EBA/RTS/2017/02

23 February 2017

Final Report

Draft Regulatory Technical Standards

on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2)

Contents

1. Executive Summary

In accordance with Article 98 of the revised Payment Services Directive (EU) 2015/2366 (PSD2), the EBA has developed, in close cooperation with the European Central Bank (ECB), draft regulatory technical standards (RTS) specifying the requirements of strong customer authentication (SCA), the exemptions from the application of SCA, the requirements with which security measures have to comply in order to protect the confidentiality and the integrity of the payment service users' personalised security credentials, and the requirements for common and secure open standards of communication (CSC) between account servicing payment service providers (ASPSPs), payment initiation service providers (PISPs), account information service providers (AISPs), payers, payees and other payment service providers (PSPs).

The EBA had published an initial Discussion Paper (DP) in December 2015 to explain its initial ideas and interpretations of the EBA mandates and related provisions in the Directive. The DP resulted in 118 responses, which the EBA assessed. This was followed subsequently by the publication of a Consultation Paper (CP) in August 2016 containing draft RTS and the consultation closed in October 2016. The EBA presented the CP at a large number of conferences across the EU, with a view to encouraging responses from as many market participants as possible, including market challengers that may have never interacted with a regulatory authority.

The EBA succeeded in this effort, as it received a total of 224 responses, which not only represents the highest number of responses the EBA has ever received but has also provided the EBA with an unprecedentedly wide and representative view of all stakeholders. The strong interest and engagement has continued after the consultation closed in October 2016.

The EBA, in close cooperation with the ECB, has reviewed and assessed the responses, identifying around 300 different issues or requests for clarification, a small subset of which appeared to be the key issues for respondents. These key issues were (1) the scope and technologically-neutral requirements of the draft RTS; (2) the exemptions, including scope, thresholds and the request of many respondents to add an exemption for transactions identified as low risk as a result of what some respondents referred to as 'transaction-risk analysis' (TRA), and (3) the access to payment accounts by third party providers and the requirements around the information communicated.

During the assessment of the responses, the EBA has had to make difficult trade-offs between the various, at times competing, objectives of PSD2, including enhancing security, promoting competition, ensuring technology and business-model neutrality, contributing to the integration of payments in the EU, protecting consumers, facilitating innovation and enhancing customer convenience.

The EBA agreed with some of the proposals made by respondents and made a number of changes to the draft RTS as a result. For instance, references to ISO 27001 and specific characteristics for the three elements constituting SCA were removed from the RTS, to ensure technology neutrality and allow for future innovations.

With regard to the exemptions from the principle of SCA, the EBA introduced two new exemptions, one based on TRA and the other for payments at 'unattended terminals' for transport or parking fares. However, the EBA disagreed with a number of comments that suggested adding further exemptions, such as an exemption for corporate payments. The EBA also agreed with a number of comments in favour of modifying or extending existing exemptions such as increasing the limit for remote payment transactions from EUR 10 to EUR 30, and the extension from a series of credit transfers to a series of payments more generally.

The EBA also reflected on a number of respondents expressing confusion and concern with regard to the communication between ASPSPs, AISPs and PISPs. Having assessed these comments, the EBA has decided to maintain the obligation for the ASPSPs to offer at least one interface for AISPs and PISPs for access to payment account information. The EBA has done so having consulted with the European Commission on the interpretation of the Directive, in that the existing practice of third-party access without identification referred to by a few respondents as 'screen scraping' or, mistakenly, as 'direct access' will no longer be allowed once the transition period under Article 115(4) PSD2 has elapsed and the RTS apply.

However, in order to address some of the concerns raised by a small number of respondents, the EBA has included additional requirements in the RTS, requiring ASPSPs that decide to use a dedicated interface to provide the same level of availability and performance as the interface offered to, and used by, their own customers, as well as to provide the same level of contingency measures in case of unplanned unavailability.

Next steps

The final draft RTS will be submitted to the Commission for adoption, following which they will be subject to scrutiny by the European Parliament and the Council before being published in the Official Journal of the European Union.

By reference to Article 115(4) PSD2, the RTS will be applicable 18 months after its entry into force, which would suggest an application date of the RTS in November 2018 at the earliest. The intervening period provides the industry with time to develop industry standards and/or technological solutions that are compliant with the EBA's RTS.

2. Background and rationale

2.1 Background

1. On 12 January 2016, Directive (EU) 2015/2366 on payment services in the internal market (PSD2) entered into force in the European Union, and it 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 ECB, of draft RTS 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 (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

   - RTS on authentication and communication (Article 98).

2. The last mandate (Article 98) lays down that the EBA shall develop, in close cooperation with the ECB, draft RTS addressed to Payment Service Providers (PSP) specifying:

   a) the requirements of SCA when the payer accesses its 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 SCA, 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' (PSUs') 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], PISPs, AISPs, payers, payees and other PSPs.

[1] Article 4(17) PSD2: 'account servicing payment service provider' means a payment service provider providing and maintaining a payment account for a payer.

3. PSD2 provides in Article 98(2) 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 had to make difficult trade-offs between at times competing demands. For example, the objective of PSD2 to facilitate innovative payment services would suggest that the EBA should pitch the technical standards at a higher, i.e. less detailed level, so as to allow room for the industry to develop industry standards or technical solutions that are compliant with the EBA's Technical Standards but that also allow for innovation over time, to exploit technological advancements and to respond to future security threats. However, this may result in many different industry solutions emerging across the EU, in particular for communication between ASPSPs, PISPs, AISPs, payers, payees and other PSPs. This, in turn, could lead to a fragmentation across geographical, sectoral and/or other lines, which would undermine PSD2's objective of integrating retail payments in the EU and facilitating competition across the EU.

5. In addition, the objective of ensuring a high degree of security and safety would suggest that the EBA's technical standards should be rather demanding in terms of authentication, whereas the objective of user-friendliness would suggest that the RTS should be less strict.

6. 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 by publishing a DP in December 2015, to which the EBA received 118 responses.

7. The EBA assessed the responses and started drafting the RTS. The draft RTS were published as CP in August 2016. The CP included a number of specific questions for respondents to consider. The consultation period closed in October 2016 and the EBA received 224 responses, the highest number of responses ever received to an EBA CP. All the major types of participants in the payment services market were represented among the respondents, including a large number of future AISPs, PISPs and unregulated service or IT providers, a significant number of e-money and payment institutions, merchants, acquirers and card schemes. The EBA assessed the responses and made changes where relevant.

8. Given the very large number of responses assessed, the rationale section focuses on a small subset of what appeared to be the key issues for respondents. The Feedback Table in Chapter 4.3 (pages 48 to 153) provides an exhaustive and comprehensive list of all the responses

received by the EBA, with the EBA's assessment, as well as any changes that the EBA decided to make to the RTS as a result, where applicable.

2.2 Rationale

9. In order to explain how the EBA arrived at the provisions in the draft RTS that are proposed in the final report, the rationale section summarises the EBA's understanding of some of the PSD2 provisions where relevant, and elaborates on what appeared to be the three key issues to respondents to the CP, namely:

    a) the scope and technology-neutrality of the draft RTS;

    b) the exemptions, including scope, thresholds and the request of many respondents to add an exemption for transactions identified as low risk as a result of what some respondents referred to as TRA; and

    c) the access to payment accounts by third party providers and the requirements around the information communicated.

10. The rationale discusses each area in turn and, where necessary, summarises the EBA's interpretation of PSD2.

2.2.1 Scope and technology-neutrality of the draft RTS

11. A number of respondents sought clarification with regard to the overall scope of the RTS in terms of the types of payment transactions that are and are not subject to the RTS. By way of response, the EBA wishes to clarify that the scope of any RTS that is conferred on the EBA is defined not by the EBA but in the Directive itself.

12. In this particular case, the scope is defined in Article 97(1) PSD2 which requires that 'Member States shall ensure that a payment service provider applies SCA where the payer:

    - accesses its payment account online;
    - initiates an electronic payment transaction;
    - carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.'

13. In relation to payment instruments, and as stated in the CP, the EBA understands that Article 97(1)(b) applies to electronic payments initiated by the payer, or by the payer through the payee such as credit transfers or card payments, but does not apply to electronic payments initiated by the payee only. Given Article 97(1)(c), an exception is a transaction where the payer's consent for a direct debit transaction is given in the form of an electronic mandate with the involvement of its PSP. The different types of payment instruments include e-money payment transactions. For instance, credit transfers include e-money transfers.

14. In relation to how Article 97(1)(b) should be applied by PSPs for the provision of payment initiation services (PIS), the EBA understands, as stated in the CP, that PIS Providers have the right to rely on the authentication procedures provided by the ASPSP to the user. In such cases, the authentication procedure will remain fully in the sphere of competence of the ASPSP.

15. Based on the clarification received from the Commission on the most plausible interpretation of the Directive, the EBA understands that the payee's PSP has the option not to accept SCA both (1) before and during the transitional period between the application date of PSD2 (13 January 2018) and the application date of the RTS under consultation (in November 2018 at the earliest) and (2) after this transitional period but in this case only within the limits of the authorised exemptions and where applicable. The liability rules as described in article 74(2) PSD2 apply before, during and after the transitional period.

16. In the case of cross-border transactions where payment instruments issued under a national legal framework that does not require the use of SCA (such as magnetic stripe cards) are used within the EU or when the PSP of the acquirer is established in a jurisdiction where it is not legally required to support the strong customer authentication procedure designed by the European issuing PSP, the European PSPs shall make every reasonable effort to determine the legitimate use of the payment instrument. Those types of cross-border transactions are not included in the transactions for the purpose of the calcuation of fraud rates under the new Article 16 of the final draft RTS.

17. In addition, a number of respondents queried if the characteristics of the three elements that form part of SCA are technology neutral. Some respondents suggested modifying the examples while others suggested removing them to allow for future innovations. The EBA concurs with the view of those respondents that were of the view that, in order to ensure technology and business-model neutrality and to allow PSPs to be able to continuously adapt to evolving fraud scenarios, the draft RTS should be positioned at a higher level in these particular instances.

18. A number of respondents also queried the reference to specific standards, and in particular ISO 20022 and ISO 27001, as well as the reference to HTTPs, in Articles 19(3), 21(6) and 1(3)(d), respectively, of the draft RTS as published in August 2016. The EBA concurs with the view that references to ISO 27001 and HTTPs should be removed, in order to ensure technology and business-model neutrality as well as allow for future innovations. However, the EBA does not agree with removing the reference to ISO20022, as it believes having a standardised message format is essential to the good functioning of the interface between the different PSPs. That said, the EBA recognised that the reference may have been unclear and has as a result clarified in a new Article 28(2) that this standard applies only to the financial messaging (rather than to the communication technology, e.g. using XML) and solely where ASPSPs are offering a dedicated interface. This ensures commonality in terms of the content and format of the messaging without being too prescriptive on the communication technology used.

2.2.2 Exemption for low risk transactions following transaction-risk analysis

19. A large number of responses were in relation to the exemptions proposed in the original Article 8 (now Articles 10 to 18) RTS, including their scope, the PSPs that can use the exemptions, the detailed exemptions themselves and additional exemptions that a number of respondents suggested the EBA should add.

20. The large majority of the comments suggested that the draft RTS should allow an exemption based on what some respondents variously referred to as 'transaction-risk analysis' (TRA) or similar terms. As stated in the CP, the EBA considered adding such an exemption in the CP but was not able at the time to identify objective criteria that would have been legally acceptable. Exemptions from any law must be defined narrowly with clear and unambiguous thresholds and on the basis of objective and verifiable criteria rather than subjective and individual assessments conducted by the individual PSPs to which the law applies. In addition, any exemption that would allow the majority of payments to be exempted from SCA would go against PSD2's objective of enhancing security, and against the definition of an exemption.

21. Nevertheless, the EBA agrees with the view expressed by these respondents that a risk-based approach, including the ability to conduct detailed transaction-risk analysis and fraud monitoring, is essential to achieve the objective under PSD2 of reducing overall fraud. Consequently the EBA arrived at the view that, in accordance with Article 98(2)(a) PSD2, an exemption based on such an analysis should be added in a new Article 16 RTS. The RTS also reiterate the importance of risk and fraud monitoring in general as a necessary complement to the principle of SCA laid out in PSD2 as stated in a new Article 2 RTS.

22. The EBA also appreciates that TRA could lead to the identification and classification of transactions (at least) between low levels and high levels of risks on a transaction–by-transaction basis. However, whereas under Directive 2007/64/EC, transactions with low levels of risk could then be exempted from strong authentication in line with the EBA guidelines on internet payments, in a post-PSD2 world, where SCA is the principle for all transactions, the balance has changed and any exemption in the RTS would need to be defined narrowly as explained in the previous paragraph.

23. Having regard to the views of respondents the EBA has re-evaluated a number of potential options for such an exemption and narrowed down a few options to finally insert a new, additional exemption in a new Article 16 RTS based on TRA. This exemption focuses on the outcome of lowering the level of fraud. The PSPs that wish to use the exemption must have an overall fraud rate for a specific payment instrument that equates to, or is lower than, the reference fraud rate defined in the new Article 16. The exemption can only be applied to remote transactions and below a specific monetary threshold that varies between EUR 100 and EUR 500, depending on the PSP's fraud rate for any given payment instrument as referenced in the new Article 16(2) RTS. The monetary thresholds have been set by the EBA with different corresponding reference fraud rates, which in turn differ between the underlying payment instruments used. The effect is that, the lower the fraud rates, the higher the monetary threshold and therefore the higher the number of use cases. In addition, the RTS now require PSPs to monitor all of their fraud rates as well as the performance of the transaction-risk

analysis method used, which must additionally be independently assessed by qualified auditors. Furthermore, the PSP must report any change related to the use of this exemption to the national authorities. The reference fraud rates should be reviewed on a regular basis and updated based on the fraud reporting under Article 96(6) PSD2.

24. A number of comments, particularly from merchants' acquirers or payees' PSPs, express confusion with regard to the scope of the exemptions and the type of PSPs that could use exemptions, in particular regarding a (then potential) new exemption based on transaction-risk analysis. Some of the respondents that are merchants' acquirers or payees' PSPs, explain that they perform transaction risk analysis and are well positioned to identify any potential fraud or other abuse from a payee's perspective and should therefore not always have to perform SCA but should instead have the choice to use a (now new) exemption based on transaction-risk analysis. The EBA concurs with the views expressed by these respondents and has made it clearer in the RTS that both payees' and payers' PSPs could trigger such an exemption under their own and exclusive responsibility but with the payer's PSP having the final say.

25. There were also a large number of responses on other existing exemptions, seeking clarification, pointing out technical unfeasibility, and requesting further exemptions to accommodate existing situations. The EBA has reflected on these, concurs with the views expressed in relation to a number of the comments and has made some amendments accordingly in some areas. For instance, the EBA has added a new exemption for unattended terminals for fares related to transport and parking services, since it may not be proportionate and may also not be in the general public interest for operational (e.g. to avoid queues and potential accidents at toll gates) or security reasons (e.g. the risk of shoulder surfing).

26. In addition, the low-value exemption for remote transactions that was proposed in the CP has been increased from EUR 10 to EUR 30, taking into account the general provision now introduced under Article 2, with the clarification, however, that PSPs may always revert back to SCA if a risk of fraud or other abuse is identified for a specific transaction. The EBA has also recognised potential technical difficulties in calculating cumulative monetary thresholds and has as a result introduced a choice for PSPs to apply SCA either every time the cumulative threshold is reached or after five consecutive transactions.

27. The EBA has not concurred with some other views expressed by some respondents, including exempting all corporate payments. The EBA is of the view that an exemption for all such payments would not be proportionate to the risk. The EBA also understands that SCA-enabled technology is already in place for a number of corporate payment systems.

28. To ensure technology neutrality, the exemption focusing on a series of credit transfers with the same payee and the same value has been extended to a series of payments in general, as the risk does not vary between different payment instruments.

2.2.3 Access to payment account

29. The majority of responses received on this topic focused on the communication exchanges, frequency of requests and type of information communicated between AISPs, PISPs, PSPs

issuing card-based payment instruments, and ASPSPs. There was in general a difference of views between ASPSPs on the one hand and third-party providers on the other.

30. With regard to frequency, the draft RTS proposed in the CP enabled AISPs to request information no more than two times a day, and at any time when the payment service user is actively requesting such information. Many third-party providers (TPPs) requested an hourly interval because of the increasingly real-time nature of payments and to better serve their customers, while some ASPSPs suggested it should be limited to once a day and others to office hours or at specific times to enable ASPSPs to manage the load of information being communicated, as they are of the view that many different AISPs, PISPs, PSPs issuing card-based payment instruments will potentially want to request the same information at the same time. The EBA considered the different arguments and, while it recognises the importance of regular access for TPPs (understood as AISPs, PISPs, and PSPs issuing card-based payment instruments), it also felt that four times a day should be the maximum (unless agreed bilaterally between the parties), in line with the domestic clearing cycle in some EU member states.

31. A number of comments from TPPs, and PISPs in particular, requested clarity on the modality of access to payment accounts and in particular clarification on whether or not 'screen scraping' (also sometimes erroneously referred to as 'direct access') would be allowed. While these providers did not appear to be opposed to communication via a dedicated interface, they considered it essential to remain free to have access to payment accounts in other ways, particularly in case a dedicated interface did not work properly.

32. After consulting with the Commission on the most plausible interpretation of the Directive, the EBA is of the view that accessing accounts through screen scraping will no longer be allowed, once the transitional period comes to an end, on the basis of a number of provisions under PSD2, especially on TPPs' identification, the requirements on secure communication by the ASPSP and by the AISPs, PISPs, and PSPs issuing card-based payment instruments, on relying on the authentication procedures, and on restrictions on TPPs in accessing to data and accessing information from designated payment accounts and associated payment transactions.

33. The EBA is of the view that it is very important for the AISPs, PISPs and PSPs issuing card-based payment instruments to be able to initiate a payment order, to access information or to obtain the information they are entitled to under PSD2 when they provide their payment services to their customers. This legal right shall not be intentionally diminished. The EBA has, to that end, added a new Article 28 requiring ASPSPs, if they choose to develop and offer a dedicated interface, to provide the same level of availability and performance as the interface offered to and used by their customers (e.g. online banking), as well as to provide the same level of contingency measures in case of unplanned unavailability.

34. The EBA recognises that it is also important to balance out the technical method of access (and business-model neutrality) with the security measures under PSD2, including the requirements under PSD2 that AISPs, PISPs, PSPs issuing card-based payment instruments and ASPSPs providing AIS and PIS shall identify themselves to the ASPSP, and that AISPs, PISPs, PSPs issuing card-based payment instruments and ASPSPs shall communicate securely with each other.

35. While the pre-existing AISPs, PISPs, PSPs issuing card-based payment instruments shall not be forbidden to continue to perform the same activities during the transitional period, they will have to use the access route offered by the ASPSPs after that period, whether the ASPSP opts to develop a dedicated interface or not. Article 27(2) RTS clarifies that the ASPSPs may want to opt for a dedicated interface or may allow the use of the interface used for identification and communication with their payment services users.

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

COMMISSION DELEGATED REGULATION (EU) No …/..

of XXX

supplementing Directive 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of 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[2],

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. The authentication procedure should include, in general, transaction monitoring mechanisms to detect attempts to use a payment service user's personalised security credentials that were lost, stolen, or misappropriated and should also ensure that the payment service user is the legitimate user and therefore is giving consent for the transfer of funds and access to its account information through a normal use of the personalised security credentials. Furthermore, it is necessary to specify the requirements of the strong customer authentication that should be applied each time a payer accesses its 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 abuse, by requiring the generation of an authentication code which should be resistant against

[2] OJ L 337, 23.12.2015 p. 35.

the risk of being forged in its entirety or by disclosure of any of the elements upon which the code was generated.

(2) As fraud methods are constantly changing, the requirements of strong customer authentication should allow for innovation in the technical solutions addressing the emergence of new threats to the security of electronic payments. To ensure that the requirements in this Regulation are effectively implemented on a continous basis, it is also appropriate to require that the security measures for the application of strong customer authentication and its exemptions, the measures to protect confidentiality and integrity of the personalised security credentials, and the measures establishing common and secure open standars of communication are documented, periodically tested, evaluated and audited by internal or external independent and qualified auditors. Such review should report on the compliance of the payment service provider with this Regulation and should be made available to competent authorities upon their request.

(3) As electronic remote payment transactions are subject to a higher risk of fraud, it is necessary to introduce additional requirements for the strong customer authentication of such transactions, ensuring that the elements dynamically link the transaction to an amount and a payee specified by the payer when initiating the transaction.

(4) Dynamic linking is possible through the generation of authentication codes which is subject to a set of strict security requirements. To remain technologically neutral these technical standards should not require a specific technology for the implementation of authentication codes. Therefore authentication codes should be based on solutions such as generating and validating one-time passwords, digital signatures or other cryptographically underpinned validity assertions using keys and/or cryptographic material stored in the authentication elements, as long as the security requirements are fulfilled.

(5) It is necessary to define specific requirements for the situation where the final amount is not known at the moment the payer initiates an electronic remote payment transaction, in order to ensure that the strong customer authentication is specific to the maximum amount that the payer has given consent for as referred to in Article 75 of Directive (EU) 2015/2366.

(6) In order to ensure the application of strong customer authentication, it is also necessary to require adequate security features for the elements of strong customer authentication categorised as knowledge (something only the user knows), such as length or complexity, for the the elements categorised as possession (something only the user possesses), such as algorithm specifications, key length and information entropy, and for the devices and software that read elements categorized as inherence (something the user is) such as algorithm specifications, biometric sensor and template protection features, in particular to mitigate the risk that those elements are uncovered, disclosed to and used by unauthorised parties. It is also necessary to define 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 are used through a multi-purpose device, i.e. a device such as a tablet or a mobile phone which can be used for both giving the instruction to make the payment and for being used in the authentication process.

(7) In order to allow the development of user-friendly and accessible means of payment for low-risk payments, it is important to allow for some exemptions to the principle of

applying strong customer authentication. It is equally important for these exemptions to be objectively defined with clear and unambiguous criteria.

(8) Exemptions based on low-value contactless payments, which also take into account a maximum number of consecutive transactions or a certain fixed maximum value of consecutive transactions without SCA, allow the development of user friendly and low risk payment services and should be included in these technical standards. It is also appropriate to establish an exemption for the case of electronic payment transactions initiated at unattended terminals where the use of strong customer authentication may not always be desirable due to operational reasons (e.g. to avoid queues and potential accidents at toll gates) or safety or security risks (for instance the risk of shoulder surfing). Actions which imply access to the balance and the recent transactions of a payment account without disclosure of sentitive payment data, recurring payments to the same payees which have been previously set up by the payer through the use of strong customer auhtentication, and payments to self from a natural or legal person within accounts in the same payment service provider, also pose a low level or risk and should therefore listed as exemptions in these technical standards.

(9) To improve confidence in transactions over the internet, these technical standards should strike a proper balance between the interest in enhanced security in remote payments and needs of user-friendliness and accessibility. In line with these principles, thresholds below which no strong customer authentication needs to be applied should be set in a conservative manner for purchases of goods and services of low value (corresponding to low amounts to be paid). Such an exemption conforms with the purpose of developing user friendly and accessible means of payment in respect of low risk payments and should therefore be included in these technical standards.

(10) In the case of real-time transaction risk analysis that categorise a payment transaction as low risk, it is also appropriate to introduce an exemption, providing that a number of criteria are met by the payment service provider that intend not to apply strong customer authentication through the adoption of effective and risk-based requirement which ensure the safety of the payment service user's funds and personal data. Those risk-based requirements should combine the scores of the risk analysis, confirming that no abnormal spending or behavioural pattern of the payer has been identified, also by relation to other risk factors including information on the location of the payer and of the payee, with conservative monetary thresholds based on fraud rates calculated for remote payments. These technical standards should set the maximum value of such risk based exemption in a conservative manner ensuring a very low corresponding fraud rate, also by comparison to the fraud rates of all the payment transactions of the payment service provider, including those authenticated through strong customer authentication, within a certain period of time and on a rolling basis.

(11) With the aim of considering new historical evidence on the fraud rates of electronic payment transactions, it is necessary that payment service providers regularly monitor and make available to competent authorities, upon their request, for each payment instrument, the value of unauthorised payment transactions and the observed fraud rates for all their payment transactions, whether authenticated through strong customer authentication or executed under a relevant exemption. Where new available information provides evidence contributing to an effective review of the thresholds for an exemption to strong customer authentication based on a real-time transaction risk

analysis, EBA should update these regulatory technical standards, where appropriate, by setting new thresholds and corresponding fraud rates with the aim of enhancing the security of remote electronic payments, in accordance with Article 98(5) of Directive (EU) 2015/2366 and with Article 10 of Regulation (EU) No 1093/2010[3].

(12) The measures that protect the confidentiality and integrity of personalised security credentials, as well as authentication devices and software, should limit the risks relating to fraud through unauhtorised use of payment instruments and unauthorised access to payment accounts. To this end it is necessary to introduce requirements on the secure creation and delivery of the personalised security credentials and their association with the payment service user, and to provide conditions for the renewal and deactivation of the credentials.

(13) In order to ensure effective and secure communication between the relevant actors in the context of account information services, payment initiation services and confirmation on the availabilty of funds, it is necessary to specify the requirements of common and secure open standards of communication to be met by all relevant payment service providers.

(14) Each account servicing payment service provider with payment accounts that are accessible online should offer at least one interface enabling secure communication with account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments. The interface should enable the account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments to identify themselves to the account servicing payment service provider. It should also allow 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.

(15) In order to allow account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments to develop their technical solutions, the technical specification of the interface should be adequately documented and made publicly available. Moreover, the account servicing payment service provider should offer a facility enabling the payment service providers to test the technical solutions. To ensure the interoperability of different technological communication solutions, the interface should use standards of communication which are developed by international or European standardisation organisations.To ensure technology and business-model neutrality, the account servicing payment service providers should be free to decide whether the interface they offer should be dedicated to the communication with account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments, or to allow use of the interface for the identification and communication with the account servicing payment service providers' payment service users.

(16) Where access to payment accounts is offered via a dedicated interface, to ensure the right of payment service users to make use of payment initiation service providers and of services enabling access to account information, as referred to in Article 66 and 67

[3] Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (OJ L 331, 15.12.2010, p. 12).

respectively of Directive (EU) 2015/2366, it is necessary to require that the dedicated interface have the same service level as the interface available to the payment service user, including same level of contingency measures. Dedicated interfaces shold use ISO 20022 elements, since this latter standard for financial messaging is already widely used in the payments sector, between and within Member States.

(17) In order to safeguard the confidentiality and the integrity of data, it is necessary to ensure the security of communication sessions between account servicing payment service providers, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. It is in particular necessary to require that secure encryption is applied between account information service providers, payment initiation service providers, payment service providers issuing card-based payment instruments and account servicing payment service providers when exchanging data.

(18) In accordance to Articles 65, 66 and 67 Directive (EU) 2015/2366, payment initiation service providers, payment service providers issuing card-based payment instruments and account information service providers will only seek and obtain the necessary and essential information from the account servicing payment service provider for the provision of a given payment service and only with the consent of the payment service user. This consent may be given individually for each request of information or for each payment to be initiated or for account information service providers, as a general mandate for designated payment accounts and associated payment transactions as established in the contractual agreement with the payment service user. Payment initiation service providers and account information service providers shall only request information on behalf of the payment service user with his/her consent.

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

(20) EBA has conducted open and transparent 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
GENERAL PROVISIONS

Article 1
Subject matter

1. This Regulation establishes the requirements to be complied with by payment service providers for the purpose of the implementation of security measures which enable them to do the following:

   (a) apply the procedure of strong customer authentication in accordance with Article 97 of Directive (EU) 2015/2366;

   (b) exempt the application of the security requirements of strong customer authentication, subject to specified and limited conditions based on the level of risk, the amount and the recurrence of the payment transaction and of the payment channel used for its execution;

   (c) protect the confidentiality and the integrity of the payment service user's personalised security credentials;

   (d) establish common and secure open standards for the communication between account servicing payment service providers, payment initiation service providers, account information service providers, payers, payees and other payment service providers in relation to the provision and use of payment services in application of Title IV of Directive (EU) 2015/2366.

2. Compliance with the requirements in this Regulation does not entail any consequence for the provisions governing rights, obligations and liability for unauthorised payment transactions set out in Title IV, Chapter 2 of Directive (EU) 2015/2366.

Article 2
General authentication requirements

1. For the purpose of the implementation of the security measures referred to in points (a) and (b) of Article 1, payment service providers shall have transaction monitoring mechanisms in place that enable them to detect unauthorised or fraudulent payment transactions.

2. The transaction monitoring mechanisms shall be based on the analysis of payment transactions taking into account elements which are typical of the payment service user in the circumstances of a normal use by the payment service user of the personalised security credentials.

3. Payment service providers shall ensure that the transaction monitoring mechanisms takes into account, at a minimum, each of the following risk-based factors: lists of compromised or stolen authentication elements; the amount of each payment transaction; known fraud scenarios in the provision of payment services; signs of malware infection in any sessions of the authentication procedure.

4. Where payment service providers exempt the application of the security requirements of the strong customer authentication in accordance with Article 16, in addition to the requirements in paragraphs 1, 2 and 3, they shall ensure that the

transaction monitoring mechanisms take into account, at a minimum, and on a real-time basis each of the following risk-based factors: the previous spending patterns of the individual payment service user; the payment transaction history of each of the payment service provider's payment service user; the location of the payer and of the payee at the time of the payment transaction providing the access device or the software is provided by the payment service provider; the abnormal behavioural payment patterns of the payment service user in relation to the payment transaction history; in case the access device or the software is provided by the payment service provider, a log of the use of the access device or the software provided to the payment service user and the abnormal use of the access device or the software.

Article 3
Review of the security measures

1. The implementation of the security measures referred to in Article 1(1) shall be documented, periodically tested, evaluated and audited by internal or external independent and qualified auditors in accordance with the applicable audit framework of the payment service provider.

2. The period between the audit reviews referred to in paragraph 1 shall be determined taking into account the relevant accounting and statutory audit framework applicable to the payment service provider. Payment service providers that make use of the exemption under Article 16 shall perform the audit for the methodology, the model and the reported fraud rates at a minimum on a yearly basis.

3. The audit review shall evaluate and report on the compliance of the payment service provider's security measures with the requirements set out in this Regulation. The report shall be made fully available to competent authorities upon their request.

CHAPTER 2
SECURITY MEASURES FOR THE APPLICATION OF STRONG CUSTOMER AUTHENTICATION

Article 4
Authentication code

1. Where payment service providers apply strong customer authentication in accordance with Article 97(1) of Directive (EU) 2015/2366, the authentication based on two or more elements categorized as knowledge, possession and inherence shall result in the generation of an authentication code. The authentication code shall be accepted only once by the payment service provider when the payer uses the authentication code to access its payment account online, to initiate an electronic payment transaction or to carry out any action through a remote channel which may imply a risk of payment fraud or other abuses.

2. For the purpose of paragraph 1 payment service providers shall adopt security measures ensuring that each of the following requirements is met:

   (a) no information on any of the elements of the 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 any other authentication code previously generated;

   (c) the authentication code cannot be forged.

3. Payment service providers shall ensure that the authentication by means of generating an authentication code includes each of the following measures:

   (a) where the authentication for remote access, remote electronic payments and any other actions through a remote channel which may imply a risk of payment fraud or other abuses has failed to generate an authentication code for the purposes of paragraph 1, none of the elements categorised as knowledge, possession and inherence can be identified as incorrect;

   (b) the number of failed authentication attempts that can take place consecutively, within a given period of time, and after which the actions referred to in points (a), (b) and (c) of Article 97(1) of Directive (EU) 2015/2366 shall be temporarily or permanently blocked, shall in no event exceed five times. Where the block is temporary the duration of the block and the number of retries before applying a permanent block shall be established based on the characteristics of the service provided to the payer and all the relevant risks involved, taking into account, at a minimum, the factors referred to in Article 2(3). The payer should be alerted before the block is permanent. Where the block is permanent, a secure procedure shall be established allowing the payer to regain use of the blocked electronic payment instruments;

   (c) the communication sessions are protected against the capture of authentication data transmitted during the authentication and against manipulation by unauthorised parties in accordance with the requirements in Chapter 5;

(d) a maximum time without activity by the payer after being authenticated for accessing its payment account online shall not exceed five minutes.

Article 5
Dynamic linking

1. Where payment service providers apply strong customer authentication in accordance with Article 97(2) of Directive (EU) 2015/2366, in addition to the requirements of Article 4, they shall adopt security measures that meet each of the following requirements:

   (a) the payer is made aware of the amount of the payment transaction and of the payee;

   (b) the authentication code generated shall be specific to the amount of the payment transaction and the payee agreed to by the payer when initiating the transaction.

   (c) the authentication code accepted by the payment service provider corresponds to the original specific amount of the payment transaction and to the payee agreed to by the payer. Any change to the amount or the payee shall result in the invalidation of the authentication code generated.

2. For the purpose of paragraph 1, payment service providers shall adopt security measures which ensure the confidentiality, authenticity and integrity of each of the following:

   (a) the amount of the transaction and the payee through all phases of authentication.

   (b) the information displayed to the payer through all phases of authentication including generation, transmission and use of the authentication code.

3. For the purpose of the requirement under point (b) in paragraph 1 and where payment service providers apply strong customer authentication in accordance with Article 97(2) of Directive (EU) 2015/2366 in relation 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 shall be specific to the amount that the payer has given consent to be blocked and agreed to by the payer when initiating the transaction.

4. For the purpose of the requirement under point (b) in paragraph 1 and where payment service providers apply strong customer authentication in accordance with Article 97(2) of Directive (EU) 2015/2366 in relation to payment transactions for which the payer has given consent to execute a batch of remote electronic payment transactions to one or several payees, the authentication code shall be specific to the total amount of the batch of payment transactions and to the specified payees.

Article 6
Requirements of the elements categorised as knowledge

1. Payment service providers shall adopt measures mitigating the risk that the elements of strong customer authentication categorised as knowledge are uncovered by, or disclosed to, unauthorised parties.

2. The use by the payer 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 7
Requirements of the elements categorised as possession

1. Payment service providers shall adopt measures mitigating the risk that the elements of strong customer authentication categorised as possession are used by unauthorised parties.

2. The use by the payer of elements categorized as possession shall be subject to measures designed to prevent replication of the elements.

Article 8
Article Requirements of devices and software linked to elements categorised as inherence

1. Payment service providers shall adopt measures mitigating the risk that the authentication elements categorised as inherence and read by access devices and software provided to the payer are uncovered by unauthorised parties. At a minimum, the access devices and software shall ensure a very low probability of an unauthorised party being authenticated as the payer.

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

Article 9
Independence of the elements

1. Payment service providers shall ensure that the use of the elements of strong customer authentication referred to in Articles 6, 7 and 8 shall be subject to measures in terms of technology, algorithms and parameters, which ensure 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 mobile phones and tablets, payment service providers shall adopt security measures to mitigate the risk resulting from the multi-purpose device being compromised.

3. For the purposes of paragraph 2, the mitigating measures shall include each of the following:

   (a) the use of separated secure execution environments through the software installed inside the multi-purpose device;

   (b) mechanisms to ensure that the software or device has not been altered by the payer or by a third party or mechanisms to mitigate the consequences of such alteration where this has taken place.

