ECIJA | Torre de Cristal Pº de la Castellana, 259C
28046 Madrid · Tel: +34 917 816 160
www.ecija.com

Nota Informativa – Fin de la moratoria en la aplicación de los mecanismos de autenticación reforzada (SCA) bajo la directiva de servicios de pago DSP2 y RTS

Madrid, 21 octubre 2019

El pasado 21 de junio, la Autoridad Bancaria Europea (EBA) emitió una Opinión Legal [EBA Opinion on SCA elements under PSD2 .pdf Anexo 1] sobre la aplicación de los mecanismos de autenticación reforzada (SCA) bajo la Directiva (UE) 2015/2366 de servicios de pago (DSP2).

En dicha Opinión Legal la EBA reconocía la complejidad de los mercados de pagos en la Unión Europea y la necesidad de acometer cambios que permitan a los emisores aplicar SCA (Strong Customer Authentication), en particular, aquellos que afectan a actores involucrados que no tienen la condición de Prestador de Servicios de Pago (PSPs), tales como comercios electrónicos. Contemplaba asimismo la EBA la posibilidad de que las autoridades nacionales de cada estado miembro aprobaran un período de moratoria en la aplicación del Reglamento Delegado (UE) 2018/389 (RTS) que desarrolla la DSP2, el cual entró en vigor el pasado 14 de septiembre de 2019.

En este sentido, EBA entendió que las autoridades nacionales competentes debían colaborar con los proveedores de servicios de pago (PSP) y los *stakeholders* en los servicios de pago (incluidos *merchants* y usuarios) para establecer dicho periodo de moratoria, que se otorgaría en todo caso, bajo la condición de que los prestadores de servicios de pago elaboraran y acordaran con las autoridades nacionales un plan definido de migración hacia soluciones que cumplieran con la SCA.

En base a dicha posibilidad, algunos reguladores nacionales como, por ejemplo, el de Francia, el de Reino Unido o el de Dinamarca ya se pronunciaron concediendo a los PSP de sus respectivos estados, una prórroga de 18 meses. En nuestro entorno, el Banco de España, tal y como comunicó el pasado 11 de septiembre de 2019 [Banco de España110919.pdf Anexo 2], está trabajando en la revisión de los planes de migración que presenten los PSPs, de acuerdo con lo señalado en la ya citada Opinión Legal de la EBA con el objetivo de asegurar el debido cumplimiento de la PSD2 y del RTS. Dicho lo anterior, el Banco de España no se ha pronunciado hasta ahora en relación con la fecha límite en la que dichos planes de migración debían haber finalizado con el fin de asegurar el cumplimiento del SCA por parte de los PSP.

Así las cosas, **la EBA ha dejado clara esta cuestión, tal y como se puede ver en la nueva Opinión Legal emitida el pasado 16 de octubre de 2019 sobre la fecha límite para la migración a SCA de las transacciones de pago con tarjeta en comercio electrónico [**Opinion on the deadline for the migration to SCA.pdf Anexo 3].

La EBA ha definido en dicha Opinión Legal como fecha límite de la moratoria el **31 de diciembre de 2020**, es decir, 15 meses desde la entrada en vigor del RTS sobre autenticación reforzada de clientes.

No obstante, en esta nueva Opinión Legal, la EBA vuelve a hacer hincapié en que este plazo adicional no es equivalente a una demora en la fecha de aplicación de los requisitos de SCA, sino que las Autoridades Competentes en este tiempo habrán de ser flexibles en la supervisión

y no tomarán medidas ni aplicarán sanciones contra los proveedores de servicios de pago que no cumplan, siempre que se respeten los hitos y las acciones que se espera de ellos y que se especifican en la propia Opinión Legal.

Sobre la base de lo anterior, cualquier PSP que deje de atender los requisitos de la DSP2 y RTS desde el 14 de septiembre de 2019, sin perjuicio de la moratoria referida anteriormente, estará incumpliendo la normativa.

Además, recuerda la EBA que la responsabilidad del ordenante y del PSP en caso de operaciones de pago no autorizadas, según se establece en el artículo 74 DSP2, es también de aplicación sin ningún tipo de demora, por lo que los PSP deberían tener por ello interés en establecer y migrar a soluciones compatibles con SCA de manera expeditiva.

