment services (e.g. the opening of a payment account). Alternatively "enrolment" may be carried out prior to signing up for the payment services or at a later stage by the PSP itself (e.g. provision of new or additional types of credentials) or undertaken by providers of electronic

identification services (e.g. see below chapter 4.5 on e-IDAS Regulation). In both cases, PSPs conduct a customer due diligence, taking into account, amongst others, the identification requirements of the European anti-money laundering legislation prior to registering or acknowledging a personalised security credential and opening an account. In addition, later modifications or re-issuance of the credentials by the PSU need to be protected.

B. stored in a physical device, such as an electronic device (e.g. a mobile device) or a chip on a card, or remotely such as in a hardware security model of server's database. Fraudsters can then attempt to access PSU data by hacking the physical device or the database where the data is stored.

C. transmitted via different communication channels, such as standard telephone line, internet or via radio technologies (e.g. GSM/GPRS/UMTS, Wi-Fi, NFC, and Bluetooth) which are not always especially protected. Fraudsters can then attempt to enter the transmission channel to get access to this data during its transmission.

D. unwittingly supplied by the PSU, as fraudsters may attempt to obtain such data directly from the PSU, for example by social engineering phone calls, sending phishing messages, directing the user to a fraudulent website, or infecting the user PC with malware that for example captures users' keystrokes during log in and sends the information to the attacker. There are many ways to compromise the PSU's device with malware, including drive-by downloads, watering hole attacks and infected USB devices.

E. accessed by a third party in the course of a payment service. In such a case, the probability of the risk increases as the attacks described above can be performed also against this third party. In the context of the PIS/AIS services, Art. 66 3(b) and 67 (2) (b) PSD2 require PIS/AIS providers to ensure that the PSCs of the PSU are not accessible to other parties, with the exception of the user and the issuer of the personalized credentials (see further details on this topic in chapter 4.4 below).

52. A potentially helpful way to address this issue would be for the EBA to provide clarification in its future regulatory technical standards that:

i. the creation, issuance, modification and re-issuance of the credentials needs to be secured to guarantee (a) the confidentiality, and the *integrity* of the enrolled personalised security credentials and (b) their delivery to, or possession by, the intended PSU.

ii. all communication channels and technical components hosting, providing access to or transmitting the personalised security credential (e.g. via a mobile device, storage in a cloud, hardware or software) need to be resistant to tampering and unauthorized access. The EBA could then also clarify how such communication

channels and technical components should be certified or evaluated by independent third parties to ensure such resistance.

iii. the security measures to protect the confidentiality and the integrity of the payment service users' personalised security credentials should be proportionate to the risks related to a fraudulent use of the PSCs to carry out fraud or to access sensitive payment data.

Questions:

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

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

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

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

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

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

Background on PSD2 provisions

53. Article 98 states that EBA shall develop draft regulatory technical standards specifying "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."

54. EBA acknowledges that this scope of the draft RTS is wide and concerns all types of electronic payment services. For traditional payment services, the EBA is already quite familiar with the industry standards and market practices. However, some questions arise with respect to potential requirements for new payment services which emerged as stated in recital 27 of PSD2: "*Since the adoption of Directive 2007/64/EC new types of payment services have emerged, especially in the area of internet payments. In particular, payment initiation services (PIS) in the field of e-commerce have evolved. Those payment services play a part in e-commerce payments by establishing a software bridge between the website of the merchant and the online banking platform of the payer's account servicing payment service provider in order to initiate internet payments on the basis of a credit transfer. Moreover, technological developments have given rise to the emergence of a range of complementary services in recent years, such as account information services (AIS). Those services provide the payment service user with aggregated online information on one or more payment accounts held with one or more other payment service providers and accessed via online interfaces of the account servicing payment service provider. The payment service user is thus able to have an overall view of its financial situation immediately at any given moment*." It is further specified in Article 67(d) that this relates only to the information from designated payment accounts and associated payment transactions.

55. This development has increasingly lead to PSUs accessing the online facility of their ASPSPs payment account via the IT infrastructure of a third party provider, involving the transmission or storage of the PSU's PSC. In order to achieve the aim expressed in recital 33 PSD2, which is to ensure continuity in the market, by enabling existing and new service providers, regardless of the business model applied by them, to offer their services with a clear and harmonised regulatory framework, the PSD2 brings AIS and PIS providers in the scope of regulated entities

56. Thus, PSD2 includes AIS and PIS in the catalogue of payment services (ANNEX I 7. and 8.) and make thus the provision of such services subject to authorisation and supervision by competent authorities in accordance with the conditions and requirements defined in PSD2 (in particular chapter 1). While providers of PIS have to apply at least for a payment institution license, AIS providers will only be required to register (see Article 5.3 PSD2).

