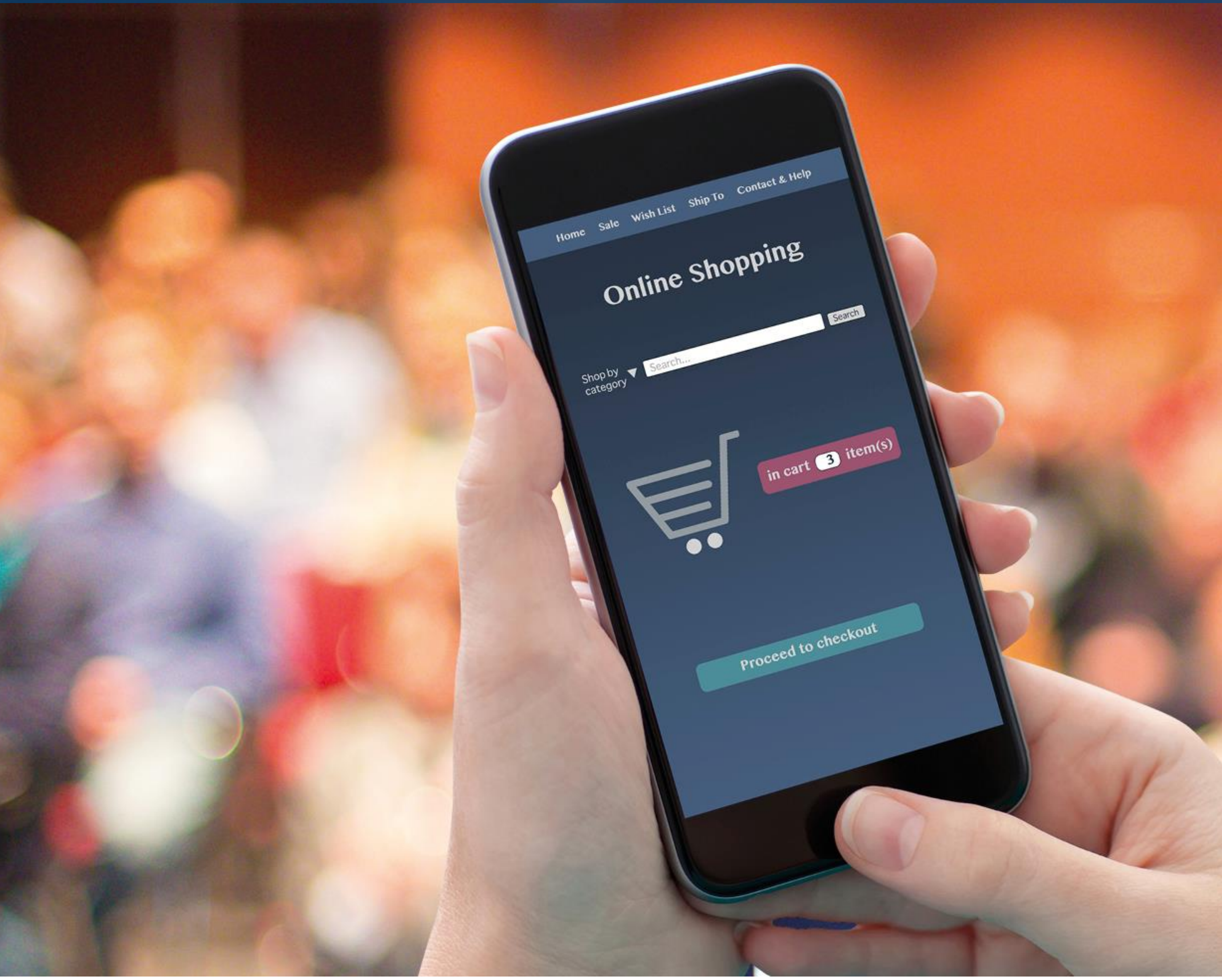
ECOMMERCE EUROPE WHITE PAPER

Regulatory Technical Standard on Strong Customer Authentication and Common Secure Communication

October 2018



INTRODUCTION

On 13 January 2018, the revised Payment Services Directive (PSD2) entered into application, and on 13 March 2018, the accompanying Regulatory Technical Standards (RTS) on Strong Customer Authentication (SCA) and Common and Secure open standards of Communication (CSC) were published in the Official Journal of the European Union. The RTS on SCA and CSC will come into full effect in September 2019.