Para cualquier aclaración en relación con los planes de migración o la implementación de los mecanismos de autenticación reforzada, no dudes en contactar con nosotros.

Área de *FinTech* y Regulación Financiera
+ 34 91 781 61 60
info@ecija.com

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

BANCO DE ESPAÑA
Eurosistema

11.09.2019

Nota informativa sobre la aplicación de la autenticación reforzada del cliente (SCA) en los pagos electrónicos

El Banco de España revisará los planes de migración que presenten los proveedores de servicios de pago de acuerdo con la flexibilidad condicionada que contempla la Autoridad Bancaria Europea

---

A partir del 14 de septiembre de 2019 es de aplicación el Reglamento Delegado (UE) 2018/389, uno de cuyos objetivos es mejorar la seguridad de los pagos y reducir el fraude en el proceso de autenticación. El Reglamento Delegado establece, entre otros, los requisitos para la aplicación de la autenticación reforzada del cliente (SCA). Por consiguiente, tal y como ha señalado la Autoridad Bancaria Europea (ABE) en su Opinión de 21 de junio, a partir de la citada fecha de aplicación del Reglamento Delegado, todos los proveedores de servicios de pago (PSPs) tienen que cumplir con los requisitos establecidos en el mismo.

En la referida Opinión de 21 de junio, la ABE reconoce la complejidad de los mercados de pagos en la Unión Europea y la necesidad de acometer cambios que permitan a los emisores aplicar SCA, en particular, aquellos que afectan a actores involucrados que no tienen la condición de PSPs, tales como comercios electrónicos.

Para evitar posibles efectos negativos para algunos usuarios de servicios de pagos tras el 14 de septiembre, en su Opinión la ABE acepta que, de manera excepcional, las autoridades nacionales competentes puedan trabajar con los PSPs y otras partes interesadas, incluyendo consumidores y comercios, para conceder un tiempo adicional limitado que permita a los emisores de instrumentos de pago y a los adquirentes de operaciones migrar hacia soluciones que cumplan con los requisitos de SCA. Esta flexibilidad supervisora se condiciona a que los PSP acuerden con sus respectivas autoridades nacionales competentes los correspondientes planes de migración y los ejecuten de forma urgente.

El Banco de España, en el marco de esa flexibilidad, está trabajando con las autoridades europeas al objeto de asegurar el debido cumplimiento de la Directiva (UE) 2015/2366 de servicios de pago (PSD2) y del Reglamento Delegado (UE) 2018/389 y revisará los planes de migración que presenten los PSPs, de acuerdo con lo señalado en la ya citada Opinión de la ABE.

EBA-Op-2019-11

16 October 2019

Opinion of the European Banking Authority on the deadline for the migration to SCA for e-commerce card-based payment transactions

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 June 2019, the EBA published an Opinion on the elements of strong customer authentication (SCA) under PSD2 (EBA-Op-2019-06)[2], which provided clarity on the different elements of SCA (inherence, knowledge and possession) that would constitute compliant factors for SCA. The Opinion also acknowledged the complexity of the payments markets across the EU and the challenges arising from the changes that are required, in particular by actors that are not payment service providers (PSPs), such as e-merchants, which may lead to some actors in the payments chain not being ready by 14 September 2019.

3. In that regard, the Opinion took the exceptional step of acknowledging that national competent authorities (NCAs) may provide limited additional time for e-commerce card-based payment transactions to allow card-issuing PSPs to migrate to authentication approaches that are compliant with SCA and acquiring PSPs to migrate their merchants to solutions that support SCA.

[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).

[2] See https://eba.europa.eu/documents/10180/2622242/EBA+Opinion+on+SCA+elements+under+PSD2+.pdf

This supervisory flexibility was made available under the condition that PSPs set up migration plans, agree their plan with their NCA, and execute the plan in an expedited manner.

4. The EBA also communicated that the deadlines by which the aforementioned actors will have to have completed their migration plans will be communicated later in 2019, in order to fulfil its statutory objective of contributing to supervisory convergence in the EU/European Economic Area (EEA) and to contribute to a single payments market, and to do so in the context of Directive (EU) 2015/2366 on payment services in the internal market (PSD2) and the regulatory technical standards (RTS) on SCA and common and secure communication.

