Guidance on the Regulatory Technical Standards on Strong Customer Authentication

What are the RTS on Strong Customer Authentication?

On 14 September 2019, new Regulatory Technical Standards (RTS) on Strong Customer Authentication (SCA) will apply in the EU. The RTS on SCA define specific requirements to ensure secure authentication and communication between different actors of the payment ecosystem.

The principle of Strong Customer Authentication is to increase the level of security of electronic payments to ensure consumer protection against fraud. The standards cover the scope, the application, and also the authentication exemptions that may be applied to Strong Customer Authentication for electronic payments.

The information presented in these documents are provided to the best of our knowledge and do not constitute legal advice. Interpretation of the RTS on SCA can vary between Member states.

Why should Merchants care?

If not prepared, the introduction of the new standards on 14 September could affect merchants' conversion rate in Europe. SCA affects the way consumers authenticate themselves, and therefore their online purchasing experience.

After September, the proper management of authentication and exemptions to offer a seamless and secure payment experience to customers will be one of the key drivers for the growth of ecommerce in Europe.

Exemptions listed in the RTS and the fast development of authentication technologies, such as biometrics, can help guarantee a good customer experience while ensuring security of transactions. However, preparedness ahead of the September launch date is uneven across Europe.

What are the key next steps for merchants?

1. Merchants need to be aware of the upcoming changes and engage with the other stakeholders responsible for implementing strong customer authentication, in particular their card acquirer or payment service provider. Merchants should investigate and discuss the solutions that will be available and be clear about what preparatory steps they need to take to ensure their customers continue to receive a smooth and seamless shopping experience.

2. If not already doing so, Merchants should deploy EMV 3D Secure (3DS) as approval rates are likely to drop if no authentication is used. Some issuers may even systematically decline transactions without 3DS being deployed for fear of not being compliant with the RTS.

3. If 3DS is skipped (because an acquirer exemption is applied) and the authorization is declined, merchants should try again with 3DS.

4. If the issuer does not yet support EMV 3DS, then merchants should try with 3DS v1.0 to achieve higher approval rates.

5. Merchants should ensure that their correct brand or trading name (recognizable by the consumer) is correctly held by their card acquirer in order to avoid misunderstanding by the consumer and purchase disputes being raised. Best performance of authentication and authorization processes is obtained when the merchant's name is consistent with their customer facing brand name. Merchants may also benefit optimally from whitelist exemptions when they can be recognized with one unique name;

What is the scope of the RTS on SCA?

Strong Customer Authentication has to be applied in 3 cases:

1. When a customer accesses their payment account online
2. When a customer makes an electronic payment
3. When a customer 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 consumer (payer)**. Payments initiated by the merchant are excluded.

What about "merchants-initiated transactions"?

Electronic payments that are initiated by the merchant (payee) only on the basis of (1) an initial mandate* by the consumer (payer) authorizing the merchant to initiate the periodic payments and (2) a pre-existing agreement between the consumer and the merchant for the provision of products or services **are not subject to SCA**. (*Note: the initial mandate, is subject to SCA)

The EBA has clarified that any payments that are based on an existing agreement between a customer and a merchant, and in which the customer has previously authorized the merchant to initiate subsequent transactions in relation to the agreed delivery of goods or services can be **considered as a merchant initiated transaction, provided that these payments are not dependent on a specific action of the consumer to trigger the initiation of the payment by the merchant**.

However, where a standing agreement between a customer and a merchant results in a subsequent billing by the merchant without the merchant having been provided with the mandate by the customer to initiate any subsequent payment, such payments cannot be considered as a consumer-initiated payment.

What is the Strong Customer Authentication?

The RTS define SCA as authentication through at least <u>two</u> out of the following three factors:

1. **Knowledge** – Something only the user knows e.g. a PIN or a password. (Note: The European Banking Authority currently considers that the card number with CVV and expiry date, as well as a user ID cannot be considered as belonging to the "knowledge category".)
2. **Inherence** – Something the user **is** e.g. the use of a biometric such as fingerprint, face, iris or voice recognition, including behavioral patterns etc.
3. **Possession** – Something only the user possesses e.g. a mobile phone or token. The EBA's current view is that for a device to be considered as possession, there needs to be a reliable means to confirm actual possession, for example by generating a receipt of a dynamic validation. A One-Time Password (OTP) sent via SMS to a mobile phone currently qualifies as a possession factor.

