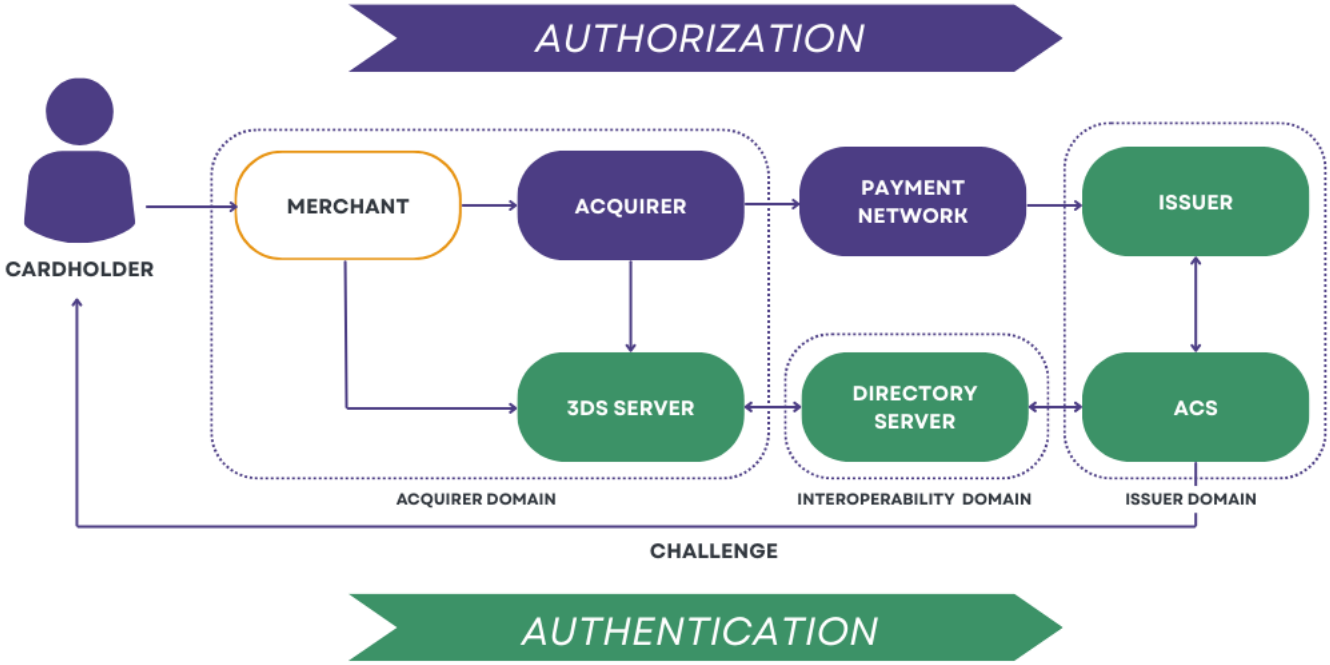
EMV® 3-D SECURE: A U.S. PAYMENTS FORUM RESOURCE BRIEF

Background

EMV® 3-D Secure (EMV 3DS) enables secure data exchange between merchants and issuers, helping to address the critical issue of eCommerce fraud. At the same time, EMV 3DS provides merchants with chargeback protection in cases of fraud, reducing financial risk and liability. North American adoption of EMV 3DS has been low because of the friction it might create during checkout flow. This U.S. Payments Forum resource brief highlights some of the adoption issues, benefits, and use cases to help educate merchants on EMV 3DS.

The diagram below illustrates the EMV 3DS system.



U.S. Payments Forum ©2025

EMV 3DS has three domains: acquirer, interoperability, and issuer.

The acquirer domain includes:

- 3DS Client: Initiates an EMV 3DS authentication from a component on the customer's device, for example a mobile application or web browser. The authentication process is typically integrated in the merchant checkout.
- 3DS Server: Provides the interface between the EMV 3DS requestor environment, validates the EMV 3DS message, and integrates with the EMV 3DS Directory Server.
- Acquirer for payment processing: Has the contractual agreement with the merchant to accept transactions.

The interoperability domain includes:

- Directory Server: Routes messages between the EMV 3DS Server and the Access Control Server (ACS) for payment authentication.

The issuer domain includes:

- Cardholder: Provides the account number on the customer device.
- Consumer device: The mobile application or web browser used by the cardholder.
- Access Control Server: Processes authentication messages from the Directory Server and authenticates the cardholder account information using rules defined by the issuer. The ACS interacts with the cardholder during step-up authentication processing.
- Issuer: Has the financial institution relationship with the cardholder and the issuer card. The issuer's ACS system verifies the cardholder with a one-time authentication code during the checkout flow when additional cardholder verification is required.

Regulation and Compliance

The European Union's (EU) Payment Services Directive (PSD2) mandates strong customer authentication (SCA) for certain types of online transactions. This mandate has driven merchants in the EU to adopt EMV 3DS to comply with regulatory requirements. India is another market with EMV 3DS mandatory for all eCommerce transactions. While this is not yet a regulatory requirement in North America, the requirement is a trend that could influence adoption since similar regulations may be introduced in the future. As merchants expand internationally, adopting EMV 3DS can help facilitate secure cross-border transactions. A consistent authentication process can create a smoother experience for customers and help prevent fraud when merchants are selling globally.

