EMV 3-D Secure

Regulatory Requirements

EBA Mandate

The European Banking Authority (EBA) mandated that all payer who access their payment account online and initiate electronic payment transactions through a remote channel must be strongly authenticated (aka Strong Customer Authentication (SCA)) commencing September 14, 2019. The card organizations seized this opportunity to overhaul the established 3D-Secure protocol for cardholder authentication and to address several issues that curbed adoption in the market.

3-D Secure 2.0

Previously, internet merchants had the choice to either present a cardholder challenge (e.g. TAN / password) or to give 3-D Secure a pass entirely. Some adopted a dynamic approach based on PSP or own risk assessment, but many merchants valued a frictionless checkout and high conversion rates more than the potential benefits of a liability shift. The card organization's overall strategy for 3-D Secure 2.0 is to reduce friction through an improved cardholder experience (device awareness) and to leverage exemptions from SCA based on robust transaction risk analysis (TRA) with the ultimate goal of delivering optimal authorization performance and conversion rates. Thus, TRA is key to delivering frictionless payment experiences for low-risk remote transactions. Therefore the 3-D Secure 2.0 protocol introduced a plethora of additional data points that can be transferred to the issuer to aid transaction risk analysis and to apply exemptions from SCA.

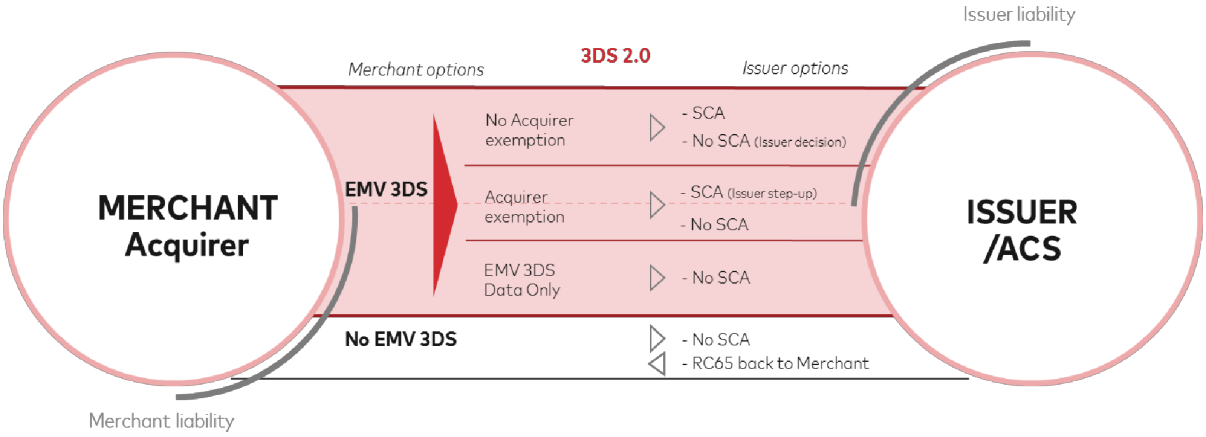
SCA will be required when:

- The transaction is not out of scope of the PSD2 RTS
- No PSD2 SCA exemption applies for a payment transaction
- Adding a card to a Merchant's file (card-on-file)
- Starting a recurring payment arrangement for fixed and variable amounts, including setting the initial mandate for Merchant-Initiated Transactions
- Changing a recurring payment agreement for a higher amount (premium offering for example)
- Setup of white-listing (or viewing/amending white-lists)
- Binding a device to a Cardholder

Liability Shift

As a rule of thumb, when cardholder authentication was performed through 3-D Secure, merchants are typically protected against e-commerce fraud-related disputes and liability shifts from the merchant / acquirer to the issuer. There are exceptions to merchant dispute protection though. In the context of 3-D Secure 2.0 merchants are regularly not protected if granted exemptions according to PSD2 RTS were actively requested by merchant / acquirer.

The following diagram depicts options and liabilities under PSD2 RTS requirements according to MasterCard.

