SMART PAYMENT ASSOCIATION

shaping the future of payment technology

SPA Analysis of the RTS on SCA

Regulatory Technical Standard on Strong Customer Authentication

May 2018

Table of Contents

1. Overview 3

2. Chapter 1: General provisions 3

3. Chapter 2: On the security measures for the application of strong customer authentication 4

4. Chapter 3: On the exemption regime 4

5. Chapter 4: On the confidentiality and integrity of the payment service users' personalized security credentials 5

6. Chapter 5: On common and secure open standards for communication 6

7. Final review and take-aways 8

1. Overview

SPA considers the Regulatory Technical Standard (RTS) on Strong Customer Authentication (SCA) as a fundamental regulatory pillar in the battle to combat the expected increase in payment fraud resulting from (1) the boom of e- and m-commerce transactions (2) the diversity of security solutions implemented by payment service providers (3) the entrance of non-bank competitors into the payments market (4) the growing use of vulnerable mobile devices to make payments and (5) the risk of cyberattacks. SPA shares the view that enhancing customer authentication using certified personal hardware devices remains the most efficient security countermeasure to minimize the risk of increased fraud.

SPA notes that the content of the RTS on SCA reflects the original valuable work on the security recommendations for Internet, Mobile and Third Party Payment Provider payments undertaken by SecurePay under the aegis of the European Central Bank (ECB). Some of these recommendations have now become legal requirements, with the remainder providing useful guidelines to implementing the security requirements of the RTS on SCA.

SPA believes that a higher level of prescription may have proven useful to avoid ambiguities and misinterpretations of the RTS on SCA text. However, SPA recognizes that the final text is a trade-off exercise especially difficult to achieve given (1) the complex nature of the payments industry with its conflicts of interest (2) the need to preserve past investments that have proven successful (3) the demands of many players not to constrain innovation and (4) the disagreements between the European Commission and the European Banking Authority responsible for drafting the last public version of the document in February 2017 prior to production of the final version in November 2017.

The RTS on SCA text was published in the Official Journal of the European Union in March 2018 and its provisions will apply from September 2019 (however, the provisions that relate to the availability of documentation on the technical specifications of and testing facility for banks' dedicated interfaces will apply from March 2019).

The next sections of this document provide an analysis of the different chapters of the RTS on SCA text.

2. Chapter 1: General provisions

As was the case with the draft version published in February 2017, very early in the text Article 1.1 (b) outlines the potential exemption scenarios from Strong Customer Authentication. By doing so, the attention of the Payment Service Provider (PSP) is focused from the outset on avoidance of the authentication regime. That said, Article 3 goes on to clarify that PSPs making use of exemptions will be subject to audits and also redirects readers to Article 18 which sets out transaction risk analysis and monitoring requirements.

We notice that Article 1.2 of the February 2017 draft has now been removed. SPA believes this is a good decision, because the formulation of this Article was confusing and failed to clarify the relationship between conformance with the RTS on SCA and other legal provisions, such as liability shift as per PSD2. It's the understanding of the SPA that compliance with the obligations set out by the RTS on SCA is also intended to facilitate contractual liability terms and conditions between the involved parties.

Article 2 is now focused exclusively on authentication requirements, excluding provisions for the exemption regime (now partially moved to Article 3), facilitating improved readability of the document. Yet the requirements for transaction monitoring to be applied by the PSPs now excludes those risk-factors based on the unusual pattern behaviors of the consumer (which have been moved to Recital 14). The transaction monitoring process is now simplified and the risk of infringement of Data Protection regulation by PSPs is lowered.

3. Chapter 2: On the security measures for the application of strong customer authentication

SPA considers that it would have been preferable that Article 2.1 precisely articulated (rather than implied) that strong customer authentication requires *multi-factor* authentication elements and not merely two or more independent elements from a security point of view.

