

# 3DSV2 and frictionless

The PSD2 (Payment Service Directive version 2) is a European directive that aims to encourage innovation, improve consumer protection and enhance the security of payment services.

RTS regulations (Regulatory and Technical Standards) related to PSD2 require the use of the authentication process for all e-commerce payments initiated by cardholders.

The aim is to meet the requirements of Strong Customer Authentication to reduce the risk for the merchant and both simplify and smooth the customer journey.

## 3DSV2 Definitions

### Strong Customer Authentication (SCA)

Strong Customer Authentication is a regulatory requirement introduced under PSD2.

During an online payment, a strong two-factor authentication can be requested to the cardholder, in order to confirm that the person doing the online payment is the holder of the card used for the payment.

Authentication is considered strong when it combines two of the following three authentication factors:

- **an element known** to the cardholder (password, secret code, etc.)
- **an item owned by the cardholder** (mobile phone via the bank application, a bank card, etc.)
- **a biometric feature** (a fingerprint, voice recognition, etc.)

### Frictionless

The merchant can request an exemption of the customer authentication. The final decision is owned by the cardholder issuing bank.

In a frictionless transaction a passive authentication of the holder is performed, he has nothing to do.

In few words, this process reduces the actions of the buyer during the payment process.

In the case of frictionless transactions, the liability shift is related to the card brand : [Liability shift and 3DS Matrix](#)

### Merchant choices : no Preference / challenge / mandate

The merchant can request a strong authentication or an exemption. He has several choices:

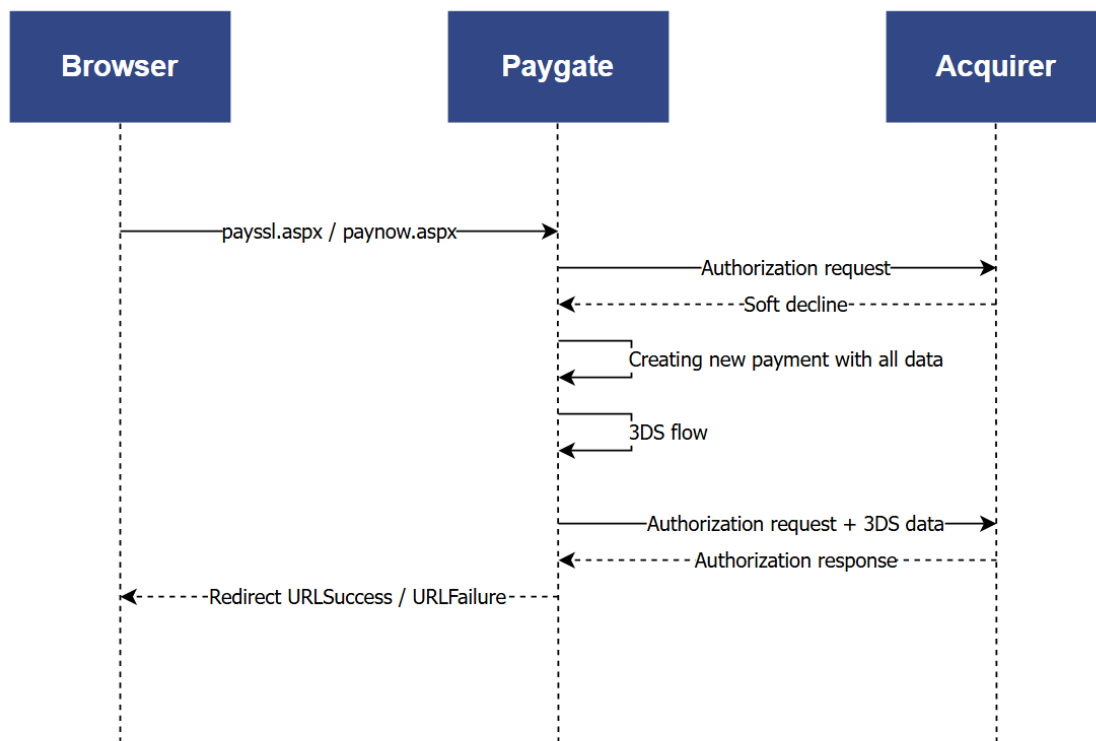
- **The merchant takes no action** (no preference): the choice of exemption is left to the issuer.
- **The merchant requires strong authentication (challenge):**
  - Mandatory (**mandate**): the issuer must authenticate the buyer (e.g. for the first subscription transaction)
  - Preference (**request**): The merchant wishes to authenticate the buyer. The final choice remains with the issuer.
- **The merchant requests an exemption of the strong authentication (no Challenge - Frictionless):** The issuer will accept or not the merchant's request according to the information he sent.

In the case of frictionless transactions, the liability shift is related to the card brand : [Liability shift and 3DS Matrix](#)

### Soft decline

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, Axepta BNP Paribas Platform will react to the soft decline response by automatically restarting the payment forcing SCA. Axepta BNP Paribas Platform 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 Axepta Platform.
- Please note that this solution is not available for **server-to-server** integrations, as Axepta Platform 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*).

## Transactions not affected by SCA

With PSD2, some payment cases are exempted from strong customer authentication, such as:

- **Recurring payments (MIT-Merchant Initiated Transactions):** The initial payment requires strong authentication but the following payments will be exempted. If there is a change in subscription price, the cardholder will have to do a new strong authentication.
- **MOTO transactions (Mail Orders and Telephone Orders)** : this type of transaction is not considered an electronic payment.

## Exemptions

The merchant can request an exemption for :

- **Low-value transactions (below 30€)** : Banks must, however, request authentication if the exemption has been used five times since the cardholder's last successful authentication or if the sum of the previously exempted payments exceeds €100.
- **Low risk transactions (TRA: Transaction Risk Analysis)** : a derogation of the strong customer authentication may be granted. This requires the prior agreement of the acquirer (based on a real-time risk analysis of each transaction).

## Increase 'Frictionless' payments

Several parameters can be added to the payment request to increase frictionless payments.

For further details : [Exemptions & 'Frictionless' payments](#)