CHAPTER 3
EXEMPTIONS FROM STRONG CUSTOMER AUTHENTICATION

Article 10
Payment account information

1. Subject to paragraph 2 of this Article and to compliance with the requirements laid down in paragraphs 1, 2 and 3 of Article 2, payment service providers are exempted from the application of strong customer authentication where a payment service user is limited to accessing either or both of the following items online without disclosure of sensitive payment data:

   (a) the balance of one or more designated payment accounts;

   (b) the payment transactions executed in the last 90 days through one or more designated payment accounts.

2. For the purpose of paragraph 1, payment service providers are not exempted from the application of strong customer authentication where either of the following condition is met:

   (a) the payment service user is accessing online the information specified in points (a) and (b) of paragraph 1 for the first time;

   (b) the last time the payment service user accessed online the information specified in point (b) of paragraph 1 and strong customer authentication was applied more than 90 days ago.

Article 11
Contactless payments at point of sale

Subject to compliance with the requirements laid down in paragraphs 1, 2 and 3 of Article 2, payment service providers are exempted from the application of strong customer authentication where the payer initiates a contactless electronic payment transaction provided that both the following conditions are met:

(a) the individual amount of the contactless electronic payment transaction does not exceed EUR 50;

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

Article 12
Transport and parking fares

Subject to compliance with the requirements laid down in paragraphs 1, 2 and 3 of Article 2, payment service providers are exempted from the application of strong customer authentication where the payer initiates an electronic payment transaction at an unattended payment terminal for the purpose of paying a transport or parking fare.

Article 13
Trusted beneficiaries and recurring transactions

1. Subject to paragraph 2 of this Article and to compliance with the requirements laid down in paragraphs 1, 2 and 3 of Article 2, payment service providers are exempted from the application of strong customer authentication in each of the following situations:

   (a) the payer initiates a payment transaction where the payee is included in a list of trusted beneficiaries previously created or confirmed by the payer through its account servicing payment service provider;

   (b) the payer initiates a series of payment transactions with the same amount and the same payee.

2. For the purpose of points (a) and (b) of paragraph 1 the following cases do not constitute an exemption:

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

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

Article 14
Payments to self

Subject to compliance with the requirements laid down in paragraphs 1, 2 and 3 of Article 2, payment service providers are exempted from the application of strong customer authentication where the payer initiates a credit transfer where the payer and the payee are the same natural or legal person and both payment accounts are held by the same account servicing payment service provider.

Article 15
Low-value transaction

Subject to compliance with the requirements laid down in paragraphs 1, 2 and 3 of Article 2, payment service providers are exempted from the application of strong customer authentication, where the payer initiates a remote electronic payment transaction provided that both the following conditions are met:

(a) the amount of the remote electronic payment transaction does not exceed EUR 30;

(b) the cumulative amount, or the number, of previous remote electronic payment transactions initiated by the payer since the last application of strong customer authentication does not, respectively, exceed EUR 100 or 5 consecutive individual remote electronic payment transactions.

Article 16
Transaction risk analysis

1. Subject to compliance with the requirements laid down in Article 2 and to paragraph 2 of this Article, payment service providers are exempted from the application of strong customer authentication, where the payer initiates a remote electronic

payment transaction, identified by the payment service provider as posing a low level of risk according to the transaction monitoring mechanisms referred to in Article 2(1).

2. For the purposes of paragraph 1 all the following conditions shall apply:

(a) the amount of the electronic payment transaction does not exceed the Exemption Threshold Value ('ETV') specified in the following table for 'remote card-based payments' and 'credit transfers' respectively, corresponding to the payment service provider's fraud rate for such payment services calculated in accordance with point (d) of this paragraph and up to a maximum value of EUR 500;

	Reference Fraud Rate (%) for:	
ETV	***Remote card-based payments***	***Credit transfers***
EUR 500	***0.01***	***0.005***
EUR 250	***0.06***	***0.01***
EUR 100	***0.13***	***0.015***

(b) the transaction monitoring mechanisms enable the payment service provider to perform a real-time risk analysis of the electronic payment transaction which takes into account, at a minimum, the risk factors set out in paragraphs 3 and 4 of Article 2 and to combine them in a detailed risk scoring enabling the payment service provider to assess the level of risk of the payment transaction;

(c) irrespective of the specific arrangements of the transaction monitoring mechanisms, an electronic payment transaction is identified as posing a low level of risk only where the following conditions, in combination with the risk analysis referred to in point b) of this paragraph, are met:

(i) no abnormal spending or behavioural pattern of the payer has been identified;

(ii) no unusual information about the payer's device/software access has been identified;

(iii) no malware infection in any session of the authentication procedure has been identified;

(iv) no known fraud scenario in the provision of payment services has been identified;

(v) the location of the payer is not abnormal;

(vi) the location of the payee is not identified as high risk.

(d) for each type of transaction referred to in the table under point (a) ('remote card-based payments' and 'credit transfers'), the payment service provider's overall fraud rate covering both payment transactions authenticated through strong customer application or executed under any relevant exemption in accordance with Article 13 to 16 shall be equivalent to or lower than the reference fraud rate for the same type of payment transaction in line with the relevant table under point (a). The overall fraud rate for each type of payment

instrument should be calculated as the total value of unauthorised or fraudulent remote transactions, whether the funds have been recovered or not, divided by the total value of all remote transactions for the same type of payment instrument, whether authenticated with the application of strong customer authentication or executed under any relevant exemption in accordance with Articles 13 to 16 on a rolling quarterly basis (90 days);

(e) the calculation of the fraud rate and resulting figures shall be assessed by the audit review referred to in Article 3, ensuring that they are complete and accurate;

(f) the methodology and the model, if any, used by the payment service provider to calculate the fraud rates, as well as the fraud rates themselves shall be adequately documented and made fully available to competent authorities upon their request;

(g) the payment service provider has notified the competent authorities of its intention to make use of the transaction risk analysis exemption in accordance with this Article.

Article 17
Monitoring

1. Payment service providers that make use of the exemptions laid down in this Chapter shall record and monitor the following data for each payment instrument, with a breakdown for remote and non-remote payment transactions, at least on a quarterly basis (90 days):

(a) the total value of unauthorised payment transactions in accordance with Article 64(2) of Directive (EU) 2015/2366, the total value of all payment transactions and the resulting fraud rate, including a breakdown of payment transactions initiated through strong customer authentication and under the exemptions;

(b) the average transaction value, including a breakdown of payment transactions initiated through strong customer authentication and under the exemptions;

(c) the number of payment transactions where any of the exemptions was applied and their percentage in respect of the total number of payment transactions.

2. Payment service providers shall make the results of the monitoring in accordance with paragraph 1 available to competent authorities upon their request.

Article 18
Invalidation and optionality of exemptions

1. Payment service providers that make use of the exemption laid down in Article 16 shall cease to be exempted from the application of strong customer authentication for a given payment instrument where their monitored fraud rate exceeds for two consecutive quarters (180 days) the EUR 100 ETV reference fraud rate applicable for that payment instrument, as defined in the table in point (a) of Article 16(2).

2. Following non-compliance with the applicable reference fraud rate according to paragraph 1, payment service providers shall not be exempted from the application of strong customer authentication, in accordance with Article 16, until their

calculated fraud rate equals to, or is below, the EUR 100 ETV reference fraud rate applicable for that payment instrument, in accordance with the table in point (a) of Article 16(2), for one consecutive quarter (90 days).

3. Payment service providers that make use of the exemption in accordance with Article 16 shall immediately report to the competent authorities where one of their monitored fraud rates, for any given payment instrument, exceeds the applicable reference fraud rate , in accordance with the table in point (a) of Article 16(2), and shall provide to the competent authorities a description of the measures that they intend to adopt to restore compliance of their monitored fraud rate with the applicable reference fraud rates.

4. Payment service providers that ceased to be exempted from the application of strong customer authentication according to paragraph 1 and that intend to make use again of the exemption in accordance with Article 16 shall notify competent authorities, in a reasonable timeframe, before making use again of the exemption, providing evidence of restoration of compliance of their monitored fraud rate with the applicable reference fraud rate according to paragraph 2.

5. Payment service providers that make use of any of the exemptions set out in Article 10 to 16 may choose to apply strong customer authentication to the actions and to the payment transactions referred to in those provisions where they determine, according to the transaction monitoring mechanisms set out in Article 2, that a risk of unauthorised or fraudulent use of the payment instrument is increased.

CHAPTER 4
CONFIDENTIALITY AND INTEGRITY OF THE PAYMENT SERVICE USERS' PERSONALISED SECURITY CREDENTIALS

Article 19
General requirements

1. Payment service providers shall ensure the confidentiality and integrity of the personalised security credentials of the payment service user, including authentication codes, during all phases of authentication including display, transmission and storage.

2. For the purpose of paragraph 1, payment service providers shall ensure that each of the following requirements is met:

   (a) personalised security credentials are masked when displayed and not readable in their full extent when input by the payment service user during the authentication;

   (b) personalised security credentials in data format, as well as cryptographic materials related to the encryption of the personalised security credentials are not stored in Plaintext;

   (c) secret cryptographic material is protected from unauthorised disclosure.

3. Payment service providers shall fully document the process related to the management of cryptographic material used to encrypt or otherwise render unreadable the personalised security credentials.

4. Payment service providers shall ensure that the processing and routing of personalised security credentials and of the authentication codes generated in accordance with Chapter 2 take place in secure environments in accordance with strong and widely recognised industry standards.

Article 20
Creation and transmission of credentials

Payment service providers shall ensure that the creation of personalised security credentials is performed in a secure environment. Payment service providers shall mitigate 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.

Article 21
Association with the payment service user

1. Payment service providers shall ensure that only the payment service user is associated with the personalised security credentials, with the authentication devices and the software in a secure manner.

2. For the purpose of paragraph 1, payment service providers shall ensure that each of the following requirements is met:

(a) the association of the payment service user's identity with personalised security credentials, authentication devices and software is carried out in secure environments. In particular, the association shall be carried out in environments under the payment service 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 service provider. The environments under the payment service provider's responsibility include, but are not limited to the payment service provider's premises, the internet environment provided by the payment service provider or in other similar secure websites and its automated teller machine services;

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

Article 22
Delivery of credentials, authentication devices and software

1. Payment service providers shall ensure that the delivery of personalised security credentials, authentication devices and software to the payment service user is carried out in a secure manner designed to address the risks related to their unauthorised use due to their loss, theft or copying.

2. For the purpose of paragraph 1, payment service providers shall at least apply each of the following measures:

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

(b) mechanisms that allow the payment service provider to verify the authenticity of the authentication software delivered to the payment services user via the internet;

(c) arrangements ensuring that, where the delivery of personalised security credentials is executed outside the premises of the payment service 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 have to be activated before their first use, the activation shall take place in a secure environment in accordance with the association procedures referred to in Article 21.

Article 23
Renewal of personalised security credentials

Payment service providers shall ensure that the renewal or re-activation of personalised security credentials follows the procedures of creation, association and delivery of the credentials and of the authentication devices in accordance with Articles 20, 21 and 22.

Article 24
Destruction, deactivation and revocation

Payment service providers shall ensure that they have effective processes in place to apply each of the following security measures:

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

(b) where the payment service provider distributes reusable authentication devices and software, the secure re-use of a device or software 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 service provider's systems and databases and, where relevant, in public repositories.

CHAPTER 5
COMMON AND SECURE OPEN STANDARDS OF COMMUNICATION

SECTION 1
GENERAL REQUIREMENTS FOR COMMUNICATION

Article 25
Requirements for identification

1. Payment service providers shall ensure secure 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 service providers shall ensure that the risks against misdirection of communication to unauthorised parties in mobile applications and other payment services users' interfaces offering electronic payment services are effectively mitigated.

Article 26
Traceability

1. Payment service providers shall have processes in place which ensure that all payment transactions and other interactions with the payment services user, with other payment service providers and with other entities, including 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.

2. For the purpose of paragraph 1, payment service providers shall ensure that any communication session established with the payment services user, other payment service providers and other entities, including merchants, relies on each of the following:

   (a) a unique identifier of the session;

   (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 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 27
Communication interface

1. Account servicing payment service providers that offer to a payer a payment account that is accessible online shall have in place at least one interface which meets each of the following requirements:

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

   (b) account information service providers can communicate securely to request and receive information on one or more designated payment accounts and associated payment transactions;

   (c) payment initiation service providers can communicate securely to initiate a payment order from the payer's payment account and receive information on the initiation and the execution of payment transactions.

2. Account servicing payment service providers shall establish the interface(s) referred to in paragraph 1 by means of a dedicated interface or by allowing use by the payment service providers referred to in points (a) to (c) of paragraph 1 of the interface used for authentication and communication with the account servicing payment service provider's payment services users.

3. For the purposes of authentication of the payment service user, the interfaces referred to in paragraph 1 shall allow 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. In particular the interface shall meet all of the following requirements:

   (a) a payment initiation service provider or an account information service provider shall be able to instruct the account servicing payment service provider to start the authentication;

   (b) communication sessions between the account servicing payment service provider, the account information service provider, the payment initiation service provider and the payment service user(s) shall be established and maintained throughout the authentication; and

   (c) the integrity and confidentiality of the personalised security credentials and of authentication codes transmitted by or through the payment initiation service provider or the account information service provider shall be ensured.

4. Account servicing payment service providers shall ensure that their interface(s) follows standards of communication which are issued by international or European standardisation organisations. Account servicing payment service providers shall also ensure that the technical specification of the interface is documented and, as a

minimum, available, at no charge, upon request by authorised payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments or payment service providers that have applied with their competent authorities for the relevant authorisation. 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. Account servicing payment service providers shall make the summary of the documentation publicly available on their website.

5. In addition to paragraph 4, account servicing payment service providers shall ensure that, except for emergency situations, any change to the technical specification of their interface is made available to authorised payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments (or payment service providers that have applied with their competent authorities for the relevant authorisation) in advance as soon as possible and not less than 3 months before the change is implemented. Payment service providers shall document emergency situations where changes were implemented and make the documentation available to competent authorities on request.

6. Account servicing payment service providers shall make available a testing facility, including support, for connection and functional testing by authorised payment initiation service providers, payment service providers issuing card-based payment instruments and account information service providers, or payment service providers that have applied for the relevant authorisation, to test their software and applications used for offering a payment service to users. No sensitive information shall be shared through the testing facility.

Article 28
Obligations for dedicated interface

1. Subject to compliance with Article 27, account servicing payment service providers that have put in place a dedicated interface in accordance with Article 27(2), shall ensure that the dedicated interface offers the same level of availability and performance, including support, as well as the same level of contingency measures, as the interface made available to the payment service user for directly accessing its payment account online.

2. For the purpose of paragraph 1, the following requirements shall apply:

   (a) account servicing payment service providers shall monitor the availability and performance of the dedicated interface and make the resulting statistics available to the competent authorities upon their request;

   (b) where the dedicated interface does not operate at the same level of availability and performance as the interface made available to the account servicing payment service provider's payment service user for when accessing its payment account online, the account servicing payment service provider shall report it to the competent authorities, shall restore the level of service for the dedicated interface referred to in point (b) without undue delay and shall take any action that may be necessary to avoid its reoccurrence. The report shall

include the causes of the deficiency and the measures adopted to reestablish the required level of service;

(c) payment service providers making use of the dedicated interface offered by the account servicing payment service provider after reporting to the account servicing payment service provider may also report to the national competent authority any deficiency in the level of availability and performance required of the dedicated interface.

3. Account servicing payment service providers shall also ensure that the dedicated interface uses ISO 20022 elements, components or approved message definitions, for financial messaging.

4. Account servicing payment service providers shall include, in the design of the dedicated interface, a strategy and plans for contingency measures in the event of an unplanned unavailability of the interface and systems breakdown. The strategy shall include communication plans to inform payment service providers making use of the dedicated interface in case of breakdown, measures to bring the system back to business as usual and a description of alternative options payment service providers may make use of during the unplanned downtime.

Article 29
Certificates

1. For the purpose of identification, as referred to in point (a) of Article 21(1), payment service providers shall rely on qualified certificates for electronic seals as defined in Article 3(30) of Regulation (EU) No 910/2014[4] or for website authentication as defined in Article 3(39) of that Regulation.

2. For the purpose of this Regulation, the registration number as referred to in the official records in accordance Annex III (C) of Regulation (EU) No 910/2014 shall be the authorisation number of the payment service provider issuing card-based payment instruments the account information service providers and payment initiation service providers, including account servicing payment service providers providing such services, available in the public register of the home Member State pursuant to Article 14 of Directive (EU) 2015/2366 or resulting from the notifications of every authorisation granted under Article 8 of Directive 2013/36/EU[5] in accordance with Article 20 of that Directive.

3. For the purposes of this Regulation, qualified certificates for electronic seals or for website authentication referred to in paragraph 1 of this Article shall include in English additional specific attributes in relation to each of the following:

(a) the role of the payment service provider, which maybe one or more of the following: an account servicing payment service provider; a payment initiation service provider; an account information service provider; a payment service provider issuing card-based payment instruments.

[4] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 53).

[5] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 26.6.2013, p. 338).

(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 electronic seals or website authentication.

Article 30
Security of communication session

1. Account servicing payment service providers, payment service 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 access sessions offered by account servicing payment service providers as short as possible and they shall actively terminate the session with the relevant 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(s) in order to prevent the possibility that any message or information communicated between them could be misrouted.

4. Account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments with the account servicing payment service provider shall contain unambiguous reference to each of the following items:

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

(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, payment initiation service providers and payment service providers issuing card-based payment instruments shall ensure that where they communicate personalised security credentials and authentication codes, these are not readable by any staff at any time. In case of loss of confidentiality of personalised security credentials under their sphere of competence, account information service providers, payment initiation service providers issuing card-based payment instruments and payment initiation service providers shall inform without undue delay the payment services user associated with them and the issuer of the personalised security credentials.

Article 31
Data exchanges

1. Account servicing payment service providers shall comply with each of the following requirements:

   (a) they shall provide 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 requesting access to the account information, provided that this information does not include sensitive payment data;

   (b) they shall provide, immediately after receipt of the payment order, payment initiation service providers with the same information on the initiation and execution of the payment transaction provided or made available to the payment service user when the transaction is initiated directly by the latter;

   (c) they shall, upon request, immediately provide payment service providers with a confirmation whether the amount necessary for the execution of a 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 payment initiation service provider or the account information service provider and the payment service provider issuing card-based payment instruments which explains the reason for the unexpected event or error. Where the account servicing payment service provider offers a dedicated interface in accordance with Article 28, the interface shall provide for notification messages concerning unexpected events or errors to be communicated by any payment service provider that detects the event or error to the other payment service providers participating in the communication session.

3. Account information service providers shall have in place suitable and effective mechanisms that prevent access to information other than from 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 initiating the payment transaction directly, unless the collection of additional information for the purposes of the provision of the payment initiation service is agreed otherwise between payment initiation service provider, payer, and account servicing payment service provider.

5. Account information service providers shall be able to access information from designated payment accounts and associated payment transactions held by account servicing payment service providers for the purposes of performing the account information service in either of the following circumstances:

   (a) whenever the payment service user is actively requesting such information;

   (b) where the payment service user is not actively requesting such information, no more than four times in a 24 hour period, unless a higher frequency is agreed

between the account information service provider and the account servicing payment service provider, with the payment service user's consent.

CHAPTER 6
FINAL PROVISIONS

Article 32
Review

Without prejudice to Article 98(5) of Directive (EU) 2015/2366, in accordance with Article 10 of Regulation (EU) No 1093/2010 EBA shall review and, if appropriate, propose updates to the fraud rates referred to in Article 16 of this Regulation by 18 months after the date of application referred to in Article 33.

Article 33
Entry into force

1. This Regulation shall enter into force on the 20th day following that of its publication in the *Official Journal of the European Union*.
2. This Regulation shall be binding in its entirety and directly applicable in all Member States.
3. This Regulation shall apply from [OJ please add date corresponding to '18 months after entry into force date'].

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

Done at Brussels,

For the Commission

The President
Jean-Claude Juncker

4. Accompanying documents

4.1 Cost-benefit analysis and 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, also hampering the cross-border purchase of goods and services by EU consumers. Besides this imperfect competition between PSPs in Europe, the retail payments market has been found to be lacking an effective, transparent and secure governance framework, to the detriment of consumers. [6]

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.[7] 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[8], has increased significantly in recent years. Also, a quarter of European consumers indicates a subdued level of confidence regarding the security of their payment card details when shopping online.[9] Those observations reflect a barrier to the flourishing of the European digital economy.

[6] GREEN PAPER on retail financial services Better products, more choice, and greater opportunities for consumers and businesses, COM/2015/0630 final;, GREEN PAPER Towards an integrated European market for card, internet and mobile payments,
COM/2011/0941 final.

[7] EBA: Consumer trends report 2016, published 21 June 2016; Discussion Paper on future Draft Regulatory Technical Standards on strong customer authentication and secure communication under the revised Payment Services Directive (PSD2), published 08 December 2015.

[8] ECB: Fourth report on card fraud, July 2015, https://www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf

[9] 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[10]. They are developed with a view to increasing the efficiency and security of financial services and the protection of consumers in the EU[11].

PSD2 provides that these draft RTS shall be developed by the 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[12]. 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 continue to increase, with possible breakdowns of confidence if adverse scenarios become material at a larger scale or more frequently.

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, has been assessed by EU legislators as insufficient to address the risks and problems identified. This is in particular owing 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 and card payments at the physical point of sale). To fill this gap while PSD2 negotiations were ongoing, the EBA decided to address the security of internet payments which are comprehensively covered by the EBA's Guidelines on the Security of Internet Payments (EBA GL/2014/12)). PSD2 aims to reflect the changes to the payment market through innovation and the entry of new players to ensure a safe and competitive environment to thrive, laying down a number of legal rights and obligations for the different actors. PSD2 has in turn mandated the EBA to develop these RTS on authentication and

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

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

[12] ECB, Fourth report on card fraud, July 2015, https://www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf

communication between service providers with the same objective in mind. The existing legal framework, including the EBA guidelines, remains in force until the adoption and entering into force of these RTS.

D. Options considered

Developing these draft RTS, the EBA has considered a set of technical options, related to the following

1. SCA

   - Develop principle-based and technology-neutral 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 exemptions with which PSPs are obliged to comply (option 2.1.1)

   - Develop exemptions which PSPs may decide to apply unless they identify a risk of fraud or other abuses. (option 2.1.2)

   - Develop a very narrow list of risk-based exemptions (option 2.2.1)

   - Develop a broader list of risk-based exemptions (option 2.2.2)

3. Protection of the personalised security credentials (PSC)

   - Develop principle-based and technology-neutral 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 PSPs

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

   - Develop clear principle-based and technology-neutral requirements for access to the payment account (Option 4.1.2)

   - Require identification using a certificate issued by an eIDAS qualified trust service provider (Option 4.2.1)

   - Allow identification using a certificate issued by a general certificate authority (Option 4.2.2)

E. Assessment and preferred options[13]

The requirements in these draft RTS affect a broad range of stakeholders, such as providers in the payment service market (ASPSPs, AISPs, PISPs, other PSPs) 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, short-term or long-term effects. Given the broad range and diverse interests of the stakeholders possibly concerned, the summary below 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, SCA, 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 as the provision of new payments solutions in Europe, authentication requirements should be developed in the form of high-level and technology-neutral principles, to facilitate adaptability to emerging security threats and implementation of innovative security solutions. With authentication solutions being developed by the PSPs (option 1.1), it can also be reasonably expected that consumer convenience is addressed intrinsically. Developing high-level principles also ensures that, while there are likely to be some initial costs, the EBA would not expect recurring costs as high-level principles enable some flexibility and room for future improvements and innovation without the providers needing to make significant changes to fit the regulatory framework. In addition, high-level and technology-neutral principles do not discriminate between providers and therefore their costs.

Regarding the second consideration, the scope of exemptions, the EBA has duly considered increasing the security of payments, contributing to lowering the level of fraud and ensure fair competition between PSPs. Against this background, compulsory exemptions would not satisfy the security and fraud objectives as PSPs would not have any flexibility in deciding to use SCA if a risk was detected even though an exemption could apply. The EBA therefore proposes a list of possible exemptions from SCA which PSPs may decide to apply, subject to the outcome of the provider's own transaction risk analysis. This solution (option 2.1.2) is expected to provide a sufficient level of legal clarity, at the same time facilitating optimal protection of consumers by granting PSPs discretion to apply full customer authentication requirements if their transaction analysis identified an elevated level of risk (of fraud or other form of abuse). Similarly, providers also need to have some flexibility,

[13] As a background, in particular also concerning the rationale behind mandating the EBA to develop these draft RTS on strong customer authentication and communication, see 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)

where lower risks are identified to apply another form of authentication than SCA. The EBA has therefore chosen an option with a longer list of exemptions, technology-neutral where applicable (option 2.2.2). 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 and technology-neutral approach to protecting confidentiality and integrity in the creation, association with PSUs, delivery, renewal and destruction of PSCs (option 3.1). Also, and against the background of the mandates given to the EBA under PSD2, Article 95 PSD2 (Development of Guidelines on Management of Operational and Security Risks) and to the Commission under Article 106 (Development of an electronic leaflet), these draft RTS focus on requirements that are 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 accounts 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 (ASPSPs, AISPs, PISPs) render it necessary for EBA to adopt high-level principles which give sufficiently concrete guidance for the communication between stakeholders involved in the payment service market, as well as clear but technology-neutral requirements for the ASPSPs, in line with PSD2, to ensure that TPPs, AISPs and PISPs in particular, can access the information they need to provide services to their customers (option 4.1.2).

It should also be noted, that PSD2 sets out that, once the Commission has adopted the EBA's RTS, market participants have another 18 months until the RTS apply. As a result, and depending on the speed with which the EBA's RTS are adopted, the RTS will apply from November 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 PSD2 can be achieved.

In addition, technical choices need to be made regarding the identification of ASPSPs, PSPs, AISPs and PISPs when communicating. That identification could be either based on certificates issued by a qualified trust service provider under eIDAS or based on certificates issued by a general certificate authority. To maximise the 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 to increased competition, cross-border activities and efficiency in the market for retail payment services while at the same time sufficiently protecting consumers and ensuring the security of payments. In particular, sufficient protection against fraud and theft of confidential customer information has

been carefully considered in the development of these draft RTS. Its net overall impact is expected to be beneficial for PSPs, consumers and businesses.

4.2 Views of the Banking Stakeholder Group

1 The Banking Stakeholder Group (BSG) made a number of comments on the draft RTS and, reflecting the general diversity of comments received, also expressed some conflicting views between BSG members.

2 As a general principle the BSG expresses its preference for 'setting out objectives at a reasonably high level' focusing on outcomes rather than specific solutions because the area of IT security is so fast moving. The BSG has accordingly suggested a number of changes to ensure that the rules would rapidly and adequately adapt to changes. For instance:

- it took issue with the concept of a 'unique authentication code' as privileging one technical solution.
- it also challenged listing a number of characteristics in relation to knowledge authentication as not technologically neutral.
- it suggested a more general phrasing than 'tamper resistance devices and environments'.
- Finally, it expressed its disagreement with the requirement of complying with the standard ISO 27001 for the entire PSP industry when it comes to the processing and routing of the Payment Security Credentials. The BSG also mentions that it might be preferable not to refer to ISO20022.

However, the submission also highlights that some members did not think there was any such need and thought that the current balance in the draft RTS as published in August 2016 was adequate.

3 With regard to exemptions from the principle of SCA, the BSG commented on three main areas:

- The BSG calls for the addition of a transaction-risk analysis exemption, citing innovation and PSPs' more detailed understanding of the risks posed. It also argued that the ASPSP alone should be able to trigger such an exemption. The response also, however, also points out that some of the BSG members disagreed with the introduction of such an exemption on the basis of simplicity for consumers.
- The BSG calls for an increase in the low-value exemption for remote transactions up to EUR 50, in line with the contactless exemption, for simplicity, as well as to enable faster transactions with less user friction. Again, however, the response highlights that some members were opposed to such an increase and that other suggested that the EBA reviews the threshold yearly.
- With regard to the white list exemption, the BSG suggests adapting the drafting to ensure encompassing a PSP-assisted creation of the whitelist (rather than creation solely by the payer directly).

4 With regard to access, and in particular the frequency of information requests, BSG suggested a distinction between individual requests and bulk automated service requests, whereby the latter could be less frequent. It also suggested developing systems that proactively update registered applications when changes occur.

5 Finally, the BSG requested clarification in a number of areas including the application of the liability rules under article 74(2) PSD2, the extent to which PSPs could control the security in multi-purpose devices and the reasoning behind limiting article 10 to card-based payment transactions only.

4.3 Feedback on the public consultation and on the opinion of the BSG

1 PSD2, which entered into force on 12 January 2016 and applies from 13 January 2018, 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 PSD2 lays down that that EBA shall develop, in close cooperation with the ECB, draft RTS specifying the requirements of SCA, the exemptions from the application of SCA, the requirements with which security measures have to comply in order to protect the confidentiality and the integrity of the PSUs' personalised security credentials, and the requirements for common and secure open standards of communication between ASPSPs, PISPs, AISPs, payers, payees and other PSPs.

2 In order to deliver this mandate, the EBA sought early input from the market, national authorities and the BSG to understand the issues they were facing, including by publishing late 2015 a DP on the subject. Having analysed this input, the EBA published a CP in August 2016 with draft RTS on SCA and common and secure communication. The consultation period lasted for two months and ended on 12 October 2016. A total of 224 responses were received, of which 148 were published on the EBA website.

3 This paper presents a summary of the key points and other comments arising from the consultation, the analysis and discussion triggered by these comments, and the actions taken to address them if deemed necessary.

4 In many cases several industry bodies made similar comments or the same body repeated its comments in the response to different questions. In such cases, the comments, and the EBA's analysis are included in the section of this paper where the EBA considers them most appropriate.

5 Changes to the draft RTS have been incorporated as a result of the responses received during the public consultation.

4.3.1 Summary of key issues and the EBA's response

1. Typically, while some respondents wished further detail to be included in the RTS to ensure inter-operability, others took the opposite view, asking for the draft RTS to allow for future

developments and innovation. For instance, the BSG argued in favour of 'setting out examples at a reasonably high level'. The EBA concurs that at times the draft RTS may have been too specific and as a result no longer technology-neutral. Changes have been made in a number of areas to that end. In some areas, such as communication interface, there was an identifiable split of responses between credit institutions (as well as other payment service providers) on the one hand and TPPs on the other. By contrast, in other areas, the respondents from all the different sectors, although not all consumer groups, concurred in requesting the EBA to make a specific change, for example adding what many have been referred to as TRA as an exemption to SCA. These distinctions are reflected in the response submitted by the BSG where at times conflicting views are detailed.

2. All members of the BSG agreed that the general principle of liability in Article 74(2) PSD2 applies before and after the transitional period. The EBA concurs with this view. By contrast, for instance, views differed on the low-value exemption, some arguing in favour of an increase of the threshold on the basis of user simplicity and costs while others argued against it on the basis that consumers were sufficiently familiar with SCA. Similar split views were expressed with regard to the need for a TRA exemption, some BSG members arguing against it on the basis of simplicity for consumers, while others argued in favour of it to ensure better competition in the market.

3. The main areas of discussion focused on (1) the scope of the draft RTS and technology-neutral requirements, (2) the exemption, including scope, thresholds and the request to add an exemption for transactions identified as low risk as a result of TRA analysis, and (3) the access to payment accounts by third party providers, including the requirements on information sharing.

4. A number of comments sought clarification with regards to the overall scope of the RTS. This is by and large a matter of PSD2 interpretation, and clarification has been provided in the rationale as well as in a large number of responses to respondents' comments in the feedback table.

5. A number of the responses queried the technology neutrality of a number of measures and suggested an approach that would be at a higher level. The EBA concurs with the view of the participants that, in order to ensure technology and business-model neutrality and to allow PSPs to be able to continuously adapt to evolving fraud scenarios, the draft RTS should be positioned at a higher level in a number of instances (including by deleting the reference to a number of specific standards or technology solutions as well as deleting requirements for the three elements constituting SCA which reflect current practices).

6. A very large number of comments focused on the exemptions, including their scope, the PSPs that can use the exemptions, the detailed exemptions themselves and further exemptions that a number of respondents suggested adding. The large majority of the comments suggested the draft RTS should allow for an exemption based on transaction-risk analysis, although consumer groups expressed concerns about doing so. The EBA concurred with the view expressed by these respondents that a risk-based approach, including the ability to conduct detailed TRA and fraud monitoring, is essential to achieve the objective under PSD2 of reducing fraud. Consequently the EBA arrived at the view that, in accordance with Article 98(2)(a) of PSD2, an exemption based on such an analysis should be added in a new Article 16 RTS. The RTS also reiterates the importance

of risk and fraud monitoring in general as a necessary complement to the principle of SCA laid out in PSD2 as stated in a new Article 2 of the RTS. While under PSD1, transactions with low levels of risk could be exempted from strong authentication in line with the EBA guidelines on internet payments, in a post-PSD2 world where SCA is the principle for all transactions, the balance has changed and any exemption in the RTS would need to be defined narrowly as explained in the previous paragraph. Consequently it decided, in accordance with Article 98(2)(a) of PSD2, to include such analysis; it ensured that consumers were protected by requesting payment service providers that would want to use such exemption to have fraud rates that are lower or equivalent to given reference fraud rates set lower than current average fraud levels in the industry. The EBA acknowledges that this exemption will require in-depth supervision.

7. Finally, with regard to access, the majority of answers received on this topic focused on the communication exchanges, frequency of request and type of information shared between AISPs, PISPs, PSPs issuing card-based payment instruments, and ASPSPs. There was in general a difference of views between ASPSPs and TPPs. For instance, TPPs wished more information to be shared and that this information be shared more frequently. A number of comments from TPPs, and payment initiation service providers in particular, requested clarity on the modality of access to payment accounts and in particular clarification on whether 'screen scraping' (also sometimes erroneously referred to as 'direct access') would be allowed. While these providers did not appear to be opposed to communication via a dedicated interface, they considered it essential to remain free to have access to payment accounts in other ways, particularly in the event that a dedicated interface would not be working properly. After consulting with the Commission on the most plausible interpretation of the Directive, the EBA is of the view that the accessing of accounts through screen scraping will no longer be allowed once the transitional period comes to an end, on the basis of a number of provisions under PSD2. The EBA is of the view that it is very important for the AISPs, PISPs and PSPs issuing card-based payment instruments to be able to initiate a payment order, to access information, or to obtain the information they are entitled to under PSD2 when they provide their payment services to their customers. This legal right shall not be intentionally diminished. The EBA has, to that end, added a new Article 28 requiring ASPSPs, if they choose to develop and offer a dedicated interface, to provide the same level of availability and performance as the interface offered to and used by their customers (e.g. online banking), as well as to provide the same level of contingency measures in case of unplanned unavailability. The EBA recognises that it is also important to balance out the technical method of access (and business-model neutrality) with the security measures under PSD2, including the requirements under PSD2 that AISPs, PISPs, PSPs issuing card-based payment instruments and ASPSPs providing AIS and PIS shall identify themselves to the ASPSP and that AISPs, PISPs, PSPs issuing card-based payment instruments and ASPSPs shall communicate securely with each other.