The security requirements for the different categories of authentication elements set out in Articles 6 to 8 have been relaxed. SPA interpret this decision as being driven by the need to respect the principle of technological neutrality in the context of fast innovation. However, SPA draws attention to the risk this may pose as technical solutions offering very different levels of security will claim compliance with these high-level requirements, and this has to potential to facilitate fraud.
With respect Article 9, SPA considers that the breaking of one authentication element facilitates the breaking of another authentication element of the same category. In other words, authentication elements in the same category should not be considered as completely independent from a security point of view.

SPA also points out that Article 9.1 refers to the "reliability" of an authentication element. This term is misguiding, because lack of "reliability" refers usually to the failure of the element to fulfill its intended functionality as a result of intrinsic wear out, not as a result of an attack. In that sense, if the compromise of one authentication element compromises the reliability of a second one required for the strong customer authentication, this consequence would be protective rather than detrimental for the legitimate end-user.

4. Chapter 3: On the exemption regime

The exemption regime set out in Chapter 3 is potentially debatable and contentious since the primary objective of the RTS on SCA is to fight payments fraud, especially online, and strong customer authentication is the privileged tool with which to achieve this objective.

It should be remembered that e-commerce expanded rapidly due to the acceptance of payment cards by online retailers. But the authentication of cardholder in CNP (cardholder not present) transactions is relatively weak and, as a result, a shift in payment fraud is to be expected from the CP (cardholder present) to the CNP context. So, it stands to reason that applying strong customer authentication for CNP payments should fix the online fraud issue; a position and stance has been adopted and defended by SPA in different position papers.

The principle underlying Chapter 3 is that enforcing strong customer authentication is not justified if a PSP succeeds in achieving very low fraud rates without strictly following the strong customer authentication principles of PSD2. These low fraud target values are actually challenging. The question is whether local regulators could provide some flexibility in the application of the RTS on SCA.

Two scenarios should in, our opinion, be differentiated:

- **When a card is used**: DCV (Dynamic Code Verification) cards were designed to objectively protect against more frequent online attack patterns and represent a significant step forward for card online security. Indeed, DCV cards have succeeded in limiting fraud to a level that seems acceptable (see for instance fraud data released in 2017 by the Banque de France: https://www.banque-france.fr/sites/default/files/medias/documents/osmp2016web.pdf) and consequently should be exempt from the strong customer authentication requirement as set out in Chapter 2.
- **Alternative authentication methods claiming to be successful cutting down fraud**: SPA believes that these alternative authentication methods (the identification of suspicious payments) complement more robust authentication processes (based on certified hardware under end-user control) and are useful for PSP risk management. But while these methods are useful to prove the lack of unusual payer behavior they do not authenticate a legitimate customer and don't constitute evidence in the event of a contested transaction. SPA is not against the use of these methods; we merely note their intrinsic limitations and submit that granting exemptions for these cases should be carefully considered.

A final issue is that the exemption regime potentially incentivizes the use of biased payment fraud accounting practices to avoid the strict strong customer authentication constraints. That said, the SPA recognizes that two countermeasures designed by the European regulators seem appropriate:

- The initiative by the European Banking Authority to harmonize practices for fraud reporting appears an important complementary measure.
- The decision to specify extremely low fraud figures in the RTS on SCA Annex to be eligible for the exemption regime, especially for remote payments. It should be noted, however, that in the case of credit transfers, PSPs already seem to be below target as per the Annex (see for instance fraud data released in 2017 by the Banque de France: https://www.banque-france.fr/sites/default/files/medias/documents/osmp2016web.pdf)

5. Chapter 4: On the confidentiality and integrity of the payment service users' personalized security credentials

The PSD2 defines Personalized Security Credentials (PSCs) as those issued by the PSP for the purpose of payment service user (customer) authentication. Thus, strong customer authentication (SCA) will rely on the security properties featured in the personalized security credential.

Proper SCA can only be achieved if the overall lifecycle management of the personalized security credentials is under appropriate security controls and, importantly, if a proven mechanism is used by the PSP to link these to the legitimate user. Chapter 4 is comprehensive in that Articles 23 to 27 effectively cover the overall lifecycle of personal security credentials.

The RTS on SCA doesn't provide details on the nature of the PSC other than some insight in recital (1). Chapter 4 Article 22.2 states that personalized security credentials may be in data format, while Article 22.1 qualifies the authentication code itself as a kind of personalized security credential and states that the PSP is responsible for its secure processing and routing.

