PSD2: Overview on Regulation

1. Status

Final RTS published and will enter into force on **September 14th, 2019**

To help RTS implementation, EBA has:

Published new papers (Opinion on the implementation of the RTS on SCA, Guidelines)

Opened a Q&A portal for additional clarification

2. Key Considerations

SCA is the new standard (payment transactions and access to accounts)

SCA Exemptions are permitted but are not a given. Actions are required (fraud monitoring, White List, …)

SCA **Exemptions enable higher flexibility** to create a frictionless customer user experience (One Click check-out)

The final authorisation will **be approved (or declined) by the issuer**

3. RTS Requirements on SCA and Exemptions

Scope

Online / **Remote payments** (incl. card on file)

In store electronic payments (e.g. mobile/ contactless)

Access to **mobile banking app**

Two-leg transactions*

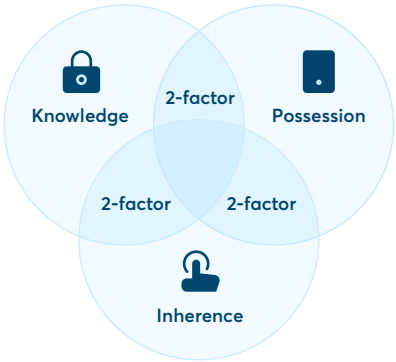
MIT are **out of scope** of **SCA requirements****

* Payment transactions where both the issuer and the acquirer are located within the EEA

** **MIT** (Merchant Initiated Transactions) are card payments initated '*by the payee only*'. There is pre-existing agreement between payer and payee for provision of services. **SCA is required for initial mandate**.

MIT use cases are limited and **clearly defined**:
- Utilities bill payments (e.g. electricity and gas)
- Mobile phone subscriptions
- Digital services subscriptions (e.g. Google Ads)
- Funding transactions for staged wallets (e.g. PayPal)

Key Principle



Possession: Something you own

- Mobile phone
- Wearable device
- Smart card
- Token
- Badge

Inherence: Something you are

- Fingerprint
- Facial features
- Voice patterns
- Iris format

Knowledge: Something you know

- Password
- Passphrase
- Pin
- Sequence
- Secret fact

Main exemptions (for low risk transactions)

Remote transactions **up to EUR 30** (for 5 consecutive transactions, or alternatively for total of EUR 100)

Remote transactions between **EUR 30** and **EUR 500** provided **RBA** is applied** by the issuer or the acquirer and **their fraud rates are under specific thresholds**

TRA Thresholds

Issuer bps	Exempt up to:
< 13 bps	€ 100
< 6 bps	€250
< 1 bps	€500

Remote transactions to **white lists of trusted beneficiaries and recurring transactions** (SCA is required for the initial 'subscription')

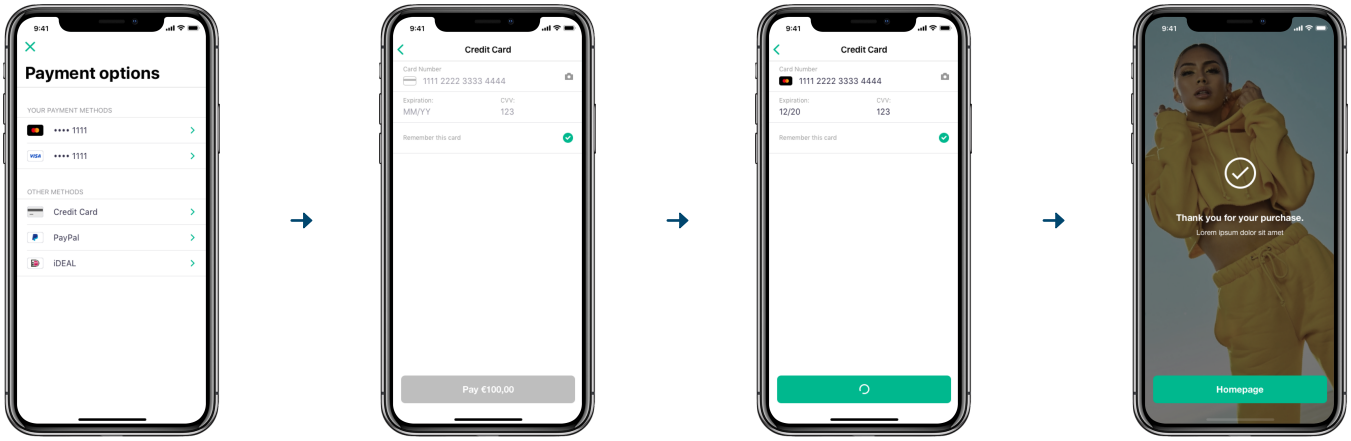
Contactless transactions up to **EUR 50** (for 5 consecutive transactions, or alternatively for total of EUR 150)

