verifone

3D Secure FAQ

Frequently Asked Questions

Q: **What is the 3DS Method, which was introduced in EMV 3-D Secure (2.0)?**

A: The 3DS Method is integrated with the 3DS Requestor's website and is invoked within a browser on the Consumer Device. The 3DS Method is a scripting call provided by the 3DS Integrator placed on the website on which the Cardholder is interacting, such as a Merchant checkout page in a payment transaction. The purpose of the 3DS Method is to obtain additional browser information to help facilitate risk-based decisioning. As the 3DS Method is the core element of the automating the information fed on the Issuer's Risk Engine, its successful completion ensures higher posibilities of achieving a frictionless authentication.

Q: **How is the 3DS Method performed? Why is the BIN Detection needed at the 3DS JavaScript?**

A: If the Issuer supports the 3DS Method they shall provide in advance their 3DS Method URL to the 3DS Server. When a session is initiated the 3DS JavaScript creates a connection with the Issuer by using the 3DS Method URL provided earlier, which allows the ACS (Issuers 3DS component) to obtain additional browser information for risk-based decisioning. Important information in this flow is the Issuer's BIN (first digits of the PAN), so the 3DS Javascript knows which Issuer's 3DS Method URL to use. There are different ways a merchant can provide the BIN, the suggested ones is to use either a field decorator at the PAN area for first transactions or feed the BIN manually. For more information please refer in Section 1.6.

Q: **What browser information does the 3DS Javascript gather?**

A: The 3DS JavaScript assists the 3DS Method and allows the Issuer to 'interogate' the user's browser. The 3DS JavaScript gathers the following data element which describe the browser's fingerprint: BrowserJavaEnabled, BrowserJavaEnabled, BrowserLanguage, BrowserColorDepth, BrowserScreenHeight, BrowserScreenWidth, BrowserTimeZone, UserAgent, IPAddress, BrowserJavascriptEnabled.

Q: **What should I do in case the Cardholder uses an Ad blocker on their browser?**

A: For maximizing the Cardholder's user experience, please suggest to your customers to remove any Ad blockers that may prevent the 3DS JavaScript to retrieve their browser information. If however an Ad blocker is used, the browser information should be sent to Issuer using the lookup API

Q: **EMV 3-D Secure (2.0) has many optional fields than its predecessor, should we send all those?**

A: EMV 3-D Secure (2.0) has been enhanced to support larger transfer of data to Issuers. The more information the Issuer has for the Cardholder and his past transactions the higher possibility are that an Issuer will decide on a frictionless authentication.

Q: **Is there guidance as to how different address types (`billingAddress1`) should be incorporated? How should the concatenation of different values be represented to make sure they match with the address details as held by the customers bank? For example, my address would be ["House Name" + "Street" + "Village"].**

A: The best practice would be to pass in the billing data exactly as you would had it been passed directly for authorization with the gateway. Each bank is different, however the overwhelming majority are equipped with the means to normalize address data to assist with their validation.

Q: **How should I use the `reorderIndicator` field when the shopping basket has more than one items?**

A: `reorderIndicator` indicates whether the cardholder is reordering previously purchased merchandise. Therefore, use:

- 01 = the consumer is re-ordering the same item or group of items again
- 02 = the consumer is ordering for the first time the item(s)

Q: **How to use the the `preOrderDate` field when the basket has two items with different availability dates? (e.g. an iPhone available next month and an iPhone case available next week)**

A: In case the customer's basket has items that will be available on different dates, use the later date in which both products, will be available.

Q: **How should the field `giftCardAmount` be used if the customer purchases multiple gift cards of differing amounts?**

A: When the customer purchases multiple gift cards, set the `giftCardAmount` equal to the total amount of prepaid or gift cards.

Q: **What's the difference between `accountPurchases` and `transactionCountYear`?**

A: `accountPurchases` represents the number of purchases with this cardholder account during the previous six months, while `transactionCountYear` the number of transactions (successful and abandoned) for this cardholder account with the 3DS Requestor across all payment accounts in the previous year.

Q: **What are the circumstances in which `authenticationStatus = R` (Rejected)?**

A: Receiving `authenticationStatus = R` means that the Authentication or Account Verification is rejected by the Issuer and requests that authorisation is not attempted. This scenario may happen if the card has been blocked for transactions for any reason.

Q: **How should the `authenticationIndicator` field should be used?**

A: If it's a one time payment transaction then it is set by default to `01` and you dont need to set it. If you want to send any recurrent (`02`), installment (`03`) or NPA (`04`, `05`, `06`) transaction, you need to send the element with the correct value.

Q: **Automatic fallback to 3-D Secure 1.0.2 if the Issuer does not support EMV 3-D Secure 2.1.0; What does that practically mean?**

A: When using Verifone's 3DS solution, the 3DS Server will always try to route the transaction through EMV 3-D Secure (2.0) rails. If the issuer does not support or the card is not enrolled for the latest version of 3-D Secure an automatic fallback to 3DS 1.0 takes place. In such a way, if the enrollment response is not positive for EMV 3-D Secure there is no need to initiate a new 3-D Secure 1.0 transaction.

Q: **How to use the `challengeIndicator` ? Will the decision to request `02 - No challenge requested` affect my liability?**

A: The `challengeIndicator` is only showing the merchant's preference on how to continue with the authentication flow and has no impact on the liability shift. The final decision though for a step-up authentication or not always lies with the Issuer. For transactions that an SCA mandate apply, it is suggested from the payment networks to use `04 - Challenge requested: Mandate`.