4.3.2 The EBA's response to the Banking Stakeholder Group's submission

1. As described in section 4.2, the BSG made a number of comments on the draft RTS which are addressed below.

2. The BSG expressed its preference for outcome-focused, rather than specific, solutions. As described in the summary of the comments and the EBA's responses above, the EBA concurs that in a number of cases in the draft RTS it would indeed be preferable. As a result, the EBA has deleted the reference to specific characteristics for the knowledge element of the SCA and the reference to 'tamper resistance devices and environments'. It has also deleted the reference to ISO 27001, has limited the use of ISO 20022 to the message template, as the EBA is of the view that some standardisation in this area is needed, and has clarified in recital (4) that the authentication code can be generated in different ways, remaining technologically neutral.

3. With regard to exemptions from the principle of SCA, the EBA concurs with the view that a TRA exemption should be added. It has done so with a clear and objective focus on fraud rates, using lower rates than currently achieved, to ensure consumers are protected against fraud. The EBA discussed the low-value exemption and came to the view that the threshold was slightly low but also disagreed with setting it at the same level as for contactless payments, as the EBA believes that the risk posed is different and higher. The threshold agreed was EUR 30. The EBA concurs with the suggestion made by the BSG on adding PSP-assisted creation of a whitelist and the exemption has been redrafted accordingly.

4. With regard to access, and in particular the frequency of information requests, the draft already distinguishes between individual active requests and automatic requests. The EBA has not made any further amendments. The revised draft, however, has increased the number of automatic requests from two to four a day. The EBA agrees that at the implementation stages ASPSPs may consider different models such as push notifications or other systems that proactively update registered applications when changes occur.

4.3.3 Summary of responses to the consultation and the EBA's analysis

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Chapter 1 (now Chapter2)			
Feedback on responses to Question 1			
[1] Article 1 (now Article 4 in the revised draft RTS)	Many respondents requested that a distinction be made between authentication and authorisation codes because, in their view such codes relate to different processes (see also: [274] General responses).	*The payment process contains three phases: authentication, authorisation by the payer and authorisation by the PSP of the payer. The first two are within the scope of the RTS while the last is not.* *Authentication refers to a procedure that allows the PSP to verify a customer's identity.* *Authorisation refers to a procedure that checks whether or not a customer or PSP has the right to perform a certain action, e.g. to transfer funds or have access to sensitive data.* *In order to authorise a payment transaction initiated by a Payer, and to execute it, the payer's PSP needs to authenticate the payer to make sure that it is really the payer and that the payer gives its consent.*	*None*
[2] Article 1 (now Article 4)	Some respondents interpreted Article 1 as suggesting that magnetic stripe card transactions will no longer be allowed once the RTS apply, including as a fall-back option, which in their view could create hardship or inconvenience for consumers, particularly for consumers shopping within the EEA who come from non-EEA member which may not have the chip and pin technology or for EEA card holders when paying at non-EEA POS terminal or websites. This could therefore affect international commerce.	*The security requirement established in PSD2 is SCA. Further details are set out in Article 4 (former Article 1) RTS. Most variants of magnetic stripe cards currently in operation are unlikely to fulfil the relevant criteria under SCA, including as fall-back solutions.* *The EBA interprets PSD2 as meaning that the payee's PSP has the option not to accept SCA, not only during the transitional period between the application date of PSD2 (13 January 2018) and the application date of the RTS under consultation (in November 2018 at the earliest), but also after that period has ended within the limits of the applicable exemptions. In the case of cross border transactions, however, where payment instruments issued under a national legal framework that does not require the use of SCA (such as*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		magnetic stripe cards) are made within the EU or when the PSP of the acquirer is established in a jurisdiction where it is not legally required to support SCA designed by the European issuing PSP, the European PSPs shall make every reasonable effort to determine that the payment instrument is used legitimately.	
[3] Article 1(2)(b) (now Article 4(2)(b))	One respondent argued that the term 'generated for the same payer' should be deleted, given that an authentication code should not be derivable from a previous one independent of the payer.	*The EBA agrees with this comment and has changed the RTS.*	*Article 4(2)(b):* *'(b) it is not possible to generate a new authentication code based on the knowledge of ~~another~~ <u>any other</u> authentication code <u>previously</u> generated ~~for the same payer~~;'*
[4] Article 1(3)(a) (now Article 4(3)(d))	Several respondents suggested that the term 'time out' in Article 1(3)(a) can have several meanings, such as inactivity time-out, session time-out, and that the RTS should specify which of them is being referred to.	*The EBA agrees with this comment and has clarified the provision. In the process, a time limit of five minutes was also defined and the requirement has been moved from (a) to (d) to follow the consequential order.*	*Article 4(3)(d):* *<u>'a maximum time without activity by the payer after being authenticated for accessing its payment account online shall not exceed five minutes.</u>* *Article 1(3)(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");~~*
[5] Article 1.(3)(b) (now Article 4(3)(a))	Several respondents were of the view that the current model of transaction failure feedback for card transactions, i.e. "wrong PIN message" should be kept to avoid confusion for the payer and payee.	*The EBA agrees with the comment but only for the non-remote payments, and has altered the relevant provision by introducing a reference to remote access and payments.*	*Article 4(3)(a):* *<u>'where the authentication for remote access, remote electronic payments and any other actions through a remote channel which may imply a risk of payment fraud or other abuses has failed to generate an authentication code for the purposes of paragraph 1, none of the elements categorised as knowledge, possession and inherence</u> ~~of strong customer~~*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			~~authentication~~ can be identified as incorrect~~, where the authentication procedure has failed to generate an authentication for the purposes of paragraph 1~~;'
[6] Article 1(3)(d) (now Article 4(3)(c))	Several respondents suggested that the reference to 'HTTPS over TLS' should be avoided as it is not technologically neutral and tthe technology may change in the future, making the reference obsolete. Relatedly, other respondents suggested that the RTS be more specific, such as by prescribing a specific version of these standards, as they deem some older versions of TLS to be insecure.	*The EBA agrees with deleting the reference to 'HTTPS over TLS'. The RTS as proposed attempted to balance a number of objectives that are at times conflicting. In this case we believe that a higher degree of prescription would undermine the objectives of technology neutrality and future proofing.*	*Article 4(3)(c):* *'the ~~protect~~ communication sessions are protected against the capture of authentication data transmitted during the ~~authentication procedure or,~~ and against manipulation by unauthorised parties, in accordance with the requirements in Chapter 5 ~~communication including but not limited to by relying where applicable on HTTP over TLS~~.'*
[7] Article 1(3)(e) (now Article 2)	Several respondents suggested that the requirement to have transaction monitoring mechanisms in place to prevent, detect and block fraudulent payment transactions should not be placed in Article 1 (3) [now Article 4 (3)] as this paragraph relates to SCA while the respondents considered such mechanisms to be more related to the authorisation rather than the authentication procedure. In the respondents' view, the provision seems to be intended to counter fraud during the whole transaction process. Some respondents also argued that some of these requirements might be overly prescriptive, e.g. Article 1(3)(e)(ii): Difficulty in detecting signs of malware in some contexts, e.g. signs of malware infection in certain card POS terminals. Some respondents also noted that the repeated references to 'customer device' (in (e)(iv) and (v)) which refers to 'payer's device' could be clarified.	*The EBA agrees with the general comment that the requirement to have monitoring mechanisms in place was not appropriately located under Article 1(3)(e) as the requirement is broader than at the authentication stage only. The EBA has therefore amended the text, by converting this point into a new Article 2 to provide greater clarity about its purpose. The EBA has also established a clear link with Article 16, which contains a new exemption based on transaction risk analysis (TRA) and monitoring.* *The EBA disagrees, however, with the view that to authorise the payment transaction initiated by a payer, and to execute it, the payer's PSP needs to authenticate the payer to make sure that it is the payer.* *The PSD2 requires this authentication to be 'strong'. PSD2's mandate refers to setting requirements on the authentication procedure for it to be considered strong. One such requirement is that the authentication should be used to improve the security of the payment transaction by containing processes that prevent fraud.* *The terminology used is consistent with other parts of the*	*Article 2:* *'General authentication requirements* *1. For the purpose of the implementation of the security measures referred to in letters (a) and (b) of Article 1, payment service providers shall have transaction monitoring mechanisms in place that enable them to detect unauthorised or fraudulent payment transactions.* *2. The transaction monitoring mechanisms shall be based on the analysis of payment transactions taking into account elements which are typical of the payment service user in the circumstances of a normal use by the payment service user of*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		RTS.	*the personalised security credentials.* *3. Payment service providers shall ensure that the transaction monitoring mechanisms takes into account, at a minimum, each of the following risk-based factors: lists of compromised or stolen authentication elements; the amount of each payment transaction; known fraud scenarios in the provision of payment services; signs of malware infection in any sessions of the authentication procedure.* *4. Where payment service providers exempt the application of the security requirements of the strong customer authentication in accordance with Article 16, in addition to the requirements in paragraphs 1, 2 and 3, they shall ensure that the transaction monitoring mechanisms take into account, at a minimum, and on a real-time basis each of the following risk-based factors: the previous spending patterns of the individual payment service user; the payment transaction history of each of the payment service provider's payment service user; the location of the payer and of the payee at the time of the*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			payment transaction providing the access device or the software is provided by the payment service provider; the abnormal behavioural payment patterns of the payment service user in relation to the payment transaction history; in case the access device or the software is provided by the payment service provider, a log of the use of the access device or the software provided to the payment service user and the abnormal use of the access device or the software.' *~~The strong customer authentication procedure shall include mechanisms to:~~* *5. ~~prevent, detect and block fraudulent payment transactions before the PSP's final authorisation. These mechanisms shall take into account, but not be limited to:~~* *6. ~~parameterised rules, including black lists of compromised or stolen card data,~~* *7. ~~signs of malware infection in the session and known fraud scenarios,~~* *8. ~~an adequate transaction history of the payer to evaluate its typical spending behavioural patterns,~~* *9. ~~information about the customer~~*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			~~device used,~~ *10. ~~a detailed risk profile of the payer and/or the payer's device.~~*
[8] Article 6(2) (now Article 9(2))	Several respondents requested clarification of the concept of segregation of channels, devices or mobile applications as they argued that a uniform interpretation by the market was required to ensure a level playing field for the different stakeholders. The same concerns were expressed with regards to article 2(2)(b) – see further detail under [10] More specifically, the respondents mentioned the following concerns: i) the respondents pointed out that multi-purpose devices themselves are out of the PSP 'scope' of influence; some platforms might render the separation (or some specific requirements) not feasible , which would prevent mitigation of the risks associated to these devices being compromised. ii) some of the respondents thought that customers should not be allowed to use their personalised security credentials issued by the ASPSPs in any other website, application or channel than the secure online environment of the ASPSP. iii) Respondents were concerned that when initiating the transaction via PISP, the ASPSP would not have information on the device, environment or payer. They therefore suggested the RTS should require the PISP to collect the risk-related information and forward it to the ASPSP although they acknowledged that this may pose confidentiality issues. iv) some of the respondents argued that the segregation may not be necessary if the whole environment is secure. For example, segregation is not required when the entire transaction process is encrypted end-to-end, with a two-factor authentication and a dynamic linking between the transaction amount and the payee. Furthermore, commenting on Article 6 (3), they argued that mandating some form of uniform security protocol, as the reference to 'trusted execution environments' suggests, may hinder innovation in the authentication and ID solutions industry.	*Article 6(2) (now Article 9(2)) does not refer to segregation, only Article 2.2.b does. See comments [10] and [11] on that. The EBA has therefore not made any changes to the Article.* *However, in relation to comment i), the EBA agrees that PSPs can mitigate only the risks within their realm of competence. The EBA has made changes to Article 6(3) (now Article 9(3)) to specify that the focus is on the software used by the PSP rather than the hardware itself.* *With regard to comment ii), the EBA is of the view that banning customers from ever using the same personalised security credentials would be overly invasive and might create new types of security issues if they were not able to remember all their credentials. In addition, PSD2 (recital 30 and Article 66) specifically allows AISPs and PISPs to use the credentials issued by the ASPSP.* *With regard to comment iii), the EBA would like to point out that requiring PISPs to share risk-related information with the ASPSPs is out of the scope of the RTS. The industry may wish to consider it in the implementation phase if deemed appropriate.* *With regard to comment iv), the EBA agrees that the concept of segregation was confusing. It has deleted the sentence to avoid confusion. The EBA also agrees that the reference to 'trusted execution environments' in Article 6(3) would not be technologically neutral and has replaced 'trusted' with 'secure'.*	*No change to Article 6(2)(now Article 9(2))* *Changes to Art. 6(3)(a) (now Article 9(3)):* *1. 'For the purposes of paragraph 2, the mitigating measures shall include <u>each of the following</u> ~~but not be limited to~~:* *a) the <u>use</u> ~~implementation~~ of separated ~~trusted~~ <u>secure</u> execution environments <u>through the software installed</u> inside the multi-purpose device;* *b) mechanisms to ensure that the software or device has not been altered by the payer or by a third party or mechanisms to mitigate the <u>consequences of</u> ~~risks related to~~ such alteration where this has taken place.'*
Feedback on responses to Question 2			
[9] Article 2(2)(a) (now	A number of respondents asked for clarification on what the 'change of	*The requirement intends to ensure the integrity of the link itself. The EBA agrees that it is a little unclear and has*	*Article 2(2)(a) (now 5(2)(a)):* *'For the purpose~~s~~ of paragraph 1,*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Article 5(2)(a))	the authentication code' requirement in Article 2 (2)(a) refers to. They were unclear whether it related to a property of the code or a process control.	*changed the wording of the Article as a result.*	*payment service providers shall adopt security measures ~~the authentication procedure shall~~ which ensure the confidentiality, authenticity and integrity of each of the following ~~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~~;'*
[10] Article 2(2)(b) (now Article 5(2)(b))	A large number of respondents, while generally agreeing with the reasoning on neutrality, at least with respect to timing of the dynamic linking, asked for further clarification regarding the independence and segregation of channels. Many of the respondents understood the segregation requirement in Article 2(2)(b) to mean that people would have to use multiple devices to be able to perform SCA. The respondents demanded that the RTS allow PSPs to use a single device. The respondents proposed the following changes to the draft: • *completely deleting the second sentence of Article 2(2)(b)* • *simply deleting the reference to the "mobile" application* • *mandating 'logical' independence or segregation.* • *A risk based approach to when stricter segregation should be applied.*	*As explained at the public hearing the EBA is of the view that the independence of the elements constituting SCA does not require different devices and can be hosted on the same device.* *The EBA agrees with the respondents that the requirement was unclear and confusing. In line with some respondents' redrafting suggestions, it has deleted the reference to segregation.* *The EBA has also clarified the meaning of the independence of the elements when using a multi-purpose device by adding some text in recital (4) (now recital (6)).*	*Changes to Art. 2(2)(b) (now Article 5(2)(b)):* *'For the purpose~~s~~ of paragraph 1, payment service providers shall adopt security measures ~~the authentication procedure shall~~ which ensure the confidentiality, authenticity and integrity of each of the following ~~have in place technological solutions ensuring~~:* *(b) ~~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. ~~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~~*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			~~*channel, device or mobile application used for initiating the electronic payment transaction.'*~~ *New recital (6) (former recital (4)):* *'In order to ensure the application of strong customer authentication, it is also* ~~*It is*~~ *necessary to require adequate* ~~*define the*~~ *security features for* ~~*of*~~ *the elements of strong customer authentication categorised as knowledge (something only the user knows),* *such as length or complexity, for the elements categorised as possession (something only the user possesses), such as algorithm specifications, key length and information entropy, and for the devices and software that read elements categorised as inherence (something the user is) such as algorithm specifications, biometric sensor and template protection features* ~~*for the application of strong customer authentication,*~~ ~~*as well as requirements,*~~ *in particular to mitigate the risk that those elements are uncovered, disclosed to and used by unauthorised parties. It is also necessary to define 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*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			through a multi-purpose device, i.e. a device such as a tablet or mobile phone used which can be used both for giving the instruction to make the payment and for being one of the elements used in the authentication process.'
[11] Article 2(2)(b) (now Article 5(2)(b))	Some respondents asked the EBA to clarify several aspects related to the SCA procedure. They have in particular asked the EBA to include several segregation techniques, in addition to those already mentioned in the RTS, as a way of enhancing the possibility of using a sole device in the SCA procedure (especially in the case of multipurpose devices). Among other mechanisms, the respondents have suggested: - secure Element (SIM or dedicated chip) for storage of sensitive data, accessible only by PSU and authorized app; - app-separation or sandboxing; - remote security updates, to prevent or react on possible weaknesses; - hardening of an app / secure coding; - white-box cryptography; - device binding (secure activation of an app for use by only one PSU on only one device), based on continually refreshed data elements or challenge/response; - detection of mobile malware and fraud on the device; and - app-store monitoring (for malicious apps)	*As explained in comment [10] the EBA takes the view that the independence of the elements constituting SCA does not require different devices and they can be hosted on the same device. In other words, it does not dispute this possibility. Most of the respondents' suggestions focus on specific segregation techniques within a single device. While those comments and suggestions may be considered at the implementation stage if the industry deems it appropriate, the EBA believes that a higher degree of prescription would undermine the objectives of technology neutrality and future proofing of the RTS themselves and has therefore not provided any further detail in the RTS.*	*None*
[12] Article 2(3) (now Article 5(3))	Some respondents requested that the requirements in Article 2(3) be extended to all payment transactions without restricting them to card payment transactions.	*The EBA does not agree with this comment, as the relevant Level-1 text (Article 75 PSD2) refers to card-based payment transactions only.*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
[13] Article 2(4) (now Article 5(4))	Some respondents requested that 'batch payments' be defined and that the treatment of some particular cases (multiple currencies, fees and exchange rates, split orders, etc.) be clarified.	*The EBA believes that batch payments are well-known in the industry and does not find it necessary to add any further detail.* *With regard to the comments suggesting further clarification on particular cases, the EBA does not agree with adding any further detail, as it believes that a higher degree of prescription would undermine the objectives of technology neutrality and future proofing. In this case the EBA ultimately believes that it is a matter more appropriately addressed at the implementation stage.*	*None*
Feedback on responses to Question 3			
[14] General responses Recital (5) (now recital 2) Recital (7) (now deleted as redundant) Article 7(1) (now Article 3(1))	One respondent argued that the RTS should be flexible and light-touch in order not to impede innovation. The respondent focused in particular on certification, pointing out practical difficulties in the context of auditing users' devices and arguing that certification is too slow, costly, and complex and impedes technology-neutrality in the mobile authentication solutions. In this respondent's view, relying on certification is unlikely to contribute in solving fraud issues, while a standard that responds to the evolution of fraud would be more effective. In his view, it would not cause a shift in liability.	*The comment is of a very generic nature and the EBA is unclear what it specifically refers to and whether or not it proposes any changes that would be applicable in the context of the RTS. However, as mentioned in comment [15] the EBA agrees that in the context of auditing referring to 'certified' and certification may be overly onerous and discriminatory and has therefore replaced 'certified' by 'qualified' in the relevant recitals and in Article 3(1).*	*'Certified' has been replaced by 'qualified' auditors in new Article 3(1) and recital (2).* *Article 3(1) (merging previous Articles 7 and 16):* *~~'The overall security of the strong customer authentication procedure~~ The implementation of the security measures referred to in Article 1(1) shall be documented, periodically tested, evaluated and audited by internal or external independent and ~~certified~~ qualified auditors in accordance with the applicable audit framework of the payment service provider.'*
[15] Article 7(1) (now Article 3(1)) Recital (7) (now deleted as	A number of respondents requested clarification of the term 'certified auditor' in recital (5) and in Articles 7(1) and 16(1) of the draft RTS. In particular, the respondents were unclear about the identity of the person/organisation that would be certifying and on what basis they would so. The respondents also highlighted that the practice of certification of auditors did not exist in all EU member states. These respondents therefore suggested replacing 'certified auditor' with	*The EBA agrees with the respondents that a more generic approach would be appropriate in this instance. It is important to consider these comments in view of the different status of auditors in different member states. They are not always a regulated profession and, as illustrated in comment [147], auditors are not certified in all member states.*	*'Certified' has been replaced by 'qualified' auditors in new Article 3(1) and recital (2).* *Article 3(1) (merging previous Articles 7 and 16):* *~~'The overall security of the strong customer authentication procedure~~*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
redundant) Article 16(1) (now consolidated as part of Article 3(1))	'qualified auditor', to be more generic, and suggested that 'qualified' could be defined as 'recognised, referenced, labelled or certified by a competent authority or organisation'. These respondents also asked the EBA to specify the periodicity of testing, evaluation and audit in the RTS.	*Imposing such a burden on member states would not appear to be proportionate.* *In the light of the overall objectives of the RTS, we therefore agree that it would be an appropriate solution to change 'certified' to 'qualified' auditors.* *The EBA has consolidated the former Articles 7 and 16 into one Article 3 for clarity.*	*The implementation of the security measures referred to in Article 1(1) shall be documented, periodically tested, evaluated and audited by internal or external independent and ~~certified~~ qualified auditors in accordance with the applicable audit framework of the payment service provider'.*
[16] Article 3 (now Article 6)	Many respondents, while generally agreeing with the content of Article 3 (now Article 6), asked the EBA for further clarification regarding Article 3(1). They expressed confusion with regard to the reference to the use of 'non-repeatable characters', which if in their view already embedded in the term 'complexity'. A number of respondents asked the EBA to remove the reference to 'expiration time', as they were of the view that it was less and less considered as a best practice in security policies. These respondents were also of the view that both terms were overly prescriptive and not technology-neutral (e.g. expiry date for card PINs).	*The EBA agrees with the view of the respondents that the security features referred to in the Article may not be technology-neutral and that they reflect past and current practices without accounting for innovation. The EBA believes that such prescriptive terminologies would undermine the objectives of technology neutrality and future proofing and has therefore decided to delete all the features and focus on the outcome.*	*Article 3.1 (now Article 6.1):* *'Payment service providers shall adopt measures mitigating the risk that 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~~ are uncovered by or disclosed to unauthorised parties.'*
[17] Article 3 (now Article 6)	A few respondents suggested adding measures ensuring a certain entropy against guessing attacks, for instance setting the maximum number of erroneous trials in order to exclude exhaustive trial attacks.	*The EBA is of the view that this is covered by Article 4(3)(b) (former Article 1(3)(c)) and therefore does not require any additions under Article 6 (former Article 3). However the EBA agreed with the respondent with regards to specifying the number of failed attempts and has done so under Article 4(3)(b) (former Article 1(3)(c)).*	*Change to Article 4(3)(b) (former Article 1(3)(c)):* *'Payment service providers shall ensure that the authentication by means of generating an authentication code ~~The strong customer authentication procedure shall~~ include each of the following measures ~~mechanisms to~~:* *b) ~~determine~~ the ~~maximum~~ number of failed authentication attempts that can take place consecutively within a given period of time, and after which the actions referred to in letter (a),(b)*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			and (c) of Article 97(1) of Directive (EU) 2015/2366 ~~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~~ shall be temporarily or permanently blocked, shall in no event exceed five times. Where the block is temporary ~~the number of retries and~~ the time period of the block and the number of retries before applying a permanent block shall be established ~~taking into account~~ based on the characteristics of the service provided to the payer and all the relevant risks involved, taking into account, where available, the factors referred to in Article 2(3). The payer should be alerted where the block is permanent. 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;'
[18] Article 3 (now Article 6)	According to one respondent, article 3 should enable multiple facets of authentication to be managed within the one factor, i.e. the multiple claims delivered over the single device (for example GPS location on mobile).	*The EBA is of the view that Article 3 (now Article 6) does not exclude such a possibility.*	*None*
[19] Article 3 (now Article 6)	One respondent remarked that Article 3 should also address the risks that "trivial questions" would be considered elements categorised as knowledge.	*The EBA is of the view that the issue of trivial questions mentioned by the respondent is something that would be better considered at the implementation stage if the PSPs deem it fitting.*	*None*
[20] Article 3(1)	Knowledge element:	*As highlighted in comment [16] the EBA agrees with the view*	*Article 3(1) (now Article 6(1)):*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
(now Article 6(1))	Several respondents stated that the security features mentioned should be considered not a minimum list, but rather examples, to avoid limiting innovation and remaining technology neutral. Other respondents suggested deleting article 3(1) altogether for the same technology neutrality reasons. One respondent was also of the view that the EBA should exempt card PIN from the requirements of Article 3.1.	*that that the security features referred to in the Article may not be technology neutral and that they reflect past and current practices without accounting for innovation. The EBA believes that such prescriptive terminologies would undermine the objectives of technology neutrality and future proofing and has therefore decided to delete all the features, focusing purely on the outcome instead.* *In addition, legal requirements within the RTS cannot contain examples.* *The EBA is of the view that the Article has value without the security features and therefore disagrees with deleting the whole Article.*	*'Payment service providers shall adopt measures mitigating the risk that ~~T~~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~~ are uncovered by or disclosed to unauthorised parties.'*
[21] Article 3(1) (now Article 6(1))	One respondent requested clarification of whether the user's ID was part of the knowledge element or the password was the only parameter classified as knowledge.	*The EBA is of the view that the user's ID is not part of the knowledge element.*	*None*
[22] Articles 3(1), 4(1), 5(1) (now Articles 6(1), 7(1) and 8(1))	Two respondents reflected that the requirements related to elements categorised as knowledge and possession seem to be related to specific elements (password, token generator) and may therefore not suit innovative solutions such as image or pattern selection or mobile phones associated with the customer. As a result, one respondent asked the EBA to remove paragraph 1 of Articles 3, 4 and 5.	*The EBA agrees with the view that that the security features referred to in Articles 3, 4 and 5 (now Articles 6, 7 and 8) may not be technology neutral and that they reflect past and current practices. The EBA believes that such prescriptive terminologies would undermine the objectives of technology neutrality and future proofing and has therefore decided to delete all the specific features, focusing purely on the outcome instead. Some of these practices are mentioned as examples in recital 6.*	*Article 3.1 (now Article 6.1):* *'Payment service providers shall adopt measures mitigating the risk that ~~T~~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~~ are uncovered by, or disclosed to, unauthorised parties.'* *Article 4.1 (now Article 7.1):* *'Payment service providers shall adopt measures mitigating the risk that t~~T~~he elements of strong customer authentication categorised as possession ~~shall be characterised by security features including, but not~~*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			~~limited to, algorithm specifications, key length and information entropy ensuring resistance against the risk of the elements being~~ are used by~~, or disclosed to,~~ unauthorised parties.' *Article 5.1 (now Article 8.1):* *'Payment service providers shall adopt measures mitigating the risk that the access devices and software provided to the payer in order to read authentication elements categorised 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~~ are uncovered by ~~disclosed to~~ unauthorised parties. At a minimum, the access devices and software ~~These security features~~ shall ~~also guarantee~~ ensure a very ~~sufficiently~~ low probability ~~likelihood~~ of an unauthorised party being authenticated as the payer ~~payment service user~~.'*
[23] Article 3(2) (now Article 6(2))	Two respondents argued that Article 3(2) is not sufficiently detailed. The respondents suggested that the EBA detail best practice rather than solely refer to 'mitigation measures', such as the NIST special publication (SP) 800-63B document (specific authentication methods, with corresponding requirements for verification standards).	*The RTS have to balance different, and at times competing, demands, such as technology neutrality and innovation, competition, integration and harmonisation of European payments, etc. The EBA disagrees with the suggestion of adding best practice as a legal requirement as it would be too prescriptive and could undermine the objectives of technology neutrality and future proofing. It would not be appropriate in this example to be anymore prescriptive.*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
[24] Article 3(2) (now Article 6(2))	One respondent asked the EBA to acknowledge that the risk of disclosure to unauthorised parties under Article 3(2) (now Article 6(2)) is to some extent, for instance in case of voluntary disclosure due to phishing, outside the PSP's control. In the respondent's view, such risk should be addressed through education and awareness campaigns.	*The requirement under Article 3(2) (now Article 6(2)) refers to the 'knowledge' element of the SCA. The mitigation measures can only be in relation to this specific element that constitutes SCA at the time of authorisation. The risk of voluntary disclosure would not be addressed at the authentication stage and therefore is not within the scope of this particular Article. The EBA notes, however, that Article 2 requires all PSPs to have monitoring mechanisms in place to detect unauthorised or fraudulent transactions.*	*None*
[25] Article 4 (now Article 7)	One respondent argued that possession elements have different attack surfaces and that the objective of preventing or reducing the ability to intercept possession elements was missing from Article 4.	*Article 4 (now Article 7) states that 'Payment service providers shall adopt measures mitigating the risk that the elements of strong customer authentication categorised as possession are used by unauthorised parties'. The EBA is of the view that 'used' includes cases of potential interception and that there is therefore no missing element in the Article.*	*None*
[26] Article 4 (now Article 7)	One respondent asked the EBA to include in Article 4 for completeness, the threat posed by the device, associated with the possession element, being shared between persons, and, more specifically, that one device should be allowed to be shared.	*The EBA is of the view that the Article does not preclude the sharing of the device and that there is no necessity to mention it within the RTS.*	*None*
[27] Article 5 (now Article 8)	Many respondents asked the EBA to further clarify the quality of inherence element e.g. by reference to: - maximum/minimum false positive rates; - mechanisms and procedures to capture biometric features; - accepted biometric features (fingerprint, retina patter, facial recognition etc.); - security measures used to store biometric data.	*The EBA disagrees with the suggestion to add detail on the quality of inherence element as a legal requirement, as it would be too prescriptive in that context and could undermine the objectives of technology neutrality and future proofing. In addition, a legal requirement cannot include examples, but rather can include only a finite list of elements.*	*None*
[28] Article 5	A number of respondents asked the EBA to consider the following when	*The EBA is of the view that such elements and specifications*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
(now Article 8)	defining the features of inherence elements: i) testing the strength of biometrics for use in authentication – by reference to the NIST paper focused on measuring Strength of Function for Authenticators (SOFA)[14] (on different threats involving biometrics); ii) the fact that inherence features could deteriorate over time: false positive and false negative parameters could be adjusted (or attacked) to allow for impersonation; mechanisms should be in-place to re-calibrate inherence factors (recapture fingerprint / face print, etc.); iii) behavioural biometrics should be accepted as inherence elements – one respondent, however, was of the view that using behavioural data as a standalone inherence element should be clearly excluded in article 5 of the draft RTS (as an early technology which has to be monitored and tested in detail in combination with a specific threat model); iv) distinguishing between behavioral data in general and behavioral biometrics (such as typing recognition), of which the latter can very well be used as an inherence element; and v) considering 'protection against presentation attacks';	*are too detailed for the RTS themselves and could undermine future innovation, and the need to be technology- and business-model neutral. The EBA considers, however, that PSPs may want to take such elements into consideration at the time of implementation.*	
[29] Article 5 (now Article 8)	One respondent was of the view that detecting devices compromised by malware should be another 'security mitigation measure' and asked the EBA to amend Article 5 as follows: 'PSPs should perform constant monitoring of the threats landscape in order to understand the current relevant risks to their system and to assess the effectiveness of their SCA scheme'. The respondent mentions malware detection for example.	*The EBA does not agree that malware detection should be added to this Article. The EBA highlights that there is a broader requirement for PSPs to have monitoring mechanisms in place to identify risks under Article 2. The EBA is therefore of the view that no such addition should be made to Article 8 as it would be redundant.*	*None*
[30] Article 5 (now Article 8)	One respondent suggested that, once the biometric template is lost or compromised, it should never be used again for any other Inherence type of verification. Therefore, the respondent argued that the storage of and access to a biometric template were paramount. The respondent asked the EBA to mandate at least one of the following: a. If the biometric template is held by an institution or held centrally, there should be use of algorithms with sufficient strength and	*The legal requirements contained in the Articles of the RTS are requirements that would apply to all providers irrespective of their specificities. The EBA disagrees with the request to add more detailed requirements as suggested by the respondent and is of the view that adding specific detailed obligations relating to particular use cases would undermine the need to be technology- and business-model neutral.*	*None*