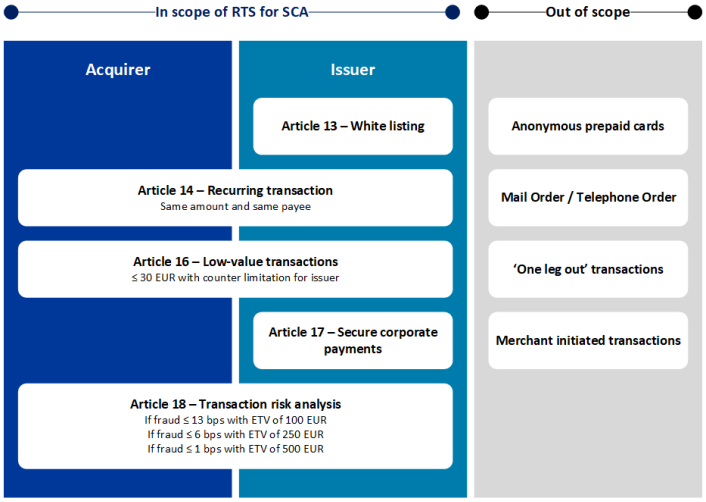


3-D Secure 2.0 and GDPR Compliance

Cardholders must be provided with detailed information about how their data is collected, used and processed. This can be ensured via a Privacy Notice including at a minimum the types of data being processed, the purposes of their processing, data uses, etc. Card organizations and Issuers will not use EMV 3-D Secure data for other purposes than fraud prevention and authentication. It excludes the usage of personal data for other purposes, such as sales, marketing and data mining (other than fraud prevention as purpose) activities.

PSD2 SCA Exemptions and Exclusions

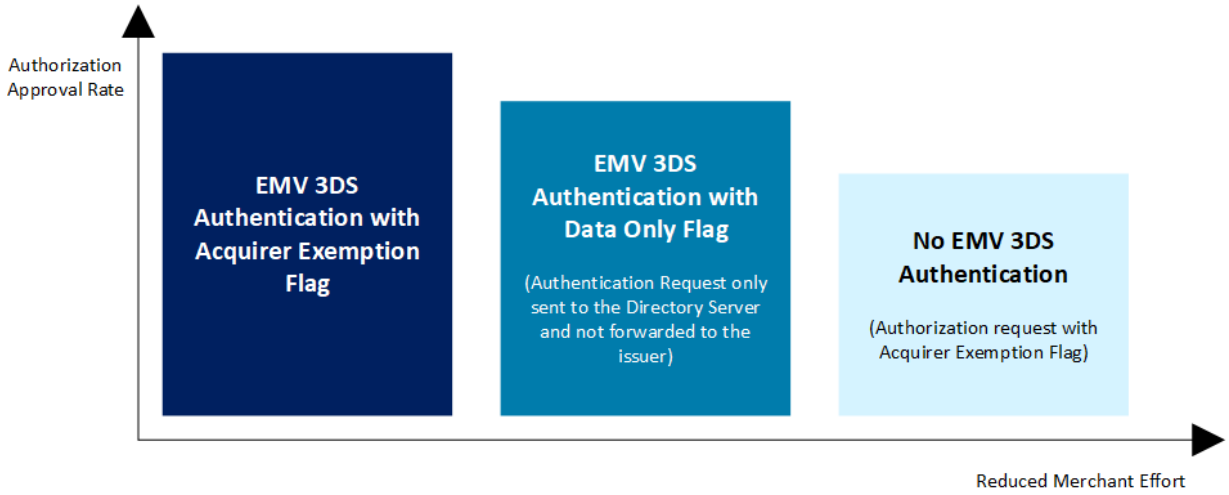
There are some important exemptions to SCA according to the regulatory technical standards (RTS) that may apply in various conditions which are depicted in the following diagram.



Computop Paygate

Authentication Options

An acquirer may be allowed to not apply SCA due to to low fraud rates and TRA. For these exemptions there are various processing options available as depicted in the diagram below.



As a standard, Computop Paygate will submit (where supported) applicable exemptions through the EMV 3-D Secure authentication flow to the issuer to achieve best possible authorization approval rates.