The RTS require that the selected factors must be mutually independent in that the breach of one does not compromise the reliability of the other. The EBA has also made it clear that the two (of the possible three) authentication factors required must belong to **different categories**.

Is it possible to use one single device for authentication?

The use of a single device for authentication and shopping is permitted. This means, for example, that a smartphone may be used at the same time for transacting and for authenticating the cardholder.

The risk connected to the use of multi-purpose devices (e.g. smartphones and tablets) must be mitigated through the use of separated secure execution environments.

Mechanisms to ensure that the software or device have not been altered by the payee or by a third party must be in place.

What is dynamic linking?

For remote transactions, each SCA must be linked to a specific amount and payee otherwise referred to as dynamic linking.

This requirement, effectively binding authentication to the merchant and the amount, is to ensure that a valid authentication code is only used once and for the specific transaction for which the authentication is requested.

Card on File merchants: Are there exemptions available?

Card on File (CoF) merchants provide a better consumer experience at checkout, as the merchant offers the consumer to store their card details, such as card number and address so that this information does not have to be re-keyed every time the consumer wishes to initiate a payment.

The RTS do not contain a specific exemption for CoF transactions. Unless an exemption applies, SCA is required on every CoF transaction where the cardholder is triggering a payment. **White-listing is particularly relevant to allow for one-click payments with CoF**. See point 3 under section headed ‘Exemptions to Strong Customer Authentication” to understand more about White-listing.

Is delegated authentication to a smartphone allowed?

There are a number of devices (e.g. smartphones) that include a Consumer Device Cardholder Verification Method (CDCVM) to access the device.

This is a great opportunity for these devices to be used by consumers to authenticate themselves for a payment, especially for mobile NFC payments, as most of them occur via mobile wallets (e.g., Apple Pay, Samsung Pay etc.).

Is delegated authentication to a merchant allowed?

Card Issuers can take into account the security credentials issued by the merchant to authenticate cardholders, - provided the security credentials are compliant with the SCA requirements under the RTS (for example, they allow for secure biometric authentication).

This would require SCA of the credentials issued by the merchant and an express delegation by the Issuer. In addition, it would only be allowed for low-risk merchants and the card details are digitized and tokenized in the merchants Card on File (CoF) solution.

Card schemes will soon announce delegation programs, and merchants interested in joining should contact their card acquirer or payment services provider

Exemptions to Strong Customer Authentication

The RTS includes exemptions to the Strong Customer Authentication. Only one of the following exemptions is required to enable a merchant to waive the requirements of SCA. The application of the exemption remains largely in the hand of the issuer.

Merchants are encouraged to rely on exemptions – particularly the exemption for low-value transactions and for low-risks transactions

1. Recurring transactions

If a consumer sets up a recurring transaction of the same amount and to the same merchant, a Payment Service Provider (PSP) can choose to apply SCA when the series of payments is initially created or subsequently amended and offer an exemption for the following transactions:

(a) Recurring transactions meeting the criteria and created before the introduction of the RTS, SCA should only be required if any recurring transaction is subsequently amended.

(b) Recurring transactions that are merchant-initiated are out of the scope of the RTS and do not require SCA.

2. Low-value transactions

Remote electronic transactions that meet the following conditions can also be exempted from SCA:

- The amount does not exceed EUR 30
- The cumulative amount of previous transactions since the SCA was last undertaken does not exceed EUR 100
- The number of previous transactions of up to EUR 30 does not exceed 5 or a maximum of EUR 100 since the last SCA.

3. Trusted beneficiaries or "White-listing"

SCA is not needed where the merchant (payee) is included in a list of trusted beneficiaries. SCA would only apply when the merchant wishes to create or amend the list. Only the consumers card issuer may apply this exemption. **Unfortunately, it is likely that issuers will not be in a position to support this exemption by September. Merchants should therefore consider other exemptions.**

4. Fraud rates and Transaction Risk Analysis (TRA)

For transactions considered as having a low risk of fraud, PSPs do not need to apply SCA. The conditions for this exemption are detailed in the RTS, and concerns transactions up to EUR 500. Merchants cannot apply this exemption directly but must rely on their card acquirer or PSP applying the exemption. If the card acquirer applies the exemption, it will be liable for the transaction and the merchant is guaranteed payment.

5. Other exemptions

Other exemptions are included in the RTS for transactions such as contactless payment, secure corporate payment transfers, access to payment account information or transfer to another account held by the same person with the same PSP.