This lack of definition in the text allows for different interpretations in terms of the way in which PSCs are implemented. The requirements in Chapter 4, in terms of authentication and integrity for example, are more appropriate for data than for physical devices. These requirements make it clear, for instance, that authentication solutions based on an SMS-OTP for online payments don't comply with the regulation.

Yet for the SPA, a PSC is the physical possession authentication element: payment cards, tokens, national ID cards, perhaps mobile devices (or at least some embedded certified security devices). This physical PSC offers a definitive advantage: not only is it a possession authentication element but it also acts as the enabler for any of the two remainder authentication categories recognized by the PSD2 - knowledge-based (mobile code, PIN) and inherence (biometrics).

Physical authentication components must prove to be authentic themselves, feature certified anti-clone features, be under exclusive control of the legitimate user, and act as secure storage for other types of personalized security credentials ensuring their confidentiality and integrity. Thus, *credentials*, or keys, are stored securely in the EMV smart cards to prevent card cloning by proving that the card is authentic. SPA would have preferred all these security properties to have been clearly set out in Chapter 4.

The SPA has concerns that as a result of this low level of prescription, solutions claiming compliance with the RTS on SCA may differ broadly in terms of the actual level of security offered. It is the reason why SPA submitted a proposal to the European Cards Stakeholders Group (ECSG) to include a security assessment of the different authentication solutions known in the market, so that PSPs could proceed to make justified choices.

6. Chapter 5: On common and secure open standards for communication

A general comment on Chapter 5

This chapter applies to the communication channels that should be established 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) when a third party payment provider (TPP) intermediates a financial transaction.

Two characteristics differentiate Chapter 5 from the remainder of the RTS on SCA:

- The fact that two very different sections coexist under the same title, namely Section 1 on the identification and traceability of transactions and Section 2 which focuses exclusively on the new regulated TPP services.
- The structure of Section 2 of Chapter 5 seems to be the result of many trade-offs to conciliate the conflicts of interest between account servicing payment service providers (ASPSPs) and third party payment providers (TPPs).

Chapter 5 Section 1 focus on two aspects: identification (Article 28) and traceability of regulated electronic payments (Article 29). Article 28 and Article 29 requirements enable PSPs to gather information about an individual payment "as a whole" and applies to any electronic payment transaction.

- For those transactions initiated using TPP services, Article 34 in Section 2 elaborates on the generic Article 28 requirements. Article 34 applies to the identification of PSPs involved in TPP services. For instance, Article 34 requires the use of role certificates from qualified trust service providers (QTSPs) in accordance with the eIDAS1 Regulation.
- SPA notes that Article 28 includes a requirement for the secure identification of the payer's device and the payee's acceptance device. In the security industry, such a requirement is implemented using mutual authentication of the communicating parties. But mutual authentication is absent in the text and an ambiguity remains on the precise meaning of "secure identification". This point should be clarified.
- Article 29 in Section 1 contains requirements that correspond to usual PSP practices and are not especially contentious. In addition, the record of the payment transaction details is a requirement from Article 72 of the PSD2. Compliance with Article 29 is the baseline to elaborate liability policies between the entities involved in regulated transactions.

Section 2 of Chapter 5 (Articles 30 to 36) focuses exclusively on Third Party Payment Providers (TPPs) intermediated financial services. This is a fundamental new piece of controversial regulation. One reason is that Section 2 bans existing TPP practices in terms of authentication (for example, screen scraping) considered as a risk for the end user. However, the European Banking Authority has stated that to assure continuity of TPP services, screen scraping (impersonation by the TPP of the end user to grant access to its payment accounts) will be tolerated during the migration period.

SPA considers that the objectives of Section 2 are twofold:

- A business objective - ensuring that third party payment providers (TPPs) can offer a good user experience and effectively compete with banks (account servicing payment service providers); and
- A security objective - to further protect the end users of TPP services.