** Risk based authentication

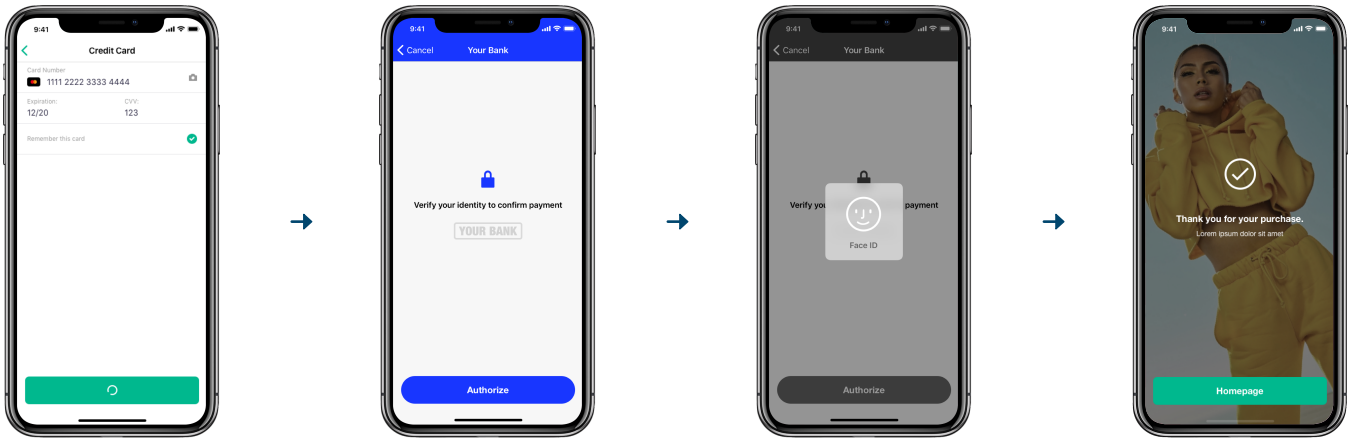
PSD2: Overview on Regulation

4. Checkout examples

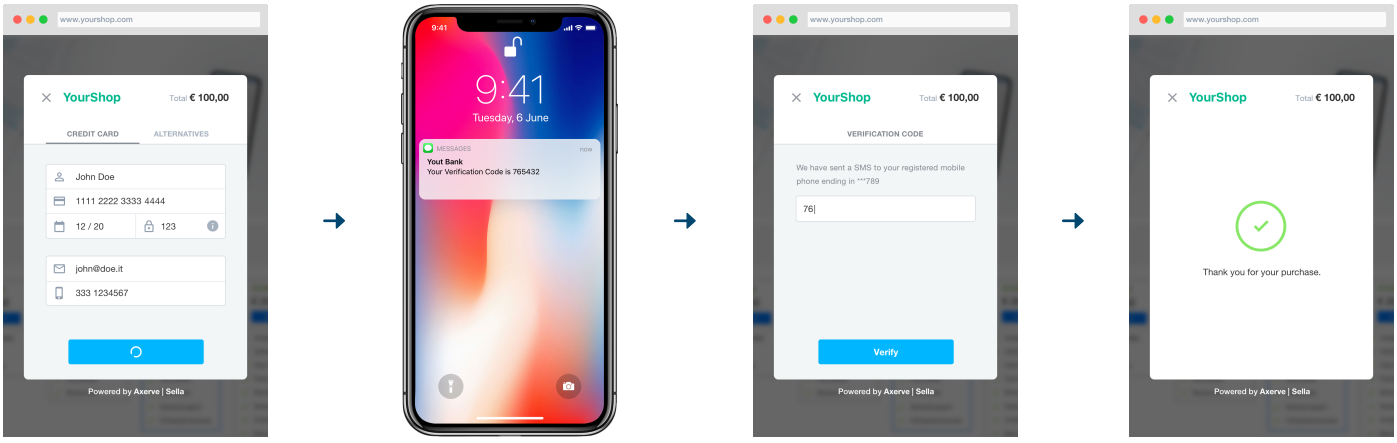
Frictionless in mobile app



Biometric (Bank app) in mobile app



2 factor in browser



5. Mastercard Recommandations

1. **EMV 3DS 2.0** is the best way to achieve compliance with PSD2 RTS
2. Leverage the **additional authentication & authorization** information provided by Mastercard
3. Maximize SCA **Exemptions**
4. Leverage **Biometric Authentication** for SCA
5. Issuers can **delegate the SCA**

PSD2: Overview on Regulation

6. Richer Authentication Message – EMV 3DS versus 3DS 1.0

3DS 1.0 Data (Initial Message – VEReq)

- Message, Extension, Version
- Browser User-Agent
- Acquirer BIN
- Acquirer Merchant ID
- DS URL
- Cardholder Account Number

More than 10x Data

EMV 3DS Data (Initial Message – AReq)

- Merchant Risk Indicator (Delivery Timeframe, Re-order, Pre-order, Gift Card)
- Cardholder Account Information (Account Age, Change, Password Change, Number of Transactions per Day / Year, Shipping Name Indicator, Suspicious Activity, Payment Account Age etc.)
- DS Reference Number, Transaction ID
- Cardholder Shipping Address
- 3DS Requestor Authentication Information (Method), Challenge Indicator, ID, Initiated Indicator
- Purchase Date & Time
- SDK Reference Number, SDK Transaction ID
- Purchase Amount, Currency, Date & Time
- Transaction Type
- Device Channel, Device Information, Rendering Options Supported