57. Inclusion of the AIS and PIS services under PSD2 has in particular the following consequences for market participants:

    i. AIS and PIS providers will be able provide their services in the Member State where they are licensed / registered (Art11) and also in a Member State other than their home Member State, in exercise of the right of establishment or the freedom to provide services (Article 28). They will be registered in the Home Competent Authority register as authorized payment institution for the services delivered (i.e. services identified in ANNEX I 7. and/or 8) as well as in the future EBA register as defined in Article 14 of PSD2. As any other payment services listed in PSD2, such services may also be offered by any other categories of payment service provider listed in Article 1 (1).

    ii. Regulated PSPs, including AIS, PIS providers will have to comply with all the security measures deriving from the PSD2 (title IV) and delegated acts (title V). As explained in the background section, it is important to underline that only 18 months *after* their adoption by the Commission, will PSPs have to comply with the Regulatory Technical Standards on strong customer authentication and secure communication. The exact application date of the RTS is dependent on a number of factors that are currently unknown and can therefore at this stage not be predicted. However, the date will certainly not be earlier than September 2018, is likely to fall into calendar year 2019, and will therefore definitely be after the transposition and application date of all other PSD2 provisions in January 2018.

    iii. AIS and PIS providers are required to act only upon the explicit consent of the PSU (Article 65-67). The way how consent is given will be agreed between the payer and the relevant provider (Article 64).

    iv. The PSUs' right to make use of a PIS/AIS provider shall not apply where the payment account is not accessible online (Article 65-67).

    v. AIS and PIS providers will be able to rely on the authentication procedures provided by the ASPSP to the PSU to provide their services (Article 97.5). Recital 30 outlines in particular that "the personalised security credentials used for secure customer authentication by the payment service user or by the payment initiation service provider are usually those issued by the account servicing payment service providers".

    vi. PIS providers are not allowed to store sensitive payment data of the PSU (Article 66 (g)). AIS may not request sensitive payment data linked to the payment accounts (Article 67 (e)). Both need to ensure that the personalised security credentials of the PSU are not, with the exception of the user and the issuer of the personalised security credentials, accessible to other parties (Articles 66(b) and 67(b)).

vii. AIS, PIS providers will have to identify themselves with the ASPSPs every time a payment is initiated or for each communication session (Article 65 (2(c)), Article 66 3 (d), Article 67 2(c)) and communicate with them following the requirements for common and secure open standards of communication that will be defined by the EBA see Articles 66(4)(a) and 67(2)(c)).

viii. Each ASPSP offering payment accounts which are accessible online will have to be reachable by AIS, and PIS (Articles 65(1)(a), 66(1), and 67 (1)). The provision of AIS and PIS shall not be dependent on the existence of a contractual relationship between the account information service providers and the account servicing payment service providers for that purpose (Articles 66(5) and 67(4)).

58. The Article 98 (d) of PSD2 confers on the EBA the mandate to define the requirements for the common and secure open standards of communication for the purpose of identification, authentication, notification, and information between account servicing payment service providers, AIS and PIS providers, payers, payees and other payment service providers. These requirements will also apply for the confirmation of availability of funds between an issuing card-based payment instruments' PSP and the ASPSP (Article 65).

59. According to Recital 93, these regulatory technical standards shall in particular "ensure that the ASPSP is aware that he is being contacted by a PIS or an account information service provider and not by the client itself". They shall also "ensure that PIS and AIS communicate with the account servicing payment service provider and with the customers involved in a secure manner." They shall finally "allow for the use of all common types of devices (such as computers, tablets and mobile phones) for carrying out different payment services."

60. When developing these requirements, recital 94 of PSD2 states that "EBA should systematically assess and take into account the privacy dimension, in order to identify the risks associated with each of the technical options available and the remedies that could be put in place to minimise threats to data protection."

Issues for discussion

61. Article 98 states that EBA shall develop draft regulatory technical standards specifying "the requirements for common and secure open standards of communication". However, PSD2 does not mandate EBA to develop or maintain these open and common standards of communication themselves or to appoint a central entity in charge of developing or maintaining these standards. Moreover, the requirements set by the EBA "should ensure the interoperability of different technological communication solutions." (Recital 93).

62. EBA is of the view that one of the main challenges behind the development of these future requirements will be to find an appropriate balance between several competing demands. For example, achieving harmonisation that allows different secure technological communication solutions implemented by ASPSPs, AIS and PIS providers in compliance with the future requirements to co-exist, facilitate innovation and avoid a scenario where in

practice the solutions implemented by APSPs are so divergent that these become a barrier for AIS and PIS to provide payment account access services.