[14] https://pages.nist.gov/SOFA/

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	encrypted with a token, so that the inherence element is never used solely without a secondary element used to proceed with verification; b. If a secure device with Trusted Execution Environment (TEE) is available (such as a mobile phone), it should be used so that the inherence template is only ever stored and verified locally on the secure device (to protect against loss /theft in transit). The respondent also asked the EBA to add a reference to NIST Special Publication 800-63B in addition to any other European security standards bodies.		
[31] Article 5(1) (now Article 8(1))	One respondent argued that using the word 'sensor' could limit biometric innovation in the future and asked the EBA to delete it, replacing 'biometric sensor' with 'biometrics'. The respondent also asked the EBA to replace 'shall' by 'may' in Article 5(1).	*As highlighted in comments [16] and [22], the EBA has deleted the specific security features mentioned in Article 5(1) in line with the objective of technology- and business-model-neutrality.*	*None*
[32] Article 5(1) (now Article 8(1))	Some respondents suggest that behavioural data should be included within the inherence element, as, in the respondents' view, they do not suffer from the vulnerabilities of the other factors (possession and knowledge). The respondents added that such data are recorded by the PSP as events occur and stored in a way that prevents manipulation or compromise as required under NISD and the General Data Protection Regulation (GDPR).	*As highlighted in comments [16] and [22], the EBA has deleted the specific security features mentioned in Article 3(1) to ensure technology- and business-model neutrality. The revised Article 3(1) (now Article 6(1)) does not exclude such data from being considered as an inherence element.*	*None*
[33] Article 5(1) (now Article 8(1))	A number of respondents argued that strict and strong requirements on inherence may not be suitable, as the respondents were of the view that it would be very difficult to comply with them (Article 5(2)).	*As highlighted in comments [16] and [22], the EBA has deleted the specific security features mentioned in Article 5(1) to ensure technology- and business-model- neutrality. The EBA is of the view that PSPs must focus on the outcome and ensure that the inherence element is robust and limits the risk of any illegitimate use.*	*None*
[34] Article 5(1) (now Article 8(1))	A respondent pointed out that the use of the word 'guarantee' should be revised to be consistent with Articles 3 and 4.	*The EBA agrees that the terminology used should be consistent and has replaced the word 'guarantee' with the word 'ensure'.*	*Article 5.1 (now Article 8.1): 'Payment service providers shall adopt measures mitigating the risk that the access devices and software provided to the payer in order to read authentication elements categorised as inherence ~~shall be characterized by security features including, but not~~*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			~~limited to, algorithm specifications, biometric sensor and template protection features ensuring resistance against the risk of~~ sensitive information related to the elements ~~being~~ are uncovered by ~~disclosed to~~ unauthorised parties. At a minimum, the access devices and software ~~These security features~~ shall ~~also guarantee~~ ensure a very ~~sufficiently~~ low probability ~~likelihood~~ of an unauthorised party being authenticated as the payer ~~payment service user~~.'
[35] Article 6(3)(a) (now Article 9(3)(a))	Many respondents, while agreeing that the principle of mechanisms to mitigate the risk of compromise of the multipurpose device is well stated, expressed strong objections to what they considered an overly prescriptive reference to 'separated trusted execution environments'. Some of the respondents asked the EBA to define the objectives of separating the environments instead of referring to 'separated trusted execution environments'.	*The EBA agrees that the term used in Article 6(3) refers to a specific detailed concept that may be too prescriptive and it is of the view such detailed obligation would undermine the objectives of being technology- and business-model-neutrality. The EBA has decided to delete 'trusted' and has replaced it by 'secure' instead to avoid being overly prescriptive.*	*Changes to Art. 6(3)(a) (now Article 9(3)(a)):* *'For the purposes of paragraph 2, the mitigating measures shall include~~,~~ ~~but not be limited to~~ each of the following:* *a) the use ~~implementation~~ of separated ~~trusted~~ secure execution environments through the software installed inside the multi-purpose device;'*
[36] Article 6(3)(a) (now Article 9(3)(a))	Some respondents were of the view that the definition of TEE is too specific and not technologically neutral. The respondents suggested clarifying that TEE refers to a concept instead of a specific technology. The respondents suggested re-wording the paragraph as follows: (a) 'the implementation of separated trusted execution environments inside the multi-purpose device in a way that trust and security is maintained.'	*See comment [35]*	*Article 6(3)(a) (now Article 9(3)(a)):* *'For the purposes of paragraph 2, the mitigating measures shall include~~,~~ ~~but not be limited to~~ each of the following:* *a) the use ~~implementation~~ of separated ~~trusted~~ secure execution environments through the software installed inside the multi-purpose device;'*
[37] Article	A few respondents also argued that TEE as referred to in Article 6(3)(a)	*See comment [35]*	*Article 6(3)(a) (now Article 9(3)(a)):*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
6(3)(a) (now Article 9(3)(a))	has not yet reached maturity on devices available to consumers, and that, if the EBA insisted on separate TEEs, it would exclude the possibility of both storing data and carrying out sensitive operations in an embedded secure element. Redrafting proposal for Article 6(3) to achieve technological neutrality: 'For the purposes of paragraph 2, the mitigating measures COULD include, FOR EXAMPLE, but WOULD not be limited to:(...)'		*'For the purposes of paragraph 2, the mitigating measures shall include~~,~~ ~~but not be limited to~~ each of the following:* *a) the use ~~implementation~~ of separated ~~trusted~~ secure execution environments through the software installed inside the multi-purpose device;'*
[38] Article 7(1) (now Article 3(1)) and recital (5) (now recital (2)) Article 16(1) (consolidated under Article 3(1))	One comment asked the EBA to include the role of a 'card scheme' within Article 7 (now Article 3) because in the respondent's view, card schemes play a role in supervising the security (in particular via type approval procedures for products and systems).	*Card schemes are not within the scope of the RTS and therefore cannot be captured.*	*None*
Chapter 2 (now Chapter 3)			
Feedback on responses to Question 4			
[39] Chapter 2, Article 8 (now Chapter 3, Articles 10 to 18)	A large number of respondents were of the view that the list of exemptions should not be exhaustive. They argued that only a non-exhaustive list would: - allow for innovation; - enable the PSP to remain in control; - be in line with the liability principle set out in Article 74(2) PSD2, which would exonerate the payer's PSP and would always apply in cases where SCA is not used; and - not conflict with Article 98 PSD2, in respect of the need to consider risk and take it into account.	*The principle set out under PSD2 is SCA. By definition, an exemption can remain an exemption only if it is limited. The EBA is of the view that having an open-ended list of exemptions would undermine the principle of SCA and would therefore potentially be in breach of PSD2.* *On the specific arguments listed by the respondents, the EBA is of the view that innovation is not restricted through having an exhaustive list of exemptions. In fact, innovation is already taking place in the SCA space.* *The exhaustive nature of the exemptions does not have an impact on the PSPs' ability to control or on the liability principle.*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		The existing exemptions have been designed and defined on the basis of risk. The EBA has also agreed to add a new exemption based on transaction-risk analysis in a new Article 16.	
[40] Chapter 2, Article 8 (now Chapter 3, Articles 10 to 18)	A number of respondents were of the view that the list of exemptions was too rigid. They argued that the EBA should add exemptions based on randomised triggers as well. They mentioned that they could possibly be based on time, risk profile of the payer and payee and also the intermediaries. They were of the view that fraudsters would otherwise easily be able to target specific exemptions.	*The EBA agrees that some easily definable criteria, and in particular a monetary threshold might become targets for fraudsters, which is part of the reason why the EBA has introduced cumulative thresholds in the case of the low-value exemption. As discussed in detail in comment [42] the EBA has also introduced a new extension based on TRA.*	*None*
[41] Chapter 2, Article 8 (now Chapter 3, new Article 12)	A number of respondents were of the view that the EBA should add an exemption for specific (contactless or contact) POS such as parking meters, vending machines, petrol stations, tolls on motorways, underground, transport and payment instruments with limited use.	*The EBA agrees that there is a valid argument for adding an exemption for unattended terminals for parking or transport fares, since it may not be proportionate, inconvenient and subject to operational and security risks (e.g. to avoid potential accidents at toll gates) to impose SCA.*	*Article 12: Transport and parking fares* *'Subject to compliance with the requirements laid down in paragraphs 1, 2 and 3 of Article 2, payment service providers are exempted from the application of strong customer authentication where the payer initiates an electronic payment transaction at an unattended payment terminal for the purpose of paying a transport or parking fare.'*
[42] Chapter 2 (now Chapter3), Article 8 (New Article 16)	A large number of respondents were of the view that in order to be able to innovate and manage the risks for which they are responsible (and in particular fraud risk), a risk-based approach was essential and therefore asked the EBA to include a transaction-risk analysis (TRA) exemption. Most of these respondents were of the view that 'risk based authentication' or TRA was an industry standard and a best practice that should be recognised as a tool able to provide the highest security and the best convenience for the customer. They also quoted Article 98(2) PSD2, which states that the RTS should adopt 'effective and risk-based requirements', and concluded that the	*As stated in the CP, the EBA considered adding such an exemption in the original draft but was not able at the time to identify objective criteria that would have been legally acceptable. Exemptions from any law must be defined narrowly with clear and unambiguous thresholds and on the basis of objective and verifiable criteria rather than subjective and individual assessments conducted by the individual PSPs to which the law applies. In addition, any exemption that would allow for the majority of payments to be exempted from SCA would go against PSD2's objective of enhancing security and against the definition of an exemption.*	*New Article 16:* 1. *Subject to compliance with the requirements laid down in Article 2 and to paragraph 2 of this Article, payment service providers are exempted from the application of strong customer authentication, where the payer initiates a remote electronic payment transaction, identified by the payment service provider*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	EBA was not in a position not to allow a risk-based exemption. Some of the respondents, however, highlighted the difficulties faced by the EBA in defining an exhaustive and definitive list of all requested elements that should be taken into account by the TRA and the risk that they may not be technologically independent and future proofed. These respondents suggested developing different categories as a result. Others asked the EBA to focus the risk-based approach exemption on scoring and risk methodology, etc. They were of the view that PSPs should be able to apply more or less stringent security based on specific and pre-approved risk-metrics. A respondent also thought that the EBA may wish to request ASPSPs to prove to the national competent authority that using transaction-risk analysis leads to lower levels of risk and fraud than under the application of SCA. A number of respondents also asked the EBA to consider defining a fraud objective with which the PSPs would have to comply, such as a maximum fraud percentage calculated as the number of the fraudulent transactions among transactions exempted from SCA based on the PSP's TRA divided by the total number of the transactions exempted from SCA based on the PSP's TRA. Some respondents were of the view that PSPs have a vested interest in preventing fraud and argued that PSPs, simply out of self-interest, will not adopt a risk-based authentication solution that cannot deliver strong fraud detection rates simply to comply with EBA regulations. In their view, the payments industry itself has already embraced a risk-based approach as a way to balance strong security with consumer convenience. In their view this approach would be preferred to always applying SCA.	*Nevertheless, the EBA agrees with the view expressed by these respondents that a risk-based approach, including the ability to conduct detailed TRA and fraud monitoring, is essential to achieve the objective under PSD2 of reducing overall fraud. Consequently, the EBA arrived at the view that, in accordance with Article 98(2)(a) PSD2, an exemption based on such an analysis should be added in a new Article 16 of the RTS. The RTS also reiterate the importance of risk and fraud monitoring in general as a necessary complement to the principle of SCA laid out in PSD2 as stated in a new Article 2 RTS.* *The EBA also appreciates that TRA could lead to the identification and classification of transactions (at least) between low levels and high levels of risks on a transaction-by-transaction basis. However, while under PSD1, transactions with low levels of risk could then be exempted from strong authentication in line with the EBA guidelines on internet payments, in a post-PSD2 world, where SCA is the principle for all transactions, the balance has changed and any exemption in the RTS would need to be defined narrowly as explained in the previous paragraph.* *Having regard to the view of respondents, the EBA has re-evaluated a number of potential options for such an exemption and narrowed down a few options to finally insert a new, additional exemption in a new Article 16 RTS based on TRA. This exemption focuses on the outcome to lower the level of fraud. The PSPs that wish to use the exemption must have an overall fraud rate for a specific payment instrument that equates to, or is lower than, the reference fraud rate defined in the new Article 16. The exemption can only be applied to remote transactions and below a specific monetary threshold that varies between EUR 100 and EUR 500 depending on the PSP's overall fraud rate. The reference fraud rate differs depending on the underlying payment instrument used. The effect is that the lower the fraud rates, the higher the number of use cases. In addition, the RTS now*	*as posing a low level of risk according to the transaction monitoring mechanisms referred to in Article 2(1).* 2. *For the purposes of paragraph 1 all the following conditions shall apply:* *(a) the amount of the electronic payment transaction does not exceed the Exemption Threshold Value ('ETV') specified in the following table for 'remote card-based payments' and 'credit transfers' respectively, corresponding to the payment service provider's fraud rate for such payment services calculated in accordance with letter d) of this paragraph and up to a maximum value of EUR 500;* ***Reference Fraud Rate (%) for:*** ***ETV** / **Remote card-based payments** / **Credit transfers*** ***EUR 500** / **0.01** / **0.005*** ***EUR 250** / **0.06** / **0.01*** ***EUR 100** / **0.13** / **0.015***

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		require PSPs to monitor all of their fraud rates as well as the performance of the TRA method used, which must additionally be independently assessed by qualified auditors. Furthermore, the PSP must report any change related to the use of this exemption to the national authorities.	*(b) the transaction monitoring mechanisms enable the payment service provider to perform a real-time risk analysis of the electronic payment transaction which takes into account, at a minimum, the risk factors set out in paragraphs 3 and 4 of Article 2 and to combine them in a detailed risk scoring enabling the payment service provider to assess the level of risk of the payment transaction;* *(c) irrespective of the specific arrangements of the transaction monitoring mechanisms, an electronic payment transaction is identified as posing a low level of risk only where the following conditions, in combination with the risk analysis referred to in point b) of this paragraph, are met:*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			i. no abnormal spending or behavioural pattern of the payer has been identified; ii. no unusual information about the payer's device/software access has been identified; iii. no malware infection in any session of the authentication procedure has been identified; iv. no known fraud scenario in the provision of payment services has been identified; v. the location of the payer is not abnormal; vi. the location of the payee is not identified as high risk. (d) for each type of transaction referred to in the table under letter (a) ('remote card-based payments' and 'credit transfers'), the payment service provider's overall fraud rate covering both payment transactions authenticated through strong customer application or executed under any relevant exemption in accordance with Article 13 to 16 shall be equivalent to or lower than the