EBA-Op-2018-04, Paragraph 47 - Clarification on PSP (Acquirer Fraud Rates)

The fraud rate as defined in Annex A of the RTS is calculated for all credit transfer transactions and all card payment transactions and cannot be defined per individual payee (e.g. merchant) or per channel (whether app or web interface). The fraud rate that determines whether or not a PSP qualifies for the SCA exemption cannot be calculated for specific merchants only, i.e. where the payer wants to make a payment to a specific merchant and this specific merchant has a fraud risk that is below the threshold. While the payee's PSP (acquirer) may contractually agree to 'outsource' its transaction risk analysis monitoring to a given merchant, or allow only certain predefined merchants to benefit from that PSP's exemption (based on a contractually agreed low fraud rate), the fraud rate making a given PSP eligible for an exemption under Article 18 would still need to be calculated on the basis of the payee PSP's executed or acquired transactions, rather than on the merchant's transactions.

Message Version 2

To handle the amount of additional non-payment data and to maintain downward compatibility as much as possible Computop decided to version its Paygate card interface via the additional data element **MsgVer**. The upgraded API is still based on key-value pairs but relies heavily on Base64 encoded JSON objects to aid readability and client-side scripting.

Merchants will still be able to use our classic interface for requests even with 3-D Secure 2.0 but there are some limitations:

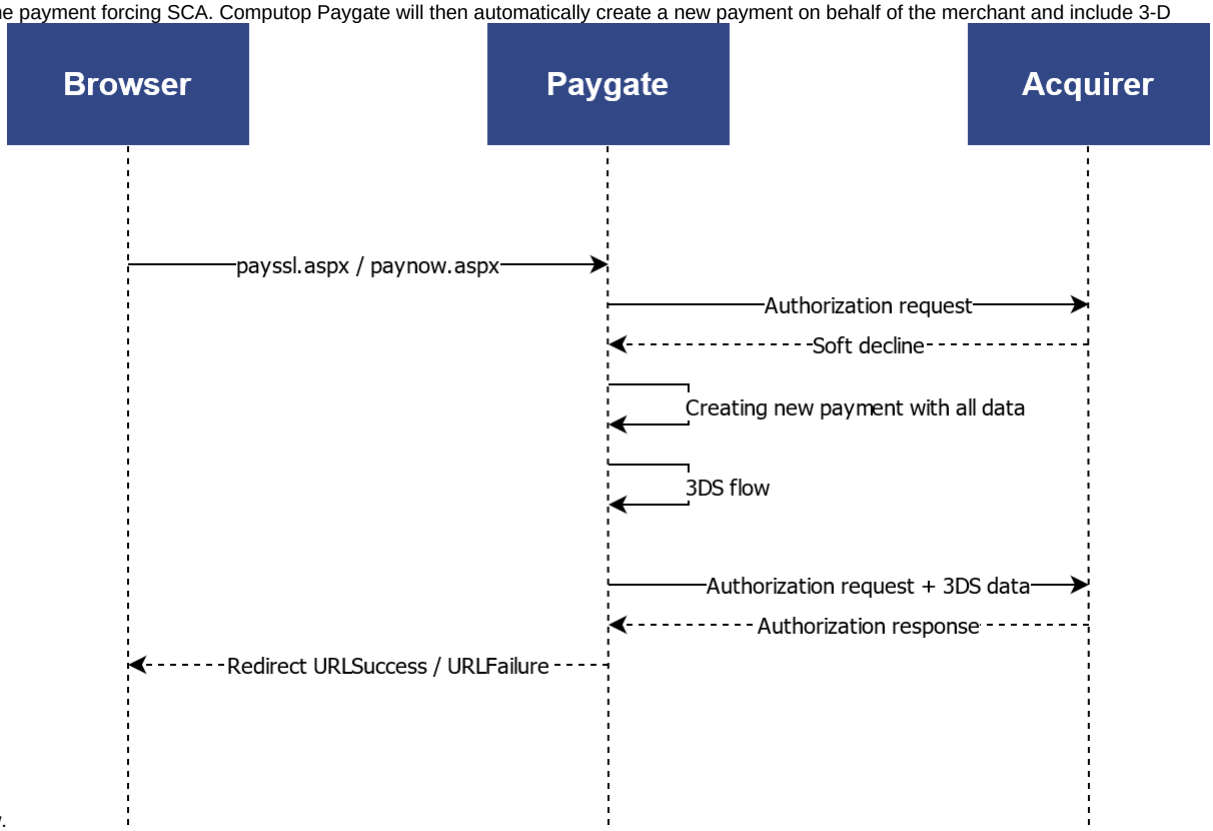
- Many additional data points for issuer risk analysis are not available and thus, the frictionless ratio might be lower
- API responses and notifications do include new JSON objects to cater for 3-D Secure 2.0 protocol specifications and require modification of existing merchant integrations