63. A potentially helpful way to address this issue would be for the EBA to consider clarification in its future regulatory technical standards on the following aspects:

    a. Define what makes a standard “common” and “open”

    b. The way AIS, PIS providers will have to identify themselves towards the ASPSPs for access to payment account information (e.g. exchange of electronic certificates, see as well chapter 4.5), and every time a payment is initiated including the purpose for which the AIS and/or PIS is authorised by the PSU and requesting access to the ASPSP upon each connection. Such requirements could clarify whether or not trusted third-parties need to provide assurance (e.g. in the form of security assertions) about the identification of entities involved in such communication,

    c. The way PIS, AIS and ASPSPs communicate between themselves and with the PSUs in a secure manner,

    d. The minimum functionalities requirements that the future common and secure open standards of communication will have to provide. This includes for example what kind of information/services can be requested via the standard of communication (e.g. information on the availability of funds or initiation of a payment), how the identification of the account to be accessed and consent of the PSU should be conveyed,

    e. The minimum security controls that the future common and secure open standards of communication will have to provide related to the potential unauthorised or fraudulent access to payment accounts or initiation of a payment transaction,

    f. the minimum technical requirements that could apply to the common and secure open standards of communication, the minimum reachability requirements for each ASPSPs to provide at least one interoperable interface serving all requirements of the RTS and compliant with PSD2 regulation, while AIS and PIS would have to adapt their services to the respective standardised interfaces used.

Questions:

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

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

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

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

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

64. The Regulation (EU) N 910/2014 on electronic identification and trust services for electronic transactions in the internal market (e-IDAS Regulation) aims at providing a regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities. The EBA is interested in gauging views from external stakeholders as to the extent of possible synergies between the e-IDAS Regulation and the security requirements under the PSD2 that the EBA will be developing.

65. By way of background, the e-IDAS Regulation:

    a. lays down the conditions under which Member States recognise electronic identification means of natural and legal persons falling under a notified electronic identification scheme of another Member State;

    b. sets out a supervisory and liability regime to enable qualified trust services providers to deliver, at domestic and cross-border level, qualified trust services with a high level of assurance for electronic transactions;

    c. establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication; and

    d. is mandatory for cross-border access to public services in EU countries where eIDs are available.

66. The e-IDAS Regulation requires the adoption of implementing act, two of which have primary relevance:

    a. Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance)

    b. Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance)

67. This regulation is mandatory for cross-border access to public services in EU countries where eIDs are available. The above mentioned implementing acts include criteria and specifications for the various assurance levels and interoperability. In the context of the interoperability framework the Commission is establishing further detailed technical specifications (version 1.0 will be published towards November 2015).

68. The question arises whether the e-IDAS regulation might offer one (of possibly many) suitable solution on which PSPs could rely for ensuring strong authentication of payments, for protecting the confidentiality and the integrity of the payment service users' personalised security credentials; or for implementing 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.

69. The "qualified trust services" provided by "qualified trust service providers" under e-IDAS can also be of relevance for the identification between the AIS or PIS providers with the ASPSPs as well as for ensuring the integrity and correctness of the origin of the data transmitted between AIS or PIS providers and the ASPSPs. Indeed, these services include in particular:

    a. a qualified electronic signature, which shall have the equivalent legal effect of a handwritten signature including at least the name of the signatory;

    b. a qualified electronic seal, which shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked;

    c. a qualified electronic registered delivery service, which enjoy the presumption of the integrity of the data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt indicated by the qualified electronic registered delivery service.

    d. A qualified certificate for website authentication, which shall ensure, for a legal person, at least the name of the legal person to whom the certificate is issued and, where applicable, registration number as stated in the official records;

Issues for discussion

70. These "qualified trust services" are considered as an important enabler of data protection and prevention of online fraud. However, the question arises whether such solutions are compatible with the different technological solutions available and would allow for the use of all common types of devices (such as computers, tablets and mobile phones) for carrying out different payment services, as required by recital 93 of PSD2.

71. Against this background, the EBA is keen to receive an early input from relevant stakeholders, in particular on the use of "qualified trust services" for the purpose of communication, between AIS, PIS providers and ASPSPs.

Questions:

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

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

Annex - Summary of questions

Chapter 4.1: Requirements on strong customer authentication

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

2. Which examples of possession elements do you consider as appropriate to be used in the context of strong customer authentication, must these have a physical form or can they be data? If so, can you provide details on how it can be ensured that these data can only be controlled by the PSU?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

19. Do you agree that the e-IDAS regulation could be considered as a possible solution for facilitating the strong customer authentication, protecting the confidentiality and the integrity of the payment service users' personalised security credentials as well as for common and secure open standards of communication for the purpose of identification,

authentication, notification, and information? If yes, please explain how. If no, please explain why.

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