EMV® 3DS Data Only Mode in EMV 3-D Secure 2 (3DS2) Protocol: A U.S. Payments Forum Resource Brief

Background

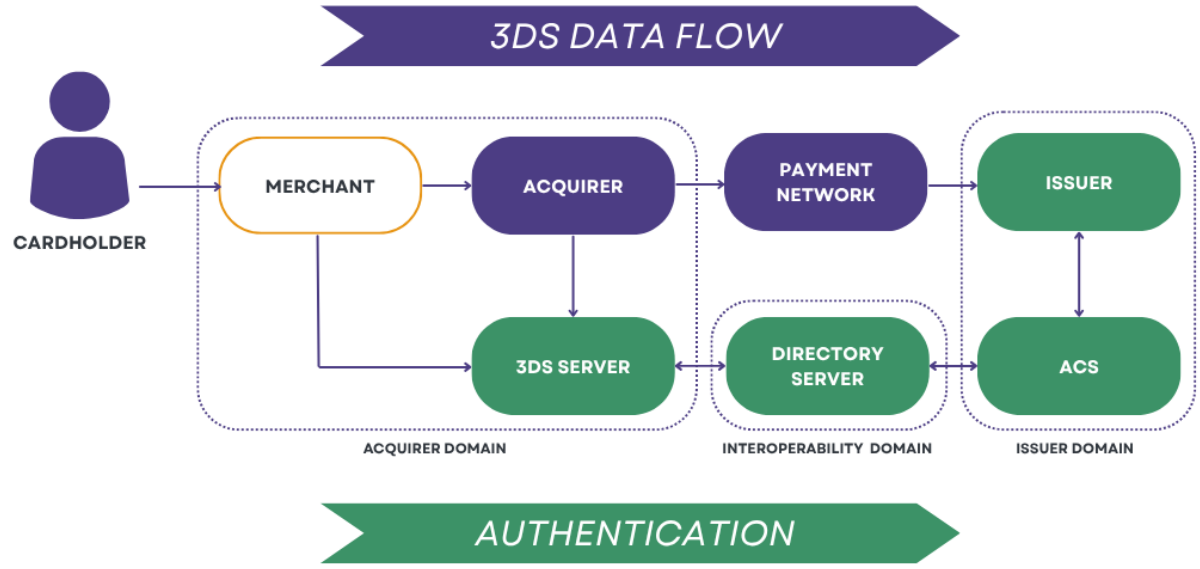
The previous U.S. Payments Forum brief on EMV 3-D Secure (3DS) introduced the fundamentals of EMV 3DS domains, highlighted the benefits of reducing merchant e-commerce fraud, and discussed major use cases. The brief also addressed some of the main adoption issues, such as cardholder friction and system complexity. This brief will explore the EMV 3DS Data Only mode.

What Is 3DS Data Only?

EMV 3DS Data Only (Data Only) is a variation of EMV 3DS that focuses on sharing transaction data between the merchant and the card issuer. Instead of prompting the cardholder for authentication, the system uses data analysis to assess the risk of the transaction. The shared data and risk analysis can include cardholder, device, purchase and location information as well as behavioral patterns. The aim is to provide a smoother, more "frictionless" checkout experience for the customer, especially for low-risk transactions. This exchange often occurs without direct cardholder participation or authentication. Instead of relying on traditional cardholder verification methods like passwords or one-time codes, Data Only leverages a risk-based assessment model. EMV 3DS Data Only transactions typically have no liability shift for the merchant.

The Data Only model analyzes a wide array of data points to gauge the potential risk associated with a given transaction. By scrutinizing these factors, the system can effectively identify low-risk transactions. The following diagram illustrates the data sharing flow.[1]

[1] Note: Data Only may require acquirer support; merchants are advised to check with their acquirer.