For these reasons it is highly recommended to upgrade to version 2.

Soft decline handling

In case a transaction is missing SCA, issuers might respond with so-called soft declines. This means that the transaction authorization request is declined by the issuer, however, the same transaction can be initiated again. The main reason for soft declines emerging in the context of 3D Secure is that issuers are not accepting SCA exemptions requested by the merchant when such is sent directly to authorization or when the merchant requests payment without authentication being carried out beforehand. The best practice is to restart the payment including 3-D Secure.

With **Automated Soft Decline Handling** feature, configuration based, Computop Paygate will react to the soft decline response by automatically restarting the payment forcing SCA. Computop Paygate will then automatically create a new payment on behalf of the merchant and include 3-D



Secure flow.

IMPORTANT:

- From a user's point of view, customers will not notice any difference and will not need to re-enter their credit card data. The whole process is managed by the Computop Paygate.
- Please note that this solution is not available for **server-to-server** integrations, as Computop Paygate does not have the client (browser) in control to start the 3-D Secure flow. For server-to-server integration, the merchant is responsible to re-trigger the payment with 3-D Secure flow and most important forcing the SCA challenge through the available parameter JSON threeDSPolicy (*challengePreference* = *mandateChallenge*).

Whitelisting of trusted beneficiaries

A cardholder might opt to add a merchant to a list of trusted beneficiaries maintained at the issuer to exempt this particular merchant from SCA with future payments. This will usually occur during a cardholder challenge but cardholder's might also be able to manage a list of trusted beneficiaries through their banking app for instance.

Merchants may benefit from a whitelist exemption if requested and if a cardholder challenge is not required otherwise.

Please note that whitelisting is available with 3-D Secure version 2.2 and higher. Currently issuer most support 3-D Secure 2.1.

Recurring transactions

Recurring transactions are a series of transactions processed following an agreement between a cardholder and a merchant where the cardholder pur chases goods or services over a period of time and through a number of separate transactions with the same amount. The initial transaction must be authenticated (i.e. cardholder initiated transaction (CIT)). Subsequent recurring payments are out of scope of RTS SCA since they are regularly merchant initiated (i.e. without customer being in session).

Low-value transactions

Issuers may exempt transactions from SCA provided that the following conditions are met:

- the payment amount does not exceed EUR 30,
- the cumulative amount of previous payment transactions without SCA does not exceed EUR 100,
- the number of previous payment transactions without SCA does not exceed five consecutive payment transactions.

Please note that low-vale exemptions must be requested to be considered for a frictionless authentication flow.

Transaction risk analysis

Acquirers and issuers are allowed not to apply SCA provided the overall fraud rate is not higher than the reference fraud rate for the exemption threshold value (ETV) specified in the table below and where the risk-based assesment of each individual transaction can be considered as low risk.

ETV	Card-based payments
EUR 500	1 bps
EUR 250	6 bps
EUR 100	13 bps

One-leg out transactions

One-leg out transactions are such transactions where either the payer’s payment service provider or the payee’s payment service provider are located outside the European Union.

Payment service provider in the context of a card based transaction and in the spirit of the PSD2 are regularly **acquirer** and **issuer**.

Thus, neither the nationality of the cardholder nor the merchant's business location are relevant for the assessment whether a transaction is out of scope due to the 'one-leg out' rule.