# Mastercard Identity Check Program Guide

Generated on 3 March 2025

# Mastercard Identity Check transaction flows

Mastercard Identity Check supports two primary transaction flows for payment authentication: the frictionless flow and the challenge flow.

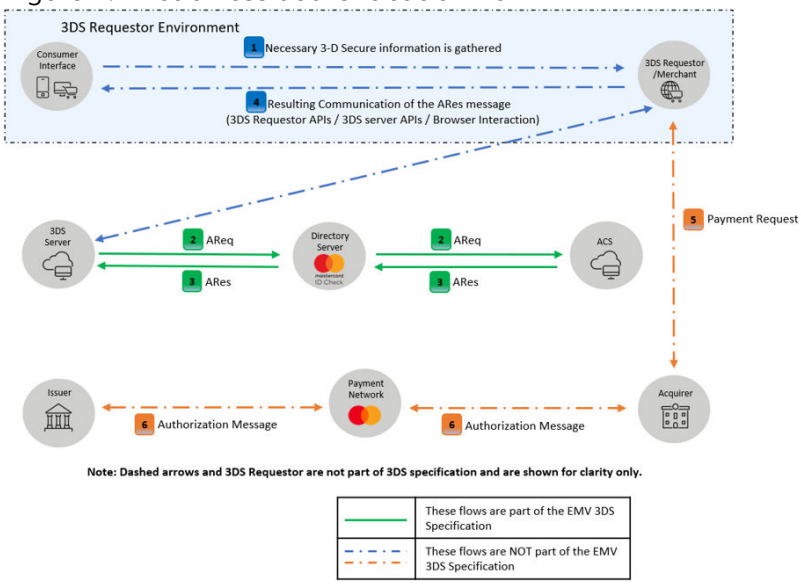
## Frictionless authentication flow

A frictionless authentication flow demonstrates that when the cardholder initiates the payment authentication

- the transaction can be authenticated by way of risk-based decisioning, and
- no additional interaction is required.

This figure illustrates the frictionless authentication flow.

Figure 1. Frictionless authentication flow



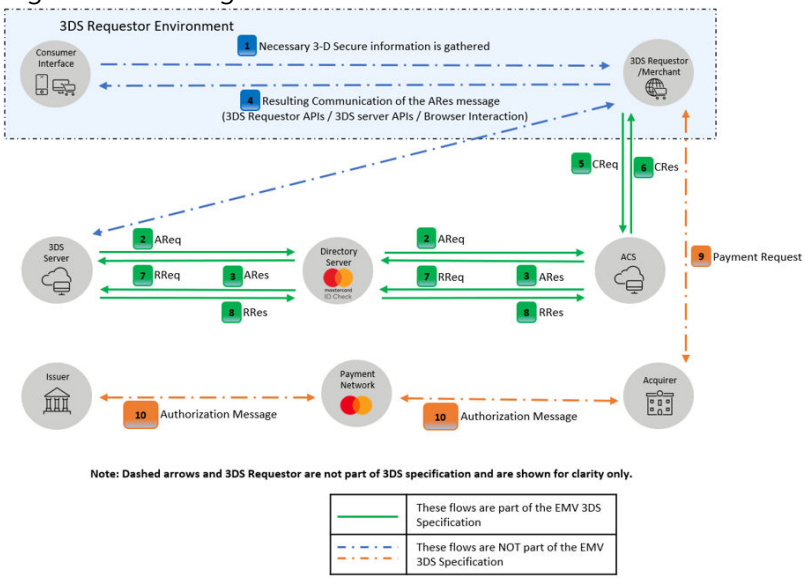

1. The 3-D Secure requestor sends an authentication message with all the necessary information required to formulate an AReq message to the 3DS Server.
2. The 3DS Server creates the AReq message and sends it to the DS.
3. The DS adds the Smart Authentication assessment to help evaluate the risk of the transaction and sends the AReq message to the issuer's ACS.
4. The issuer responds to the DS with an ARes message indicating that no further interaction or information is required from the cardholder.
5. The DS sends this message to the 3DS Server, which in turn sends it to the 3-D Secure requestor to complete the transaction with the cardholder.
6. The merchant and issuer then work together to complete the business authorization flow.

## Challenge authentication flow

A challenge or step-up authentication flow requires that the cardholder perform other steps, such as entering a one-time pass code, to successfully authenticate the transaction.

This figure illustrates the challenge step-up authentication flow.

Figure 2. Challenge authentication flow




1. The challenge flow is the same as a frictionless flow except that once the ACS and their issuers respond with the ARes message; the ARes Message indicates that further interaction is required with the cardholder.
2. This initiates a new set of messages, CReq and CRes, between the 3-D Secure requestor and ACS and their issuers, where the challenge is performed.
3. Then the ACS sends an RReq message to the 3DS Server through the DS, which responds with an RRes message to complete the transaction.
4. Merchant and issuer then work together to complete the business authorization flow.

**Successful authentication**

Upon completion of a successful authentication through the Mastercard Identity Check program, the merchant realizes the full benefits of the liability shift.

For more information on processing and data requirements, refer to chapter 5, 'Identity Check Liability Shift and Processing Requirements'.

For more information on message types, refer to EMVCo website https://www.emvco.com/document-search/ to read EMV 3-D Secure Protocol and Core Functions Specification.