Benefits

Data Only allows merchants to provide issuers with additional data so that issuers can make more informed decisions. Because Data Only provides additional information to issuers, issuers are able to better differentiate between legitimate transactions and fraudulent transaction attempts. By reducing the number of false declines, Data Only allows more legitimate transactions to be approved. The benefits of Data Only include the following:

- Improves the overall quality of transactions the issuer sees in authentication (i.e., merchants are likely to pass new transaction traffic that they did not previously want subjected to a challenge), which gives issuers a chance to feed the risk engines at their Access Control Server (ACS) with enriched data.
- Leverages existing EMV 3DS implementations.
- Reduces latency compared to a full EMV 3DS authentication cycle.
- Helps ensure a frictionless EMV 3DS experience for customers.
- Enhances authorization messages to improve decisioning, increase approvals, and reduce false declines.
- Reduces shopping cart abandonment.
- Results in transactions having a higher probability of approval without the authentication challenge, due to the additional data provided by the merchant to the issuer.

Merchant Adoption

Merchants have been slow to adopt EMV 3-D Secure in the U.S. In the U.S., approximately 3% of transactions were sent over EMV 3DS rails.[2] To support Data Only, a merchant must first be using EMV 3DS.

[2] https://www.entersekt.com/resources/blog/tpost/g38gb925k1-3-d-secure-payment-rails-the-highways-no

Merchant Processing

Using existing EMV 3DS rails, the merchant submits the authentication request with the 3DS Requestor Challenge Indicator to the Directory Server indicating no challenge requested, data share only. The merchant decides to flag the EMV 3DS message as Data Only vs. the standard EMV 3DS message.

Frictionless 3DS Experience

EMV 3DS Data Only flow helps reduce customer challenge/friction, which may help with the issue of cart abandonment, which was highlighted in the first brief.

Reduced Fraud Risk

EMV 3DS Data Only provides additional data points to enhance issuer risk models and fraud protection. Fraud detection algorithms can make better-informed, data-driven, real-time decisions and predictions, helping to minimize the risk of payment fraud. Improvements to fraud prevention help maintain the integrity of transactions and build customer trust, which is essential in markets with high online fraud rates.

Higher Authorization Rates

Because EMV 3DS Data Only expands the information available, issuing banks are better equipped to approve purchases they might otherwise decline due to lack of information. By minimizing false declines, EMV 3DS Data Only helps ensure that more legitimate transactions go through, enhancing the customer experience and retaining sales that might otherwise be lost.

EMV 3DS Data Only's capabilities are particularly essential in today's competitive e-commerce landscape where every transaction counts toward the bottom line. EMV 3DS Data Only gives issuing banks more information, so they can approve more purchases.

Chargeback Protection

For EMV Data Only, merchants do not typically get chargeback protection and are liable for fraud on transactions. For example, if a merchant sends an authentication request indicating it is Data Only and the transaction is successfully authorized by the issuer, the merchant will remain liable for fraud on that transaction. This difference from standard EMV 3DS is because issuers do not have the option to present authentication challenges to their cardholders; they must make authentication decisions based on the data provided in the EMV 3DS authentication request alone.

About this Brief

As the adoption of EMV® 3-D Secure continues to expand, the U.S. Payments Forum mini-series aims to highlight less common use cases and address some of the challenges encountered during its implementation. While many of these topics deserve an in-depth project, the Payments Fraud Working Committee has identified the need to provide quick and concise guidance to stakeholders in the form of an ongoing mini-series of short summaries specific to EMV 3DS. This is the second brief in the mini-series; additional topics the working committee will explore in subsequent briefs include 3DS Requestor Initiated (3RI)/Merchant-Initiated Authentication and EMV 3DS Software Development Kits (SDK). Additional resources can be found on the U.S. Payments Forum's website.

DISCLAIMER

The U.S. Payments Forum endeavors to ensure, but cannot guarantee, that the information described in this document is accurate as of the publication date. This document is intended solely for the convenience of its readers, does not constitute legal advice, and should not be relied on for any purpose, whether legal, statutory, regulatory, contractual, or otherwise. All warranties of any kind are disclaimed, including but not limited to warranties regarding the accuracy, completeness, or adequacy of information herein. Rules (including but not limited to liability shifts), requirements, use cases, costs and benefits relating to EMV 3-D Secure may differ based on various factors and a full discussion is beyond the scope of this Resource Brief. Merchants and others considering EMV 3-D Secure are therefore strongly encouraged to consult with the relevant payment networks, other stakeholders, and their professional and legal advisors prior to implementation.