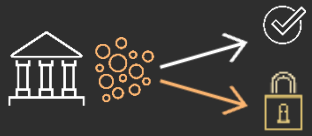
E-commerce purchase on mobile device with Credit/Debit/Prepaid card:
Strong Customer Authentication with biometrics in mobile banking app

Authenticaton flow

Risk Evaluation

Under PSD2 (SCA), before requesting authorisation, the Merchant is required to provide EMV® 3DS data to the card Issuer (Bank) via the Acquirer/ PSP for authentication purposes.



The Bank (or ACS operator) performs required Risk Based Authentication on the Merchant's and its own data. The RBA score determines if the Consumer is required to perform an additional step to complete the transaction.

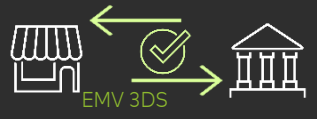
Authentication

In this example, the 'step up' is required and the Consumer's Bank sends a push notification to the Consumer's mobile device with a link to the mobile banking app.

The Consumer authenticates into the mobile banking app using biometrics, e.g. fingerprint, iris scan, face recognition.

Authorisation

The Bank (or ACS operator) replies to Merchant via EMV® 3DS with confirmation that cardholder authentication was successful.



The Merchant sends authorisation request including authentication code returned by EMV® 3DS. By approving such requests, the Bank accepts transaction liability*.

Purchase completed!

ACS = Access Control Server, PSP = Payment Service Provider, OTP = One Time Passcode, RBA = Risk Based Authentication, SCA = Strong Customer Authentication, PSD2 = 2nd Payment Service Directive

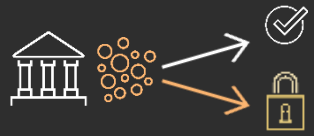
* for fraud-related chargebacks

E-commerce purchase on mobile device or desktop with Credit/Debit/Prepaid card:
Strong Customer Authentication with SMS OTP with 'knowledge-based' question or PIN/password

Authenticaton flow

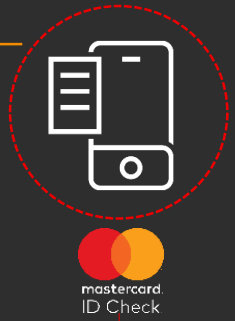
Risk Evaluation

Under PSD2 (SCA), before requesting authorisation, the Merchant is required to provide EMV® 3DS data to the card Issuer (Bank) via the Acquirer/ PSP for authentication purposes.



The Bank (or ACS operator) performs required Risk Based Authentication on the Merchant's and its own data. The RBA score determines if the Consumer is required to perform an additional step to complete the transaction.

Authentication



In this example, the 'step up' is required and the Consumer's Bank sends an OTP via SMS to the Consumer's registered mobile number.

The Consumer authenticates by typing the OTP into the Mastercard Identity Check box, he/she also provides a PIN/password or response to a security question.

Authorisation

The Bank (or ACS operator) replies to Merchant via EMV® 3DS with confirmation that cardholder authentication was successful.

The Merchant sends authorisation request including authentication code returned by EMV® 3DS. By approving such requests, the Bank accepts transaction liability*.

Purchase completed!

ACS = Access Control Server, PSP = Payment Service Provider, OTP = One Time Passcode, RBA = Risk Based Authentication, SCA = Strong Customer Authentication, PSD2 = 2nd Payment Service Directive

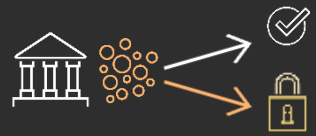
* for fraud-related chargebacks

E-commerce purchase on desktop with Credit/Debit/Prepaid card:
Strong Customer Authentication through a card reader with OTP-generator

Authenticaton flow

Risk Evaluation

Under PSD2 (SCA), before requesting authorisation, the Merchant is required to provide EMV® 3DS data to the card Issuer (Bank) via the Acquirer/ PSP for authentication purposes.



The Bank (or ACS operator) performs required Risk Based Authentication on the Merchant's and its own data. The RBA score determines if the Consumer is required to perform an additional step to complete the transaction.

Authentication

In this example, the 'step up' is required and the Bank's ACS uses the Mastercard Identity Check box for the request to enter the payment card into the card reader to generate the OTP.

The Consumer authenticates by inserting his/her card in the card reader and entering the PIN: this generates an OTP which the Cardholder enters into the Mastercard Identity Check box.

Authorisation

The Bank (or ACS operator) replies to Merchant via EMV® 3DS with confirmation that cardholder authentication was successful.

The Merchant sends authorisation request including authentication code returned by EMV® 3DS. By approving such requests, the Bank accepts transaction liability*.

Purchase completed!

ACS = Access Control Server, PSP = Payment Service Provider, OTP = One Time Passcode, RBA = Risk Based Authentication, SCA = Strong Customer Authentication, PSD2 = 2nd Payment Service Directive

* for fraud-related chargebacks