5. To that end, the EBA is issuing the Opinion on hand to communicate the deadline by which the period of supervisory flexibility should end and the actions that NCAs should require PSPs to perform before that date.

6. The opinion is addressed to NCAs but, given the supervisory expectations it is conveying, it should also prove useful for PSPs, card schemes and payment service users (PSUs), including merchants. In accordance with Article 14(5) of the Rules of Procedure of the Board of Supervisors[3] the Board of Supervisors has adopted this opinion.

General comments

7. Since the publication of the EBA Opinion on the elements of SCA in June 2019, the EBA took note that all NCAs in the EU made use of the flexibility granted and communicated this to their respective industries. Furthermore, and in order to be able to make a well-informed decision as to the most appropriate deadline and the actions that the industry should take until then, the EBA and NCAs carried out a fact-finding exercise in July and August 2019.

8. They did so by approaching a wide range of stakeholders in the payments sector across the EU through a survey. The survey was aimed at better understanding the state of readiness of the industry, and was sent to issuing PSPs, acquiring PSPs, and EU and national merchant and consumer associations. The EBA received input from more than 90 respondents from 30 jurisdictions, which the EBA assessed during September 2019.

9. The large majority of stakeholders indicated that they prefer a consistent and harmonised implementation of SCA with regard to e-commerce card-based payment transactions, with a single common deadline. In their view, this would avoid otherwise negative impacts on cross-border payments, the decline of legitimate payment transactions, customer drop-out, level-playing field issues across jurisdictions, regulatory arbitrage and further complexity. The EBA agrees with these views and the underlying arguments and therefore recommends to NCAs to take a consistent approach toward the SCA migration period by abiding by the deadline specified in the next section and requiring their respective PSPs to carry out the actions set out in this Opinion.

10. In addition, the EBA recommends that, where required, NCAs communicate to their PSPs that the supervisory flexibility granted by the EBA is not equivalent to a delay in the application date of

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

the SCA requirements in PSD2 and the RTS but rather means that NCAs would not take enforcement/sanction actions against PSPs if they respect the milestones and the expected actions specified in the next section of this Opinion. Rather, the requirements apply as of 14 September 2019, as imposed in the Directive, and this means that any PSP not complying with them is in breach of law.

11. Furthermore, NCAs should also communicate to their PSPs that the liability regime under Article 74 of PSD2 also applies, without any delay, that issuing and acquiring PSPs are therefore liable for unauthorised payment transactions and that PSPs should therefore have a self-interest to migrate to SCA-compliant solutions and approaches in an expedited way.

Specific comments

12. These specific comments refer to the deadline for the migration to SCA and the actions issuing and acquiring PSPs need to take during that period.

Deadline for the migration to SCA

13. The EBA has arrived at the view that migration plans of PSPs, including the implementation and testing by merchants, should be completed by **31 December 2020**.

14. The EBA acknowledges there are many different views on the appropriate timelines for migration of each type of industry stakeholder. The feedback to the questionnaires indicated that most issuing and acquiring PSPs in half of the Members States were likely to be ready with SCA-compliant solutions and approaches by the end of 2019, with PSPs in a number of other Member States being ready in the first half of 2020. With regard to merchants, in turn, the majority of respondents were concerned about the readiness of small and medium sized merchants and indicated that, with the exception of a few sectors such as travel and hospitality, these merchants will need between 3 and 9 months to implement solutions supporting SCA in their systems.

15. In this context the majority of the respondents to the questionnaires indicated that they would prefer 18-months period for smooth, frictionless and ordered migration of the entire e-commerce card-based payment ecosystem to SCA-compliant approaches and solutions. They argued that this timeline takes into account:

    - the complex relationships and dependencies between various stakeholders, such as issuing and acquiring PSPs, payment gateways, merchants, consumers, card schemes and others; and
    - the dependency with the roll-out and implementation of the 3DS V2.2. communication protocol that is made available by the major card schemes, which should enable the application of the full range of SCA exemptions specified in the RTS and the out-of-scope of SCA transactions, such as payee initiated transactions.