The RTS on SCA are instrumental to the application of the PSD2 as they define specific security measures that were only addressed through general principles in PSD2. It is therefore vitally important that remaining questions be answered, and provisions clarified in a harmonized fashion at European level.

The position of Ecommerce Europe has been constant throughout the drafting and adoption process of the RTS on SCA. After the publication of the European Banking Authority's (EBA) Opinion on the implementation of the RTS earlier this year and considering that some National Competent Authorities (NCAs) are still interpreting the rules, Ecommerce Europe wishes to reiterate its stance. While we fully recognize the need for customer protection in online payments, we continue to advocate for additional clarifications and a balanced interpretation of the RTS on SCA by the relevant NCAs.

Ecommerce Europe believes that a restrictive and uncoordinated interpretation of the RTS on SCA could have harmful effects on online merchants in Europe. It is therefore important that the interpretation of the RTS on SCA balances security concerns with the customer experience.

The impact of the RTS on SCA will also greatly depend on authentication alternatives and innovation as well as cooperation between stakeholders to find common solutions.

SECURITY MEASURES FOR THE APPLICATION OF SCA

1. Scope of the application of the Strong Customer Authentication

As required per PSD2, strong customer authentication has to be applied when a customer accesses their payment account online, makes an electronic payment or carries out any action through a remote channel that may imply a risk of fraud. The requirements apply to payments that are initiated by the payer, and therefore payments initiated by the payees (so-called "Merchant Initiated Transactions" or "MITs") are excluded.

MITs are transactions initiated by the payees without interaction of the payer. They are characterized by a lack of involvement of the payer in triggering each individual payment.

They are based on an initial mandate by the payer authorizing the payee to initiate periodic payments and a pre-existing agreement between the payer and the payee or the provision of products and services.

In practice, MITs include a variety of use cases mainly built on recurring transactions, such as utilities bill payments, pay-TV and mobile phone subscriptions, car/bike sharing transactions, digital services subscriptions, insurance premium payments, hotel charges and funding transactions for staged wallets.

Therefore, MITs have to be considered as out of the scope of the RTS SCA requirements because:

- There is a pre-existing agreement between the payer and the payee for the provision of products and services;
- The payer has given a mandate to the payee to initiate the recurring payments. This initial mandate requires SCA;
- The payer is technically unable to authenticate the payment and is not involved in initiating the transaction such as for direct debit;

Recommendation

Ecommerce Europe would encourage National Authorities to provide an interpretation of the RTS on SCA that ensures that Merchant Initiated Transactions only (such as recurring payments for variable amounts and/or frequencies) are not in the scope of RTS/SCA. A clear interpretation in favor of integrating MITs would preserve the business model of e-commerce platforms and web shops.

2. How is SCA applied?

The authentication process as defined in the RTS should be based on **two or more** of the following factors:

1. Knowledge – Something only the user knows (PIN, password, …)
2. Possession – Something the user possesses
3. Inherence – Something the user is (fingerprint, facial, iris, …)

The RTS require that in order to be fully effective, those three elements be independent of one another and that the breach of one of the elements will not compromise the reliability of the other. This is commonly referred to as two-factor authentication. They also require, in case of the authentication happening on a multi-purpose device, that Payment Service Providers adopt security measures to mitigate these risks, such as a separated execution environment or mechanisms to ensure that the device has not been altered.

Recommendation

The European Banking Authority's interpretation of the two-factor authentication in its Opinion of 13 June 2018 will severely impact existing secure authentication mechanisms. By considering that the card number with the Card Verification Value (CVV, being the 3 digit code on the back) and expiry date cannot be considered a knowledge element, the EBA is jeopardizing the One-Time Password (OTP) SMS models such as Secure 3DS in France, that would only be based on the possession factor. This interpretation would have heavy consequences for merchants and issuers, and Ecommerce Europe believes that the use of the OTP SMSs should be permitted under the RTS on SCA at least until similar and adequate authentication methods are developed, or until issuers and merchants can adapt to changes that will affect consumers' experience, particularly those with no access to smartphones or a proper internet connection.

3. Dynamic linking

According to the RTS, a unique authentication code which dynamically links the transaction to a specific amount and a specific payee (for remote internet and mobile payments) should be generated as a result of the two-factor authentication. The dynamic linking requirement also applies to batch transactions or bulk payments, whereby multiple transactions to different beneficiaries are combined. More specifically, the final RTS states that, for batch transactions, the authentication code must be specific to both the total amount of money of all the transactions combined and to the various beneficiaries.