- Card Expiry Date
- and more…

You can easily integrate the mandatory data like Cardholder, Card, Acquirer, Billing and Shipping informations with Gestpay by Axerve API. For further information see our documentation and our API.

7. GDPR

The 3DS 2.0 will require more information from the buyer. It is therefore essential to collect a **specific consent from the card holder for the transmission of all data entered during the purchase** (shipping address, addresses, etc ...) that will be sent to third parties for the correct processing of the payment transaction.

Without such consent the transaction will be deprived of the information needed for the assessment of its riskiness: the authentication will be processed through SCA. Ask your acquirer how to modify your GDPR policy.

8. "Call to Action" for Merchants

Increase Transparency

- Enrol into EMV 3DS
- Enrich authentication message to encourage issuers to maximise exemptions
- Adapt terms and conditions (GDPR)

Drive Loyalty

- Promote whitelisting solutions for customers
- Leverage recurring transactions and MITs

Adopt Innovative Solutions

- Implement or adopt biometric solutions

Reduce Fraud

- Increase visibility on your fraud levels
- Implement new solutions (e.g. tokenization, fraud engines)
- Collaborate with acquirers (e.g. bring down fraud levels and leverage TRA exemptions)

PSD2: Overview on Regulation

9. Increase your conversion rate with Axerve Guaranteed Payment