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			reference fraud rate for the same type of payment transaction in line with the relevant table under letter (a). The overall fraud rate for each type of payment instrument should be calculated as the total value of unauthorised or fraudulent remote transactions, whether the funds have been recovered or not, divided by the total value of all remote transactions for the same type of payment instrument, whether authenticated with the application of strong customer authentication or executed under any relevant exemption in accordance with Articles 13 to 16 on a rolling quarterly basis (90 days); *(e) the calculation of the fraud rate and resulting figures shall be assessed by the audit review referred to in Article 3,*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			ensuring that they are complete and accurate; *(f) the methodology and the model, if any, used by the payment service provider to calculate the fraud rates, as well as the fraud rates themselves shall be adequately documented and made fully available to competent authorities upon their request;* *(g) the payment service provider has notified the competent authorities of its intention to make use of the transaction risk analysis exemption in accordance with this Article.'*
[43] Chapter 2, Article 8 (now Chapter 3, Articles 10 to 18)	A number of respondents asked the EBA to have a more dynamic approach and adopt an 'adaptive authentication/authorisation' approach to allow more flexibility for ASPSP to their customers.	*As stated in comment [43], the principle laid out in PSD2 is SCA. The scope for the RTS does not include determining the authentication process itself but rather to define the parameters and exemptions of the principle of strong customer authentication. The EBA is therefore not in a position to consider and request PSPs to adopt an 'adaptive authentication/authorisation' model that would essentially replace SCA. Similarly, the EBA could not consider and request PSPs to adopt TRA as an alternative to SCA; TRA can only be considered as an exemption and therefore within clear and defined parameters as explained in comment [42]. Article 2 clearly states, however, that PSPS should have*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		monitoring mechanisms in place to identify risks as a complement to SCA.	
[44] Chapter 2, Article 8 (now Chapter 3, Articles 10 to 18)	A number of respondents asked the EBA to exclude card fall-back transactions in case the primary technology failed.	*See comment [2].*	*None*
[45] Chapter 2, Article 8 (now Chapter 3, Articles 10 to 18)	Some respondents asked the EBA to add an exemption for cards used where the amount of the transaction is not known (for instance for car hire). The respondents argued that it is impossible for the payer to initiate the payment because it is contingent on the payee computing the amount to be included in the payment order. Other respondents made a similar point with regards to payments that are future-dated or contingent upon certain events such as reserving a hotel room.	*The eventuality of an unknown amount for a payment transaction at the time of the authorisation is included in Article 75 PSD2. The EBA disagrees that there should be an exemption for such payment transactions on the basis that there is no suggestion of any specific obstacles in applying SCA or evidence that they may be at less risk.*	*None*
[46] Chapter 2, Article 8 (now Chapter 3, Articles 10 to 18)	Some respondents asked the EBA to clarify whether or not mail and telephone orders were exempted from the principle of SCA.	*In the EBA's view, mail and telephone orders are out of the scope of the principle of SCA under PSD2 and therefore not subject to the RTS requirements.*	*None*
[47] Chapter 2, Article 8 (now Chapter 3, Articles 10 to 18)	A few respondents also queried if 'closed communities' to allow online payments systems to continue to work were exempted from the principle of SCA.	*It is the EBA's understanding that the respondents refer to the 'closed loop' exemption under PSD2. Therefore, in the EBA's interpretation of PSD2, these cases are out of the scope of PSD2 and therefore not subject to the principle of SCA or the RTS requirements.*	*None*
[48] Chapter 2, Article 8 (now Chapter 3, Articles 10 to 18)	Some respondents asked the EBA to exempt cash withdrawals and payment orders via ATM from the dynamic linking requirement on the basis of the specific nature of such transactions.	*This is the EBA's understanding that ATM cash withdrawals are generally in scope of PSD2, except independent ones. However the EBA considers that this is a proximity payment and therefore not subject to the dynamic linking obligation under Article 97(2) PSD2. The EBA remarks that a payment order is generally based upon EMV DDA which authentication includes dynamic codes in a way that would appear to comply with the principle of SCA.*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
[49] Chapter 2, Article 8 (now Chapter 3, Articles 10 to 18)	A number of respondents asked the EBA to exclude corporate products and payments. In their view, SCA cannot be applied to commercial cards, in particular in the case of 'three-card-schemes' whereby the owner of the card, signing the contract and making the decisions, is the corporate, although the user will be one of the employees. Respondents highlighted that the usage of cards for commercial users differs greatly, citing 'closed-loop' systems or 'three-card-schemes' with very low fraud levels recorded.	*The EBA considers that in the context of commercial cards, in line with PSD2, such arrangements could be made contractually between the relevant parties and therefore does not consider that there is any need for a general exemption to be added.* *More generally with regard to corporate payments, the EBA is of the view that any exemption is not warranted as there are risks although they may be lower than for consumers. The EBA also remarks that payment systems that process corporate payments already enable SCA to be applied.*	*None*
[50] Chapter 2, Article 8 (now Chapter 3, Articles 10 to 18)	A number of respondents were of the view that applying the exemptions on a mandatory basis for corporates (non-consumers) was not suitable. In particular their view was that corporate PSUs may have implemented authorisation matrixes which are integrated in the authorisation procedures/SCA of the ASPSP and apply to all of their payments and access to electronic channels and that these matrixes may not be fully aligned with the exemption under the RTS. They were also of the view that applying SCA would be better for the consumers than having to block them if they could not decide to apply SCA even in a case where an exemption would apply.	*As explained in comment [40] the EBA agrees with the respondents' view that exemptions should not be compulsory, as the PSPs should be able to apply SCA (where practically possible), even if it falls under an exemption, in case an increased risk of fraud or unauthorised use is detected as one of the objectives of PSD2 is security and as the principle remains SCA. This is clarified under a new Article 18. There is therefore no need to specify in the RTS that the exemptions are not mandatory in the case of corporate payments.*	*None*
[51] Chapter 2, Article 8 (now Chapter 3, Articles 10 to 18)	Some respondents expressed some confusion and a lack of clarity with regards to all the different corporate types of payments and their status under the RTS. In their view, bank-to-bank transactions fall outside the scope of PSD2, under the closed-loop exemption in PSD2, and thus SCA requirements do not apply to them. The respondents asked the EBA to provide more detail in this area.	*PSD2 excludes some corporate types of payments. For instance, Article 3 PSD2 states that payment transactions carried out between PSPs, their agents or branches for their own account as well as payment transactions and related services between a parent undertaking and its subsidiary or between subsidiaries of the same parent undertaking, without any intermediary intervention by a PSP other than an undertaking belonging to the same group, are out of the scope of PSD2 and therefore not subject to the SCA requirement.* *The EBA is of the view that this is a Level-1 text issue and therefore out of that scope of the RTS and which the EBA cannot comment on.*	*None*
[52] Chapter 2, Article 8	A number of respondents queried whether or not card-on-file solutions where merchants accepting card payments have registered the card	*The EBA is of the view that this refers to the interpretation of the Level-1 text. It is the EBA's understanding that card-on-*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
(now Chapter 3, Articles 10 to 18)	number in a card-on-file solution (merchant knows the PAN and initiates the payment without the SCA procedure) were exempted from SCA.	*file solutions and their providers are not within the scope of PSD2 and therefore not within the scope of these RTS. Providers of card-on-file solutions are not PSPs in the sense of PSD2 unless of course the PSP conducts other activities that are within the scope of PSD2 and would therefore be regulated for that purpose.*	
[53] Chapter 2, Article 8 (Now Chapter 3, new Article 16)	A number of respondents asked the EBA to ensure that merchants and their PSPs are able to use the transaction-risk analysis exemption. In their view, merchants, especially larger organisations, are well positioned to control risk. They have access to large amounts of predictive customer data. In many cases they already know their customers' spending habits, purchasing frequency, location etc. In addition, many merchants and acquirers have invested heavily in risk management solutions. They also argued that it would be in line with Article 74 PSD2 where the PSP applying the exemption will support losses in case of frauds (liability shift). In their view, the draft RTS as published in August 2016 contradict, or are not aligned with, the liability shift in Article 74 PSD2.	*The EBA's interpretation of PSD2, after consulting the European Commission, is that the exemptions could be triggered by both the payer's PSP and the payee's PSP. In some cases only the payer's PSP will be able to do so.* *In other cases, which includes the TRA-based exemption, the EBA, following conversations with the EC, interprets PSD2 as meaning that both the payer's and the payee's PSP will be able to trigger it, with the last decision residing with the payer's PSP in line with Article 74(2) PSD2 as mentioned in paragraphs 13 and 24 of the rational section.* *The EBA however disagrees with the view that it can be triggered directly by the payee, as the RTS applies to PSPs only; rather than the payer or payee directly.* *The EBA has also added a new Article 2 to clarify general requirements for PSPs to have monitoring mechanisms in place to detect unauthorised or fraudulent transactions as the complement to authentication measures.*	*None*
[54] Chapter 2, Article 8 (Now Chapter 3, new Article 16)	A few respondents sought clarification on whether the exemptions applied only to ASPSPs, or they could, in particular, be applied by the AISPs and PISPs.	*Article 97.5 PSD2 indicates that other PSPs are allowed to rely on the authentication procedures provided by the ASPSP. The authentication procedure includes the decision whether or not to follow an exemption. It is therefore implied that the ASPSP also decides whether or not to follow the exemptions.* *With regard to the payer's PSP, see comment [53].*	*None*
[55] Chapter 2, Article 8 (Now Chapter 3, new Article 16)	A number of respondents disagreed with the EBA's interpretation of PSD2 in the rationale of the CP published in August 2016 suggesting that PSPs are obliged to require SCA even from merchants outside Europe. In their view, this would be very detrimental to PSPs and merchants.	*The comments relate to the interpretation of PSD2, the Level-1 text, and more specifically whether or not the principle of SCA applies to cross-border transactions, whether EEA transactions that are carried out outside the EU or foreign cards (that may not comply with the principle of SCA) used*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		within the EEA (physically or online). *If it is not practically possible to use SCA, or transactions take place in jurisdictions that are not subject to EU law, the EBA is of the view that the European PSPs shall make every reasonable effort to determine the legitimate use of the payment instrument.* *The EBA is of the view that there is therefore no need to add a specific exemption under the RTS. The EBA is however of the view that such payment transactions shall not be counted when calculating the fraud rates as defined under Article 16.*	
[56] Chapter 2, Article 8 (Now Chapter 3, new Article 16)	Some respondents were of the view that if credentials were compromised, exemptions should not be valid and therefore should be optional.	*As mentioned in comment [40], the EBA agrees with the respondents' view that PSPs should always be able to apply SCA (where practically possible) even if it falls under an exemption in case a risk of fraud or unauthorised use is detected as one of PSD2's objectives is security and as the principle remains SCA. For the purpose of clarity, the EBA has introduced a new Article 18(5) to the RTS.*	*Article 18(5)* *'Payment service providers that make use of any of the exemptions set out in Article 10 to 16 may choose to apply strong customer authentication to the actions and to the payment transactions referred to in those provisions where they determine, according to the transaction monitoring mechanisms set out in Article 2, that a risk of unauthorised or fraudulent use of the payment instrument is increased.'*
[57] Chapter 2, Article 8 (Now Chapter 3, new Article 16)	A number of respondents asked the EBA to add exemptions on the basis of the liability principle. They argued that the PSPs should be able not to use SCA as long as they accept responsibility in case of fraud.	*The EBA is of the view that the request from the respondents to add an exemption on the basis of the liability would contradict the principle of SCA laid down in PSD2. Exemptions from any law must be defined narrowly with clear and unambiguous thresholds and on the basis of objective and verifiable criteria rather than subjective and individual assessments conducted by the individual PSPs to which the law applies. Such exemption would be entirely left at the discretion of the PSP and cannot therefore be added.*	*None*
[58] Articles 8(1)(b) and 8(2)(d) (now Articles 11	A number of respondents disagreed with having fixed monetary thresholds on the basis of discrepancies between different countries. They also argued that such thresholds are not future proof, especially as there is no mechanism included to adapt to the rapidly changing	*While the EBA acknowledges the potential downsides listed by the respondents, the EBA is of the view that there is a clear value in having fixed monetary thresholds in order to ensure some harmonisation across the different EEA member states*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
and 15)	payments ecosystem. Ultimately respondents were of the view that such fixed thresholds could hamper the European payments sector	*and certainty for all the PSPs.*	
[59] Articles 8(1)(b) and 8(2)(d) (now Articles 11 and 15)	A number of respondents suggested that thresholds for low-value payments should be aligned for all types of payments (including with PSD2).	*The EBA appreciates the value in harmonising all the thresholds. However the EBA also has to consider whether or not the risks posed are different. Thus, on the basis that fraud rates are lower for contactless payments at the POS than for remote card payments, the EBA has maintained different monetary thresholds, although it has raised the monetary threshold for low-value remote payments. See comment [60].*	*None*
[60] article 8(2)(d) (now Article 15)	A number of respondents disagreed with the low monetary threshold of EUR 10 as well as the cumulative amount under Article 8(2). They asked the EBA to increase it to the same level as for the other exemption, namely EUR 50.	*The EBA considered the risk of fraud through remote payments and the need to balance it against customer-friendly solutions. In line with ECB fraud data, the EBA agreed with the respondents to increase the threshold to EUR 30. EUR 50 because remote payments are riskier than payments at the point of sale.*	*Article 8(2)(d) (now Article 15):* *'Subject to compliance with the requirements laid down in paragraphs 1, 2 and 3 of Article 2, payment service providers are exempted from the application of strong customer authentication ~~in accordance with of Article 97(2) of Directive (EU) 2015/ 2366 is exempted~~ where the payer initiates a remote electronic payment transaction provided that both ~~where all~~ the following conditions are met:* *a) the ~~individual~~ amount of the remote electronic payment transaction does not exceed ~~the maximum amount of~~ EUR 30 ~~10 Euros; and~~* *b) the cumulative amount, or the number, of previous remote electronic payment transactions initiated by the payer since the last ~~without~~ application of strong customer authentication does not, respectively, exceed EUR100 ~~EUR~~ or 5 consecutive individual remote electronic payment transactions.'*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
[61] Articles 8(1)(b) and 8(2)(d) (now Articles 11 and 15)	Some respondents suggested that exemptions should be based, on how these terminals work, to ensure a consumer-friendly experience and suggested defining two levels of exemption: - Level 1: off-line terminals, where the minimum level for SCA application should be EUR 25, with no authentication mode; - Level 2: online terminals, where the minimum level for SCA application should be EUR 100 with no authentication mode.	*As explained in comment [60] the EBA has agreed with increasing the monetary threshold to EUR 30. The EBA does not, however, agree with distinguishing between on-line and off-line terminals. However, as stated in comment [42], the EBA has introduced a new exemption for unattended terminals, some of which may be offline.*	*None*
[62] Articles 8(1)(b) and 8(2)(d) (now Articles 11 and 15)	A number of respondents also queried the cumulative monetary thresholds. A number were of the view that in practice not all payment methods would be able to identify cumulative amounts. They pointed out, in particular, that some off-line terminals may not know what may have taken place online beforehand. The respondents also explained that the currency fluctuations might complicate the calculation of the limit. In addition, respondents underlined that current contactless chip technology implements this kind of SCA refresh based on 'transaction counters' rather than on the basis of a cumulative monetary threshold. The respondents were of the view that changing the current industry approach could have a significant impact on existing technical solutions. A number of respondents also queried the time period. Some suggested daily, others monthly.	*The EBA acknowledges the practical difficulties in calculating cumulative monetary thresholds and has therefore introduced in the RTS an alternative limit based on transaction counters, in line with industry practices.* *The EBA decided not to define any time period.*	*Article 8(1)(b) (now Article 11):* *1. 'Subject to compliance with the requirements laid down in paragraphs 1, 2 and 3 of Article 2, payment service providers are exempted from the ~~The~~ application of strong customer authentication ~~in accordance with Article 97(1) of Directive (EU) 2015/ 2366 is exempted~~ where the payer initiates a contactless electronic payment transaction provided that both the following conditions are met:* *~~within the limits of both the following conditions~~* *(i) the individual amount of contactless electronic payment transaction does not exceed EUR 50;* *(ii) the cumulative amount or the number of previous non-remote electronic payment transactions initiated via the payment instrument offering a*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			contactless functionality since the last application ~~without application of~~ strong customer authentication does not, respectively, exceed EUR 150 or 5 consecutive individual payment transactions.' *Article 8(2)(d) (now Article 15):* *'Subject to compliance with the requirements laid down in paragraphs 1, 2 and 3 of Article 2, payment service providers are exempted from the application of strong customer authentication ~~in accordance with of Article 97(2) of Directive (EU) 2015/ 2366 is exempted~~ where the payer initiates a remote electronic payment transaction provided that both ~~where all~~ the following conditions are met:* *a) the ~~individual~~ amount of the remote electronic payment transaction does not exceed ~~the maximum amount of~~ EUR 30 ~~10 Euros; and~~* *b) the cumulative amount, or the number, of previous remote electronic payment transactions initiated by the payer since the last ~~without~~ application of strong customer authentication does not, respectively, exceed EUR100 ~~EUR~~ or 5 consecutive individual remote*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			electronic payment transactions.'
[63] article 8(1) and 8(2) (now Articles 10 to 18)	A few respondents were of the view that the national competent authority should be allowed to set domestic thresholds for low-value payments, below the thresholds set by the RTS, to set round figures in local currencies instead of the actual conversion in the local currency.	*The difficulties with setting thresholds in local currencies is exchange rate fluctuation and for that reason the EBA is of the view that thresholds should remain in EUR.*	*None*
[64] Article 8(1) (now Articles 10 to 18)	A few respondents expressed confusion on what should be applied if the PSP was exempted from using SCA.	*This is out of the scope of the mandate of the RTS but the EBA is of the view that the absence of strong authentication is not synonymous with absence of authentication overall and, under other general security principles and requirements, the PSP would be expected to perform some form of authentication.*	*None*
[65] Article 8(1)(a) (now Article 10)	A number of respondents were of the view that there should be an additional exemption for e-banking with a read-only function and no payment functions.	*The EBA agrees that there should be an exemption for read-only functionalities, whether a customer accesses them directly through online or mobile banking or does so using an AISP. In fact, the exemption under the then Article 8(1)(a), now Article 10, has this specific purpose. However, the EBA acknowledges that it may not have been drafted in clear enough terms and has therefore re-drafted it to ensure better clarity.*	*Article 10 (former Article 8.1.a) – 'Payment account Information* *1. ~~The application of strong customer authentication in accordance with Article 97(1) of Directive (EU) 2015/2366 is exempted where:~~ Subject to paragraph 2 of this Article and compliance with the requirements laid down in paragraphs 1, 2 and 3 of Article 2, payment service providers are exempted from the application of strong customer authentication ~~in accordance with Article 97(1) of Directive (EU) 2015/ 2366~~ where a ~~the payer accesses exclusively the information of its payment account online, or the consolidated information on other payment accounts held,~~ payment service user is limited to accessing either or both of the following items online without disclosure of sensitive payment data:* *(a) the balance of one or more designated payment accounts;* *(b) the payment transactions*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			executed in the last 90 days through one or more designated payment accounts. *2.For the purpose of paragraph 1 payment service providers are not exempted from the application of strong customer authentication ~~shall not be exempted~~ where either of the following condition is met:* *(a) the payment service user ~~payer~~ is accessing~~es~~ ~~the information of its payment account, or the consolidated information on other payment accounts held,~~ online the information specified in letters (a) and (b) of paragraph 1 for the first time,* *(b) the last time the payment service user ~~payer~~ accessed~~s~~ ~~the information of its payment account, or the consolidated information on other payment accounts held,~~ online the information specified in letter (b) of paragraph 1 and ~~later than one month after the last day on which~~ strong customer authentication was applied more than 90 days ago.'*
[66] Article 8(1)(a) (now	One respondent noted that the exemption on account access is very wide and possibly exposes too much sensitive data without proper	*As stated in comment [65], the EBA acknowledges that the exemption on read-only access may not have been drafted in*	*Article 10 (former Article 8.1.a) – 'Payment account Information*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Article 10)	authentication.	*clear-enough terms and has therefore been re-drafted to ensure better clarity. The Article states that the read-only information accessed cannot include sensitive payment data.*	*1. ~~The application of strong customer authentication in accordance with Article 97(1) of Directive (EU) 2015/ 2366 is exempted where:~~ Subject to paragraph 2 of this Article and compliance with the requirements laid down in paragraphs 1, 2 and 3 of Article 2, payment service providers are exempted from the application of strong customer authentication ~~in accordance with Article 97(1) of Directive (EU) 2015/ 2366~~ where a ~~the payer accesses exclusively the information of its payment account online, or the consolidated information on other payment accounts held,~~ payment service user is limited to accessing either or both of the following items online without disclosure of sensitive payment data:* *(c) the balance of one or more designated payment accounts;* *(d) the payment transactions executed in the last 90 days through one or more designated payment accounts.* *2.For the purpose of paragraph 1 payment service providers are not exempted from the application of strong customer authentication ~~shall not be exempted~~ where either of the following condition is met:* *(a) the payment service user ~~payer~~ is accessinge~~s~~ ~~the information of its payment account, or the~~*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			~~consolidated information on other payment accounts held,~~ online the information specified in letters (a) and (b) of paragraph 1 for the first time, *(b) the last time the payment service user ~~payer~~ accesseds ~~the information of its payment account, or the consolidated information on other payment accounts held,~~ online the information specified in letter (b) of paragraph 1 and ~~later than one month after the last day on which~~ strong customer authentication was applied more than 90 days ago.'*
[67] Article 8(1)(a) (now Article 10)	A number of respondents disagreed with the one-month period to carry out SCA in article 8(1)(a)(ii) because this would worsen the customer experience and not be justified by a risk analysis. Suggestions included carrying out SCA: • only once a year (majority), particularly with regard to read-only access to payment account; • once in a longer period; • once in a shorter period, if agreed upon by PSPs; • once in 30 calendar days Some even suggested deleting this paragraph entirely, for instance in case a user of the account accessed it frequently, e.g. once a week. A number of respondents argued that it was a departure from existing	*The EBA agrees with some of the respondents that an obligation to apply SCA every month may be too short a period, especially where the information is accessed through an AISP. The EBA believes, however, that a period of a year or more as suggested by a large number of respondents, would be too long from a consumer protection perspective and would not, for instance, adequately protect consumers against a potential fraudster impersonating the customer when setting up an account with an AISP and using this information. The EBA considers that 90 days is an appropriate balance between consumer-friendliness and ease of use, on the one hand, and security, on the other.* *The respondents also expressed concern with regard to the ASPSPs going beyond the RTS requirements and requesting*	*Article 10(2)(b):* *'2.For the purpose of paragraph 1 payment service providers are not exempted from the application of strong customer authentication ~~shall not be exempted~~ where either of the following condition is met:* *(b)the last time the payment service user ~~payer~~ accesseds ~~the information of its payment account, or the consolidated information on other payment accounts held,~~ online the information specified in letter (b) of paragraph 1 and ~~later than one month after the last day on which~~*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	practice and did not believe it would significantly raise security. Respondents felt that it was disproportionate for a service in read-only mode in comparison with other existing protocols such as EBICS or SWIFT. They were also concerned by the fact that, once the minimum number of annual SCAs determined by the RTS has been reached, the bank may have the right to request more for the AISP, which will result in constituting an obstacle to the usage that it develops. They recommended that it be specified that the ASPSP cannot go beyond the requirements specified by the RTS.	*SCA more often. The EBA is of the view that, if ASPSPs were to do so, they would be in breach of the RTS.*	*strong customer authentication was applied more than 90 days ago.'*
[68] Article 8(1)(a) (now Article 10)	Another respondent expressed confusion on the interaction between this paragraph and the EBA guidelines on the security of internet payments	*The EBA guidelines on the security of internet payments are guidelines that applied under PSD1 and will continue to apply during the transitional period. However, once the RTS are in force, the RTS will supersede those guidelines and all requirements within the scope of these RTS will cease to apply.*	*None*
[69] Article 8(1)(a) (now Article 10)	One respondent asked for SCA to be applied for each AISP separately, rather than being mandated by the ASPSP.	*PSD2 allows the AISPs to rely on the SCA performed by the ASPSP. The ASPSP chooses the interface for information to be communicated to all but it cannot mandate the AISPs with regards to SCA.*	*None*
[70] Article 8(1)(a) (now Article 10)	A number of respondents expressed concerns, arguing that, once the minimum number of annual SCAs determined by the RTS was reached, the bank might have the right to request more for the AIS, which would result in an obstacle to the usage that it develops. The respondents asked the EBA to specify that the ASPSP cannot go beyond the requirements specified by the RTS.	*The read-only exemption in the RTS does not set a minimum number of SCAs a year. The new Article 10 requires SCA to be applied on the first use and every 90 days thereafter. The ASPSPs would not be able to go beyond such requirement and the ASPSP would have the right to revert back to SCA only if there was an objective risk of fraud (or other such abuses) as specified in PSD2. As highlighted in comment [41], Article 68(2) PSD2 clearly states that the ASPSP cannot discriminate against AISPs, PISPs and card-based PISPs.*	*None*
[71] Article 8(1)(a) (now Article 10)	Some respondents asked the EBA to modify Article 8(1)(a)(ii) to allow a PSU to use an AIS to pull information even if the PSU does not access the information.	*As highlighted in recital 20, in accordance with Articles 66 and 67 Directive (EU) 2015/2366, PISPs and AISPs will only seek and obtain the necessary and essential information from the ASPSP for the provision of a given payment service and only with the explicit consent of the account holder, the PSU. PISPs and AISPs shall only request information on behalf of the PSU with his/her consent. The AISP may then "pull"*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		information for its customer as highlighted under the new Article 31(5) (formerly Article 22(5)).	
[72] Article 8(1)(a) (now Article 10)	A respondent asked the EBA if the consumers have to use SCA every time they access information about their accounts through an AISP as that respondent believed that it was what was required from Article 97(4) PSD2. The respondent argued that such a provision would make AISPs unattractive in comparison with accessing the information about the payment account online for which the respondent believed there was an exemption in Article 8(1)(a) RTS.	*The exemption under Article 8(1)(a) (now Article 10) covers both situations where the customer would access its account directly online or through an AISP (for instance through an app). Article 97(4) PSD2 does not preclude any such exemption. As stated in comment [70], the new Article 10 requires SCA to be applied on the first use and every 90 days thereafter.*	*None*
[73] article 8(1)(a)(i) (now Article 10)	Some respondents asked the EBA to delete the exemption on SCA for read-only access to payment accounts but to leave the possibility for the user to revoke the access from his/her AISP or his ASPSP interface as well as for the AISP to offer the user a connection diary to see the status of his/her approval at any time.	*The EBA is of the view that the user can always revoke the access from an AISP or ASPSP under PSD2 and that this is not within the scope of the RTS according to the mandate given to the EBA under PSD2. This cannot therefore be addressed here. In addition, the EBA is of the view that the exemption under the new Article 10 has a different purpose which is not to overburden the user when accessing a limited set of read-only information, whether through an AISP or directly on the ASPSP's customer interface.*	*None*
[74] Article 8(1)(a)(i) and (ii) (now Article 10)	A number of respondents asked the EBA to delete Article 8(1)(a)(i) and (ii) or rephrase them to clarify that it is optional to allow for a practical and timely execution. In their view, it would allow one-factor password users to remotely register and activate strong authentication (i.e. via a mobile app) using their existing (one-factor) credentials when setting up two-factor authentication for the first time.	*Article 10 (former Article 8(1)(a)) provides an exemption for a limited set of read-only information unless the user is using it for the first time or every 90 days thereafter. The user cannot use a one-factor password to remotely register and set up an account.*	*None*
[75] Article 8(1)(b) (now Article 12)	A number of respondents asked the EBA to extend the contactless exemption to contact proximity payments. They were of the view that it would be aligned with the objectives of technology-neutrality and customer convenience. They also argued that it would be consistent, as contact payments at point of sale (POS) are not riskier than contactless payments. In addition, a number of comments were of the view that it would be consistent with existing practices, citing in particular parking tolls and transport where the POSs are not necessarily contactless.	*The EBA agrees with the view as highlighted in comment [41] that payment transactions for transport and parking fares at unattended terminals should be exempted and has added a new Article 12 to the RTS. However, the EBA disagrees that it should be more widely extended to all payment transactions at POS below EUR 50. In line with PSD2, the principle remains SCA and there is no justification for not applying SCA at POS for contact payments.*	*Article 12: Transport and parking fares* *'Subject to compliance with the requirements laid down in paragraphs 1, 2 and 3 of Article 2, payment service providers are exempted from the application of strong customer authentication where the payer initiates an electronic payment transaction at an*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			unattended payment terminal for the purpose of paying a transport or parking fare.'
[76] Article 8 (now Article 11)	A few respondents asked the EBA to remove the contactless exemption, arguing that there were existing methods to perform strong authentication in a contactless electronic payment transaction executed with a mobile device (e.g. Patent WO2015104387A1). Moreover, emerging technologies such as radio beacons and Bluetooth low energy would allow new interaction models which will benefit from SCA payment security.	*The EBA is of the view that the exemption should remain risk-based and encouraging innovation, such as contactless payments. As contactless payments without SCA are capped at a cumulative threshold or a number of transactions, the solutions mentioned by the respondents could be applied to transactions where SCA is needed. In addition, if the PSP identifies an increased risk of fraud, the PSP can always decide to apply SCA instead.*	*None*
[77] Article 8(2) (now Articles 13 to 16)	Several respondents asked the EBA to refer to Article 97(1) PSD2, in addition to Article 97(2) PSD2. Respondents argued that the exemptions under Article 8(2) could otherwise be misunderstood as only exempting from dynamic linking under Article 97(2) and not as exempting from dynamic authentication under Article 97(1). In their views, this could lead to the situation where an internet payment transaction exempted under Article 8(2) RTS would be required to apply a SCA.	*The EBA agrees that the mention of Article 97(2) PSD2 without reference to Article 97(1) could be ambiguous. To avoid confusion, the EBA has removed the references altogether, as the principle is laid down in Chapter 2.*	*Articles 13 to 16 (formerly Article 8(2)):* *'Subject to compliance with the requirements laid down in paragraphs 1, 2 and 3 of Article 2, payment service providers are exempted from the application of strong customer authentication ~~in accordance with Article 97(2) of Directive (EU) 2015/ 2366 is exempted~~ where […]'*
[78] Article 8(2)(a) (now Article 13)	A number of respondents were of the view that ASPSPs should be able to set a predefined 'white-list' for the PSU. Others asked the EBA to at least let ASPSPs add national authorities and other pre-authorised institutions as trusted beneficiaries.	*The EBA agrees with the respondents that the objective of the whitelist is to be used by the user and that, for convenience purposes, the list can be populated and/or set by the ASPSP as long as it is confirmed by the user. The EBA has adapted the wording accordingly.*	*New Article 13(1)(a) and 13(2)(a) (former Article 8(2)(a)):* *'1. Subject to paragraph 2 of this Article and to compliance with the requirement laid down in paragraphs 1, 2 and 3 of Article 2, payment service providers are exempted from the application of strong customer authentication ~~in accordance with Article 97(2) of Directive (EU) 2015/ 2366 is exempted where~~ in each of the following situations:*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			(a)the payer initiates ~~online a credit transfer~~ a payment transaction where the payee is included in a list of trusted beneficiaries previously created or confirmed by the payer ~~with~~ through its account servicing payment service provider; *2. For the purpose of letter (a) and (b) of paragraph 1 the following cases do not constitute an exemption ~~The application of strong customer authentication shall not be exempted where~~:* *(a) In relation to letter 1(a) the payer or the payer's payment service provider, provided that the payer gave its consent, creates, confirms or subsequently amends, the list of trusted beneficiaries ~~with its account servicing payment services provider.'~~*
[79] Article 8(2)(a) (now Article 13)	A few respondents were of the view that the trusted beneficiaries exemption under Article 8(2)(a) may contradict the exemption under Article 2(1)(b) for a series of payments with the same amount and payee in the case of a payment transaction initiated through a PISP.	*The exemption for trusted beneficiaries only applies to payment transactions made on an online account by the payer. The PISP cannot create a list of trusted beneficiaries.*	*None*
[80] Article 8(2)(a) (now Article 13)	Some respondents were of the view that the exemption for white-listing trusted payees should be extended to cards and direct debits (level playing field).	*This exemption originates from the payer. Extending the ability to create a safe list to cards, and therefore giving the payee the ability to set it up would extend the scope of the exemption significantly as well as the risk accompanying the exemption and the EBA does not consider it appropriate. The EBA also considers that the exemption would overlap with the exemption for recurring payments, which does apply to cards.* *With regards to direct debits, the EBA notes that they are out of the scope of the RTS as they are initiated by the payee.*	*None*
[81] Article 8(2)(b) (now	With regard to the recurring payments transaction, a number of respondents were of the view that the exemption was too narrow and	*The EBA is of the view that unlimitedly extending it to payments to the same payee regardless of the amount is too*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Article 13)	limited. They asked the EBA to include recurring payments where the amount was not known up front and might therefore vary from one payment to another.	*wide and would introduce too-high a risk.*	
[82] Article 8(2)(b)	A number of respondents asked the EBA to extend the exemption for recurring credit payments to recurring card payments. They argued that both the customer and the merchant benefit from an experience where the first payment is made, and each payment thereafter happens seamlessly without a further payment interaction. In their view, the customer benefits from reduced friction in the consumption of services, and the merchant benefits from the consistent revenue streams provided by recurring payments. A respondent also mentioned that card-on-file/recurring/in-app remote card payments as well as the so-called virtual single-use cards should be exempted from SCA, in a similar way to the exemption applying to credit transfers in Article 8(2) RTS. The respondents were of the view that using SCA as part of the initial registration of the card was sufficient to prevent fraud.	*The EBA agrees that for the RTS to be technology neutral and, given that the risk of fraud is unlikely to be different, the exemption should be drafted more neutrally to encompass different payment instruments. The new Article 13 follows this approach.* *With regards to card-on-file solutions, see comment [52].*	*New Article 13(1)(b) and 13(2)(b) (former Article 8(2)(b)):* *1. Subject to paragraph 2 of this Article and to compliance with the requirement laid down in paragraphs 1, 2 and 3 of Article 2, payment service providers are exempted from the application of strong customer authentication ~~in accordance with Article 97(2) of Directive (EU) 2015/2366 is exempted where~~ in each of the following situations:* *b) the payer initiates a series of payment transactions with the same amount and the same payee.* *2. For the purpose of letter (a) and (b) of paragraph 1 the following cases do not constitute an exemption ~~The application of strong customer authentication shall not be exempted where~~:* *(b) In relation to letter (b) of paragraph 1, the payer initiates the series of payment transactions for the first time, or subsequently amends, the series of payments.*
[83] Article 8(2)(c)	One respondent asked the EBA to remove the exemption allowing transfers on own accounts with the same PSP, but without providing any further reasoning.	*The EBA is of the view that such transfers involve a low level of risk, and has not received any information suggesting otherwise, and that the exemption should therefore remain on the basis of proportionality.*	*None*
[84] Article 8(2)(c)	By contrast to the previous comment, some respondents asked the EBA to extend the extension to all 'in-house' payments, whether or not they are made to the same payee.	*The EBA does not agree with the view of the respondents to extent the exemption to all 'in-house' payments. The risk is not the same and some of the transactions may not be lower*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		risks. The EBA has therefore decided not to make any changes to that exemption.	
Feedback on responses to Question 5 (responses and comments similar to those made under Q4 are not repeated under Q5)			
[85] Chapter 2, Article 8 (now Chapter 3, Articles 10 to 18)	Responding to the specific query asked by the EBA, a number of respondents argued that the exemptions should not be mandatory. They argued in particular that, where relevant, the PSP should be allowed to apply SCA even if it falls under an exemption if a risk is detected, in particular a risk of fraud. Indeed, these respondents were of the view that mandatory exemptions would limit the ability of the PSP to manage their own risk by deciding to apply SCA rather than blocking the transaction, which they considered an extreme scenario. In addition, they were of the view that PSPs may have to challenge every transaction, which could have the unexpected and undesirable effect of increasing fraud because of payer alert fatigue. A large number of the respondents were of the view that mandatory exemptions could lead to fraudsters targeting the exemptions, since fraudsters would have certainty that the PSPs would not apply SCA even if fraud was detected. These respondents were of the view that such rigidity would lead to an increased risk of fraud and reduced level of security. The respondents argued that, as a result, fraud would be likely to increase for low-value payments. Others were of the view that mandatory exemptions would prevent PSPs from using new authentication methods that are often more customer-friendly and offer a more seamless experience, as they are based on SCA. They mentioned for example a transaction via mobile phone with biometric reader. Most of these respondents were also of the view that mandatory exemptions conflicted with the liability regime of PSD2 and in particular the liability shift under Article 74 PSD2. Another argument that many respondents mentioned was that, in their view, having mandatory exemptions would contradict Article 1(3)(e)	*The EBA agrees with the respondents' view that PSPs should always be able to apply SCA (where practically possible) even if it falls under an exemption, if a materially increased risk of fraud or unauthorised use is detected, as one of the objectives of PSD2 is security and as the principle remains SCA. For the purpose of clarity the EBA has introduced a new Article 18 to the RTS. In addition and as outlined under Article 68(2) PSD2, PSPs can apply SCA only in a way that is not discriminatory against TPPs, and in particular PISPs.*	*Article 18(5)* *'Payment service providers that make use of any of the exemptions set out in Article 10 to 16 may choose to apply strong customer authentication to the actions and to the payment transactions referred to in those provisions where they determine, according to the transaction monitoring mechanisms set out in Article 2, that a risk of unauthorised or fraudulent use of the payment instrument is increased.'*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	(now Article 3) that required PSPs to consider risk and have a risk-based approach. In their views a risk-based approach should be the prevailing trigger for SCA and the exemptions should therefore only be considered for low-risk transaction scenarios. In their view, mandatory exemptions would equate to preventing PSPs from lowering their risks. Finally, a number of the respondents highlighted the importance of having the ability to revert back to SCA in the context of the low-value exemption as not all low-value payment transactions are low risk.		
[86] Chapter 2, Article 8 (now Chapter 3, Articles 10 to 18)	A few respondents, in contrast, favoured a mandatory list of exemptions in order to ensure a level playing field among all actors.	*As highlighted in comment [85], the EBA is of the view that PSPs should always be able to apply SCA (where practically possible) even if it falls under an exemption, if a materially increased risk of fraud or unauthorised use is detected, as one of the objectives of PSD2 is security and as the principle remains SCA. For the purpose of clarity the EBA has introduced a new Article 18 to the RTS. In addition, the EBA agrees with the overall non-discriminatory objective and, as clearly outlined under Article 68(2) PSD2, PSPs can apply SCA only in a way that is non-discriminatory to third-party providers, and in particular PISPs. The RTS cannot simply restate the obligations under the Level-1 text; the EBA was therefore unable to add any additional text. If a PSP were found discriminating against third parties, for instance, it would be in breach of EU law.*	*None*
