EBA-Op-2019-06

21 June 2019

Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2

Introduction and legal basis

1. The competence of the European Banking Authority (EBA) to deliver this opinion is based on Article 29(1)(a) of Regulation (EU) No 1093/2010,[1] as part of the EBA's objective to 'play an active role in building a common Union supervisory culture and consistent supervisory practices, as well as in ensuring uniform procedures and consistent approaches throughout the Union'.

2. In order to support the objectives of Directive (EU) 2015/2366 on payment services in the internal market (Payment Services Directive 2 — PSD2), namely enhancing competition, facilitating innovation, protecting consumers, increasing security and contributing to a single EU market in retail payments, the Directive gave the EBA the task of developing 12 technical standards and guidelines to specify detailed provisions in relation to payment security, authorisation, passporting, supervision and more.

3. The regulatory technical standards (RTS) on strong customer authentication (SCA) and common and secure communication (CSC) underpin the new security requirements under PSD2 and regulate the access by account information service providers and payment initiation service providers to customer payment account data held by account servicing payment service

[1] 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).

providers. The RTS were published in the Official Journal on 13 March 2018[2] and will legally apply from 14 September 2019.

4. To fulfil its statutory objective of contributing to supervisory convergence in the EU/European Economic Area (EEA), and to do so in the specific context of the RTS, the EBA is issuing a further opinion with a view to responding to the large number of queries that the EBA and national competent authorities (CAs) have received from market participants on SCA and, in particular, on what procedure or combination of authentication elements may or may not constitute SCA, in the meaning set out by PSD2. The opinion is addressed to CAs but, given the supervisory expectations it is conveying, it should also prove useful for payment service providers (PSPs), payment schemes and payment service users (PSUs) (including merchants).

5. The opinion contains both general and specific comments addressed to CAs in relation to what may or may not constitute SCA. It focuses on the different elements (inherence, knowledge and possession) that would constitute compliant factors for SCA and it considers the existing authentication approaches in e-commerce. This opinion is complementary to the EBA Opinion on the implementation of the RTS, published in June 2018 (EBA-Op-2018-04),[3] as well as the questions and answers (Q&As) published on the topic.

6. In accordance with Article 14(5) of the Rules of Procedure of the Board of Supervisors,[4] the Board of Supervisors has adopted this opinion, which is addressed to CAs.

General comments

7. PSD2 entered into force on 12 January 2016 and has applied since 13 January 2018. One of the objectives of PSD2 is to ensure the security of electronic payments and 'to reduce, to the maximum extent possible, the risk of fraud' (recital 95). Recital 7 of PSD2 states that 'the security risks relating to electronic payments have increased'. Recital 95 further states that the 'security of electronic payments is fundamental for ensuring the protection of users and the development of a sound environment for e-commerce'.

8. One of the fundamental changes introduced by PSD2 is to formalise payment security requirements in national law. One such requirement is for PSPs to apply SCA to electronic transactions in the instances defined in Article 97(1) of PSD2.

9. The EBA Guidelines on the security of internet payments (EBA/GL/2014/12),[5] which are based on the recommendations of the European Forum on the Security of Retail Payments and have been

[2] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 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 (OJ L 69, 13.3.2018, p. 23).

[3] See https://eba.europa.eu/-/eba-publishes-opinion-on-the-implementation-of-the-rts-on-strong-customer-authentication-and-common-and-secure-communication

[4] Decision adopting the Rules of Procedure of the European Banking Authority Board of Supervisors of 27 November 2014 (EBA/DC/2011/01 Rev4).

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

applicable since August 2015, already require the use of SCA for internet payments and will continue to apply until the RTS become applicable on 14 September 2019. That being said, and as stated in paragraph 31 of the EBA opinion on the implementation of the RTS, 'a number of Member States have not yet applied those requirements and, in those that have, the scope has often been more limited, given that the EBA guidelines applied only to online payments'.

10. Under PSD2, and as reiterated in the RTS, SCA is defined as an 'authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data'.

