

3D Secure - Strong Authentication for Secure Payments (EN)

The **PSD2 (Second Payment Services Directive)** is a European directive aimed at encouraging innovation, improving consumer protection, and enhancing the security of payment services. The **RTS (Regulatory Technical Standards)** related to PSD2 mandates the use of the authentication process for all e-commerce payments initiated by the cardholder. The goal is to meet the requirements of strong customer authentication (**Strong Customer Authentication - SCA**) to minimize risk for merchants while simplifying and streamlining the user journey.

Glossary on 3DSV2

Strong Customer Authentication (SCA)

Strong customer authentication (SCA) is a regulatory requirement introduced under PSD2. During an online payment, strong two-factor authentication may be requested from the cardholder, confirming that the person making the payment is indeed the cardholder. An authentication is considered strong when it combines two of the following three authentication factors:

- **Something known to the cardholder** (a password, a secret code, etc.)
- **Something possessed by the cardholder** (mobile phone via the bank's application, a bank card, etc.)
- **Something inherent to the cardholder** (a fingerprint, voice recognition, etc.)

Frictionless

The merchant has the option to request an exemption from cardholder authentication during online payment. The final decision is left to the issuing bank.

In a "frictionless" transaction, passive authentication of the cardholder is performed without any action on their part. In summary, this is a process that reduces buyer intervention during the payment process.

In the case of a frictionless transaction, liability shift depends on the card brand. For more details, refer to our documentation on **Liability Shift and 3D-Secure Matrices**.

Merchant Preferences: no Preference / challenge / mandate

The merchant can request the issuer to grant or not grant an exemption from strong authentication. Several options are available:

- **The merchant takes no action (no preference):** The choice of exemption is left to the issuer.
- **The merchant requests strong authentication (challenge):**
 - **Mandatory (mandate):** The issuer must authenticate the buyer (e.g., for the first transaction of a subscription).
 - **Preferred (request):** The merchant wishes to authenticate the buyer. The final choice remains with the issuer.
- **The merchant requests an exemption from strong authentication (no Challenge - Frictionless):** The issuer will accept or reject the merchant's request based on the information provided (data to be transmitted).

Liability shift depends on the merchant's choice and the card brand. For more details, refer to our documentation on **Liability Shift and 3D-Secure Matrices**.

Soft Decline

In the case of a transaction made without SCA (3DS Strong Authentication), issuers may respond with a **Soft Decline**. This means that the transaction authorization request is refused by the issuer; however, the same transaction can be initiated again. The main reason why Soft Declines occur in the context of 3D Secure is that issuers do not accept SCA exemptions requested by the merchant when they request a payment without prior authentication.

With the automated Soft Decline management feature, based on configuration, the **Axepta BNP Paribas** platform will react to the Soft Decline response by automatically restarting the payment by forcing strong authentication. The **Axepta BNP Paribas** platform will then automatically initiate a new payment on behalf of the merchant and include the 3-D Secure flow.

Important:

- From the user's perspective, customers will notice no difference and will not need to re-enter their credit card details. The entire process is managed by the **Axepta BNP Paribas** platform.
- Please note that this solution is not available for server-to-server integrations, as the **Axepta BNP Paribas** platform does not control the client (browser) to initiate the 3-D Secure process. For server-to-server integration, the merchant is responsible for reactivating the payment with the 3-D Secure flow and, above all, forcing SCA via the available JSON parameter **threeDSPolicy (challengePreference = mandateChallenge)**.

Transactions Not Subject to SCA

Under this new regulation, some payment cases may be exempt from strong customer authentication:

- **Recurring payments (MIT - Merchant Initiated Transactions):** The initial payment requires strong authentication; however, subsequent payments will be exempt. In the case of a change in the subscription amount, the buyer will need to go through a strong authentication procedure again.
- **MoTo (Mail Orders and Telephone Orders) transactions:** This type of transaction is not considered an electronic payment.

Exemptions

The merchant can request an exemption from authentication for some transactions subject to strong authentication:

- **Low-value transactions (less than €30):** Banks must, however, request authentication if the exemption has been used five times since the last successful authentication of the cardholder or if the sum of previously exempted payments exceeds €100.
- **Low-risk transactions (TRA: Transaction Risk Analysis):** An exemption from the strong authentication obligation may be granted. For this, prior agreement from the acquirer is required (based on a real-time risk analysis of each operation).

Promoting 'Frictionless' Payments

Several parameters can be added to the payment request to promote frictionless payments. For more details, refer to our [documentation](#) on **Frictionless Payments and Exemptions**.