[87] Article 8 (now Chapter 3, Articles 10 to 18)	Some respondents were of the view that the exemption rules should be configurable by the PSU of the PSP. One respondent in particular reasoned that, assuming that the currently provided exemptions for online access as well as online credit transfer are also applicable to the PSU's access via an AISP and/or PISP (based on Article 97(5) PSD2), then the access requirements would technically be transferred to the PSU. In the respondent's view, the EBA should introduce a PSU will-based approach. The PSU would then be able to decide upon personal SCA exemptions for his/her PSP account and at his/her own risk, i.e. on the basis of setting up his/her own update intervals for online account access, payee whitelists as already proposed	*The EBA interprets PSD2, following conversations with the Commission, as meaning that exemptions can be triggered only by the payer's PSP or the payee's PSP. Exemptions can be triggered neither by the payer, or the PSU more generally, nor by the payee. See comment [295].*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	in Article 8(2) and individual amount limitations. The respondent asked the EBA to determine the options for the PSU to choose from. The respondent was of the view that, for instance, the RTS could propose an optional criterion for PSU will-based exemptions on the basis of any artificial intelligence tools, provided that such tools were available to use.		
[88] Article 8 (now Chapter 3, Articles 10 to 18)	Some respondents were of the view that in the absence of a transaction-risk-based exemption, the existing risk-based models would become largely redundant which could perversely have a knock-on effect on how efficiently ASPSPs fight against fraud.	*The EBA disagrees with the view of the respondents, as the RTS separately require PSPs to have monitoring mechanisms in place to identify risks, above and beyond the authentication stage as highlighted in a new Article 2 (previously Article 1(3)(e)). The EBA has also added a new exemption based on transaction-risk analysis and has made links with Article 2 where relevant.*	*Article 1(3)(e) (now Article 2):* *'General authentication requirements* *1. For the purpose of the implementation of the security measures referred to in letters (a) and (b) of Article 1, payment service providers shall have transaction monitoring mechanisms in place that enable them to detect unauthorised or fraudulent payment transactions.* *2. The transaction monitoring mechanisms shall be based on the analysis of payment transactions taking into account elements which are typical of the payment service user in the circumstances of a normal use by the payment service user of the personalised security credentials.* *3. Payment service providers shall ensure that the transaction monitoring mechanisms takes into account, at a minimum, each of the following risk-based factors: lists of compromised or stolen authentication elements; the amount of each payment*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			transaction; known fraud scenarios in the provision of payment services; signs of malware infection in any sessions of the authentication procedure. 4. *Where payment service providers exempt the application of the security requirements of the strong customer authentication in accordance with Article 16, in addition to the requirements in paragraphs 1, 2 and 3, they shall ensure that the transaction monitoring mechanisms take into account, at a minimum, and on a real-time basis each of the following risk-based factors: the previous spending patterns of the individual payment service user; the payment transaction history of each of the payment service provider's payment service user; the location of the payer and of the payee at the time of the payment transaction providing the access device or the software is provided by the payment service provider; the abnormal behavioural payment patterns of the payment service user in relation to the payment transaction history; in case the access device or the software is provided by the payment service*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			provider, a log of the use of the access device or the software provided to the payment service user and the abnormal use of the access device or the software.' *~~'The strong customer authentication procedure shall include mechanisms to:~~* *~~prevent, detect and block fraudulent payment transactions before the PSP's final authorisation. These mechanisms shall take into account, but not be limited to:~~* *5. ~~parameterised rules, including black lists of compromised or stolen card data,~~* *6. ~~signs of malware infection in the session and known fraud scenarios,~~* *7. ~~an adequate transaction history of the payer to evaluate its typical spending behavioral patterns,~~* *8. ~~information about the customer device used,~~* *9. ~~a detailed risk profile of the payer and/or the payer's device,~~'*
[89] Article 8 (now Chapter 3, Articles 10 to 18)	A number of respondents also highlighted the likely high costs associated with changing their systems.	*The EBA is unclear whether this is a comment of a generic nature or whether it specifically focuses on risk-based analysis or SCA for instance. The EBA acknowledges the changes PSPs will have to make as well as the associated costs but is of the view that such costs will primarily derive from the changes requested under PSD2. The EBA does not suggest making any changes to the RTS.*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
[90] Article 8 (now Chapter 3, Articles 10 to 18)	A number of respondents asked the EBA for clarification on the definition of electronic payment transaction and therefore the scope of the SCA. The respondents were unsure whether payments via email or telephone were considered within the scope,	*As mentioned in comment [46] the EBA is of the view that anything initiated via paper or telephone is out of the scope of SCA under PSD2 and therefore out of the scope of the RTS.*	*None*
[91] Article 8 (now Chapter 3, Articles 10 to 18)	A respondent was of the view that there was a risk that certain exemptions will be inconsistent with the General Data Protection Regulation requirement.	*The respondent does not provide any further detail. The EBA is of the view that there is no conflict at the RTS level but acknowledges that at the implementation and supervision stage the interaction of the RTS with the GDPR will need to be considered.*	*None*
[92] Article 8 (now Chapter 3, Articles 10 to 18)	Some respondents asked the EBA to make an explicit link between exemptions and reversibility of transactions. For example, in their view, any transaction which did not include SCA should be reversible by the consumer and a mechanism be provided for management of disputed transactions	*As stated in comment [87], and in line with PSD2, the exemptions can only be triggered or reverted by PSPs rather than the Payment Service User.* *As highlighted in comment [85], the EBA has also added a new Article to clarify that PSPs can always revert back to SCA, in line with the liability principle.*	*Article 18.5* *'Payment service providers that make use of any of the exemptions set out in Article 10 to 16 may choose to apply strong customer authentication to the actions and to the payment transactions referred to in those provisions where they determine, according to the transaction monitoring mechanisms set out in Article 2, that a risk of unauthorised or fraudulent use of the payment instrument is increased.'*
[93] Article 8 (now Chapter 3, Articles 10 to 18)	A number of respondents requested the EBA for clarification with regards to liability. They were of the view that the RTS should clarify that PSPs are not liable when they are exempted or prevented from using SCA according to the RTS. A few of the respondents felt that the EBA could provide a clear explanation of liability for each scenario.	*As highlighted in comment [85], the EBA has added a new Article clarifying that the PSPs may always decide to use SCA even where an exemption might apply (as long as it is technically possible), in line with the liability principle. The EBA is of the view that this additional article provides the clarity the respondents requested. The EBA also notes that the liability principle itself is out of scope of the RTS as it is covered under PSD2.*	*Article 18.5:* *Payment service providers that make use of any of the exemptions set out in Article 10 to 16 may choose to apply strong customer authentication to the actions and to the payment transactions referred to in those provisions where they determine, according to the transaction monitoring mechanisms set out in Article 2, that a risk of unauthorised or fraudulent use of the payment instrument is increased.*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Chapter 3 (now Chapter 4)			
Feedback on responses to Question 6			
[94] Chapter 3 (now Chapter 4)	Respondents expressed their disagreement with the AISPs/PISPs accessing personalised security credentials (PSC). Some of these respondents also expressed their disagreement with practices such as screen scraping or OAuth2 'resource owner password credentials flow'.	*Recital 30 PSD2, Article 66(3) and 67(2) PSD2 allow AISPs and PISPs to access and use PSCs and impose security requirements on these providers when transmitting the data.* *However, with regards to certain practices such as screen scraping, as the EBA explains in the rationale paragraph 12, this is the EBA's interpretation of PSD2 that such practices are no longer permitted.*	*None*
[95] Chapter 3 (now Chapter 4)	One respondent asked the EBA to specifically cover the treatment of PSCs when they are shipped before they are activated and therefore personalised in the RTS.	*The EBA is of the view that, as they are not yet personalised and therefore not yet PSCs, they are out of the scope of these RTS and should not be further detailed than their mention under Article 23.*	*None*
[96] Chapter 3 (now Chapter 4)	Several respondents asked the EBA to either mandate technical industry standards or adopt several detailed measures deriving from these (such as PCI-DSS, ISO, NIST or EMV) while avoiding duplication with the GDPR.	*The EBA is of the view that mandating any technical industry standards as suggested by the respondents would undermine the objectives of being technology and business-model neutral and allowing future innovation. The EBA also remarks that adopting some industry standards against others may disadvantage specific parts of the industry. The EBA has therefore not made any changes.* *With regard to the GDPR, the EBA notes that PSC are not synonymous with personal data. PSD2 and the RTS set a number of requirements with regard to PSC with which PSPs have to comply. PSPs cannot rely on other regulations such as the GDPR. However, the EBA acknowledges that PSPs may need to map out the scope of any other relevant legislation such as the GDPR.*	*None*
[97] Article 9 (now Article 19)	Some of the respondents asked the EBA to distinguish between PSPs and clearly define what requirements apply to which PSPs. The respondents were of the view that only Article 9 was applicable to AISPs and asked the EBA to explicitly mention that Article 9 (now Article 19) applies to all PSPs.	*The EBA is of the view that unless specified otherwise the requirements in Chapter 4 apply to all PSPs. Article 9 (now Article 19) applies to all PSPs and the EBA has revised the drafting of the Article to ensure that this is clear.*	*Article 19: 'Requirements for security measures* *1. Payment service providers shall ensure the ~~The~~ confidentiality and integrity of the personalised security credentials of the*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			payment service user, including authentication codes, ~~shall be ensured~~ during all phases of ~~the~~ authentication ~~procedure~~ including display, transmission and storage. ~~To that end~~ *2. For the purpose of paragraph 1, payment service providers ~~the security measures to protect the confidentiality and integrity of payment service users' personalised security credentials~~ shall ~~provide~~ ensure that each of the following requirements is met:* *(a) ~~Data on~~ personalised security credentials are masked when displayed and not readable in their full extent when input by the payment service user during the authentication ~~procedure process~~;* *(b) Personalised security credentials in data format, as well as cryptographic materials related to the encryption of the personalised security credentials, are not stored in Plaintext;* *(c) Secret cryptographic material ~~related to the encryption of the credentials is stored in secure and tamper resistant~~*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			~~devices and environments~~ is protected from unauthorised disclosure. 3. Payment service providers shall fully document the ~~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~~. 4. Payment service providers shall ensure that the processing and routing of personalised security credentials and of the authentication codes generated in accordance with Chapter 2 take place in secure environments in accordance with strong and widely recognised industry standards.'
[98] Art. 9(1) (now Article 19(1))	Several respondents asked the EBA to further define PSC. Some respondents were of the view that ID should not be considered PSC; others disagreed.	*PSCs are defined in PSD2 and cannot therefore be further defined under the RTS. The EBA acknowledges, however, that a common understanding is important and that it will need to be considered at the implementation stage.*	*None*
[99] Art. 9(1)(a) (now Article 19(2)(a))	Several respondents were of the view that some PSC cannot or should not be masked. They mentioned in particular the examples of one-time passwords, username/login, biometric features, data used in look-up function of the bank and PSC delivered to the user by physical mail.	*The EBA agrees that such requirements may not be appropriate in all instances. The Article now therefore specifies that it applies only at the time the PSC are input during the authentication procedure.*	*Article 19(2)(a) (former Article 9(1)(a)):* *'~~Data on~~ personalised security credentials are masked when displayed and not readable in their full extent when input by the payment service user during the authentication ~~procedure process~~.'*
[100] Art. 9(1)(a) (now	A number of respondents asked the EBA to delete the reference to 'data on' as the reference was unclear.	*The EBA agrees with the respondents and has deleted the reference to data.*	*Article 19(2)(a):* *'~~Data on~~ personalised security*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Article 19(2)(a))			*credentials are masked when displayed and not readable in their full extent <u>when input by the payment service user during the authentication</u> ~~procedure process~~.'*
[101] Article 9(1)(b) (now Article 19(2)(b))	A number of respondents were of the view that PSC should be protected by strong encryption techniques or storage in dedicated secure modules. Some of the respondents, for instance, asked the EBA to require PSPs to complement the draft requirements with additional security measures, such as salting.	*The EBA is of the view that additional requirements based on specific technical measures as suggested by the respondents would undermine the objectives of being technology and business-model neutral and allowing future innovation. The EBA acknowledges, however, that the requirement may have been somewhat unclear and has therefore redrafted it to highlight that the scope is limited to PSC in data format.*	*Article 19(2)(b):* *'personalised security credentials <u>in</u> data <u>format,</u> as well as cryptographic materials related to the encryption of the personalised security credentials, are not stored in Plaintext.'*
[102] Article 9(1)(b) (now Article 19(2)(b))	A number of respondents, by contrast with those in comment [101], were of the view that not all PSC should be encrypted. For instance, they were of the view that PSC as well as cryptographic material could be stored in Plaintext if they were stored in either a tamper-resistant device or a device under the control of the user as long as it was tamper evident. Some noted that nowadays many PSC, such as one-time passwords, were in fact stored in plain text. Others respondents argued that the need to encrypt PSC was different if they were stored in ultra-secure chips and that that should be reflected in the RTS. A few of the respondents suggested limiting the requirement to sensitive PSC data only.	*The EBA is of the view that strong security requirements including encryption are important and should remain. The EBA acknowledges, however, that they may not be appropriate in all circumstances. The EBA acknowledges that the requirement may have been somewhat unclear and has therefore redrafted it to highlight that the scope is limited to PSC in data format.*	*Article 19(2)(b):* *'personalised security credentials <u>in</u> data <u>format,</u> as well as cryptographic materials related to the encryption of the personalised security credentials, are not stored in Plaintext.'*
[103] Article 9(1)(c) (now Article 19(2)(c))	Several respondents asked the EBA to clarify the reference to 'tamper resistant devices and environments'. They expressed confusion and one of the respondents thought that trusted execution environment (TEE) did not comply with this requirement. Some of the respondents asked the EBA as a result to detail the degree of resistance based on the different types of attack profiles. Others asked the EBA to set specific requirements for protecting PSC along the 'cryptographic lifecycle'. Finally, several respondents suggested not applying the Article to end-user devices.	*The EBA agrees with the respondents that the reference to tamper-resistant devices and environments was unclear but it disagrees with the suggestion to add any further detail, on the basis that this would be likely to undermine technology neutrality and future innovation. The EBA has instead opted to focus on the outcome and has deleted the reference to this terminology as a result.*	*Article 19(2)(c):* *'secret cryptographic material ~~related to the encryption of the credentials is stored in secure and tamper resistant devices and environments~~ <u>is protected from unauthorised disclosure</u>.'*
[104] Article 9(1)(c) (now	A number of respondents were of the view that tamper-resistance could refer only to physical devices, while software solutions are not	*The EBA agrees with this comment and, as mentioned in comment [102], the EBA is of the view that the requirement*	*Article 19(2)(c):* *'Secret cryptographic material*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Article 19(2)(c))	considered. A number of these respondents therefore asked the EBA to draft the requirement at a higher level for cost and technology neutrality considerations. Some of these respondents, for instance, suggested focusing on the outcome of protection from unauthorised disclosure.	*should remain technology neutral. The EBA has therefore deleted the reference to this terminology, focusing on the outcome.*	*~~related to the encryption of the credentials is stored in secure and tamper resistant devices and environments~~ is protected from unauthorised disclosure.'*
[105] Article 9(2) (now Article 19(2))	One respondent asked the EBA to change the reference 'authentication procedure' with 'authentication procedure documentation'.	*The EBA agrees with the respondent that the reference may be confusing but rather than adding a supplementary word, the EBA has decided to delete that reference to the authentication procedure.*	*Article 19(2):* *'Payment service providers shall fully document the ~~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~~.'*
[106] Article 9(2) (now Article 19(2))	Another respondent requested that the process related to the management of cryptographic material be documented in a different document from the authentication procedure.	*The PSP has the freedom to document the cryptographic material together with or separately from the authentication procedure. The RTS do not prescribe it.*	*None*
[107] Article 9(2) (now Article 19(2))	One respondent asked the EBA to add an audit requirement.	*There is a general review and audit requirement under the new Article 3.*	*None*
[108] Article 9(2) (now Article 19(2))	A respondent asked the EBA to provide flexibility for NCAs to notify and suggest remedies for newly detected security issues related to PSC protection.	*The respondent refers more to a question of implementation. When supervising the RTS, the NCAs will exercise their judgement and may make such decisions, provided that they remain compliant with the RTS and other relevant legislation.*	*None*
[109] Article 9(2) (now Article 19(2))	One respondent asked the EBA not to require the documentation to be publicly available.	*There are no requirements in the RTS for the documentation to be made publicly available.*	
[110] Article 10	Some respondents asked the EBA to remove the limitation to card-based transactions, citing examples of cards initiating direct debits.	*The EBA agrees that wherever possible the RTS should be technology and business-model neutral. The EBA has, however, deleted this Article on the basis that this was not something that could be enforced under these RTS. Other instruments such as Guidelines on operational and security risks might be more appropriate.*	*The Article has been deleted.*
[111] Article 11	A few respondents were of the view that this area of security could be harmonised with PCI DSS certification standards.	*The EBA is of the view that in order to ensure technology neutrality and future innovation the RTS do not refer to*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		specific industry standards. The EBA has, however, deleted this Article on the basis that this was not something that could be enforced under these RTS. Other instruments such as Guidelines on operational and security risks might be more appropriate.	
[112] Article 10	A number of respondents expressed their concerns with regard to technical service providers contracting with the payee (not with the PSP) to transmit transaction authentication data that are not regulated PSPs and therefore not directly within the scope of the RTS.	*The EBA agrees to some extent with the respondents. The EBA has therefore deleted this Article on the basis that this was not something that could be enforced under these RTS. Other instruments such as Guidelines on operational and security risks might be more appropriate. However, the EBA is of the view that PSPs should strive to ensure that (unregulated) providers with which they contract should meet the same requirements with which they themselves have to comply under the RTS and PSD2. In addition, in the context of outsourcing and as outlined by the CEBS guidelines on outsourcing in its Guideline 2, the outsourcing provider remains liable and responsible. The EBA is therefore of the view that, in the context of the RTS, PSPs remain responsible and liable for any functions that they may have chosen to outsource to a technical service provider.*	*The Article has been deleted.*
[113] Article 10	A number of respondents were of the view that the payees should not have access to PSC. Some of them were of the view that they should have access to authentication codes instead.	*The EBA is of the view that there might be instances where the payee needs to have access to these data. However, as explained in comment [112] the Article has been removed.*	*None*
[114] Article 10	A few respondents were of the view that the payees should also be required to comply with the provisions in Article 16 and liability obligations.	*The EBA has deleted the Article on the basis that this was not something that could be enforced, as the providers mentioned are unregulated. However, the EBA is of the view that PSPs should strive to ensure that (unregulated) providers with which they contract meet the same requirements that they themselves have to meet under the RTS and PSD2. The EBA also states that the liability principles are applicable only to regulated entities and cannot be passed to non-regulated entities.*	*None*
[115] Article 10	Some respondents asked the EBA to clarify the requirement for the merchant and how to monitor its compliance. In their view the requirement did not extend to actively checking the payee's implementation of the security measures required in their contract.	*The EBA has deleted the Article on the basis that this was not something that the requirement could not be enforced as the providers mentioned are unregulated. However the EBA is of the view that PSPs should thrive to ensure and check that*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		(unregulated) providers they contract with meet the same requirements they themselves have to meet under the RTS and PSD2.	
[116] Article 11 (now Article 20)	Several respondents found the second sentence of the article unclear and asked the EBA to clarify which security measures apply and to whom.	*The EBA agrees with the respondents that the second sentence of the Article was unclear and has redrafted it to provide the clarity required.*	*Article 11 (now Article 20): Creation of personalised security credentials* *'Payment service providers shall ensure that the ~~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 is performed in a secure environment. Payment service providers ~~To that end, these security measures~~ shall ~~provide that~~ mitigate 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~~.'*
[117] Article 11 (now Article 20)	One respondent asked the EBA to reflect in the Article the possibility of giving credentials in a fully digital process (considering the eIDAS Regulation). The respondent also asked the EBA to rephrase Articles 12 and 13 (now Articles 22 and 23) accordingly.	*The articles to which the respondent refers do not exclude that possibility.*	*None*
[118] Article 12 (now Article 21)	Some respondents argued against the association with the user device (in particular for AISPs) and asked that the PISP/AISP be required to be able to prove to the ASPSP, if challenged, the adequacy of its procedures and processes linked to association.	*Additional requirements not set out in PSD2 cannot be within the scope of the RTS.*	*None*
[119] Article 12 (now Article 21)	Some respondents asked the EBA to introduce an additional paragraph, referring to the contractual agreement between consumers and AISPs and between AISPs in case of third-party aggregators.	*Additional requirements not set out in PSD2 cannot be within the scope of the RTS.*	*None*
[120] Article 12	A number of respondents asked the EBA to follow NIST SP 800-638	*The EBA is of the view that a higher degree of prescription*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
(now Article 21)	Authentication Lifecycle management, including for the authentication elements section, and include requirements for the enrolment process in order to mitigate the threat of impersonation during the enrolment and when fulfilling Know Your Customer requirements.	*would undermine the objectives of technology neutrality and future proofing.*	
[121] Article 12.a (now Article 21.a)	Several respondents were of the view that the Article was not compatible with the model of PSP relying on third-party authenticators built directly into the device, which allows limited visibility or control over what is happening client-side, i.e. in environments that are not within the PSP's responsibility.	*The EBA is of the view that there is no incompatibility in the paragraph.*	*None*
[122] Article 12 (now Article 21)	Some respondents were of the view that the requirements should ensure a level of security at least at the same level of security as during the usage of the PSC.	*The RTS do not exclude the application of other relevant requirements under the RTS with regard to the usage of the PSC.*	*None*
[123] Article 12 (a) (now Article 21(2)(a))	A few respondents asked the EBA to ensure that 'environment' also includes the secure mobile application environment.	*When mentioning 'environment', the Article states 'including but not limited to', which suggests that other environments such as the one mentioned by the respondents could be included.*	*None*
[124] Article 12 (a) (now Article 21(2)(a))	Some respondents asked the EBA whether this provision does or does not limit the future use of these authentication tools in a payment by the user introducing them on the PIS secure website and forwarding them to the ASPSP by means of the PIS software.	*The EBA is of the view that the requirements do not exclude third-party authenticators and it will be up to the PSP to assess whether or not any specific model complies with the requirements under the RTS.*	*None*
[125] Article 12 (b) (now Article 21(2)(b))	Several respondents found the sub-article unclear and were of the view that it was not feasible to perform SCA before the association of PSC that are to be used in SCA procedures. One respondent also queried what the link was with Article 3 in Chapter 1 (now Article 6, Chapter 2).	*The EBA disagrees that SCA cannot be performed at the time of the creation of PSC using a remote channel but has deleted the reference to 'procedure' for greater clarity.* *The EBA was unclear on the respondent's query about the link with Article 3 (now Article 6) and, given that no further detail were provided, the EBA is unable to answer more specifically.*	*Article 12(b) (now Article 21(1) and Article 21(2)(b)): Association of the payer with personalised security credentials, authentication devices and software* *'1. Payment service providers shall ensure that ~~The security measures to protect the confidentiality and integrity of payment service users' personalised security credentials shall ensure that~~ only the payment service user ~~payer~~ is ~~exclusively~~ associated with the personalised security credentials, with the authentication devices and the software in a secure*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			manner. *2. For the purpose of paragraph 1, ~~To this end~~ payment service providers shall ensure that each of the following requirements are met: ~~these security measures shall ensure that~~* *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~~.'*
[126] Article 12 (b) (now Article 21(2)(b))	One respondent expressed concern that the scope of the Article was limited to a payment instrument.	*The EBA agrees that the term 'payment instrument' can be deleted, as generally this Article covers other means (i.e. PSC, devices), and having in mind that a payment instrument is a device or set of procedures to initiate a payment transaction.*	*Article 12.b (now Article 21(1) and Article 21(2)(b)): Association of the payer with personalised security credentials, authentication devices and software* *'1. Payment service providers shall ensure that ~~The security measures to protect the confidentiality and integrity of payment service users' personalised security credentials shall ensure that~~ only the payment service user ~~payer~~ is ~~exclusively~~ associated with the personalised security credentials, with the authentication devices and the software in a secure manner.* *2. For the purpose of paragraph 1, ~~To this end~~ payment service providers shall ensure that each of the following requirements are met: ~~these security measures shall ensure~~*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			~~*that*~~ *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*~~.*'*
[127] Article 12 (b) (now Article 21(2)(b))	Another respondent queried whether or not PSC could be linked to several payment instruments issued by the same PSP.	*The RTS do not contain any restriction.*	*None*
[128] Article 12 (b) (now Article 21(2)(b))	Another respondent asked the EBA if tokenisation could be used to achieve the requirements in the Article.	*Tokenisation is not excluded in the context of this Article.*	*None*
[129] Article 12 (b) (now Article 21(2)(b))	One respondent asked the EBA to deploy credible automated detection systems for enrolment to SCA in order to prevent a fraudster remotely issuing its own authentication device.	*The EBA does not exclude using detection systems as mentioned by the respondent but does not agree that it should be specifically added in this Article. The EBA also notes that Article 11 (now Article 21) sets a clear requirement for PSPs to mitigate the risks of PSC being used by someone other than the payer.*	*None*
[130] Article 13 (now Article 22)	Several respondents asked the EBA to remove 'authentication device and software', as they were of the view that they protect only the PSC installed on them.	*The EBA disagrees with this comment. 'Authentication device and software' shall be kept in the requirement in addition to PSC; the objective is to highlight that the responsibility extends to the device and software.*	*None*
[131] Article 13 (now Article 22)	Some respondents asked the EBA to clarify whether or not Article 13 would allow credentials to be sent in standard post, particularly considering the possibility of the card and PIN code being delivered by mail but separately.	*The EBA confirms that the RTS do not exclude the postal channel. Article 13 (now Article 23) solely requires, in line with the respondents' comments, that, when executed outside the premises of the PSP, only one feature of the PSC can be delivered through the same channel at the same time.*	*None*
[132] Article 13 (now Article 22)	A number of respondents asked the EBA if the delivery of PSC, PINs in this case, was already defined by the PCI DSS.	*The EBA is not able to comment on industry standards. This is a question that will need to be assessed by the PSPs.*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
[133] Article 13 (a) (now Article 22(2)(a))	One respondent asked the EBA to introduce the possibility for the authentication provider (i.e. a service provider to a PSP) to sign the software digitally in order to account for those solutions where the authentication activity is outsourced. The respondent as a result asked the EBA to remove the ending 'provided by the PSP' in (a).	*As outlined by the CEBS guidelines on outsourcing in its Guideline 2, the outsourcing provider remains liable and responsible. It is therefore the view of the EBA that the reference to the PSP should remain in the RTS.*	*None*
[134] Article 13 (a) (now Article 22(2)(a))	Another respondent asked the EBA to provide more guidance on secure methods for PSC delivery.	*The EBA is of the view that the RTS should not provide any further guidance on secure methods of PSC delivery, to ensure technology neutrality and future innovation.*	*None*
[135] Article 13 (b) (now Article 22(2)(b))	Several respondents were of the view that the term 'digitally signed' was not technology neutral and highlighted that other methods could be equally effective. The respondents also asked the EBA how the payer would be able to check this feature.	*The EBA agrees with the respondents that the reference to 'digitally signed' might not be technology neutral. The EBA also agreed with the respondents that the payer would not be able to check this feature. The EBA has redrafted a more technology-neutral requirement.*	*Article 13(b) (now Article 22(2)(b)):* *'1. Payment service providers shall ensure that ~~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 designed to address the risks related to their unauthorised use due to their loss, theft or copying.* *2. For the purpose of paragraph 1~~To this end~~, payment service providers shall at least apply each of the following measures ~~shall include:~~* *b) ~~M~~mechanisms that allow the payment service provider to verify the authenticity of ~~ensuring that~~ the authentication software delivered to the payment services user via the internet ~~has been digitally signed by the payment services provider~~.'*
[136] Article 13 (b) (now	One respondent asked the EBA if, when downloading an app via Google Play or Apple Store, there was still a need for digital signature.	*The EBA has clarified, as highlighted in comment [135], the requirement for the PSP to verify the authenticity of the*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Article 22(2)(b))		*authentication software. Downloading an app would not fulfil this requirement.*	
[137] Article 13 (c) (now Article 22(2)(c))	Several respondents asked the EBA what was meant by the term 'property' in case of PSC.	*This word is not used in Article 13(c) (now Article 23(c)).*	*None*
[138] Article 13 (d) (now Article 22(2)(d) and Article 9(3)(a))	Several respondents asked the EBA what was meant under the term 'secure and trusted environment'. They were of the view that the activation of a mobile app or hardware device would occur in client premises, in other words outside a PSP's control, and that Article 13(a), (b) and (c) [now Article 23(a), (b) and (c)] would already ensure that only authorised individuals can perform the registration action.	*The EBA agrees with the respondents that the requirement was unclear and not necessarily technology neutral due to its reference to a specific concept. The requirement has been redrafted in more neutral and general terms, deleting the reference to 'trusted' and referring only to 'secure environment'.* *This reference has also been deleted in Article 6(3)(a) (now Article 9(3)) as mentioned in comment [35].*	*Article 13(d) (now Article 22(2)(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 ~~1~~21.'* *Changes to Art. 6(3)(a) (now Article 9(3)(a)):* *'For the purposes of paragraph 2, the mitigating measures shall include each of the following~~, but not be limited to~~:* *a) the use ~~implementation~~ of separated ~~trusted~~ secure execution environments through the software installed inside the multi-purpose device.'*
[139] Article 13 (d) (now Article 22(2)(d))	A number of respondents were of the view that the requirement could be impossible to achieve, as the consumer may not have any other credentials to use for SCA. They also note that, in current mobile payment solutions, consumer authentication and credential activation happen before the PSC are delivered to the device.	*The EBA agrees with the respondents and, as highlighted in comment [138], has redrafted the requirement.*	*Article 13(d) (now Article 22(2)(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*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			*accordance with the association procedures referred to in Article ~~1~~2*1.'*
[140] Article 14 (now Article 23)	Several respondents asked the EBA for a more risk-based approach in order to differentiate between a scheduled renewal of expired credentials, to which they were of the view that only Articles 12 and 13 [now Articles 22 and 23] should apply, and the replacement of stolen credentials. Some of the respondents considered the Article workable as long as the aggregator receives relief from the frequent recertification of the AISPs.	*The EBA disagreed with the respondents' request to follow a risk-based approach, as the respondents did not offer any specific justification for doing so.*	*None*
[141] Article 14 (now Article 23)	One respondent was of the view that requiring SCA before renewal may stifle innovation and customer convenience.	*The EBA disagrees with the respondent. The EBA is of the view that requiring SCA is paramount for security and that the requirement should therefore remain.*	*None*
[142] Article 14 (now Article 23)	Another respondent was of the view that, during replacement or reactivation, procedures under Articles 22 and 23 should apply.	*The EBA agrees with the respondent and Article 14 (now Article 23) already specifies that this is the case. The EBA therefore does not suggest making any changes.*	*None*
[143] Article 14 (now Article 23)	Other respondents suggested adding a minimum frequency for renewal of PSC.	*The EBA disagrees with the respondents and is of the view that no further detail should be given, as this should be left to the discretion of the PSP depending on circumstances.*	*None*
[144] Article 14 (now Article 23)	A number of respondents were of the view that, as the renewal of credentials is technology dependent, PSPs should be allowed to update the procedures of creation, association and delivery of the credentials when renewed or replaced.	*The EBA prescribes not that the procedures be the same but rather that the procedures follow the same principles as under Articles 20 to 22. To avoid any ambiguity, the word 'same' has been removed.*	*Article 14 (now Article 23): 'Payment service providers shall ensure that the ~~The~~ renewal or re-activation of personalised security credentials follows ~~shall be conducted following~~ the ~~same~~ procedures of creation, association and delivery of the credentials and of the authentication devices in accordance with Articles 20, 21 and 22.'*
[145] Article 15 (now Article 24)	One respondent requested the EBA to clarify the handling and communication of authorisation withdrawals.	*The EBA was unclear what the respondent referred to and is therefore not able to respond.*	*None*
[146] Article 15 (c) (now Article 24(c))	Several respondents asked for clarity on the terms 'information related to PSC' and 'public repositories'.	*The EBA does not believe that further detail should be provided in the RTS.*	*None*
[147] Article 16	A number of respondents were confused and asked for clarity on the	*In line with comment [15], the EBA agrees that the reference*	*Article 3: Review of the security*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
(1) (now in Article 3)	meaning of 'certified' auditors. They asked the EBA who should issue the certificate and under what standard. A number of the respondents explained in addition that sometimes internal auditors are not certified and that certification is not available in all EEA member states. Others also queried whether 'independent' and 'certified' referred to internal or external auditors or both categories.	*to 'certified' may be ambiguous and may also discriminate against some auditors originating from countries where certification is not available. The EBA has therefore deleted the term and replaced it by 'qualified'.* *The EBA has consolidated all references to audits in a single Article 3 to avoid confusion. The new consolidated Article 3 clarifies that the requirements of independence and qualification refer to both external and internal auditors and that audit should be aligned to the applicable audit framework.*	*measures* *1. 'The implementation of the security measures referred to in Article 1(1) shall be documented, periodically tested, evaluated and audited by internal or external independent and qualified auditors in accordance with the applicable audit framework of the payment service provider.* *2. The period between the audit reviews referred to in paragraph 1 shall be determined taking into account the relevant accounting and statutory audit framework applicable to the payment service provider. Payment service providers that make use of the exemption under Article 16 shall perform the audit for the methodology, the model and the reported fraud rates at a minimum on a yearly basis.* *3. The audit review shall evaluate and report on the compliance of the payment service provider's security measures with the requirements set out in this Regulation. The report shall be made fully available to competent authorities upon their request.'*
[148] Article 16 (1) (now in Article 3)	A few respondents asked the EBA for clarification on the way in which the integrity of the audit report can be determined as well as whether or not breach of compliance detected based on audits should also be	*The EBA is of the view that no further detail is needed in the RTS.*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	covered.		
[149] Article 16 (1) (now in Article 3)	One respondent asked the EBA to clarify that the audit reports under Articles 7 and 16 (now both integrated under Article 3) could be done under the same report.	*The EBA is of the view that the RTS do not preclude such practice. The consolidation of all review measures in Article 3 is a clear indicator of it.*	*None*
[150] Article 16 (1) (now in Article 3)	One respondent asked the EBA to link this requirement to the Guidelines on operational and security risks.	*While the EBA acknowledges that there might be a link with the Guidelines on operational and security risks, the EBA notes that the Guidelines have not been adopted and therefore cannot be referenced.*	*None*
[151] Article 16 (1) (now in Article 3)	A number of respondents asked the EBA to specify the frequency of evaluation, documentation and reporting responsibilities.	*The EBA considered the request from the respondents and decided against it on the basis of proportionality, as frequency should be left to the discretion of the PSPs depending on a number of factors, including the complexity of the business, its size, the risks identified, etc. Article 3 specifies, however, that it is dependent on the PSP's audit framework and that review related to Article 16 shall be conducted on a yearly basis.*	*Article 3(2):* *'The period between the audit reviews referred to in paragraph 1 shall be determined taking into account the relevant accounting and statutory audit framework applicable to the payment service provider. Payment service providers that make use of the exemption under Article 16 shall perform the audit for the methodology, the model and the reported fraud rates at a minimum on a yearly basis.'*
[152] Article 16 (1) (now in Article 3)	Other respondents were against audits of the security measures on the basis of the high cost for SMEs and start-ups (or general increase in PSPs' costs) and that they might result in shifting fraud liability to the user. They suggest that audit reports should be available to customers disputing transactions.	*The EBA acknowledges the cost impacts of having audits but also believes that an independent review is paramount. The EBA believes that the requirement remains proportionate on the basis that it does not mandate a specific periodicity, such as a yearly review, except for Article 16. See comment [151].*	*None*
Chapter 4 (now Chapter 5)			
Feedback on responses to Question 7			
[153] General comment	Many respondents agreed or partially agreed 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.		
[154] General	A number of respondents were of the view that the standards should be	*While the EBA appreciates that in places the principle of*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
comment	more specific to avoid fragmentation.	*unification should prevail, it is of the view that, in the context of this Chapter, technology neutrality, including enabling competition and future innovation, is paramount. The EBA is therefore against any further detail and specification.*	
[155] General comment	A number of respondents disagreed with the use of a dedicated interface and were in favour of maintaining direct access and existing practices such as screen scraping, for TPPs, and under the TPPs' control. In the respondents' views, technical access via the customer-facing online banking interface by using screen scraping should remain regardless of the interface the ASPSP may offer. In their views, any other solution would be against PSD2 and the principle of non-discrimination in particular, as well as being against innovation and competition. These respondents expressed concerns that they would no longer be able to service their customers as they currently do if they were no longer able to screen scrape, as the ASPSP would in their view have no incentive to provide a reliable service. A large number argued, by contrast, that the PSD2 requirement for secure communication can be ensured only via a dedicated interface (i.e. not via the customer-facing online banking interface), because some information (e.g. German church taxes, other tax information) included in the online banking facility cannot legally be shared with a third party.	*The RTS remain silent on making a choice between the two options to access customer information.* *Indeed, the RTS do not mandate one or other mode of access. The EBA gives the choice to the ASPSP whether to set up a specific interface or to adapt its customer interface for AISPs and PISPs to access the customer information they need.* *However, the EBA interprets the security requirements under PSD2 as meaning that the TPPs will no longer be able to screen scrape. The EBA understands screen scraping as a way for* the PISP to access the customer's online account by pretending to be that customer, often using advanced robot technology. *The EBA disagrees with the suggestion of some of the respondents that not allowing screen scraping would be against the principle of non-discrimination.* *The EBA acknowledges that, to ensure fairness and competition between all actors, ASPSPs must ensure that the TPPs can access the information, and in particular the information they need to make a payment. The EBA has therefore refined the RTS to add further requirements for the ASPSPs in case they choose to set up a dedicated interface, including around the level of services, reporting requirements, the need to have contingency measures in place, including but not limited to communication plans with TPPs in case the interface fails, and the obligation to immediately confirm whether there are funds or not in the account under Article 31 RTS.*	*New article 28* *Obligations for dedicated interface* (a) *'*Subject to compliance with Article 27, account servicing payment service providers that have put in place a dedicated interface in accordance with Article 27(2), shall ensure that the dedicated interface offers the same level of availability and performance, including support, as well as the same level of contingency measures, as the interface made available to the payment service user for directly accessing its payment account online. (b) For the purpose of paragraph 1, (c) Account servicing payment service providers shall monitor the availability and performance of the dedicated interface and make the resulting statistics available to the competent authorities upon their request; (d) Where the dedicated