11. Since the publication of the EBA Opinion on the implementation of the RTS, the industry has continued to work towards implementing SCA. In the light of the queries received by the EBA and CAs, including through the EBA's Single Rulebook Q&A tool,[6] the EBA is of the view that it would be useful to clarify its views on how certain existing authentication approaches do or do not fulfil the SCA requirements, including what constitutes a compliant SCA element under PSD2 and the RTS. The EBA does not intend to publish any further clarification on the topic of SCA this year, beyond the existing Q&A process. A number of industry participants have also expressed concerns regarding the state of preparedness of e-commerce for the new SCA requirements. It is imperative that all actors, including card schemes and merchants, take the steps necessary to apply or request SCA and thus avoid situations in which payment transactions are rejected, blocked or interrupted.

12. The EBA reiterates that the application date of the RTS, as published in the Official Journal of the EU, is 14 September 2019, by which date all PSPs have to comply with the requirements set out therein. However, the EBA acknowledges the complexity of the payments markets across the EU and the necessary changes (including those described in this opinion) required to enable the issuer to apply SCA, in particular those required by actors that are not PSPs, such as e-merchants, which may be challenging and may lead to some actors in the payments chain not being ready. PSPs have a self-interest in ensuring that merchants, and all relevant actors in the payments chain, take all necessary steps. In addition, even if there were a liability shift to the payee or the payee's PSP for failing to accept SCA, as articulated in Article 74(2) of PSD2, this could not be considered an alleviation of PSPs' obligation to apply SCA in accordance with and as specified in Article 97 of PSD2. The EBA also acknowledges that a key component for the successful application of SCA is to explain and make customers aware of such changes and that it is paramount for customers to be able to continue making payments, including online.

13. The EBA therefore accepts that, on an exceptional basis and in order to avoid unintended negative consequences for some payment service users after 14 September 2019, CAs may decide to work with PSPs and relevant stakeholders, including consumers and merchants, to provide limited additional time to allow issuers to migrate to authentication approaches that are compliant with SCA, such as those described in this Opinion, and acquirers to migrate their

[6] See https://eba.europa.eu/single-rule-book-qa

merchants to solutions that support SCA. This supervisory flexibility is available under the condition that PSPs have set up a migration plan, have agreed the plan with their CA, and execute the plan in an expedited manner. CAs should monitor the execution of these plans to ensure swift compliance with the PSD2 and the EBA's technical standards and to achieve consistency of authentication approaches across the EU.

14. More specifically, CAs should engage with issuers to identify the two-factor authentication approach(es) used, or the migration plans for implementing such approaches, for meeting SCA requirements. CAs should also engage with acquirers, including by requesting information on the approaches they are implementing with all their merchants to support the application of SCA and on the migration plans (including clear milestones) they have established to comply with the requirements. CAs should also ensure that all PSPs have customer communication plans in place, including for the end customers of the merchants.

15. The EBA will monitor the consistency of SCA implementation across the EU, including by monitoring the way in which the views expressed in this opinion are taken into account and by requesting relevant information from CAs. Where the EBA identifies inconsistencies, despite the guidance contained in this opinion and the previous clarifications provided in the Opinion on the implementation of the RTS and Q&As, it will take the actions needed to remedy those inconsistencies in line with the powers conferred on the EBA in its founding regulation.

Specific comments

16. These specific comments refer to the SCA requirements and, in particular, what may constitute a compliant element in each of the three possible categories of inherence, possession and knowledge, as well as additional requirements on dynamic linking and the independence of elements.

Inherence element

17. Article 4(30) of PSD2 defines inherence as 'something the user is'. Article 8 of the RTS on SCA and CSC refers to the 'authentication elements categorised as inherence and read by access devices and software' and recital 6 refers to the need to have 'adequate security features' in place that could, for example, be 'algorithm specifications, biometric sensor and template protection features'.

18. As stated in the Opinion on the implementation of the RTS, inherence may include behavioural biometrics identifying the specific authorised user. The EBA is of the view that inherence, which includes biological and behavioural biometrics, relates to physical properties of body parts, physiological characteristics and behavioural processes created by the body, and any combination of these. In addition, it is (the quality of) the implementation of any inherence-based approach that will determine whether or not it constitutes a compliant inherence element. Inherence is the category of elements that is the most innovative and fastest moving, with new approaches continuously entering the market.