16. The EBA assessed the feedback above and noted that the 18-month suggestion put forward by many respondents appeared to be driven significantly by the timeline of the development of a particular version of a particular communication protocol that has been under development by some of the major card schemes (3DS 2.2.). That version is aimed at enabling the application of

the full range of SCA exemptions specified in the RTS and the transactions that are out-of-scope of SCA altogether.

17. However, other means of payment are available and taking into account the objectives of PSD2 and the RTS of technical neutrality and increasing competition in the payments market, the EBA's view cannot be based solely on providing a benefit to one or more incumbent providers, while market challengers that provide competing payment services are already ready to offer SCA-compliant solutions.

18. In addition, any potential delays in the roll-out and/or implementation of said protocol at a later stage would require further extensions of the deadline, which would be a dependency that would be controlled, not by the EBA and the NCAs, but the industry that is subject to the requirements.

19. Relatedly, the EBA's assessment of the responses also suggested that a preference for 18 months is also driven by the desire of the industry to develop a version of the protocol that is not only SCA compliant but additionally allows the application of the full range of exemptions to SCA that the RTS allows.

20. However, the majority of these exemptions were introduced by the EBA during the consultation phase to the RTS in 2016 to address requests from the industry that exemptions to SCA should apply for particular payment transactions, such as low-value transactions, transactions initiated to trusted beneficiaries, recurring transactions or transactions posing a low level of risk based on transaction monitoring mechanisms. They have therefore been known since February 2017, when the EBA published the final draft RTS. The EBA is therefore of the view that the industry had sufficient time to implement the necessary changes to the protocol and IT systems more generally.

21. More importantly, the exemptions are exceptions from the general and default rule. Therefore the delay of the application of the full-range of exemptions, albeit the requirements of Article 98(2)(e) of PSD2 aiming at the development of user-friendly means of payment, cannot justify a significant delay in the application of the security requirements. The industry may therefore wish to consider prioritising the development of the actual SCA requirements and incorporating the exemptions at a later date.

22. Nevertheless, the EBA acknowledges that:

    - those Member States where issuing and acquiring PSPs have reported that they will need more time constitute a significant proportion of e-commerce card-based payment transactions in the EU; and
    - in line with the objectives of PSD2, it is important for payment service users to have user-friendly and accessible means of payment for low-risk payment transactions, such as the SCA exemptions.

23. In that regard, and as stated above, the EBA is of the view that the supervisory flexibility should end on **31 December 2020**, which should be sufficient for issuing PSPs, acquiring PSPs and their merchants to migrate to SCA-compliant approaches and solutions.

Actions to be taken by NCAs during the SCA migration period

24. In order to ensure expedited migration to SCA, the EBA expects NCAs to take the actions specified in the below two tables towards issuing and acquiring PSPs. In line with paragraphs 14 of the EBA Opinion on the elements of SCA, these actions should also allow NCAs to ensure that PSPs follow their migration plans and to keep track of the progress made. The actions aim at ensuring harmonised and consistent migration to SCA compliance and readiness. However, these actions do not restrict NCAs from requiring more detailed information.

Table 1. Milestones and expected actions from NCAs towards issuing PSPs

Expected actions	Timeline
1. NCAs should require issuing PSPs to identify the authentication approaches that they are currently making available to their customers and separate them into two categories: those that fulfill the requirements of SCA under PSD2 and the RTS and are in line with clarifications provided by the EBA and those that are not.	31.12.2019
2. NCAs should obtain information from issuing PSPs on the authentication approaches (which should include new authentication approaches and those specified under row 1) and the SCA exemptions they intend offering to ensure compliance. NCAs should also request from issuing PSPs plans for the expedited migration, including PSUs' enrolment into these authentication approaches. These plans should contain clear migration targets of the progress made for adoption of SCA-compliant authentication approaches and the SCA exemptions (e.g. on the stages of implementation, testing and rollout). The migration plans should be based on a risk-based approach taking into account the types of transactions and the fraud rates.	31.12.2019
3. NCAs should take stock of the overall readiness of issuers to meet the SCA requirements in terms of the: a) number of payment transactions[4] where SCA was requested divided by the total number of initiated transactions; b) number of payment transactions where an SCA exemption was applied divided by the total number of initiated payment transactions; c) number of out-of-scope of SCA payment transactions (such as payee initiated transactions) divided by the total number of initiated payment transactions; and d) number of PSUs enrolled to initiate SCA-compliant payment transactions divided by the total number of PSUs. The above data should cover the period between 14 September 2019 and 13 March 2020.	31.03.2020
4. NCAs should require issuing PSPs to report on the progress made from 14 March to 13 June 2020 and from 14 June 2020 to 13 September 2020 by providing updated information under item 3 above. This reporting should be such that it provides a reliable picture of the change in the types of transactions and the fraud rates, the progress of adoption of 3DS2.X protocol where it is envisaged, and other metrics	30.06.2020 and 30.09.2020 respectively