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			interface does not operate at the same level of availability and performance as the interface made available to the account servicing payment service provider's payment service user for when accessing its payment account online, the account servicing payment service provider shall report it to the competent authorities. The report shall include the causes of the deficiency and the measures adopted to reestablish the required level of service. (e) The account servicing payment service provider shall restore the level of service for dedicated interface as referred to in letter (b) without undue delay and shall take any action that may be necessary to avoid its reoccurrence. (f) Payment service providers making use of the dedicated interface offered by the account servicing payment service provider after reporting to the account servicing payment service provider may also

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			report to the national competent authority any deficiency in the level of availability and performance required of the dedicated interface. (g) Account servicing payment service providers shall also ensure that the dedicated interface uses ISO 20022 elements, components or approved message definitions, for financial messaging. (h) Account servicing payment service providers shall include, in the design of the dedicated interface, a strategy and plans for contingency measures in the event of an unplanned unavailability of the interface and systems breakdown. The strategy shall include communication plans to inform payment service providers making use of the dedicated interface in case of breakdown, measures to bring the system back to business as usual and a description of alternative options payment service providers may make use of during the unplanned

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			downtime.'
[156] General comment	A number of respondents mention direct access but interpret it differently. Some of the respondents in fact refer to screen scraping while others more generally refer to accessing the information directly.	*PSD2 mentions direct access in a recital under PSD2 but remains silent on a definition. The notion of direct and indirect access is somewhat outdated and refers to PSD1 rather than PSD2. Under PSD2, regardless of whether TPPs access customer information through an interface specifically designed for TPPs or through an updated and adapted customer interface that will integrate TPPs, in all cases the TPP will access it directly. In a number of cases, however, the notion of direct access has been interpreted as synonymous with screen scraping (see comment [155]).*	*None*
[157] General comment	A number of respondents suggested that direct online access (not via customer interface) should be allowed as a backup in case others are not available, to ensure neutrality and a level playing field.	*The EBA considered this view but, on the basis that the EBA interprets PSD2 as meaning that screen scraping will no longer be allowed after the transitional period, the EBA considered that allowing it even as a backup would not be legally feasible. Instead, as mentioned in comment [155] the EBA has added more requirements for the ASPSPs in case of an unplanned downtime of a dedicated interface.*	*See comment [155]*
[158] General issue	A number of respondents suggested inserting a transitional period, as time is needed to decode a specification of an IT interface and develop the component needed. Some suggested that it could not be less than six months after the ASPSP had made available either the interface or the specification and testing environment, whichever occurs later.	*While the EBA appreciates the complexity and the need for some time to put solutions in place, it notes that an 18-month transitional period is already planned under PSD2 and considers that time to be sufficient and to fulfil the request from the respondents.*	*None*
[159] General issue	A respondent asked the EBA to define and set up a central body to resolve claims with PISPs/AISPs.	*While the EBA appreciates the relevance of the respondents' request, setting up such a central body is not within the scope of the RTS, which is defined by PSD2, and is therefore not something that the EBA can contemplate within the RTS.*	*None*
[160] General issue	One respondent felt that the RTS should acknowledge the use of PCI DSS as consistent with the RTS requirements.	*The RTS do not exclude the use of such industry standards provided that they fulfil the requirements under the RTS, but the EBA is also of the view that such standards should not be prescribed under the RTS to ensure that the RTS remain technology neutral.*	*None*
[161] General	A number of respondents asked the EBA for clarity with regard to ATM	*The general principle of non-discrimination defined in PSD2*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
issue	and ATM providers and access to the new interface in a non-discriminatory manner.	*applies to all requirements and providers. As this is defined in the Level-1 text, this is not something that the EBA can repeat in the RTS.*	
[162] Article 17 (now Article 25)	One respondent was concerned about the potential fragmentation derived from the NCAs' responsibility for issuing registration numbers and maintaining national registers.	*While the EBA appreciates the origins of the concern, this is not something that can be addressed within the RTS, as it is not within their scope.*	*None*
[163] Article 17 (now Article 25)	A respondent suggested that the EBA should keep a pan-European online repository for ASPSPs to check online whether an AISP/PISP has a valid licence or not (including all legal 'company data').	*This is not something that is set out in the mandate given to the EBA by PSD2 and therefore not something that the EBA can address in these RTS.*	*None*
[164] Article 17 (now Article 25)	A number of respondents asked the EBA to include the following part of the rationale published in the CP – '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 to 67 of PSD2' – in Article 17 RTS to ensure harmonisation across Europe.	*This ASPSP shall offer at least one communication interface that meets the requirements. Communication interfaces that do not meet the requirements cannot be used.*	*None*
[165] Article 17 (now Article 25)	A respondent asked the EBA for the Article not to apply to the communication between the ASPSP and PSU.	*This requirement does not apply to communication between ASPSPs and PSUs. Therefore no change is needed.*	*None*
[166] Article 17 (1) (now Article 25(1))	<u>Secure bilateral identification</u>: A large number of respondents were of the view that EMV used for card payments does not support 'secure bilateral identification', as the card is not able to authenticate the terminal. The respondents were, however, of the view that replacing 'bilateral' with 'mutual' would be equally problematic. Some of the respondents pointed out that the requirement is dependent on the payment method used; In their views, DDA should be combined with application cryptogram (CDA) for physical payment cards and terminals (rather than SDA) and combined with JSON Web Tokens for remote/internet PISP-initiated credit transfers.	*The EBA agrees with the respondents' view that bilateral identification may not be suitable for all. In order to ensure technology neutrality and to allow future innovation, the EBA has redrafted this requirement by deleting the reference to 'bilateral'.*	*Article 25(1) (former Article 17(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.'*
[167] Article 17 (2) (now Article 25(2))	Some respondents were of the view that the current text was too strictly formulated, since the PSPs cannot be responsible for mobile devices' security, which is under the control of clients. The respondents suggested including 'efforts' rather than 'to guarantee'.	*The EBA agrees that the focus of the obligation is for the PSPs to mitigate the risks within their control, for instance the security of the app on the phone rather than the phone or tablet itself. The EBA has redrafted the requirement to clarify this point.*	*Article 17(2) (now Article 25(2)):* *1. Payment services providers shall ensure that <u>the risks</u> ~~mobile applications and other payment services users' interfaces offering electronic payment services are protected~~ against*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			misdirection of communication to unauthorised ~~third~~ parties in mobile applications and other payment services users' interfaces offering electronic payment services are effectively mitigated.
[168] Article 18 (now Article 26)	A number of respondents felt that forcing acquirers to store all transaction data including card numbers in order to provide traceability (on their own) would result in additional large investments (PCI DSS) and would increase the probability of the data being stolen.	*Article 18 does not require acquirers/merchants to store data; the Article only says that technical data related to the transaction communication that allow transaction traceability without exposing personal information can be stored.*	*None*
[169] Article 18 (now Article 26)	One respondent queried the duration for which PSPs should retain the information.	*General record-keeping rules would apply.*	*None*
[170] Article 18 (now Article 26)	One respondent asked for the reference to 'merchant' to be consistent. The respondent therefore asked the EBA to refer to 'other entities including, but not limited to, merchants' throughout rather than 'merchants' only.	*The EBA agrees with the need for consistency and has made the change suggested.*	*Article 18 (now article 26): Traceability* *1. 'Payment services providers shall have processes in place which ensure ~~ensuring~~ that all payment transactions and other interactions with the payment services user, with other payment services providers and with other entities including 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.* *2.* For the purpose of paragraph 1, *~~In particular~~ payment services providers shall ensure that any communication session*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			established with the payment service user, other payment service providers and other entities, including~~, but not limited to,~~ merchants, relies on each of the following:'
[171] Article 18 (a) (now Article 26(2)(a))	A number of respondents expressed their view that, while a unique session identifier is essential to correlate messages within a dialogue, it is not possible to require the session identifier to also allow the identification of the communicating parties.	The EBA agrees with the respondents that eIDAS cannot technically identify the communicating parties. The EBA has redrafted the requirement, focusing on the unique session identifier identifying the communication session rather than identifying the communicating parties.	*Article 18(a) (now Article 26(2)(a)):* *'a unique identifier of the session; ~~allowing the identification of the communicating parties~~.'*
[172] Article 18 (c) (now Article 26(2)(c))	A number of respondents were of the view that the reference to the Network Time Protocol (NTP) is neither technology neutral nor future proof. They asked the EBA to either remove it or only mention it as an example. They explained that alternative technology existed, such as the Precision Time Protocol (PTP).	*The EBA aims to remain technology neutral where possible. There is no suggestion that NTP would be the only option, and suggestions from respondents include other already existing protocols. The article has been redrafted as a result.*	*Article 18(c) (now Article 26(2)(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.'*
[173] Article 19 (now Article 27)	A respondent was of the view that communication interfaces should be designed and implemented not to require the use of proprietary technologies or involve vendor lock-in.	*The details on the design of the interfaces are not within the scope of the RTS.*	*None*
[174] Article 19 (1)(b) (now Article 27(1))	A respondent was of the view that the current draft could be interpreted as making all services available to all PSPs. The respondent asked the EBA to clarify and asked it to add the word 'respectively' at the end of the clause.	*This EBA has reflected and decided not to add 'respectively'. It has, however, reorganised the paragraph to delineate obligations and their addressees more clearly.*	*Article 19(1)(b) (now Article 27(1)(a) to (c)):* *'Account servicing payment service providers that ~~are offering~~ offer to a payer a payment account that is accessible online shall have in place ~~offer~~ at least one ~~communication~~ interface which meets each of the following requirements ~~enabling~~* *~~b)Account information service providers, payment initiation service providers and payment service providers issuing card based payment instruments to securely communicate with the account~~*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			~~*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*~~ *(a) account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments can identify themselves towards the account servicing payment service provider;* *(b) account information service providers can* communicate securely to *request and receive information on one or more designated payment accounts and associated payment transactions;* *(c) payment initiation service providers can* communicate securely to *initiate a payment order from the payer's payment account and receive information on the initiation and the execution of payment transactions.'*
[175] Article 19 (1)(c) (now Article 27(1))	The respondents asked for authentication procedures to use the same PSC for independent AISP as for direct online access to the payment accounts.	*The RTS do not prescribe PSC but PSD2 does allow AISPs and PISPs to rely on the ASPSP's PSC.*	*None*
[176] Article 19	Screen scraping:	*Following discussions with the Commission, the EBA*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
(1) (now Article 27(1))	One respondent was unclear whether or not the RTS outlawed screen scraping and another respondent asked if ASPSPs could refuse such access. Other respondents asked the EBA to explicitly mention the outlawing of screen scraping as a consequence of the mandated adoption of APIs as a suggested Interface. These respondents feared that otherwise this would lead to a disparate service offering.	*interprets the security requirements under PSD2 as meaning that screen scraping will no longer be allowed and therefore that ASPSPs would be able to refuse access that way. This is a matter of the Level-1 text and cannot therefore be mentioned in the RTS.* *The EBA requires the ASPSPs to offer at least one interface for TPPs to access the information needed. The RTS do not mandate APIs although the EBA appreciates that the industry may agree that they are suitable.*	
[177] Article 19 (1) (now Article 27(1))	Some respondents also asked the EBA whether or not ASPSPs are free to decide to which standard of communication they will adhere, even if it is different from the national standard if any.	*ASPSPs will have to abide by rules laid down under the RTS and provide at least one interface.*	*None*
[178] Article 19 (1) (now Article 27(1))	A respondent queried what was included in the definition of 'payment account information'.	*This is a matter of interpretation of the Level-1 text.*	*None*
[179] Article 19 (1) (now Article 27(1))	A few respondents felt that the RTS should specify that the communication interface should be based not only on batch-processing uploads and downloads (i.e. FTP and similar), but also on real-time communication technology.	*This is not what the RTS suggest in Article 19 (now Article 29).*	*None*
[180] Article 19 (2) and 19(2)(b) (now Article 27(3)(a) and (b))	A respondent asked the EBA to clarify in the RTS that the ASPSP is free to develop its own authentication procedures without any technical constraints.	*The ASPSP decides on its authentication procedures but the ASPSP must meet the requirements laid down in RTS Chapters 1 and 2.*	*None*
[181] Article 19 (2)(a) (now Article 27(3)(a))	One respondent was unclear about what 'authentication procedure' meant in the context of this paragraph.	*It refers to the authentication procedure provided by the ASPSP, on which the PISP/AISP relies. The authentication procedure shall meet the requirements in RTS Chapters 1 and 2 and may consist of various steps.*	*None*
[182] Article 19 (2)(c) (now Article 27(3)(c))	A respondent was of the view that this paragraph was not applicable where credentials were transferred directly by the PSU to the ASPSP and therefore asked the EBA to replace the word 'when' by 'if'.	*The EBA disagrees with making any such change, as the requirement will apply only when they are transmitted. If they are not transmitted, the requirement will not apply. For clarity, the EBA has redrafted the paragraph.*	*Article 19(2)(c) (now Article 27(3)(c)): "~~Ensure the protection of~~ the integrity and confidentiality of the personalised security credentials and of ~~the~~ authentication codes ~~when these are~~ transmitted by or through the payment initiation service provider or the account information*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			service provider shall be ensured."
[183] Article 19 (2)(c) (now Article 27(3)(c))	One respondent asked the EBA if the paragraph referred to security at the Transport Layer level protocol, as authentication codes may already be cryptographically protected.	*The requirement does not refer to specific protocols. The purpose of the requirement is that the communication interface shall ensure the protection of the PSC. See Chapter 4 for more detail.*	*None*
[184] Article 19 (2)(c) (now Article 27(3)(c))	A respondent asked the EBA to clarify that, when PISPs and AISPs are allowed to transmit authentication codes and PSC, the former must use only the communication interface constructed with that objective, which hampers neither consumer protection nor usability.	*The EBA is of the view that there is no need to further specify, as this is already stated in Article 27.*	*None*
[185] Article 19 (4) (now Article 27(4))	Publication: A number of respondents were of the view that the information should not be public because of security risks. Some respondents thought that it could be disclosed only based on a contractual agreement between the PSP and the interested parties (PISP, AISP, etc.), while other respondents mentioned a need-to-know basis.	*The EBA agrees that the RTS should not require all documentation to be published. Only the summary should be made publicly available, while the technical specification shall be available upon request. The requirement has been redrafted accordingly.* *The EBA disagrees with those respondents who suggest that documentation could be disclosed only on the basis of contractual arrangements or on a need-to-know basis.*	*Article 19(4) (now Article 27(4)):* *'Account servicing payment service providers shall ensure that their interface(s) follows standards of communication which are issued by international or European standardisation organisations. Account servicing payment service providers shall also ensure ~~make sure~~ that the technical specification of their communication interface is documented, and, as a minimum, available, at no charge, upon request by authorised payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments or payment service providers that have applied with their competent authorities for the relevant authorisation. ~~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,*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			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. Account servicing payment service providers shall make the summary of the documentation publicly available on their website.'
[186] Article 19 (4) (now Article 27(4))	Some respondents were of the view that it would be helpful to be provided with sample messages and responses to allow validation of interpretation and implementation of the specifications.	*This is covered by Article 29(5) on testing facility for connection and functional testing.*	*None*
[187] Article 19 (5) (now Article 27(5))	A number of respondents asked the EBA to list legitimate emergency situations and define a procedure for the notification of the emergency situation.	*The EBA is of the view that this is not within the scope of the mandate of these RTS and therefore cannot be addressed.*	*None*
[188] Article 19 (5) (now Article 27(5))	Three-month duration: Some respondents asked the EBA to extend the timeline to six months ahead of the implementation of the change, to accommodate the needs of merchants. Other respondents asked the EBA to shorten the timeline to one month only, to ensure competition, adaptation to rapid change and specification of new functionalities as a result of testing. Another set of respondents asked the EBA to consider simultaneous implementation of changes but with continued support for a longer period of six months.	*Given the conflicting views and comments, with some suggesting a shorter period and others a longer period, the EBA has decided, on balance, to keep to the drafted timeline of three months.*	*None*
[189] Article 19 (5) (now Article 27(5))	A number of respondents asked the EBA to also require that the website resource identifiers for these specifications and notifications of future and emergency changes be predictable and stable.	*The EBA is of the view that it would not be appropriate to define such situations given that the communication interfaces based on the final RTS do not yet exist. It seems difficult to predict at this stage.*	*None*
[190] Article 19 (6) (now Article 28(1))	Support to online platforms: While a number of respondents agreed with the paragraph, other respondents were of the view that guaranteeing, at no charge, the availability of the same support for the online platform for the user and	*The RTS requirement of the same level of service (availability), including support, follows from PSD2. The EBA is of the view that support is included in the level of service and in line with the requirements under PSD2. The article*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	for the TPPs increased the operating costs, with no obligation for the supported PSPs to develop and properly manage their interfaces with the ASPSP. These respondents asked for free support to be limited to basic queries.	*refers to the same level of service, including support, rather than whether it is free of charge or not. The EBA has therefore not made any changes.*	
[191] Article 19 (6) (now Article 28(1))	Some respondents asked the EBA to add to this paragraph the right of independent AISPs to monitor the service level of both the direct online access to the payment accounts (the AIS of the ASPSP) as well as the alternative communications interface made available by the ASPSP, to ensure that the same level of service is provided in both interfaces.	*The RTS cannot prescribe the behaviour of AISPs in this domain. Competent authorities can act based on complaints by AISPs.*	*None*
[192] Article 19 (6) (now Article 28(1))	A number of respondents were of the view that testing environments should be excluded from the requirement to provide the same level of service, on the basis that the testing interfaces are not always available because they are being used for the development of the next releases.	*The RTS require not that the testing facility shall be available full time but rather that it shall be at the same level of performance and availability as the consumer interface. The EBA is of the view that this requirement is proportionate and derives from PSD2.*	*None*
[193] Article 19 (6) (now Article 28(1))	One respondent asked the EBA to be more specific on statistics and specify the frequency of testing.	*The EBA is of the view that any more detail would not need be proportionate in that context, as this will demand on the PSPs.*	*None*
[194] Article 19 (7) (now Article 27(6))	A respondent asked the EBA to include a common 'testing' (and potentially certification) process for both API suppliers and consumers to operate effectively without creating the burdensome need for all TPPs to test against payment institutions.	*This is covered by Article 27(6) on the testing facility for connection and functional testing.*	*None*
[195] Article 19 (7) (now Article 27(6))	A number of respondents were of the view that providing a secure test environment such as the communication interface equated to creating a new channel for external entry. They therefore argued that the ASPSPs would be exposed to risks of fraud and cyberattacks as well as extra costs. - Some respondents as a result argued that this provision should be deleted altogether. - Others asked the EBA to further specify and limit the testing environment to avoid overburdening ASPSPs. For instance, the provision could mention that only providers authorised by national authorities could perform the test and that a single testing facility could be centralised with no sensitive information shared, etc.	*Before starting to offer a payment service, a PSP needs to test its payment service. Because of the novel set-up of PIS/AIS, the EBA is of the view that the ASPSP must be required to offer a testing facility.* *The EBA is of the view that security risks are mitigated by the requirement for TPP identification and the fact that providers must be authorised (or in the process of being so).* *However, the EBA agrees with some of the respondents that there could be a risk of fraud and cyberattacks, and has therefore limited the information available under this requirement to non-sensitive information only.*	*Article 19(7) (now Article 27(6)):* *'Account servicing payment service providers ~~ASPSPs~~ shall make available a testing facility, including support, for connection and functional testing by authorised payment information service provider and account information service providers, or payment service providers that have applied for the relevant authorisation, to test their software and applications used for offering a payment service to users.*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			No sensitive information shall be shared through the testing facility.'
[196] Article 19 (7) (now Article 27(6))	A number of respondents thought that there was a risk that ASPSPs would discriminate against certain PISPs/AISPs with which they have no established contractual commercial relationships. They would welcome guidance to national competent authorities (NCAs) on the need to ensure consistent provision of interface testing and support services by the ASPSP to all PISPs/AISPs that wish to access them.	*PSD2 creates the conditions for the service, including that it is not dependent on a contractual agreement. PSD2 also includes a principle of 'no discrimination'. Article 27(6) (former Article 19(7)) also clearly lays out the obligation on the ASPSPs to provide testing facilities and support to all. As mentioned in comment [195] some further clarifications have also been provided.*	*None*
[197] Article 19 (7) (now Article 29(6))	A respondent was of the view that the testing environment should exist on a continuous basis and not only before starting to be used for offering payment services to users.	*The requirement under the RTS is that there be a testing facility. The reasoning behind it is that payment services should be able to be tested before going live. Retesting in case of a change at the TPP or testing after a change in the ASPSP's technical specification is not excluded, for the same reason.* *However, the EBA is of the view that any more stringent rules requesting continuous testing would be disproportionate and could also be riskier.*	*None*
[198] Article 21 (1) and 21(2) (Article 30(1) and 30(2))	In a number of respondents' views, the requirements under these paragraphs are customer-dependent and therefore beyond the control of the PSP in the instance referred to. The respondents asked the EBA for clarification.	*Paragraphs 1 and 2 of Article 30 RTS refer to a session between all different PSPs that may be involved in a payment transaction. The customer is not part of this communication session. However the EBA acknowledged the second paragraph may have been a little unclear and has therefore edited it for clarity.*	*Article 30(2):* *2.Payment service providers issuing card-based payment instruments, account information service providers and payment initiation service providers shall keep the access sessions offered by account servicing payment service providers as short as possible and they shall actively terminate the session with the relevant account servicing payment service provider as soon as the requested action has been completed.'*
[199] Article 21 (1) (Article 30(1))	One respondent asked the EBA to publish and maintain an updated list of the so-called 'strong and widely recognised encryption techniques', i.e. a list of existing international financial cryptography standards.	*It is not within the EBA's mandate to do so and therefore this is not something that the EBA could do within the mandate of the RTS.*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
[200] Article 21 (3) (Article 30(3))	A respondent was of the view that the RTS should be clearer in the event of dispute about the security of the communication session.	*Any dispute would need to be resolved by the relevant parties and is not within the scope of these RTS.*	*None*
[201] Article 21 4)(c) and Article 22(1)(c) (now Article 30(4)(c) and 31(1)(c))	A respondent argued that a distinction needs to be made between the confirmation process and the handling of any subsequent settlement transaction. The respondent was of the view that settlement, i.e. the debiting of the PSU's account with its ASPSP, may involve either a credit transfer (initiated by the PSU) or a direct debit (originated by the card-based payment instrument issuer). In the respondent's view, this settlement part will be subject to the normal PSD2 provisions governing payment transactions between PSPs and falls entirely outside the scope of the RTS.	*Settlement is outside the scope of the RTS and therefore not something the EBA can address in these RTS.*	*None*
[202] Article 21 (4)(a) (now Article 30(4))	A respondent was of the view that some messages are exchanged before the PSU has asserted his/her identity and therefore may not be able to contain unambiguous reference to the PSU. The respondent was of the view that this was acceptable, since the purpose of the authorisation code issued by the ASPSP is to differentiate between several requests (purportedly) from the same PSU.	*The EBA is unclear whether or not this respondent is suggesting any changes to the RTS.*	*None*
[203] Article 21 (5) (now Article 30(5))	A number of respondents are of the view that Article 21(5) (and to some extent Article 19(2)) should clarify that handing over a PSU's credentials shall not occur, either at rest or in transit.	*Given that PSD2 allows PISPs and AISPs to rely on the authentication procedures of ASPSP, this is a suggestion that the EBA cannot accommodate.*	*None*
[204] Article 21 (5) (now Article 30(5))	A number of respondents asked the EBA to add a requirement for appropriate contact data to be available so that ASIPs and PISPs can contact the issuer of PSC in case of loss. The respondents also thought that methods of informing other providers should be specified (to follow the same format and for consistency).	*The EBA appreciates the need for the AISPs and PISPs to be aware of appropriate PSPs' contact data and agree methods of informing other providers. However, the EBA is of the view that it is not something that should be addressed under the RTS but rather is a practical implementation question, and has therefore not made any changes to the RTS.*	
[205] Article 21 (5) (now Article 30(5))	Some respondents also asked the EBA to add a requirement for PISPs to have a liability to 'clean up' after any such incident.	*While the EBA appreciates and understands the rationale for this comment, such a requirement is not within the scope of the RTS.*	*None*
[206] Article 21 (5) (now Article 30(5))	A number of respondents have queried the meaning of 'without undue delay'.	*The EBA is of the view that this terminology is commonly used in EBA guidelines and other legal documents and should not be further detailed within the RTS.*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
[207] Article 21 (5) (now Article 30(5))	One respondent argued that the requirement that PSC be not accessible to any of the staff is not achievable, especially when an AISP is entitled to repeated requests for information from the ASPSP without user interaction. On the other hand, other respondents were of the view that machines, rather than just staff, can be compromised or hacked even within secure environments and also need to be shielded.	*The EBA agrees with the comment that it is impracticable for no staff at all to see any data and has therefore redrafted the RTS to specify that this requirement focuses only on 'readable' data.* *The scope of the last sentence of Article 32(5) RTS covers any losses and therefore would include machine-related incidents too.*	*Article 21.5 (now new Article 30.5): Account information service providers ~~and,~~ payment initiation service providers and payment service providers issuing card-based payment instruments shall make sure that when transmitting personalised security credentials and authentication codes, these are not readable by any ~~their~~ staff at any time. In case of loss of confidentiality of personalised security credentials under their sphere of competence, account information service providers, payment initiation service providers and payment initiation service providers issuing card-based payment instruments ~~have to~~ shall inform without undue delay the payment services user associated with them and the issuer of the personalised security credentials ~~without undue delay~~.'*
[208] Article 21 (6)	A number of respondents were concerned by the mandatory use of ISO 27001. Some pointed out that this was not currently a requirement for credit institutions, e-money institutions or payment institutions, and others queried the rationale for it being mandatory for PISPs and AISPs. The respondents suggested that the EBA remove the reference or replace the reference either by something more generic or by a reference to Legal Entity Identifier (LEI) codes.	*The EBA agrees with the view of the respondents that mandating ISO 27001 would not be technology neutral and could undermine future innovation.* *The EBA also remarks that adopting some industry standards against others may disadvantage specific parts of the industry. The EBA has therefore not made any changes.* *Based on the same rationale, the EBA disagrees with the suggestion to replace the reference by LEI codes.* *The EBA has as a result deleted the whole paragraph.*	*~~Article 21.6: 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.~~*
[209] Article 22 (now	PSU's consent: A number of respondents asked the EBA for clarification of whether or	*The EBA agrees with the respondents that the PSU's consent is very important, but the EBA also highlights that consent is*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Article 31)	not the PSU's consent could be revoked and if so how. The respondents wanted to understand if, if consent can be revoked, guidance to the norm for data retention among PSPs should be given. The respondents were of the view that data need to be held in order to enable historic payment investigations, while the provider will also have obligations under GDPR which may conflict with the holding of data. Other respondents were of the view that it should be equally important for PSPs to check the PSU's consent, and they highlighted potential solutions such as OAuth 2.0.	*detailed under PSD2 and so is out of the scope of the RTS and cannot therefore be addressed in the RTS.*	
[210] Article 22 (1)(a) and (b) (now Article 31(1))	A number of respondents asked the EBA what information was included in the data exchange. For instance, they asked if it included overdraft limit, waiting transactions (i.e. those with future execution dates), failed transactions, standing orders and their details, direct debit authorisations, list of associated payment instruments, etc.	*The EBA is of the view that, based on the fact that ASPSPs will have different online platforms for their PSUs, with potentially different information, and based on PSD2 not harmonising the information, the RTS can only require that if the ASPSP provides a dedicated interface the information should be 'the same information' as what would be available under the customer online interface.*	*None*
[211] Article 22 (1)(a) and (b) (now Article 31(1))	A large number of respondents expressed concerns about the confidential information accessed by TPPs and argued that sensitive payment data should be strictly limited to those required by payment systems and they should not include other personal information. They asked the EBA to amend the RTS accordingly.	*PSD2 states that the customer has the right to use a PISP to initiate a payment transaction, and that the ASPSP has to provide the PISP with 'all the information on the initiation and the execution'. PSD2 does not set an obligation to provide other information to the PISP, such as overdraft limits. As this is defined in PSD2, the RTS cannot reiterate the same in the RTS but the requirements of the RTS are to be understood in line with these PSD2 provisions. However, for the purpose of clarity, the EBA has added a recital 18.*	*Recital 18:* *'In accordance to Articles 65, 66 and 67 Directive (EU) 2015/2366, payment initiation service providers, payment service providers issuing card-based payment instruments and account information service providers will only seek and obtain the necessary and essential information from the account servicing payment service provider for the provision of a given payment service and only with the consent of the payment service user. This consent may be given individually for each request of information or for each payment to be initiated or for account information service providers,as a general mandate for designated payment accounts and associated*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			payment transactions as established in the contractual agreement with the payment service user. Payment initiation service providers and account information service providers shall only request information on behalf of the payment service user with his/her consent.'
[212] Article 22 (1)(b) (now Article 31(1)(c))	A few respondents were of the view that, for the benefit of both the user and PISPs, PISPs should be able to display the balances of the listed accounts, so the user can choose the account with sufficient balance, and so the PISP can limit its credit risk by checking the availability of funds before initiating the transaction and before informing the payee that the transaction has been initiated.	*The EBA agrees that the PISP should be able to know immediately whether or not funds are available, and has redrafted Article 31(1)(c) as a result to include all payment transactions rather than solely card-payment transactions.*	*Article 31(1)(c):* *'They shall, upon request, immediately provide payment service providers ~~issuing card-based payment instruments~~ 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.'*
[213] Article 22 (1) (now Article 31(1))	Some respondents asked the EBA to include a time referent such as 'short as possible' or 'as soon as'.	*The EBA agrees that in the context of the revised Article 31(1)(c) a time reference was appropriate, and has added 'immediately upon request' as a result.*	*Article 31(1)(c):* *'They shall, upon request, immediately provide Payment service providers ~~issuing card-based payment instruments~~ 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.'*
[214] Article 22 (2) (now Article 31(2))	A respondent was of the view that it is vital for all involved parties to have proper information regarding the status of a process in any stage of the procedure. However, the respondent also remarked that in some circumstances not all parties may be informed properly (e.g. server unable to respond). The respondent therefore asked the EBA to add 'if possible' to this paragraph or to rephrase it.	*The EBA is of the view that there is no such need and has decided not to make any changes.*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
[215] Article 22 (2) (now Article 31(2))	A respondent asked the EBA to standardise the notification messages in case of an error. Another respondent was of the view that the notification messages needed to be properly documented, be exhaustive and provide sufficient level of detail to be valuable in the tracking and resolution of errors.	*The respondents' suggestions are not excluded by the RTS and the EBA appreciates that the industry may wish to act on them.*	*None*
[216] Article 22 (4) (now Article 31(4))	A number of respondents were of the view that, for the ASPSP to perform fraud prevention, the PISP needed to transmit to the ASPSP all information related to the payment. They suggested the following wording: 'PISPs shall provide the ASPSPs with all payment information, included information collected from the payment service user, when initiating the payment transaction.'	*In line with PSD2 and the objective of remaining technology and business-model neutral, the EBA is of the view that the RTS should mention only 'the same information' and has made the decision not to detail it any further.*	*None*
[217] Article 22 (4) (now Article 31(4))	A respondent is of the view that PISPs should be obliged not to retain fundamental transaction data (e.g. purpose of transaction) from the ASPSP.	*In line with PSD2 and the objective of remaining technology and business-model neutral, the EBA is of the view that the RTS should mention only 'the same information' and has made the decision not to detail it any further.*	*None*
Feedback on responses to Question 8			
[218] Article 19 (3) (now Article 28(3))	A number of respondents were in favour of the mandatory use of ISO 20022 elements (similarly to the SEPA Regulation). A number of these respondents, however, were of the view that it should be mandatory only for the data dictionary/definitions for specifying fields transferred via the interface (link with SEPA), i.e. the format of the message exchanged between ASPS and PISP/AISP, rather than the format of the technical communication.	*The reference to ISO 20022 elements refers only to a dedicated interface and solely in the context of the body of the message, the message template; it does not include how this message is transferred, which remains at the PSP's discretion.*	*New Article 28(3):* *'Account servicing payment service providers shall also ensure that ~~their communication~~ the dedicated 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~~ for financial messaging.'*
[219] Article 19 (3) (now Article 28(3))	By contrast, another set of respondents were of the view that the EBA should stay neutral at the regulatory level and not recommend specific standards, to remain future proofed. The respondents suggested instead that the EBA could refer to Open APIs and the industry standard could be left to the industry to develop. In their rationale, a number of respondents were of the view that the	*The ISO 20022 standard refers only to the template of the message and is commonly in use for SEPA credit transfers, between PSPs and between corporate users and PSPs. For that reason we do not believe that it would be too onerous. As mentioned in comment [218], the reference to this specific ISO standard refers only to the message template; it does not*	*New Article 28(3):* *'Account servicing payment service providers shall also ensure that ~~their communication~~ the dedicated interface uses ISO 20022 elements, components or approved message*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	reference would: - contradict PSD2; - contradict Article 20 of the GDPR – the argument being that it is not the customers but the ASPSPs that own the customers' data; - discriminate against part of the market, as it is used only for credit transfer and direct debit, and only for bank-to-bank communication, and is not widely adopted in other geographical areas; - be incompatible with TPP's direct access; and - be very costly to install for AISPs and PISPs as well as for card payments where it is not currently in use.	*include how this message is transferred, which remains at the PSP's discretion.*	*definitions, ~~if available, as well as standards of communication which are developed by international or European standardisation organisations~~ for financial messaging.'*
[220] Article 19 (3) (now Article 28(3))	One respondent expressed the view that, if ISO 20022 were to be the final standard, then, to respect and apply the principle of neutrality, direct online access to the payment accounts (the AIS of the ASPSP) would have to connect to the ASPSP using the same standard, in the same way as the communication interface must be the same.	*The EBA confirms that the principle of non-discrimination always applies as per the rule under PSD2.*	*None*
[221] Article 19 (3) (now Article 28(3))	A number of respondents agreed with mandating ISO 20022 but were of the view that XML should not be required.	*The reference to ISO 20022 in the original text of the RTS did not extend to the prescription of XML. As referred to in comment [218], it refers only to the message template rather than to the communication of it.*	*None*
[222] Article 19 (3) (now Article 28(3))	A number of respondents were of the view that the EBA should introduce different standards instead, such as ISO 8583 (or a standard derived from that), which is used in many payment systems, or a general reference to ISO. The respondents were of the view that otherwise the paragraph could lead to detriment for non-banks, could stifle innovation and might contradict recital 93 PSD2, which makes it clear that the RTS should be compatible with the different technological solutions. Other solutions or standards mentioned by respondents included Oauth2 or UTF-8, base64 encoding, 3D Secure and tokenisation.	*See comments [218] and [219].*	*None*
[223] Article 19 (3) (now Article 28(3))	<u>Messages</u>: Some respondents were of the view that the ISO 20022 standard had constraints around the length of messages, which they felt might have an impact on speed of transactions and communication costs. They were of the view that ISO 20022 messages would have to be drafted in the market to the stated purpose. Some of these respondents argued that, if such standard were	*The mandate for the EBA is to specify the requirements, rather than to write the specifications. The EBA Is of the view that any further detail is not likely to be future proofed, be technology neutral and encourage innovation in this area.*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	mandated, English should also be mandated as the language in documentation and error/warning/success messages. A number of these respondents were of the view that the EBA should develop a standardised list of messages and that the terminology 'or approved message definitions, if available' would leave too much freedom to PSPs.		
[224] Article 19 (3) (now Article 28(3))	A number of respondents agreed with the reference to ISO 20022 and asked the EBA to require a more detailed and wider approach in order to ensure interoperability. Suggestions made by the respondents include: - a formal specification of the interface; - a method to check compliance and anticipate work needed for cards and TPPs; - protocol for direct/indirect customer authentication; - supervisory body to coordinate and regulate (local or central); - prescribing the data dictionary to be used.	*The EBA is of the view that any further detail would undermine technology and business-model neutrality as well as future innovation.*	*None*
[225] Article 19 (3) (now Article 28(3))	A number of respondents took an alternative approach and asked the EBA to require standards to be set at Member State level, with NCAs ensuring that they are implemented in a timely manner.	*The mandate is to specify the requirements rather than to write the specifications, and the supervision of the RTS falls upon the national competent authorities.*	*None*
[226] Article 19 (3) (now Article 28(3))	With regard to future innovation, a respondent felt that it would be hard to consider any new standard with at least pan-European aspiration which is created in a single EU country to be an RTS-compliant standard before it is used by any provider outside that country.	*The EBA agrees with the respondent that such a risk exists but the EBA is of the view that the period of 18 months will enable the market to evolve.*	*None*
[227] Article 19 (3) (now Article 28(3))	A number of respondents agreed with the EBA's reference to standard ISO 20022 but asked the EBA to add a transition period and/or deadline for the standard to be implemented across all areas.	*While we appreciate that the implementation of the rules may require investment and time, the EBA is of the view that the existing 18-month transitional period set under PSD2 is sufficient and no further transitional period should be added.*	*None*
Feedback on responses to Question 9			
[228] Article 20 (now Article 29)	A very large number of respondents agreed with the EBA that it was a good thing to use qualified certificates, issued by a qualified trust service provider under the eIDAS Regulation, and had no problem with the types of devices used for payment services.		*None*
[229] Article 20 (now Article 29)	A number of the respondents were of the view that the eIDAS Regulation should be seen as a possible solution but not necessarily the unique legally enforceable mechanism of mutual identification, as one should	*In the context of mutual identification between different PSPs, the EBA is of the view that interoperability is essential. The respondents do not suggest an alternative but rather*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	not underestimate the impact of the (probably) patchy adherence of Member States to the eIDAS Regulation within the EU.	*highlight potential implementation difficulties. The EBA is therefore of the view that it should not make any changes to the RTS.*	
[230] Article 20 (now Article 29)	A large number of respondents also expressed concern about the practical applicability of this rule, as there are currently no providers in the market and there might not be any by October 2018. A number felt that there should be a minimum of five (or 'multiple') providers before such a standard could be used. The respondents' suggestions in the event of an absence of providers when the RTS come into force included: - setting up a transitional period; - allowing issuance also by a general Certificate Authority (potentially the EBA); - keeping both options for website certificate issuance (providers under eIDAS and a general Certificate Authority).	*The EBA agrees that there is some practical uncertainty. However, the EBA is of the view that with the RTS becoming applicable only by November 2018 at the earliest this timeline allows some time for the European market to develop. In the event that there was no provider available by November 2018, PSPs would be able to use other available certificates.*	*None*
[231] Article 20 (now Article 29)	Some respondents disagreed with the use of qualified certificates under eIDAS and asked the EBA to ensure that the RTS remain neutral, enabling other options. The respondents' rationale was the unclear adoption timeline, the cost and the limited appeal of the eIDAS framework outside Europe. A respondent also asked the EBA to evaluate whether or not risks were already mitigated by the existing standard PCI DSS. Indeed, the respondent was of the view that this already enabled ASPSPs to monitor PIS in order to safeguard their functioning and to avoid any 'data protection issue' or 'gap'.	*See comments [229] and [230].*	*None*
[232] Article 20 (now Article 29)	A number of respondents suggested that instead of 'website certificates' the RTS should favour 'electronic seals and qualified certificates for electronic seals', which are applicable to identify client to server (AISP and PISP identification to ASPSPs).	*The EBA agrees with the respondent and the article has been rephrased to be clearer and aligned with the eIDAS Regulation, mentioning 'electronic seals' and website certificates, as the EBA is of the view that depending on the business model a PSP could use one or the other.*	*Article 20 (now Article 29):* *1. 'For the purpose of identification, as referred to in letter a) of Article 21(1), payment service providers shall rely on qualified certificates for electronic seals as defined in article 3(30) of Regulation (EU) No 910/2014 or for website authentication as defined in*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			Article 3(39) of that Regulation ~~(EU) No 910/2014~~. *2. […]* *3. For the purposes of this Regulation, qualified certificates for electronic seals or website authentication referred to in paragraph 1 of this Article shall include in English additional specific attributes in relation to each of the following:* *(a) the role(s) of the payment service provider, which maybe one or more of the following: an account servicing payment service provider; a payment initiation service provider; an account information service provider; or a 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 electronic seals or website authentication.'*
[233] Article 20 (now Article 29)	A number of respondents were of the view that the standard would be helpful with regard to identification between servers of PSPs but not for devices held by users; in their views, eIDAS was not mature enough to be used as a communication interface. The respondents were of the view that such certificates should be used between servers of PSPs and not	*eIDAS certificates are not intended for PSUs; they are only for identification between servers of PSPs. The EBA therefore has made no change.* *As highlighted in comment [232], the EBA has included in the RTS both electronic seals and website certificates, to be technology and business-model neutral.*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	devices held by users. Some respondents asked the EBA to use qualified electronic stamp certificates for API-based communication.		
[234] Article 20 (now Article 29)	Some respondents were of the view that the RTS should provide more details for the certification process, including mandating security checks during certificate-based authentication, minimum technical standards, mandatory information, information needed by the ASPSP to perform authentication and contingency provisions (in case there was no provider when the RTS come into force). The respondents asked the EBA to include a reference to eIDAS Annex II or equivalent regulations in the RTS. They added that the eIDAS top-level CA certificate should be added in the list of CA certificates supported by most Internet browsers in order to have eIDAS public key infrastructure used.	*The EBA is of the view that the RTS should not go into any further detail to ensure technology and business-model neutrality. However, the EBA acknowledges that the considerations raised by the respondents are valid and will be relevant when considering the implementation of the RTS.*	*None*
[235] Article 20 (now Article 29)	A number of respondents are of the view that the RTS should include adequate protection (e.g. crypto smart cards) for PSP private key credentials, referring to international standards for PSP authentication in automated server-to-server communications. In their view, a common security policy needs to be developed, including the attributes of Article 20(3) RTS which are not part of eIDAS.	*The EBA is of the view that the RTS do not preclude any such protection and the industry may wish to act accordingly.*	*None*
[236] Article 20 (now Article 29)	Some respondents expressed the view that end-to-end (E2E) device authentication protocols regarding eID management and remote administration for tamper-resistant devices must be added to the RTS to ensure authenticity, integrity and security.	*The EBA is of the view that the RTS do not preclude such solutions and, although the EBA is of the view that the RTS should not go into any further detail to ensure technology and business-model neutrality, the EBA acknowledges that the considerations raised by the respondents are valid and will be relevant when considering the implementation of the RTS.*	*None*
[237] Article 20 (now Article 29)	Some respondents argued that there should be different types and complexities depending on the type of devices.	*The EBA is of the view that this would be complicated to operate and therefore is not in favour of adding any such requirement.*	*None*
[238] Article 20 (2) and 20(3) (now Article 29(2)	A few respondents asked the EBA to provide more details on the creation of a single specification for a common pan-European certificate for identification of PSPS that will include the requirements of Article 20(2) and 20(3) [now Article 29(2) and 29(3)], which are not part of eIDAS.	*The EBA is of the view that the RTS should not go into any further detail to ensure technology and business-model neutrality, although the EBA acknowledges that the considerations raised by the respondents are valid and will be*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
and 29(3))		*relevant when considering the implementation of the RTS.*	
[239] Article 20 (3) (now Article 29(3))	One respondent was of the view that the RTS should also consider the use of IP under an autonomous system.	*The EBA is of the view that this is not precluded by the RTS.*	*None*
[240] Article 20 (3) (now Article 29(3))	A number of respondents were of the view that more detail should be provided, including for instance providing the list of all parties in a transaction, stating the exact names of attributes, defining constraints on their values, listing the codebook for licence types and giving the link to an official list of names of competent authorities.	*The EBA is of the view that this would be a burdensome process and the more the data are shared the higher the risk of fraud or other abuse.*	*None*
[241] Article 20 (3) (now Article 29(3))	A respondent mentioned that the RTS should clarify whether a private or a public provider may issue certificates.	*The eIDAS Regulation refers to national Member State registers. This is not within the scope of the RTS.*	*None*
[242] Article 20 (3) (now Article 29(3))	A respondent was of the view that a process of maintaining a valid registry of certificates, including revocation steps, should be available for server-to-server communication.	*The eIDAS Regulation refers to national Member State registers. This is not within the scope of the RTS.*	*None*
[243] Article 20 (3) (now Article 29(3))	A number of the respondents argued that a register of qualified and registered PSPs offering PIS or AIS should be kept on a permanent basis, with real-time updates. One respondent, however, disagreed with the registration number being published.	*The eIDAS Regulation refers to national Member State registers. This is not within the scope of the RTS.*	*None*
[244] Article 20 (2) (now Article 29(2))	Some respondents asked the EBA to provide information about any authorities or initiatives that could play a leading role as service providers, as well as issuing the list of qualified service providers in each Member State.	*The eIDAS Regulation refers to national Member State registers. This is not within the scope of the RTS.*	*None*
[245] Article 20 (2) (now Article 29(2))	One respondent also suggested that the EBA should provide details about the process of examining PSPs before the issuance of certificates (including the standards used and whether it will be at European or Member State level).	*The eIDAS Regulation refers to national Member State registers. This is not within the scope of the RTS.*	*None*
[246] Article 20 (2) (now Article 29(2))	A respondent expressed the view that the development of a common certificate policy and a distribution list of certificates is needed.	*This remark touches on eIDAS regulations that are out of the scope of these RTS.*	*None*
[247] Article 20 (3) (now Article 29(3))	A number of respondents asked the EBA for clarity with regard to the certificate and whether there should be one certificate per activity or there can be a certificate for multiple roles. Some respondents specifically asked the EBA to include in Article 20(3)(a)	*We agree with the respondents that the RTS may not be very clear on this aspect. The EBA is of the view that a PSP should have only one certificate and that a certificate should therefore be able to cover different roles. The RTS have been*	*Article 20(3) (now Article 29(3)): 'For the purposes of this Regulation, qualified certificates for <u>electronic seals or</u> website authentication shall*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	the possibility of PSPs having different roles, so that one certificate can be used for different roles. The respondents also expressed the possibility of confusion if a PSP was using the wrong certificate.	*amended to provide that clarity. Where an ASPSP also decides to provide such services, the ASPSP will be registered as one of the categories mentioned under Article 20(3) RTS.*	*include additional specific attributes in relation to :* *a) the role(s) of the payment service provider, which can be one or a combination of the following: payment initiation service provider, account information service provider or payment service provider issuing card-based payment instruments.'*
[248] Article 20 (now Article 29)	A few respondents asked the EBA to harmonise the identification with the use of LEIs, internationally recognised identifiers.	*The EBA is of the view that the LEI is only an identification standard. It does not serve the same purpose of certification and is not significantly more developed than eIDAS. The EBA therefore does not wish to make any changes and has chosen to retain eIDAS.*	*None*
Feedback on Question 10			
[249] Article 22 (5) (now Article 31(5))	A large number of respondents queried how in practice the distinction could be made between 'human' (customer) PSU access (actively requesting) and 'automatic' access by an AIS. If the distinction cannot be made in practice, one respondent was of the view that the distinction should be deleted from the RTS. Another respondent suggested taking into account a further mechanism to indicate whether a request is made by the PSU on its own or by the AISP for other reasons.	*The EBA is of the view that the evidence suggests that the respondent's view is not accurate and that such distinctions can in fact be made.*	*None*
[250] Article 22(5)(b) (now Article 31(5)(b))	A large number of respondents commented on the RTS provision limiting access for the TPP to a maximum of two connections a day when the user is not actively requesting such information. - Some respondents agreed with the limit and viewed it as appropriate. - A few respondents were of the view that it was too often and asked the EBA to cap the number at once a day. - A large number of other respondents, by contrast, were of the view that the access should be more frequent to take into account the	*The EBA understands the concerns of the various respondents and has considered the different views expressed. The EBA has decided to increase the limit from two to four times a day in line with the maximum settlement cycle in a number of countries in Europe.* *The EBA has also introduced another change in the paragraph to make it clear that the ASPSPs could contractually agree to do it more often or differently, for*	*Article 31(5)(b) (former Article 22(5)(b)):* *'~~or,~~ where the payment service user is not actively requesting such information, no more than four times ~~a day~~ in a 24h period, unless a higher frequency is agreed between the account information service provider and the account servicing payment*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	real-time nature of payments. They were also of the view that two times a day would substantially limit the functionality of the AIS and in fact practically eliminate any kind of push AIS. Suggestions from respondents included: - Hourly access to have up-to-date information. The respondents' view was that it would provide an appropriate balance between AISP service priorities and the desire of the ASPSP to ensure optimal performance of the communication interface and would ensure that AISPs services are not discriminated against. - Three times a day in line with settlement/clearing. - Every 30 minutes. - Two connections a day to be kept for consumer access but a higher number to be agreed for TPP access. - Every 10 minutes (at a surcharge) in line with the current practice regarding the MT940/MT942 account statement messages. - No strict requirements for ASPSP regarding requested data amount (e.g. the historical length of an account statement) or performance (e.g. response time) and these conditions should depend on technical capabilities of a particular ASPSP, i.e. the load of its systems (if needed, the ASPSP should be able to limit account information requests to prevent systems failure). It would otherwise risk stifling innovation. - A minimum requirement of two times a day that could be configured by the user. In this scenario, the ASPSP would provide the user with an access control function in order to manage all access rights that were given to TPPs to access the payment account. The user's consent to request information without the user being present should be not only rate limited but also time limited as well and the consent should automatically expire after a time not longer than one year (cannot be automatically extended). - Specifying different expectations for different types of calls and payments (calls that seek to download bulk information may be limited to a low daily number, while calls that seek to establish if the records have changed and seek a record of the incremental change may be less intrusive and could be serviced far more frequently).	*instance using push notifications, as the EBA appreciates the importance of being flexible and ensuring that AISPs are able to continue to service their customers while the burden remains proportionate on the ASPSPs, which are likely to have many different TPPs requiring access at any one time.*	*service provider, with the customer's consent'*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	- A respondent argued that it was currently too early to define the right frequency. Whatever the appropriate number is, the respondent's view was that it should be either the same as the number of requests for an independent AISP or direct online access to the payment accounts or a global measurer that can be consumed through any AISP. - Encouraging banks to develop reporting systems to AISPs to inform them of any new operation using a secure push mechanism. In these respondents' view, it would be in line with the spirit of PSD2, as it would serve both TPPs' and banks' interest. They also argued that it would limit the risks of capacity problems, as data would be sent for only the accounts that have changed.		
[251] Article 22 (5)(b) (now Article 31(5)(b))	A number of respondents argued that Article 22(5)(b) [now Article 31(5)(b)] should be deleted, as automatic access should not be allowed. The arguments that the respondents mentioned are as follows: - For security reasons, the possibility of retrieving account information without the customer's active request should be prohibited. In the respondents' view, retrieving account data at regular time intervals, and not at the user's request, will allow the account balance and operations to be checked and behavioural data to be gathered, and in certain situations may also lead to spoofing. If obtained by criminals, such information would be a perfect source of knowledge about persons worth stealing from and would indicate the best ways of doing it. - Downloading of account information without the customer's active request would cause the need for multiplication of infrastructure capabilities, which the respondents thought would involve disproportionately large costs in relation to the aim of AIS from their user's perspective. - Modern technology allows all details necessary to reply to a customer's request to be retrieved sufficiently fast, with no need to generate automatic queries with no customer involvement. - If the customer does not want to record his/her status through	*In the EBA's view, it is important to ensure that TPPs can have automated access on the basis of competition, business-model neutrality and consumer convenience.*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	the AIS, the AISP should not request access. - In addition to the number of daily requests, there are other factors that may affect the availability of the service and system performance, such as the volume of data requested and the number of requests from different AISPs in the same timeframe. - Data requests should be made in real time, and based on a session initiated and requested only by the account holder.		
[252] Article 22 (5)(b) (now Article 31(5)(b))	Some respondents asked the EBA for clarification on what the word 'day' (in the context of two accesses a day) referred to and, more specifically, if it referred to 24 hours.	*The EBA agreed that clarification was needed and has as a result inserted the reference to 24 hours.*	*Article 31(5)(b) (former Article 22(5)(b)):* *'~~or,~~ where the payment service user is not actively requesting such information, no more than four times ~~a day~~ in a 24h period, unless a higher frequency is agreed between the account information service provider and the account servicing payment service provider, with the customer's consent'.*
[253] Article 22 (5)(b) (now Article 31(5)(b))	A respondent suggested that the roles that a PSP may have and the technical requirements for them should be further analysed in separate RTS.	*The EBA does not have any such mandate and this falls outside the scope of these RTS.*	*None*
[254] Article 22 (5)(b) (now Article 31(5)(b))	Some respondents were concerned about the risk of denial of service, especially if there was no coordination between participants.	*The EBA is of the view that the risk would be even more acute if TPPs could access information at all times. Capping at four times a day limits this risk.*	*None*
[255] Article 22 (5)(b) (now Article 31(5)(b))	Some respondents were of the view that the RTS should state that the AISP must state in the request whether the request is or is not actively requested by the service user. If such information is not provided, the ASPSP cannot introduce any throttling limits on the interface.	*The EBA is of the view that no further detail should be provided.*	*None*
[256] Article 22 (5)(b) (now Article 31(5)(b))	A number of respondents were concerned about the amount of data that can be requested. For instance, if PSUs are allowed to request their full transaction history for the past seven years, this would in their view lead to an enormous (and unacceptable) load on the ASPSP's systems. Some of the respondents assume that ASPSPs are allowed to limit the amount	*PSD2 defines AIS as 'an online service to provide consolidated information on one or more payment account ...'* *The RTS state that the ASPSP shall provide 'the same information as made available to the customer when directly accessing the information online'. PSD2 also states that the*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	of data that can be transferred in one request in order to ensure the usability and service level of online banking services. Respondents were also of the view that recurring requests for information and vast amounts of data were likely to encumber and slow down the system. They asked the EBA to ensure that the ASPSPs are able to restrict usage of the system on the same prerequisites as the ones applicable to the customer himself/herself.	*ASPSP has to provide the PISP with 'all the information on the initiation and the execution'.* *The EBA is of the view that nothing further should be added in the RTS in the light of PSD2.*	
[257] Article 22 (5)(b) (now Article 31(5)(b))	Other respondents also argued that ASPSPs should be allowed to publish time windows for AISPs to query information, and to set a maximum amount of information that can be queried, the latter expressed in hits per second, both at the level of any AISP and for all AISPs combined.	*The EBA is of the view that any further detail would likely be too prescriptive.*	
[258] Article 22 (5)(b) (now Article 31(5)(b))	A respondent was of the view that, in order to comply with Article 67(2)(a) PSD2, the PSU has to provide explicit consent and that AISPs should inform PSUs if they would like to make use of the option of Article 31(5)(b) RTS to request information without the active involvement of the PSU.	*Consent rules are laid down in PSD2 and are per se out of the scope of the RTS. However, the EBA is of the view that a clarification could be helpful and has therefore added a reference in a new recital 18.*	*New recital 18:* *'In accordance to Articles 65, 66 and 67 Directive (EU) 2015/2366, payment initiation service providers, payment service providers issuing card-based payment instruments and account information service providers will only seek and obtain the necessary and essential information from the account servicing payment service provider for the provision of a given payment service and only with the consent of the payment service user. This consent may be given individually for each request of information or for each payment to be initiated or for account information service providers,as a general mandate for designated payment accounts and associated payment transactions as established in the contractual agreement with the payment service user. Payment initiation service providers and account information service providers*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			shall only request information on behalf of the payment service user with his/her consent.'
[259] Article 22 (5)(b) (now Article 31(5)(b))	A number of respondents argued that the prior explicit consent of the customer (PSU) is essential. The PSU should also be able to withdraw or limit the option in Article 31(5)(b) RTS.	*See comment [258].*	*New recital 18; See comment [258]*
[260] Article 22 (5)(b) (now Article 31(5)(b))	A number of respondents pointed out that other factors beyond the number of accesses a day, such as the volume of data requested and the number of requests from different AISPs in the same timeframe, may affect the availability of the service.	*See comments [250] and [256].*	*None*
[261] Article 22 (5)(b) (now Article 31(5)(b))	Any activity of a service provider that affects the availability of its service to its customer should be a matter for that organisation and not come under industry standards-based limits.	*The EBA disagrees that this is solely for the ASPSP, as PSD2 obliges the ASPSPs to share their information and providing too many restrictions and conditions in the RTS would threaten the very existence of the rule.*	*None*
[262] Article 22 (5)(b) (now Article 31(5)(b))	A respondent believed that a paragraph 22(6) should be added to request the AISP to inform ASPSPs when requesting information.	*The EBA would like to remind the respondents that an AISP has to identify itself under PSD2. The EBA is of the view that any additional rule would seem overly burdensome.*	*None*
[263] Article 22 (5)(b) (now Article 31(5)(b))	A number of respondents asked the EBA to introduce the possibility for ASPSPs to charge for the services provided to AISPs, at least in the case of exceeding the specified request volume, or otherwise to allow ASPSPs to limit the interface bandwidth for TPP in such situations.	*The EBA has revised the draft RTS to provide access four times a day for free but the EBA is also of the view that if the providers would like to have a higher frequency they could contractually decide to do so provided that the customer has given consent.*	*Article 31(5)(b):* *'~~or,~~ where the payment service user is not actively requesting such information, no more than four times ~~a day~~ in a 24h period, unless a higher frequency is agreed between the account information service provider and the account servicing payment service provider, with the customer's consent'.*
[264] Article 22 (5)(b) (now Article 31(5)(b))	A respondent asked the EBA to include criteria related to the concentration of requests per time unit, so that those requests are not sent in large numbers at the same moment, as the respondent was of the view that such situation could affect the performance and stability of systems, including from the perspective of customers directly using electronic banking.	*As mentioned in comment [256] the EBA is of the view that in line with PSD2 the AISP and PISP can request only the 'same information' and that any additional criteria would probably be too burdensome for AISPs and PISPs.*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
[265] Article 22 (5)(b) (now Article 31(5)(b))	A respondent highlighted that an additional risk with automated use was dormancy, as a user may cease practical use of a service, but may not deactivate an account with AISP for some time.	*The EBA is of the view that this risk is mitigated by the obligation to use SCA every 90 days under the exemption from accessing limited payment transaction information in Article 10.*	*None*
[266] Article 22 (5)(b) (now Article 31(5)(b))	A number of respondents were of the view that, regardless of the specific number of times a day an AIS/PIS could access information, it should be the same as the number of times a customer can access his/her online banking account. They were of the view that, if the payment user received different treatment depending on how he/she accesses his/her payment accounts, this would be against the PSD2 principle of neutrality and a level playing field.	*The EBA agrees with the respondents with regard to the need to be non-discriminatory and this is exactly the reason why Article 31(5)(a) RTS on customers accessing information does not specify any numbers, in the same way as customers can access their online banking at any time. The restriction in Article 31(5)(a) comes only when the AISP itself is accessing the information. In that case, the EBA is of the view that a balance needs to be struck between the competing needs of the ASPSPs and AISPs/PISPs.*	*None*
[267] Article 22 (5)(b) (now Article 31(5)(b))	A number of respondents asked the EBA to limit the request functionality (e.g. statements for two years only).	*See comment [256].*	*None*
[268] Article 22 (5)(b) (now Article 31(5)(b))	Some respondents pointed out that banks, as ASPSPs, have to comply with other regulations as well, such as the data protection legal framework and the AML legal framework. They were therefore of the view that it was necessary to require symmetry in the information that PISPs and AISPs have to provide to banks (ASPSPs) and the information that banks have to provide to them.	*The EBA is of the view that wherever possible such symmetry has been taken into account.*	*None*
[269] Article 22 (5)(b) (now Article 31(5)(b))	A number of respondents were of the view that the right limit should be a combination of volumes of data combined with the frequency of requests.	*See comments [256] and [264].*	*None*
[270] Article 22 (5)(b) (now Article 31(5)(b))	A respondent also sought clarification on what recourse ASPSPs can have against those who breach the limit. Assuming that these AISPs use certificates to identify themselves as suggested, requests could be refused.	*The RTS will be directly applicable to all PSPs within the EU. Any breach of the RTS or PSD2 would be a breach of EU law and would have to be dealt with accordingly by the relevant supervisory authorities.*	*None*
General feedback			
[271] General responses	Definitions: A number of respondents asked for clarification and definition of the	*1) The first term originates in and is defined under recital 30 PSD2.*	*Article 10 (former Article 8.1.a) – 'Payment account Information*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	following terms used in the RTS: 1) 'Payment Service Providers'; 2) 'sensitive payment data' and its relationship to personalised security credentials. A number of respondents also asked the EBA to use clear and consistent roles and terms such as 'payer', 'payment service user', 'payee' and 'merchant'. One respondent suggested that 'payer' should be replaced by 'PSU' in appropriate areas of the text where it relates to an activity such as accessing an account online or using account information services and does not involve payment initiation (such as in Articles 8(1)(a) and 17(1) [now Articles 10 and 25]). A few respondents asked the EBA to insert some definitions in the RTS to bring them in line with PSD2 or market usage. For instance they mentioned that 'Mandate' should be understood as the expression of consent and authorisation given by the Debtor to the Creditor to allow such Creditor to initiate Collections for debiting the specified Debtor's account and to allow the Debtor Bank to comply with such instructions in accordance with the EPC SDD Rulebooks. An e-Mandate is an electronic document which is created and signed in a secure electronic manner.	*2) With regard to 'sensitive payment data', this is also a term introduced in PSD2 and the EBA has stated in the Consultation Paper that, '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' (p. 16).* *The EBA agrees with the need for consistency across the RTS on the terminology used and the EBA has made a number of changes as a result. This includes the change from 'payer' to 'payment service user' under the new Article 10. The EBA is not able to list all the changes under the comment.* *The RTS do not mention 'mandate' in the context of the comments made. The EBA therefore cannot comment any further.*	*1. ~~The application of strong customer authentication in accordance with Article 97(1) of Directive (EU) 2015/2366 is exempted where:~~ Subject to paragraph 2 of this Article and compliance with the requirements laid down in paragraphs 1, 2 and 3 of Article 2, payment service providers are exempted from the application of strong customer authentication ~~in accordance with Article 97(1) of Directive (EU) 2015/2366~~ where a ~~the payer accesses exclusively the information of its payment account online, or the consolidated information on other payment accounts held,~~ payment service user is limited to accessing either or both of the following items online without disclosure of sensitive payment data:* *(e) the balance of one or more designated payment accounts;* *(f) the payment transactions executed in the last 90 days through one or more designated payment accounts.* *2.For the purpose of paragraph 1 payment service providers are not exempted from the application of strong customer authentication ~~shall not be exempted~~ where either of the following condition is met:* *(c) the payment service user ~~payer~~ is accessing~~es~~ ~~the information of its payment account, or the~~*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			~~consolidated information on other payment accounts held,~~ online the information specified in letters (a) and (b) of paragraph 1 for the first time, *i. the last time the payment service user ~~payer~~ accesse~~d~~s ~~the information of its payment account, or the consolidated information on other payment accounts held,~~ online the information specified in letter (b) of paragraph 1 and ~~later than one month after the last day on which~~ strong customer authentication was applied more than 90 days ago.'*
[272] General responses	Scope: A number of respondents were confused with regard to the scope of the RTS and asked the EBA for clarity: 1) A number of respondents asked whether or not one-leg transactions were in the scope of the RTS. 2) A respondent suggested adding some clarifications to the recitals of the RTS regarding the scope of SCA. It was of the view that not all transactions involving some form of electronic transmission of transaction data fall under the scope of SCA, as these transactions are often paper-based from a legal point of view. In particular, he was of the view that SEPA direct debits generated at the point of sale by means of the payer's debit card are not an initiation of an electronic payment within the meaning of Article 97 PSD2 and/or	*1) The EBA agrees that the particular issue of cross-border transactions may be confusing. As mentioned in paragraph 16 of the rationale section, the EBA, following discussions with the Commission, interprets PSD2 as meaning that, where payment instruments issued under a national legal framework that does not require the use of SCA (such as magnetic stripe cards) are used within the EU or when the payment service provider of the acquirer is established in a jurisdiction where it is not legally required to support the SCA procedure designed by the European issuing PSP, the European PSPs shall make every reasonable effort to determine the legitimate use of the payment instrument. As specified in paragraph 16 of the*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	SCA, since the SEPA mandate is given not electronically but personally in writing at the point of sale. The same rationale applies to credit card transactions where the payer authorises a payment transaction by signing a credit card slip/receipt. 3) Several respondents asked the EBA to clarify in the text of the RTS that AIS is a service that may be provided by AISPs or ASPSPs to PSUs. Some respondents expressed a preference for separate RTS for AISPs if SCA is not adapted for them from a risk-based perspective and requires differentiating the credential management in this case. 4) A number of respondents asked the EBA if EMV chip cards are in scope and if chip and PIN transactions would be compliant, given that, when a card is compromised, any PIN would be accepted, defying the requirement for the independence of two elements. 5) A few respondents asked the EBA to clarify whether or not card payments and recurring card payments fell under the scope of Article 97(1)(b). 6) Several respondents wondered if magnetic stripe cards will be allowed under the RTS. 7) Several respondents asked for clarification of whether or not corporate transactions (initiated via dedicated host-to-host protocols, e.g. SWIFT, EBICS) are in scope, since 'security is already accounted for in the regulations that trust service providers must comply with', but also posing challenges in the context of dynamic linking – e.g. batch transactions with 200 payees or solutions for electronically submitted transactions where authorisation is done by an entitled person of the enterprise by giving a handwritten signature on paper to the ASPSP. 8) One respondent also mentioned that setting up a series of direct debit e-mandates should be covered by SCA. 9) One respondent mentioned that payment initiation via a PISP bears a significant risk of fraud for corporates payments and an alignment	*rationale, the EBA is of the view that, in the light of the limitations of cross-border transactions, they shall not be included in the transactions for the purpose of the calculation of fraud rates under the new Article 16.* *2) The EBA is of the view that this relates to the scope of PSD2. Direct debits are out of the scope of the requirement for SCA and therefore out of the scope of the RTS as they are initiated by the payee. However, e-mandates are not, as they are electronic by nature. Series of payments initiated through a card are in the scope of PSD2 and the RTS, as the EBA understands, following discussions with the Commission, that these transactions are transactions by the payer initiated through the payee. A card transaction is electronic, as it is initiated in the terminal, as opposed to imprinter card transactions, which are paper-based and thus exempted from SCA under PSD2.* *3) The EBA is of the view that, where ASPSPs also provide AIS, they have to comply with all the relevant requirements applicable for AISPs under the RTS.* *4) The EMV chip cards are in the scope of PSD2 and the RTS. The EBA is of the view that chip and PIN transactions are not non-compliant with SCA provided that they are DDA or higher. It is, however, up to the providers and issuers to assess whether or not their systems comply with PSD2 as well as the RTS requirements.* *5) Please see the EBA's response under 2).* *6) The EBA is of the view that, in the light of the PSD2 security requirements as well as the RTS requirements, magnetic stripe cards are unlikely to be compliant, even as a fall-back. Indeed, a magnetic stripe card (and also an EMV SDA chip card) does not create a dynamic*	