Network Tokens and Cardholder Authentication in Payment Processing

Network tokens are a non-sensitive representation of a card's primary account number (PAN). These tokens are designed to address security concerns associated with handling PANs, but they do not eliminate the need for cardholder authentication during payment processing.

EMV 3DS supports both PANs and network tokens for transaction processing. A common practice is to authenticate the cardholder using the PAN for payment processing and tokenizing the PAN.

Benefits and Use Cases of Implementing EMV 3DS

Implementing EMV 3DS offers significant advantages for both merchants and issuers by enhancing security and improving the user experience in online transactions. This advanced authentication protocol helps merchants achieve higher sales, reduce chargebacks, and prevent fraud, providing a safer and more efficient payment environment. EMV 3DS is especially beneficial for merchants in high-risk categories, helping to mitigate the risks associated with card-not-present (CNP) transactions and shifting liability from the merchant to the card issuer.

EMV 3DS benefits include the following:

- EMV 3DS data elements help the issuer to have better fraud checking to determine whether to approve a transaction.
- Merchants get chargeback protection for fraud use cases.
- By reducing fraud rates, merchants can maintain trust with issuers, ensuring they are not included in high-risk fraud rules.
- Reducing fraud is crucial for maintaining customer loyalty and trust, as fraud incidents can erode trust and lead to loss of business. Implementing EMV 3DS can reassure customers that their transactions are secure.

Use cases currently implemented include the following:

- **Card-on-file authentication**: Merchants can use EMV 3DS when a customer adds a card on file to their account or creates a new account; this would be followed by a $0 authorization to validate the card.
- **High-risk transactions**: If the merchant fraud system flags a high-risk score on a transaction, the merchant may decide to authenticate the transaction using EMV 3DS.
- **High-value transactions**: Merchants may decide to authenticate transactions using EMV 3DS for very high-value transactions.
- **International/cross-border transactions**: Merchants may decide to authenticate transactions using EMV 3DS for international cards where risk is high.

EMV 3DS also has use cases that are emerging as adoption grows and new technology is implemented. Emerging use cases include:

- **Mobile driver's license (mDL)**: Future EMV 3DS implementations may incorporate mDLs for identity verification, streamlining the authentication process.
- **Biometric information**: The potential use of biometric data, such as facial recognition or fingerprints, for authentication enhances security while maintaining a seamless user experience.
- **Enhanced data exchange**: Currently, EMV 3DS can pass up to 150 data fields, providing comprehensive information for better risk decisions, and has the potential to add or modify these fields as EMV 3DS technology evolves.
- **Data Only flows**: Data Only EMV 3DS flow allows merchants to securely share extra transaction data with card issuers during online purchases, without requiring a cardholder authentication challenge. The added information helps to increase issuers' confidence in approving transactions, leading to higher approval rates and a smoother checkout experience. Note: Data Only transactions do not shift fraud liability.

EMV 3DS Adoption Issues

While EMV 3DS has many benefits, adoption may be slow in the regions where EMV 3DS is not mandatory. Reasons may include the following:

- **Data inconsistency**. The quality of merchant data provided in EMV 3DS plays a critical role in issuer fraud detection. Merchants may be reluctant to share more data and may decide to provide a minimum set of data elements excluding optional data elements. There are cases when the data provided is not accurate, causing issues in fraud engines.
- **Approval rates and cardholder friction**. Shopping cart abandonment has been one of the major reasons that EMV 3DS adoption is low. Many enhancements have been added to the protocol from EMV 3DS 1.0 to EMV 3DS 2.x to challenge the cardholder only when needed.
- **Complexity of integration**. EMV 3DS integration is complex and adds an additional layer of authentication flow before authorization, resulting in higher implementation costs. Most systems are built with synchronous authorization request and response; EMV 3DS is a major change since it requires an asynchronous transaction processing flow with multiple steps.
- **Liability shift**. EMV 3DS is designed to help with fraud. However, determining if, how and when a liability shift occurs for merchants is not a simple answer and depends on several factors. Payment network and local regulatory requirements should be checked for specific use cases to assess any applicable liability shifts. Some factors are:
  - Region and payment network. It is important to be familiar with payment network rules for EMV 3DS usage.
  - Merchant category code (MCC). Not all MCCs are allowed for a liability shift.

Summary

EMV 3DS continues to evolve, making security and a frictionless cardholder experience synonymous. The liability shift is not the only potential EMV 3DS benefit for merchants. Merchants are encouraged to review EMV 3DS use cases and potential benefits and consider its implementation to both reduce fraud and create a secure, seamless cardholder experience.

References and Additional Information

- "EMV 3-D Secure," U.S. Payments Forum white paper, https://www.uspaymentsforum.org/emv-3-d-secure/
- "EMV 3-D Secure Data Elements," U.S. Payments Forum webinar, https://www.uspaymentsforum.org/emv-3-d-secure-data-elements-webinar/
- "EMV 3-D Secure Specification v2.3.1," EMVCo, https://www.emvco.com/whitepapers/emv-3-d-secure-whitepaper/3-d-secure-documentation/3-d-secure-specification/

About this Brief

As the adoption of EMV® 3-D Secure (EMV 3DS) continues to expand, this mini-series aims to highlight less commonly utilized use cases and address some of the prevalent 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 first brief in the mini-series; additional topics the working committee will explore in subsequent briefs include 3DS Data Only and 3DS 3RI. Additional resources can be found on the U.S. Payments Forum's website.

U.S. Payments Forum ©2025

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. As noted, 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.

U.S. Payments Forum ©2025