[4] Payment transactions, including domestic and cross-border transactions within the EEA regardless of the currency.

depending on the authentication approaches, for instance percentage of customer telephone numbers obtained to the total number of customers for SMS-OTP based approaches.	
5. NCAs should require issuing PSPs to inform PSUs about the SCA-compliant authentication approaches, the SCA exemptions and out–of–scope of SCA transactions they intend offering, and to establish educational campaigns as needed.	Continuous
6. NCAs should require issuing PSPs to make available to their NCAs information about the communications with PSUs under item 5 above.	Every 3 months, starting 14.12.2019
7. NCAs should require issuing PSPs to have completed their migration plans.	31.12.2020
8. EBA to develop a report on the status of SCA-compliance by the issuing PSPs based on consolidated information provided by NCAs.	Q1 2021

Table 2. Milestones and expected actions by NCAs towards acquiring PSPs

Expected actions	Timeline
1. NCAs should require acquiring PSPs to identify the technologies through which they allow issuing PSPs to request PSU authentication that they are currently making available to merchants and separate them into two categories: those technologies that support SCA-compliant authentication and the SCA exemptions and those that do not.	31.12.2019
2. NCAs should obtain information on the plans of acquiring PSPs for the expedited migration, including migration by e-merchants to technologies that support SCA, the SCA exemptions and/or the out-of-scope of SCA transactions. These plans should contain clear migration targets of the progress made towards: a) adoption of technologies that support SCA, the SCA exemptions and the out–of–scope of SCA transactions, if applicable; and b) the implementation of these technologies by merchants. The migration plans should be based on a risk-based approach taking into account the types of transactions, types of merchants, and the fraud rates.	31.12.2019
2. NCAs should take stock of the overall readiness of acquiring PSPs to meet the SCA requirements, and should do so by requesting the following figures: a) number of payment transactions where SCA was applied divided by the total number of acquired transactions; b) number of payment transactions where an SCA exemption was applied divided by the total number of acquired payment transactions; c) number of out-of-scope of SCA payment transactions applied (such as payee initiated transactions) divided by the total number of acquired payment transactions; d) number of e-merchants that support SCA divided by the total number of e-merchants to whom acquiring PSPs provide services; and e) number of e-merchants that support the SCA exemptions divided by the total number of e-merchants to whom acquiring PSPs provide services; and f) number of e-merchants that support the out-of-scope of SCA transactions divided by the total number of e-merchants to whom acquiring PSPs provide services. The above data should cover the period between 14 September 2019 and 13 March 2020.	31.03.2020

4. NCAs should require acquiring PSPs to report on the progress made from 14 March to 13 June 2020 and from 14 June 2020 to 13 September 2020 by providing updated information under item 3 above. This reporting should also reflect the change in the types of transactions and the fraud rates, the progress made by the different types of merchants and the progress of adoption of 3DS2.X protocol where it is envisaged.	30.06.2020 and 30.09.2020 respectively
5. NCAs should require acquiring PSPs to inform the e-merchants they work with about the necessary changes that need to be introduced to the existing technologies used to support SCA, the SCA exemptions and the out–of–scope of SCA transactions.	Continuous
6. NCAs should require acquiring PSPs to provide information about the communications to e-merchants under item 5 above.	Every 3 months, starting 14.12.2019
7. NCAs should require acquiring PSPs to have completed their migration plans.	31.12.2020
8. EBA to develop a report on the status of SCA-compliance by acquiring PSPs based on consolidated information provided by NCAs	Q1 2021

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

Done in Paris, 16 October 2019

[signed]

Chairperson for the Board of Supervisors