EMV® 3DS Requestor-Initiated (3RI) Authentications for Recurring Payments: A U.S. Payments Forum Resource Brief

The previous two briefs in the U.S. Payments Forum's EMV 3-D Secure (3DS) Mini-Series covered the fundamentals of EMV 3DS and EMV 3DS Data Only, where merchants can share data with issuers to get higher approval rates without cardholder friction. This third brief in the series explores EMV 3DS Requestor-Initiated (3RI) authentication, which allows merchants to authenticate transactions such as recurring transactions and delayed shipments and get liability protection for fraud use cases.

What Is 3RI?

EMV 3DS v2.2 (and higher) enables Requestor-Initiated (3RI) payment authentications, also known as merchant-initiated authentications. Merchants can generate the necessary authentication data for transaction authorization without the customer being directly involved. 3RI authentications also allow merchants to reference a previous authentication where the customer was involved.

Understanding 3RI Use Cases

Examples of common 3RI merchant-initiated transactions include the following:

- Recurring payments – An automated payment made on a regular schedule (usually monthly) for goods and services.
- Installments – A method of paying for something over time, dividing the total cost into smaller, regular payments rather than paying the full amount upfront.
- Card addition – The process of adding a credit or debit card to a payment system or platform.
- Split payment – The total cost of a transaction being divided across multiple payment methods.
- Delayed shipment – A product or order not being dispatched or delivered to the customer by the expected or agreed-upon shipping date.
- Top-up – A prepaid account or service having funds added.
- Mail order/telephone order – A customer purchasing goods/services without being present at the point of sale, often by sending payment details via mail or phone.
- Other payments – Payments that are not included in the standard or initially agreed-upon terms of a contract or transaction.
- Delayed delivery shipment – A product or service not being delivered to the recipient or customer by the agreed-upon date or within the specified timeframe.
- Card information storage – A business or merchant storing a customer's payment card details for future transactions.

- Account verification – Confirmation that a bank account is real and legitimate and belongs to the intended entity before any payment is made and money is transferred.

Note: Depending on the use case above, the correct indicator must be added for the initial 3DS authentication transaction.[1]

The 3RI data flow is the same as other EMV 3DS use cases, sharing data from the merchant to the issuer Access Control Server (ACS) via the acquirer, 3DS Server, and Directory Server (DS). The key distinction highlighted in the figure below is in the 3DS data flow from the merchant to the issuer/ACS and decoupled authentication, which is done directly by the ACS, out of bound and not defined by EMV 3DS.

Merchant integration for authentication is asynchronous. Once authentication is complete, the payment can then be authorized to finalize the flow.

Depending on fraud rules, if user interaction is required, the issuer ACS can use a decoupled authentication mechanism, which can differ from the standard EMV 3DS step-up flow.
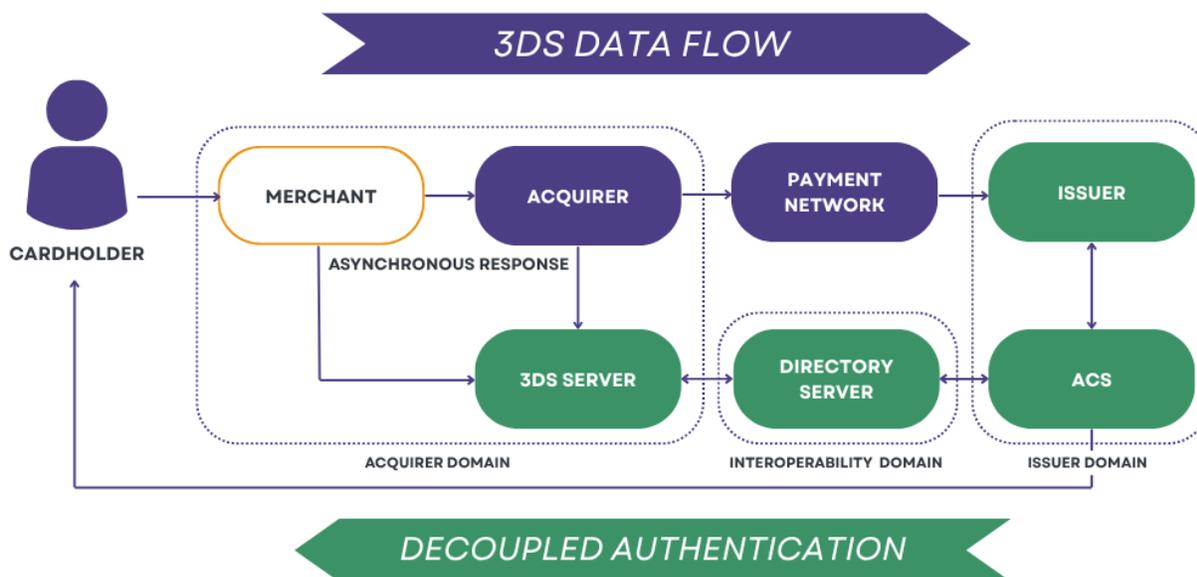
Advantages and Benefits of 3RI