Let's elaborate on these objectives, starting with those Articles (30 to 33) designed to provide guarantees to the newly regulated TPP:

- Article 30 mandates that the ASPSP offer an interface for online access to payment accounts which must comply with a set of functional and security requirements. Article 31 clarifies that this interface is not necessarily a dedicated one, providing the ASPSP with some flexibility for implementation. However, if the ASPSP decides to offer a dedicated interface for TPP access, then Articles 32 and 33 shall apply.
- Article 32 is intended to guarantee that a dedicated interface does not offer an inferior level of service compared to the service granted to the payment service user when directly connecting online to the ASPSP. Therefore, it might be reasonably expected by the TPP that in the event of a failure in the dedicated interface, a fallback mechanism is available to ensure service continuity.
- Article 33 also provides details on the requirements for the contingency plan the ASPSP must to implement to guard against the eventuality of a failure of the dedicated interface and Article 34.3 authorizes the TPP to use the ASPSP interface available to the payment service user. However, an exemption regime exists and the conditions for eligibility are described in Article 33.6. So, a bank utilizing the exception regime may refuse to allow the TPP the use of the customer online interface, even if the dedicated interface fails.

Articles 34 to 36 conclude the technical requirements of the RTS on SCA and are focused on the security and data protection requirements intended to enhance security of the end-user:

- As previously mentioned, Article 34 prescribes the use of e-IDAS role certificates for those entities participating in the TPP service. The purpose is that the bank (ASPSP) only authorizes access to payment account information to those TPPs that are securely identified by a role certificate issued to the TPP by an EU administration. As a result, all the interfaces offered by banks (Open Banking APIs) to TPPs, dedicated or not, must support the identification of the TPP using the e-IDAS certificate.
- Article 35 contains high level requirements for the encryption of data and the protection of the established communication channels established between the entities participating in the TPP. These are intended to avoid the misuse of the personalized security credentials issued by the bank (ASPSP) to its customer and mitigate the risk of impersonation. However, because of their generic nature, these requirements don't actually present a significant constraint for PSPs.

  Article 36 re-iterates the right that PSD2 provides to regulated TPPs in relation to payment account information equivalent to that provided to the end-user. Meaning, that from the bank's perspective, the direct connection by the end user is "almost" the same as that of an "indirect" connection by the same end-user initiated via the TPP. Article 36 also insists on the limitations of the data that can be obtained: no sensitive data is to be disclosed by the bank (but the nature of this "sensitive data" is not set out), only designated accounts are accessible and under control by the end user, and the information which is retrieved is purposeful and must be managed as confidential data by the TPP. Article 36 also sets out a limit to the frequency an account information service provider may consult a designated account.

While Chapter 5 mandates the use of international standards for the secure authentication and data exchange for TPP services, the market for these Open Banking APIs is highly fragmented and the interoperability between Banks (ASPSP) and TPPs is at present limited to local implementations.

7. Final review and take-aways

SPA considers that the RTS on SCA is a fundamental step forward in promoting safe innovation for retail payments. As such, if implemented, it will contribute to a better perception of security by the end-users (customers and retailers) and will help to harmonize technical implementations towards a higher level of security. The text clarifies some ambiguities contained in the Draft released by the EBA last February, yet inevitably for a legal text, others remain.

Globally the RTS on SCA is a good text, but underspecified. The European Commission policy for an open and competitive market for financial innovation justifies the level of prescription finally adopted. Yet, the business need to win market share in this huge potential market may lead to the taking of unacceptable risks in the pursuit of innovative payment solutions where end-user comfort is privileged over security considerations.

This is the reason why SPA members are committed to the development of international standards for the security of TPP services. SPA considers that despite the inevitable short-term fragmentation of currently available open banking APIs, all these interfaces should at least comply with a common architecture layer that makes it possible to achieve the security and data protection requirements of the PSD2.

The RTS on SCA will be reviewed within a two-year time period and within this time frame open international standards will need to be developed that enable Payment Service Providers to comply with Chapter 5 provisions of the RTS on SCA. The efficacy of the security countermeasures proposed can then be assessed against payment fraud data and, if needed, corrective measures to the text can be decided.