Recommendation

Dynamic linking requirement risks disrupting well-established, low-risk merchant processes where the merchant and amount associated with the transaction can change (e.g. orders of fresh produce or orders with multiple items which the customer may prefer to have immediately shipped and hence charged separately). The RTS should clarify that Transaction Risk Analysis applies also to dynamic linking which would prevent the disruption. The RTS should further acknowledge the current industry practice that allows a variation of up to 15% of the authenticated amount of the order, to allow for gratuity payments (tips), variable shipping costs and other costs like taxes due which are associated with the items

EXEMPTIONS FROM STRONG CUSTOMER AUTHENTICATION

The RTS provide exemptions from the SCA requirements. These exemptions remain optional and only one exemption needs to be applied for any given transaction. The EBA clarified that the payees can never decide whether to use an exemption. This decision often lies in the hand of the payer's PSP, which is also the one that makes the ultimate decision on whether to accept or apply an exemption.

1. Trusted beneficiaries - White listing

The RTS provide an exemption based on the possibility for the payee to be included on the list of trusted beneficiaries previously created by the payer. Dedicated application programming interfaces would therefore allow for merchants and their payment initiation service provides to transmit the intention of the payer to add the merchant into their Trusted Beneficiary list and for the payer to confirm the addition. This provision is of upmost importance as it recognizes the relationship of trust between the e-commerce platform and the client. The fact that this provision exists and allows the creation of such a list makes strong authentication unnecessary.

While the EBA has clarified that the exemption is not limited to credit transfers and may apply to cards through the payer's PSP, there are still significant barriers. There is no obligation for issuers to develop solutions to enable this exemption and guidelines on the implementation remain unclear. The exemption for trusted beneficiaries would require rethinking IT systems to create a frictionless way to list merchants.

Recommendation

White listing represents a real opportunity for both issuers and merchants. Ecommerce Europe therefore urges PSPs and merchants to work together to create workable solutions that includes user-friendly solutions to add merchants as trusted beneficiaries at European level. Clearer guidelines and a coordinated definition of workable solutions between issuers and merchants would ensure that the exemptions benefit all players and not only large platforms with the means to ensure banks offer whitelisting for their clients.

2. Transaction Risk Analysis (TRA)

Ecommerce Europe welcomes the acknowledgement of the crucial role transactional risk-based analysis of electronic payments play to the business models and the competitiveness of online merchants. As a technologically neutral alternative for fighting online fraud, TRA allows online merchants and their Payment Service Providers to adapt to new and evolving parameters and fraud patterns, while ensuring the high level of check-out convenience European e-commerce shoppers have become used to.

However, the proposed exemption to Strong Customer Authentication under Article 18 of the RTS only applies to Issuer Payment Service Providers. Online merchants, who often have access to quality customer history, tracking and identification data to assess their own transactional risk are not allowed to avail themselves of this exemption. Facilitated by increasingly sophisticated data analytics, online merchants today can efficiently, and in real-time, track and analyze the fraud-risk of an individual customer.

Recommendation

Ecommerce Europe believes that:

- In order to achieve a complete risk-scoring for each transaction, the best solution would be for the merchant to provide the Issuer with further information about the transaction such as the fraud-risk of an individual customer and its own risk-score. In this way, the Issuer may assess the risk of a transaction supported by information from the merchant and, if the risk is low and an exemption applies, decide not to apply SCA. The role of merchants in the TRA exemption should therefore be clarified by competent national authorities.
- Additional guidance and examples of application of TRA exemption is needed. For example, card acquirers could segregate their merchants into two groups give merchants with lower fraud rates the benefit of TRA up to the maximum possible transaction amount or to calculate the fraud levels at the level of the individual merchant, rather than at the level of the acquirer.

METHOD(S) OF CARRYING OUT SCA

Initiatives are currently being developed to ensure that common standards are discussed and shared by the industry regarding the design of Application Programming Interfaces (APIs). At European level, the API Evaluation Group (APIEG) recently made public its clarification on the topic of Authentication for API standards & initiatives. Ecommerce Europe supports the conclusion drawn by the API EG, that reflects the critical importance of the identification and authentication journey, influenced by the API interface, on the Payment Service Users (PSU’s) experience. Ecommerce Europe also supports the API EG’s clarification on the need for API initiatives to define specifications that supports all SCA methods and processes (e.g. redirection, embedded, decoupled/redirect and decoupled/embedded), and should not only support the redirection method.