19. Inherence may include retina and iris scanning, fingerprint scanning, vein recognition, face and hand geometry (identifying the shape of the user's face/hand), voice recognition, keystroke dynamics (identifying a user by the way they type and swipe, sometimes referred to as typing and swiping patterns), the angle at which the PSU holds the device and the PSU's heart rate (uniquely identifying the PSU), provided that the implemented approaches provide a 'very low probability of an unauthorised party being authenticated as the payer', in accordance with Article 8 of the RTS on SCA and CSC.

20. The swiping path memorised by the PSU and performed on a device would not constitute an inherence element, but may rather constitute a knowledge element, something only the user knows.

21. In addition, communication protocols such as EMV® 3-D Secure version 2.0 and newer would not currently appear to constitute inherence elements, as none of the data points, or their combination, exchanged through this communication tool appears to include information that relates to biological and behavioural biometrics (as mentioned in paragraph 18 above). That being said, if future data points exchanged via such protocols enabled the PSP to identify 'something the PSU is', in line with the examples provided in paragraph 19 above, such protocols might possibly be considered inherence elements in the future.

22. Table 1 summarises the views expressed above on what does or does not constitute an inherence element under the RTS on SCA and CSC. The table is for illustrative purposes only and is not intended to be exhaustive; the possible elements included reflect current practices and developments in the market at the time of publication of the opinion.

Table 1 — Non-exhaustive list of possible inherence elements

Element	Compliant with SCA?*
Fingerprint scanning	Yes
Voice recognition	Yes
Vein recognition	Yes
Hand and face geometry	Yes
Retina and iris scanning	Yes
Keystroke dynamics	Yes
Heart rate or other body movement pattern identifying that the PSU is the PSU (e.g. for wearable devices)	Yes
The angle at which the device is held	Yes
Information transmitted using a communication protocol, such as EMV® 3-D Secure	No (for approaches currently observed in the market)
Memorised swiping path	No

*Compliance with SCA requirements is dependent on the specific approach used in the implementation of the elements.

23. In addition, communication protocols such as EMV® 3-D Secure provide a means for merchants to support the use of SCA. The EBA notes that versions 2.0 and newer support a variety of SCA methods, while trying to ensure customer convenience, limiting fraud through data sharing and transaction risk analysis, and enable the use of exemptions set out in the RTS. For those reasons, the EBA encourages the use of such communication protocols and expedient onboarding. Older protocols such as EMV® 3-D Secure version 1.0, although supporting the use of SCA, are not fully adapted to PSD2. For instance, they do not include the possibility of using exemptions or use all forms of SCA approaches.

Possession element

24. Article 4(30) of PSD2 defines possession as 'something only the user possesses'. Possession does not solely refer to physical possession but may refer to something that is not physical (such as an app). Recital 6 of the RTS refers to the requirement to have adequate security features in place and provides examples of possession, 'such as algorithm specifications, key length and information entropy'. Article 7 of the RTS refers to the requirement for PSPs to have mitigation measures to prevent unauthorised use and to have measures designed to prevent the replication of the elements.

25. As stated in the EBA Opinion on the implementation of the RTS (paragraph 35), a device could be used as evidence of possession, provided that there is a 'reliable means to confirm possession through the generation or receipt of a dynamic validation element on the device'. Evidence could, in this context, be provided through the generation of a one-time password (OTP), whether generated by a piece of software or by hardware, such as a token, text message (SMS) or push notification. In the case of an SMS, and as highlighted in Q&A 4039, the possession element 'would not be the SMS itself, but rather, typically, the SIM-card associated with the respective mobile number'.

26. The EBA is of the view that approaches relying on mobile apps, web browsers or the exchange of (public and private) keys may also be evidence of possession, provided that they include a device-binding process that ensures a unique connection between the PSU's app, browser or key and the device. This may, for instance, be through hardware crypto-security, web-browser and mobile-device registration or keys stored in the secure element of a device. By contrast, an app or web browser that does not ensure a unique connection with a device would not be a compliant possession element.