EMV3-D Secure (EMV 3DS)

EMV 3DS is the evolution of the current authentication interface (3DS v1.0) into an industry standard that:

- Lets transaction and consumer data be exchanged (e.g. device data, shipping and billing address), allowing the issuer to apply SCA exemptions and enhance decision making.
- Supports new payment needs, such as in-app and mobile payments.
- Supports additional use cases, such as:
    - Credential-on-file (COF): no need for customers to enter card details into merchant/ retailer's website or app for each purchase if card is pre-registered.
    - Wallets, e.g. Google, Samsung Wallets.
    - Tokenisation: a token replaces the real card number being stored, avoiding the full card details becoming compromised.

PSD2 RTS require that from the 14th September 2019, Strong Customer Authentication (SCA) must be used for all remote electronic transactions, including e-commerce, unless an exemption applies (please see below for details). **Merchants are therefore strongly advised to send authentication requests using the EMV3-D Secure (EMV 3DS) protocol to minimize the possibility of card issuers declining e-commerce transactions due to suspected fraud**.

With EMV 3DS deployed, e-commerce merchants will most probably be able to achieve similar performance levels as physical store merchants, and this can be achieved by letting issuers apply SCA to every online purchase and therefore provide them with sufficient data to apply exemptions from SCA, and help ensure transactions can be completed with minimal friction. **Online merchants should therefore support EMV 3DS authentication requests.**

Authentications using EMV 3DS are also the recommended method for the merchant to advise the issuer about the exemption being applied by the acquirer. Such authentications typically won't require a cardholder challenge (e.g. could not lead to an abandonment) but they will allow the issuer to control the risk which increases the approval rate.

EMV 3DS will be compulsory for European retailers by September 2019, and globally in December 2019.

What actions are Merchants advised to take?

1. Merchants shall select and deploy their PSP (Payment Service Provider/3DS Server) that implements and operates the authentication interface on their behalf through EMV 3DS and 3DS v1.0 (as fallback when issuer does not support EMV 3DS).
2. Merchants must prepare themselves to capture incremental transaction and cardholder data (e.g. billing and shipping address, e-mail, mobile phone number or device ID) and send them to the PSP which may require the coding for a new API (Application Programming Interface) or similar provided by the PSP. Merchants should ensure that their terms and conditions reflect the collection and sharing of the consumer data (e.g. in the privacy notice) as required, for example, by the General Data Protection Regulation (GDPR).
3. Merchants need to implement an authentication policy, aligned with their PSP or card acquirer, in support of the RTS and its exemptions, specifically to the adoption of Transaction Risk Analysis (TRA) exemptions and corresponding fraud levels that apply.
4. Merchants should ask their acquirer(s) to enroll them for EMV 3DS with the card schemes.
5. Merchants should make changes to their websites in support of EMV 3DS and the RTS.

6. Should a merchant request an acquirer SCA exemption without an authentication request, and the transaction is declined by the issuer (especially for reasons other than financial or technical declines), then a mechanism should be in place that automatically sends an EMV 3DS authentication requesting a challenge and, if approved, followed with another authorisation. Similarly, if an issuer does not yet support EMV 3DS authentications then a merchant should use the current 3DS version 1.0.2 as a fall back.
7. Merchants should integrate EMV 3DS features to offer an optimal end-consumer experience, by revamping the authentication part of the merchant app in native User Interface (UI) to offer the same look and feel as the merchant app.
8. Merchants have to apply SCA to the first recurring payment. In order to increase the approval rates, it is recommended that for each subsequent payment an EMV 3DS authentication request is sent to the issuer with a reference to the initial SCA to avoid the need for the cardholder being asked to authenticate again.
9. In cases of recurring payments for variable amounts or payments where the final amount is not known, the Merchant should clearly communicate and explain to the consumer the reasons why the authenticated amount may be different than the final authorization amount.
10. Merchants should make sure that the authentication amount is equal to or above the authorization amount (or the sum of all authorization amounts related to an authentication). Otherwise the Merchant may become liable to a chargeback from the card issuer.
11. Merchants are recommended to always send an authentication request, especially as card issuers may decline authorizations that do not have prior authentication.

Ecommerce Europe

Rue d'Arlon, 69-71
B-1040 Brussel - Belgium
T. +32 (0) 2 502 31 34
info@ecommerce-europe.eu

www.ecommerce-europe.eu
www.ecommercetrustmark.eu
@Ecommerce_EU

Made in cooperation with Mastercard