3-D Secure 2

3-D Secure 1.0 has faced challenges both on technical and the user experience level. On the one hand the initial protocol added an extra step in the checkout journey (redirection page), which led to reduced conversion rates. As a result, adoption by merchants was very low, as they were seeing more and more customers to abandon during the authentication flow. On the other hand, 3DS 1.0 faced similar challenges when the smartphone era begun. 3DS 1.0 was not designed with the capability of supporting native mobile applications. Merchants who operate their own mobile applications have to break the customer journey and use a webview version of the 3DS redirection to the Issuer's website.

Due to the above reasons, the 3DS protocol had to be reviewed and updated as technology and e-commerce market evolve. With the contribution of EMVCo® and their technical associates EMV 3-D Secure became reality. The latest protocol specification was a collaborative effort of all the global payment networks apparting EMVCo® and is expected to be supported by local schemes as well. With the introduction of EMV® 3-D Secure (known as 3DS 2.0), authentication in Card-Not-Present transactions offer better user experience, more capabilities in a more secure manner. The new 3-D Secure authentication protocol supports Payment and Non-Payment use cases in App-based, Browser-based and Initiated by the Requestor transactions. In addition, new data elements were added to ensure that a larger piece of information will flow to the Issuers.

The usage of 3-D Secure can provide benefits in terms of increased security and the shift of chargeback liability to issuers.

Read more about 3-D Secure (1.0) here. 3-D Secure is not available for Alternative Payment Methods (APM), only for card transactions.

EMV® 3-D Secure enhancements

The introduction of the EMV® 3-D Secure, brought many changes on the way that Cardholder is authenticated. EMV® 3-D Secure supports different device channels, new flows, new messages and message categories, and additional data element to be included in the messages.

Device channels

EMV® 3-D Secure supports three device channels: App-based (APP), Browser-based (BRW) and 3DS Requestor Initiated (3RI).

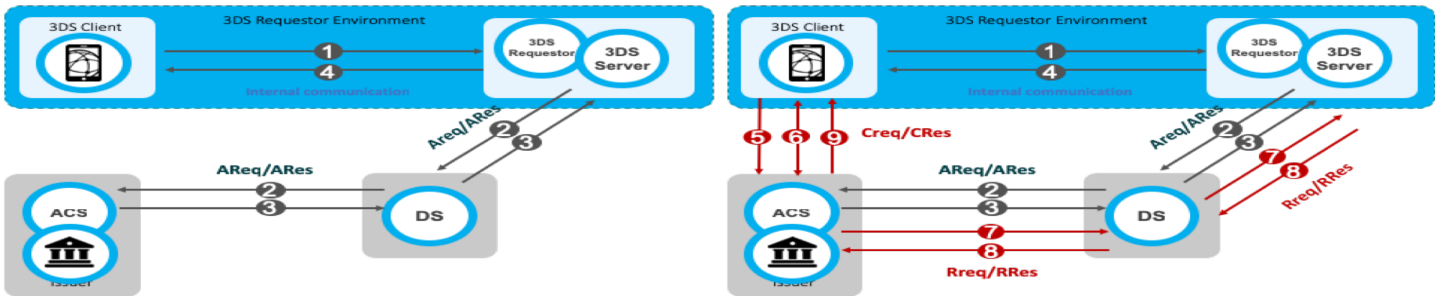
The **App-based** flow will support authentication flows, which take place through a merchant’s application (APK). To support, the APP flow, an integration to the 3DS SDK is needed.

The **Browser flow** in EMV® 3-D Secure, is an enhanced flow compared to its predecessor. During a Browser flow, the 3DS Method is used to allow the ACS to obtain additional browser information before the authentication is started.

The **3DS Requestor Initiated** is used to confirm account information when the cardholder is not directly involved (e.g. confirm that an account is still valid in a subscription).

New Flows

During the authentication in 3-D Secure 1.0.2, the Cardholder was challenged (step-up authentication) by the issuer. EMV® 3-D Secure allows a frictionless authentication (no step-up) based on a risk analysis that the issuer performs. A typical frictionless (left) and challenge (right) flow are presented below



The **frictionless** flow begins with the initiation of the the 3-D Secure transaction (step 1) and is completed with communicating the result of the risk analysis to the Browser/SDK. The **challenge** flow begins with step 1 (lookup request) and continues beyond step 4 to challenge the cardholder (steps 5,6 and 9) and communicate the result of the authentication back to the 3DS Server (step 7 and 8).

In detail:

Step 1: The cardholder initiates a 3-D Secure transaction and the relevant information is sent to the 3DS Server

Step 2: The 3DS Server sends the Authentication Request (AReq) to the payment network (DS) and finally reaches the Issuer (ACS).

Step 3: The Issuer at this point decides whether to continue with frictionless or challenge flow and returns the result within the Authentication Response (ARes).

Step 4: The 3DS Server informs the Browser or the SDK regarding the Issuers decision. If the Issuer has decided to frictionlessly authenticate the cardholder then the transaction has been completed. However, if the Issuer decided to challenge the cardholder, then the transaction continues with the next step.

Step 5: The Browser/SDK sends the Challenge Request (CReq), which initiates Cardholder interaction with the issuer and can be used to carry authentication data from the Cardholder.

Step 6: The Challenge Response (CRes) is the issuer's (ACS) response to the CReq message. It can indicate the result of the Cardholder authentication or, in the case of an App-based model, also signal that further Cardholder interaction is needed.

Step 7: Once the challenge has successfully completed the issuer sends the Result Request (RReq) to communicate the results of the authentication.

Step 8: The Result Response (RRes) is sent by the 3DS Server and acknowledges receipt of the RReq message.

Step 9: After receiving confirmation that the RReq is received, the ACS sends the Final Challenge Response to inform that the authentication has been completed.

In addition to Frictionless and Challenge flows, **Out-of-Band (OOB)** flow has been introduced. Out-of-Band flow is exactly the same flow to the standard Challenge flow with the only difference that between Step 5 and Step 6 the challenge (step up) takes place outside the 3-D Secure protocol. During the OOB authentication the Cardholder authenticates to the Issuer while interacting with the ACS outside the scope of the EMV 3-D Secure specification. For example an OOB authentication could take place using a push notification to a banking app that completes authentication and then sends the results to the ACS.

New Messages and Data elements

Besides new device channels, the new version of 3DS introduces new messages and data elements. Below a table presenting the new messages compared its predecessor. Read more about 3-D Secure (1.0) here.

Flow	3-D Secure 1.0	EMV 3-D Secure 2.0
Preparation		Preparation Request/Response (PReq/PRes)
Authentication	Verification Request/Response (VEReq/VERes)	Authentication Request/Response (AReq/ARes)

Flow	3-D Secure 1.0	EMV 3-D Secure 2.0
Challenge	Payer Authentication Request/Response (PAReq/PARes)	Challenge Request/Response (CReq/CRes)
Results		Results Request/Response (RReq/RRes)

The new messages also carry new, additional data elements. The messages have been enriched to be able to carry much more information regarding the transaction and the Cardholder to the Issuer. The new data elements refer to Cardholder information, device/browser Information, 3DS Requestor Information and they facilitate the Issuer on the authentication decision. Not all the data elements are required to initiate a 3DS transaction, however, the more information the Issuer has for the Cardholder and the merchant, the higher possibilities for a frictionless flow are.