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	of provisions of PSD2 is needed. 10) One respondent was of the view that some 'internet payment service providers' (technical service providers or TSPs) for online merchants are out of the scope of PSD2 and should therefore not be subject to SCA.	*authentication code and the PIN is also static.* *7) Corporate transactions (including via SWIFT) are within the scope of SCA in PSD2 and the RTS, except if some fall under the general exemptions of Article 3 PSD2. See comments [49] to [51] with regard to security and the request from some respondents to include an exemption for corporate payments.* *8) The EBA is of the view that creating an e-mandate falls under SCA, according to Article 97(1)(c) PSD2, and the exemption under Article 13 RTS requires SCA when creating or amending a series of payments.* *9) The EBA is of the view that nothing should be further clarified in the RTS and reminds the respondent that PSD2 includes a non-discriminatory principle. The EBA also reminds the respondent that PISPs are able to rely on the SCA performed by the ASPSP.* *10) TSPs are out of the scope of the RTS and PSD2. The EBA notes, however, that PISPs are not TSPs and that, if a PSP that is within the scope of the RTS outsources any activity to a TSP, the PSP remains ultimately responsible and must comply with all the requirements under PSD2 and the RTS.*	
[273] General responses	A number of respondents had questions with regard to the application of SCA: 1) One respondent suggested including a recital in the draft RTS clarifying that 'payments initiated by the payee, that can also include card-based payment transactions, are not subject to the mandate to perform SCA'. 2) Some respondents challenged the level playing field in the context of SCA requirements for card payments and requiring SCA for only selected SDD payments (e-mandates). According to one reference	*1) Please see the EBA's response to comment [272] 2).* *2) The EBA agrees with the view presented and confirms that this is in line with the EBA's interpretation of PSD2. As this is a matter of interpretation of PSD2 and the scope of PSD2, this is, however, not something that the EBA can include in the RTS.* *3) The EBA is of the view that, in an EMV chip offline transaction, either the PIN is verified offline (i.e.*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	to the Q&A document of the European Commission on the first PSD, '[a] transaction initiated through the payee is a transaction which is initiated by the payer through the payee'. In some payment systems, the payer will initiate a payment (for an individual payment) that will trigger a one-off direct debit. The respondent that made this reference believed that the draft RTS should clarify that in these cases – in line with paragraph 18 of the draft RTS – SCA should be required. 3) A few respondents were of the view that the current SCA requirements to be used in face-to-face payments would lead to all transactions being authorised online. This would prevent PSPs from supporting offline chip transactions even in such case as transit. 4) A respondent enquired if signature (including with a stylus on a digital tablet) is an acceptable Consumer Verification Method under the new EBA RTS.	*just between the chip and the terminal) or the transaction itself is authorised offline – usually within certain value limits.* *If the PIN is given, the offline transaction could be SCA compliant. If no PIN is given, the offline transaction would need to fall under an exemption, e.g. for low-value contactless or transactions at unattended terminals.* *4) The EBA is of the view that it complies with the requirements under the RTS, including the presence of a dynamic element.*	
[274] General responses	A number of respondents had questions with regard to the application of SCA: 1) They asked the EBA for greater clarity on authentication codes. Many respondents were of the view that a distinction should be made between authentication and authorisation (codes). In their view the codes relate to different processes. They also asked the EBA for clarification on the concept of authentication codes, as recital 96 of PSD2 notes that SCA 'may [but does not have to, in the respondents' view] result in authentication codes such as one-time passwords'. 2) More fundamentally, the respondents disagreed with the need to require the generating of an authentication code, as, in their view, this requirement limits technology neutrality. 3) One respondent was of the view that, if the authentication procedure stays in the sphere of the ASPSP, then ASPSPs should be in control of the provision of the PSU credentials.	1) *As highlighted in comment [1], the payment process contains three phases: authentication, authorisation by the payer and authorisation by the PSP of the payer. The first two are within the scope of the RTS while the last is not. Authentication refers to a procedure that allows the PSP to verify a customer's identity. Authorisation refers to a procedure that checks whether or not a customer or PSP has the right to perform a certain action, e.g. to transfer funds or to have access to sensitive data.* 2) *The EBA disagrees with the respondents on the basis that the RTS do not define the elements that should constitute the authentication code and therefore remain as technology neutral as possible. The payer's PSP needs to authenticate the payer to make sure that it is really the payer and thus gives its consent through something tangible.* 3) *The principle under PSD2 is that the credentials can be*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	4) A number of respondents were of the view that confidentiality should not be a requirement for authentication codes.	*relied upon by, and therefore shared with, AISPs and PISPs.* 4) *PSD2, in its mandate for the EBA to develop these RTS, does include a requirement for confidentiality, which the EBA has been fulfilling.*	
[275] General responses	With regard to dynamic linking, a small number of respondents asked the EBA to be less specific on dynamic linking/segregation in order to be technology neutral. Some respondents requested that the EBA add a possibility of voluntary application of dynamic linking.	*As highlighted under Chapter 2 of the RTS and in particular comment [10[, the Article is now less detailed and more technology neutral. The EBA is therefore of the view that the comment from these respondents has been addressed.* *Adding a possibility to apply SCA voluntarily is not laid down by PSD2 and cannot be added to the RTS because of the legal nature of RTS. However, this is something that PSPs may want to consider.*	*None*
[276] *SCA scope of application*	A number of respondents asked the EBA to limit the scope for SCA to online payments only.	*The scope is clearly defined in Article 98(1)(a) and Article 97(1)(b) PSD2 and is not subject to change or amendments.*	*None*
[277] General responses	Many respondents asked the EBA to state expressly that the PISP and AISP can rely on the SCA of the ASPSP.	*Recital 30 PSD2 and Articles 66 and 67 of PSD2 clearly state that the AISP and PISP can rely on the SCA conducted by the ASPSP. The RTS cannot restate PSD2 obligations.*	*None*
[278] General responses	A small number of respondents asked the EBA for clarification on the status of e-mandates.	*The EBA's interpretation of PSD2 is that e-mandates are included under Article 97(1) and therefore the rules of the RTS that relate to Article 97(1) will apply to e-mandates.*	*None*
[279] General responses	Several respondents asked the EBA to review the RTS to better address data protection and data privacy, as well as better explain the link with the Data Protection Regulation. Some also highlight that the access to data is currently treated differently among European countries, which could affect the consumers' levels of trust and consequent willingness to give access to their accounts if this information were monetised.	*While the EBA appreciates and acknowledges the importance of data protection and data privacy, this is out of the scope of the RTS and therefore not something it can address there. However, the EBA stresses the importance of this consideration for PSPs when implementing the RTS.*	*None*
[280] General	One respondent was of the view that the PSP and the authentication	*As highlighted in the 2006 CEBS Guidelines, and in particular*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
responses	provider should be allowed by the RTS to be two separate entities (e.g. in an outsourcing scenario). In order for the authentication procedure to be outsourced, the respondent was of the view that the PSP credential and authentication credential need to be separated out by certifying the authentication procedure.	*Guideline 2, the responsibility for any outsourced functions is always retained by the outsourcing institution.*	
[281] General responses	One respondent expressed concern about the high risk of phishing claims and was of the view that PSUs should only be allowed to enter their personalised security credentials received from their ASPSP in the secure internet environment of the ASPSP. The respondent was also of the view that the EBA should impose strict requirements on AISPs when storing customer transaction data (in line with the requirements set for ASPSPs).	*Article 97(5) PSD2 enables PISPs/AISPs to rely on authentication procedures of the ASPSP. This can therefore mean that PSC could be entered on a different website from the ASPSPs' website. The EBA is therefore of the view that any restriction as suggested by the respondent would be in breach of PSD2 and therefore cannot be accommodated.* *The suggestion made by the respondent about data storage is already included in Article 19 RTS.*	*None*
[282] General responses	One respondent expressed concern about the fact that the SCA procedure protects the payer (and the payee) only from involuntary disclosure of their secret(s) (secure credentials), but not from disclosure via 'social engineering'. The respondent asked the EBA to address social engineering threats and threats connected to disloyal personnel of the PSPs, whether or not it has been outsourced.	*The RTS include a requirement in Article 32(3) for PSC and authentication codes to be unreadable by any of the PSP's staff, which addresses part of the respondent's concerns. The EBA is of the view that the respondent also makes a more general point that cannot be addressed in the RTS, as it is out of their scope.*	*None*
[283] General responses	In one respondent's view, specific waivers [exemptions] should be considered for persons with disabilities. The respondent asked the EBA to launch a working group on payment for persons with disability.	*This is a general issue that has been mentioned in previous EBA consultations. While the RTS are not able to address this issue, it is important to give consideration to this when implementing and supervising PSD2 overall.*	*None*
[284] General responses	One respondent was of the view that ASPSPs should have an option of redress against third parties for losses related to incidents caused by them.	*Redress is out of the scope of the RTS.*	*None*
[285] General responses	Two respondents were of the view that most fraud occurs after the initial login. They therefore asked the EBA to include a requirement for continuous risk-based authentication and threat detection that can identify remote access (malware) and social engineering attacks that occur after login.	*While the EBA cannot add such a requirement under the RTS, it has added a new Article 2 (to replace former Article 1(4)) to clarify the need for PSPs to conduct risk-based analysis and monitoring, not just during the authentication period but before and after too.*	*New Article 2:* *'General authentication requirements* *1. For the purpose of the implementation of the security measures referred to in letters (a) and (b) of Article 1, payment service providers shall have transaction monitoring mechanisms in place that enable*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			them to detect unauthorised or fraudulent payment transactions. 2. *The transaction monitoring mechanisms shall be based on the analysis of payment transactions taking into account elements which are typical of the payment service user in the circumstances of a normal use by the payment service user of the personalised security credentials.* 3. *Payment service providers shall ensure that the transaction monitoring mechanisms takes into account, at a minimum, each of the following risk-based factors: lists of compromised or stolen authentication elements; the amount of each payment transaction; known fraud scenarios in the provision of payment services; signs of malware infection in any sessions of the authentication procedure.* 4. *Where payment service providers exempt the application of the security requirements of the strong customer authentication in accordance with Article 16, in addition to the requirements in paragraphs 1, 2 and 3, they shall ensure that the transaction monitoring*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
			mechanisms take into account, at a minimum, and on a real-time basis each of the following risk-based factors: the previous spending patterns of the individual payment service user; the payment transaction history of each of the payment service provider's payment service user; the location of the payer and of the payee at the time of the payment transaction providing the access device or the software is provided by the payment service provider; the abnormal behavioural payment patterns of the payment service user in relation to the payment transaction history; in case the access device or the software is provided by the payment service provider, a log of the use of the access device or the software provided to the payment service user and the abnormal use of the access device or the software.'
[286] General responses	One respondent was of the view that many of the trust mechanisms rely on PKI and that, in his/her view, SCA (as well as PSD2 overall) should not overly rely on any one trust chain. The respondent is of the view that a recovery mechanism should be in place to issue new credentials as well as offer alternative trust chains to ensure against systemic failure. In a similar vein, the respondent is of the view that user credentials can be compromised and that mechanisms should be in place to ensure that user credentials can be reissued and old credentials revoked on individual, group and population levels.	*The EBA is of the view that the respondent's general view and suggestions are out of the scope of the RTS but that they may be covered by the GDPR as well as potentially by the EBA Guidelines on Management of Operational and Security Risks.*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
[287] General responses	A few respondents referred to the need to reference particular standards such as NIST Special Publication 800-63B (on Authentication and Lifecycle Management) in addition to any other European security standards bodies (Articles 3 and 5), NIST, EMV, PCI and Global Platform standards (Article 4) to ensure that physical devices issued or approved for use to the payer have been market tested with the existing supply chain and that business rules/liabilities apply. The respondents also asked the EBA to mention the use of suitable cryptographic (proven) standardised protocols as well as best practices and standards such as eIDAS, STORK or NIST 800-63 (Articles 3 to 5).	*While the EBA appreciates the value of being more detailed, the EBA is of the view, as indicated in a number of previous comments, that the RTS should be as technology neutral as possible. The RTS do not preclude applying these standards provided that they comply with the RTS requirements.*	*None*
[288] General responses	A few respondents suggested that the requirements for SCA should be aligned with the eIDAS Regulation and the EU Commission Implementing Regulations on the Level of Assurance (LoA).	*The EBA is of the view that current SCA requirements seem to be aligned with those regulations as far as possible, but eIDAS is a different toolkit for eID management and LoAs cannot be pre-mapped to the SCA requirements of the RTS, as indicated by the EBA in the public hearing.*	*None*
[289] General responses	A few respondents asked the EBA to introduce reciprocal communication between AISP/PISP and ASPSP in the RTS to: i) enable the AISP/PISP to forward additional information to the ASPSP which could assist the ASPSP in mitigating fraud; and ii) enable the sending of clear and standardised return codes and warnings to ASPSP.	*The EBA acknowledges the relevance of such concerns but is of the view that this would be out of the scope of the RTS and beyond what is envisaged under PSD2.*	*None*
[290] General responses	A large number of respondents were of the view that the link with the liability regime should be made clearer in a number of places throughout the draft RTS.	*While the EBA acknowledges the link between the RTS and the liability regime, the latter is not within the scope of the RTS mandate.*	*None*
[291] General responses	One respondent was of the view that the line between card-not-present and card-present transactions for in-store payments are getting thinner by the day and that in his/her view this may be at odds with the exemptions under the RTS.	*The EBA acknowledges that innovation and change may take place in the very near future. There is a specific review clause under Article 98 PSD2 and the EBA may consider proposing that the Commission review this if such a situation arises.*	*None*
[292] General responses	A number of respondents asked the EBA for more clearly defined guidelines for operation during the transitional period, i.e. the period from January 2018, when PSD2 has to be implemented, until the RTS are applicable. In addition, given that in the UK the regulator does not have the appropriate secondary legislation to implement the security of internet guidelines, one respondent asked the EBA what the PSPs in the UK	*The EBA agrees that there is a need to provide some guidance to the payment industry with regard to the transitional period during which the Guidelines on internet payment will remain applicable. There is no mandate in the Level-1 text for the EBA to develop guidelines and at the time of writing there have been no concrete detailed discussions and agreement on a cooperative approach between all*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	should do during that transitional period.	*competent national authorities.*	
[293] General responses	A respondent asked the EBA to provide additional details or requirements for AISP data retention, data-auditing and data-reporting procedures as part of PSD2 as a whole.	*This is outside of the scope of the RTS.*	*None*
[294] General responses	A few respondents were of the view that the RTS could lead to unbalanced over-regulation in areas in which no regulation is needed or much lighter regulation would be sufficient. One respondent, for instance, argued that the present RTS were written with online credit transfers and the corresponding ASPSP services mainly in mind, while other payment methods have played a lesser role. Another respondent, however, believes that too much focus has been placed on card payments.	*The EBA has a clear mandate under PSD2, a Level-1 text, to introduce regulation in all the areas covered in the RTS. While some respondents might find that to constitute over-regulation, the Level-1 text has clearly identified its requirement for more obligation as detailed under the RTS. The RTS have had to make difficult trade-offs between a range of, at times, competing objectives and have in a number of areas adopted more technology-neutral approaches.*	*None*
[295] General responses	A number of respondents were of the view that merchants should retain control of deciding whether to apply SCA or not. The same respondents disagreed with the interpretation that card-acquiring PSPs ('acquirers'), when payments are initiated by or through the merchant, should require payees in card-based payment transactions ('merchants') to support SCA for all payment transactions; they were of the view that acquirers should be able to use exemptions. In their understanding of PSD2, the SCA requirement concerns the payer but does not bind acquirers. In their view, acquirers and merchants may make a deliberate decision to not apply SCA and to bear the risk of ultimate liability pursuant to Article 74(2) PSD2 instead. The respondents argued that a payment transaction can be authorised before or after execution and they disagreed with the interpretation that Article 74(2) PSD2 is applicable only until the RTS enter into effect. In their view, neither Article 74(2) PSD2 nor Article 115 PSD2 on transposition contains any indication to that effect. Article 115(4) PSD2 contains a detailed provision on the timeframe for implementing the RTS and it does not refer to Article 74(2) PSD2. It is the respondents' belief that European legislators have designed Article 74(2) PSD2 to generally provide for a shift of liability where SCA is not used because either the payee (e.g. a merchant) or the payee's PSP does not support SCA. There is no time limit to this shift of liability. In their view, the EBA cannot	*As stated in paragraph 16 of the rational section of the final report, the EBA's interpretation of PSD2 requirements is that merchants and payee's PSPs should make their best effort to apply SCA in the case of foreign cards or EEA cards used outside the EU.* *The EBA also explains in rationale 24 that its interpretation of PSD2 suggests that the transaction-risk analysis (TRA) exemption from SCA can be applied by the payee's and payer's PSPs, but not by the payer or the payee themselves. The liability rules also suggest that the payer's PSP should have the last say on whether or not the TRA exemption is used for a specific transaction.*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	deviate from the legislative acts on which the RTS are based. It is therefore not possible to deviate from the European legislators' decision to generally apply Article 74(2) PSD2. The respondents also mentioned that there is no compelling reason, in their view, why acquirers or merchants should be obliged to always request SCA prior to accepting a payment instrument, particularly as Title III PSD2, including Article 97 PSD2, also applies to one-leg transactions. In the respondents' view, this demonstrates that there should be no general obligation on acquirers and merchants to support SCA every time a payment transaction is initiated. They asked the EBA to clarify, in any event, that third-country-issued payment instruments may be accepted by EU merchants and acquirers without SCA.		
[296] General responses	A number of respondents have expressed confusion about the confirmation of availability of funds and which entity bears the risk.	*While the EBA acknowledges the importance of the responsibility, this falls under PSD2 and is out of the scope of the RTS.*	*None*
[297] General responses	One respondent asked the EBA to add security requirements related to the PSU's general daily usage of the PSC.	*While the EBA appreciates the importance of the use of PSC by PSUs, this is out of the scope of these RTS.*	*None*
[298] General responses	One respondent was of the view that the RTS should stipulate only 'technical requirements' rather than obligations of any PSPs. In its view, PSD2 already stipulates rights and obligations. The respondent asked the EBA to replace the term 'shall' by 'may', for instance.	*RTS set legal requirements under EU law. The RTS may not include suggestive terms such as 'may', by contrast with what the EBA may at times do under guidelines. RTS are different legal instruments, and technical requirements can include obligations on specific actors or providers.*	*None*
[299] General responses	One respondent asked the EBA to develop guidance for customers, and in particular education for customers, on using the new payment services.	*While this is out of the scope of these RTS, the EBA has a general mandate under its founding regulation to address customer education and may consider actions in this area in the future if it sees fit.*	*None*
[300] General responses	One respondent asked the EBA to add a requirement for PSPs to produce evidence that SCA is working securely, in order to better determine liability between PSP and PSU.	*The EBA is of the view that this is out of the scope of the RTS but other regulations such as the Guidelines on Security and Operational risks may cover this point. The EBA also points out that Articles 2 and 3 are general requirements requiring PSPs to conduct an overall risk analysis when applying SCA or another form of authentication under the scenario of exemptions as well as regular reviews, monitoring and auditing. The RTS also include supervision involvement from*	*None*

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		competent national authorities in a number of specific areas.	
[301] General responses	One respondent asked the EBA to further consult with security experts to ensure that available valid/compliant solutions were not disregarded or excluded from the scope of the RTS. The respondent was of the view that there were alternatives in a number of areas such as indirect identity payment instrument verification and authentication processes from global companies that allow the avoidance of man-in-the-middle and similar threats.	*The EBA has taken the unusual step of publishing a Discussion Paper before the Consultation Paper to gather all the views of the market at two different points in time while drafting the RTS. The EBA therefore considers that it has sufficiently consulted the market. However, the EBA also acknowledges that, especially around IT security, innovative solutions may be developed quickly and where it was proportionate and legally possible to do so the EBA has opted for technology-neutral solutions to allow for existing and future innovations.*	*None*