3RI authentication offers several advantages for businesses, particularly for recurring or scheduled payments. It adds an additional layer of security by allowing merchants to authenticate transactions without requiring direct customer interaction, improving the customer experience and streamlining payment processes. 3RI offers a robust and secure solution for merchants seeking to reduce fraud risk, comply with regulations, improve the customer experience, and improve the efficiency of payment processing.

Fraud Mitigation
3RI, as part of the EMV 3DS system, helps reduce fraud risk by evaluating each transaction and leveraging information from previous authenticated transactions.

---

[1] "EMV 3-D Secure White Paper Version 2.0," EMVCo, March, 2025, https://www.emvco.com/dynamic/emv-3-d-secure-whitepaper-v2/recurring-and-installment-transactions/technical-features/.

Liability Shift

When a merchant uses 3RI to authenticate a transaction and the authentication is successful, the liability for fraudulent chargebacks typically shifts from the merchant to the issuer for some chargeback reason codes.

Regulatory Alignment

3RI helps merchants meet regulatory requirements like the Strong Customer Authentication (SCA) under the European Union's (EU) Payment Services Directive 2 (PSD2), ensuring compliance and avoiding potential fines.

Streamlined Processes

3RI allows for more efficient payment processing by reducing manual input and repeated customer interactions.

Increased Conversion Rates

By simplifying the payment process and reducing the need for active customer interaction, 3RI can lead to increased conversion rates and revenue.

3RI Challenges

Complex Technical Integration

EMV 3DS 3RI customer authentication is out of band, resulting in higher overall transaction time. Existing payment processing systems need complex changes to handle such cases and implementation can be costly.

Customer Communication or Education

Customers are not accustomed to seeing issuer out-of-band authentication and may not understand the source of the transaction. Seeing transactions occur without their presence can create confusion, with customers thinking that fraud is happening on their card. In addition, since transaction processing may take time, consumers may be confused about the outcome of the transaction.

Conclusion

EMV 3DS 3RI represents a significant advance in digital payments, offering merchants a powerful tool to enhance security, streamline operations, and gain liability protection for a wide array of payment use cases, particularly those without direct customer interaction. By enabling decoupled authentication, 3RI improves the overall customer experience and supports various essential use cases, from recurring payments to account verification. The technical integration can be complex and costly, requiring significant modifications to existing payment systems. Furthermore, educating customers about these "out-of-band" decoupled authentication processes is crucial to prevent confusion and maintain trust.

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 identified the need to provide quick and concise guidance to stakeholders in the form of an ongoing series of short summaries specific to EMV 3DS. This is the third brief in the mini-series.[2] Additional resources can be found on the U.S. Payments Forum's website.

---

[2] The full set of briefs can be found on the U.S. Payments Forum web site at https://www.uspaymentsforum.org/emv-3ds-mini-series/.

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.