27. Evidence of possession could also be provided through a digital signature, for instance generated using a private key. A quick response (QR) code could also provide evidence of possession (i) of a card, through a QR code reader that would read the QR code displayed on the card, or (ii) of a device, by scanning the code using said device (uniquely identifying the device).

28. Following the publication of the EBA Opinion on the implementation of the RTS, which stated that the card details and card security code that are printed on the card cannot constitute a knowledge element, a number of industry participants have queried if such details could constitute a possession element. The EBA is of the view that such details cannot do so for

approaches currently observed in the market, in particular given the requirements under Article 7 of the RTS, and it advises CAs to closely monitor their application. That being said, dynamic card security codes[7] (where the code is not printed on the card and changes regularly) may provide evidence of possession in line with Article 7 of the RTS.

29. The EBA is also of the view that printed matrix cards or printed OTP lists that are designed to authenticate the PSU are not a compliant possession element for approaches currently observed in the market, for similar reasons to those mentioned for card details above, namely that they are unlikely to comply with the requirements under Article 7 of the RTS.

30. Table 2 summarises the views expressed above on what does or does not constitute a possession element under the RTS on SCA and CSC. The table is for illustrative purposes only and is not intended to be exhaustive; the possible elements included reflect current practices and developments in the market at the time of publication of the opinion.

Table 2 — Non-exhaustive list of possible possession elements

Element	Compliant with SCA?*
Possession of a device evidenced by an OTP generated by, or received on, a device (hardware or software token generator, SMS OTP)	Yes
Possession of a device evidenced by a signature generated by a device (hardware or software token)	Yes
Card or device evidenced through a QR code (or photo TAN) scanned from an external device	Yes
App or browser with possession evidenced by device binding — such as through a security chip embedded into a device or private key linking an app to a device, or the registration of the web browser linking a browser to a device	Yes
Card evidenced by a card reader	Yes
Card with possession evidenced by a dynamic card security code	Yes
App installed on the device	No
Card with possession evidenced by card details (printed on the card)	No (for approaches currently observed in the market)
Card with possession evidenced by a printed element (such as an OTP list)	No (for approaches currently observed in the market)

*Compliance with SCA requirements is dependent on the specific approaches used in the implementation of the elements.

Knowledge elements

[7] Where codes are changed within a reasonable period of time.

31. Article 4(30) of PSD2 defines knowledge as 'something only the user knows'. Article 6 of the RTS refers to the requirement for PSPs to mitigate the risk that the element is 'uncovered by, or disclosed to, unauthorised parties' and to have mitigation measures in place 'in order to prevent their disclosure to unauthorised parties'.

32. The EBA is of the view that the following elements could constitute a knowledge element: a password, a PIN, knowledge-based responses to challenges or questions, a passphrase and a memorised swiping path (as opposed to keystroke dynamics, namely the manner in which the PSU types or swipes, which may be considered an inherence element).

33. The EBA Opinion on the Implementation of the RTS stated that the card details and security code printed on the card would not constitute a knowledge element. In addition, while a card with a dynamic card security code may constitute a possession element, it would not constitute a knowledge element. That being said, in the event, for instance, that the card security code was not printed on the card and was sent separately to the PSU, in the same way as a PSP may send a PIN for a new card, it could constitute a knowledge element. The same may apply to virtual cards (where the PSU receives a single-use digital card number and card security code).

34. The same opinion also stated that a user ID (username) would not constitute a compliant knowledge element. Neither would an email address.

35. The EBA is also of the view that an OTP that contributes to providing evidence of possession would not constitute a knowledge element for approaches currently observed in the market. Indeed, knowledge, by contrast with possession, is an element that should exist prior to the initiation of the payment or the online access.

36. Table 3 summarises the views expressed above on what does or does not constitute a knowledge element under the RTS on SCA and CSC. The table is for illustrative purposes only and is not intended to be exhaustive; the possible elements included reflect current practices and developments in the market at the time of publication of the opinion.

Table 3 — Non-exhaustive list of possible knowledge elements

Element	Compliant with SCA?*
Password	Yes
PIN	Yes
Knowledge-based challenge questions	Yes
Passphrase	Yes
Memorised swiping path	Yes
Email address or user name	No
Card details (printed on the card)	No
OTP generated by, or received on, a device (hardware or software token generator, SMS OTP)	No (for approaches currently observed in the market)

Printed matrix card or OTP list	No

*Compliance with SCA requirements is dependent on the specific approach used in the implementation of the elements.

Other requirements, including dynamic linking and independence

37. In addition to having (at least) two elements, each from a different category, the RTS include further requirements for PSPs in the context of SCA. This includes the requirement for any electronic transaction made remotely (e.g. in the context of e-commerce) to include dynamic linking as defined under Article 5 of the RTS and required under Article 97(2) of PSD2. This requirement would not apply to credit transfers performed at automated teller machines, given that those transactions are not remote. The EBA notes that, at present, the dynamic linking element is typically produced based on the possession element. The EBA also understands that not all compliant elements may yet enable dynamic linking and therefore it encourages CAs to ensure that envisaged (new) SCA approaches can enable dynamic linking.

38. Another requirement under the RTS, in line with PSD2, is that the two elements used for SCA be independent. Independence under Article 9 of the RTS requires that the use of the elements 'is subject to measures which ensure that, in terms of technology, algorithms and parameters, the breach of one of the elements does not compromise the reliability of the other elements'.

39. The EBA is of the view that the use of a card reader in which a PIN is first inserted to access the device and then an OTP is generated following the reading of the chip of the card could constitute two elements, provided that measures have been put in place to ensure that the breach of one of the elements does not compromise the reliability of the other element, in line with Article 9 of the RTS. The same would apply to a digital signature generated by a key, if the key requires a knowledge element to be used for the key to be accessed.

40. The EBA also notes (as published in Q&A 4141) that an element used for the purpose of SCA may be reused within the same session for the purpose of applying SCA at the time that a payment is initiated, provided that the other element required for SCA is carried out at the time of the payment initiation and that the dynamic linking element is present and linked to that latter element.

41. Further requirements include, for instance, requirements regarding the authentication code (see, for instance, Q&A 4053), requirements regarding the confidentiality and integrity of the personalised security credentials of the PSU during all phases of authentication and requirements for personalised security credentials to be masked and not readable in their full extent when input by the PSU (see, for instance, Q&A 4366).

Combination of two elements in existing SCA approaches

42. In the light of the above, a number of existing approaches within e-commerce are presently in line with SCA requirements, as they combine two compliant elements (and would comply with the other requirements mentioned in the previous section). This includes approaches in which device binding to an app is used in combination with a knowledge or inherence element (e.g. some mobile wallet approaches). This also, for instance, includes an OTP-based approach with a PIN or an inherence element (such as fingerprint scanning) and a card reader that requires a knowledge element to be input, as well as approaches in which the PSU authenticates itself in its online bank account domain using two compliant SCA elements.

43. By contrast, a number of existing approaches within e-commerce, for card payments in particular, would not be compliant with SCA. This includes approaches in which card details printed in full on the card are used as stand-alone elements or used in combination with a communication protocol such as EMV® 3-D Secure or with only one compliant SCA element (such as SMS OTP). In case some actors are not ready by the application date of the RTS, as pointed out in paragraphs 13 and 14 above, CAs have an important role to play, including by communicating with issuers and acquirers to identify SCA approaches, migration plans and customer communication plans. With regard to acquirers, CAs should, in particular, request information on the approaches they are implementing with all their merchants to support the application of SCA and on the migration plans (including clear milestones) that they have established to comply with the requirements.

44. In addition, approaches that would have two elements from the same category, such as an SMS OTP and dynamic card security codes, would not be compliant, as the two elements should belong to two different categories as highlighted in the previous EBA Opinion on SCA published in June 2018.

45. This opinion will be published on the EBA's website.

Done in Paris, 21 June 2019

[signed]

José Manuel Campa

Chairperson for the Board of Supervisors