Advanced EMV® 3DS Products and Emerging Use Cases: A U.S. Payments Forum Resource Brief

This fourth and final brief in the U.S. Payments Forum Mini-Series discusses advanced EMV 3-D Secure (3DS) products and emerging use cases. This series has been a journey through some of the less common use cases and the challenges encountered with EMV 3DS implementation. This final brief continues our exploration into various aspects of EMV 3DS. Previous briefs have covered topics such as the basics of EMV 3DS, EMV 3DS Requestor-Initiated (3RI)/Merchant-Initiated authentication, and EMV 3DS Data Only.

Decoupled Authentication

EMV 3DS decoupled authentication is a method defined in the EMV 3DS 2.0 specification that allows cardholders to authenticate a transaction outside of the merchant's website or app, typically through a separate channel (e.g., a mobile banking app, single-use link, login to a cardholder website). This approach aims to streamline the payment process by separating the authentication step from the immediate payment flow, reducing friction and potential abandonment during the transaction. Traditional EMV 3DS authentication (e.g., entering a password or code) happens directly within the merchant's checkout flow and often involves redirects to the issuer's website or app.

Examples of decoupled authentication use cases include the following:

1. Decoupled authentication simplifies the customer experience for collecting consent for open banking digital payments by allowing users to authenticate and provide consent through their bank's app.
2. A mobile app can use decoupled authentication to send a push notification to the user's banking app for a challenge, providing a smoother customer experience within the app.
3. For card-on-file payments, recurring billing, or installment payments, a user might not be active on the merchant's site when a challenge is required. Decoupled authentication sends a notification to the user's banking app, allowing them to approve the transaction from anywhere.
4. For payments taken over the phone, decoupled authentication allows the cardholder to authenticate the transaction on their mobile device or another separate application, rather than having to re-enter payment details on a potentially insecure phone line.
5. Decoupled authentication allows for convenient and secure approval of future payments for subscriptions without the cardholder being present at the time of the transaction.

FIDO® Authentication Data in EMV 3DS

EMV 3DS v2.2 and subsequent versions incorporate a mechanism to receive data elements resulting from FIDO authentication. Merchants use this data to authenticate the user within their respective environments. Merchants act as a FIDO relying party in verifying the user, and these results are then transmitted to the issuer's fraud engine to facilitate an enhanced risk assessment. FIDO authentication data provides greater confidence in the transaction, since the user has strongly authenticated with the merchant, and FIDO authentication furnishes proof of this authentication.[1]

Secure Payment Confirmation (SPC): A Paradigm Shift in Online Authentication

Secure Payment Confirmation (SPC) represents a significant leap forward in securing online transactions, offering a more robust and user-friendly alternative to traditional authentication methods. This innovative standard, developed through World Wide Web Consortium (W3C), EMVCo, and FIDO Alliance collaboration, addresses critical challenges in e-commerce, primarily the reduction of fraud and the improvement of the customer experience. Support for SPC was first introduced with EMV 3DS v2.3.

Enhanced Security and User Experience

SPC fundamentally redefines the challenge flow in online transactions, making it significantly more secure and less cumbersome than conventional methods like one-time passwords (OTPs). While traditional EMV 3DS authentication often introduces customer friction that can lead to cart abandonment and lower authentication success rates, SPC streamlines this process.

Leveraging Passkeys and FIDO Standards

A key SPC differentiator lies in its sophisticated use of FIDO authentication and passkeys. Unlike the FIDO authentication data in EMV 3DS messages where the merchant acts as the FIDO relying party verifying the customer, SPC delegates this critical role. In the SPC model, the issuer or a party specifically delegated by the issuer acts as the FIDO relying party. This distinction is vital for maintaining a high level of security and trust.

The SPC protocol simplifies the authentication process by invoking well-defined W3C application programming interfaces (APIs). These APIs prompt the user to present their passkeys, which are cryptographic credentials securely stored on their devices. The issuer's Access Control Server (ACS) then verifies these previously established passkeys. Alternatively, if no passkey exists or a new device is being used, the ACS can verify the user through an alternative method and then allow the user to set up new passkeys for future authentications. This flexibility ensures both security and adaptability.

Benefits of SPC

- **Reduced eCommerce fraud**. By employing strong cryptographic methods like passkeys, SPC is expected to improve the security of online transactions, making it far more difficult for unauthorized parties to compromise accounts or complete fraudulent purchases.
- **Improved customer experience**. The elimination of cumbersome authentication steps like entering OTPs helps promote a faster, smoother, and more intuitive payment experience. This directly addresses customer expectations for quick and easy online payments, which is a major factor in reducing cart abandonment rates.

[1] "EMV® 3-D Secure White Paper – Use of FIDO® Data in 3-D Secure Messages to Support Issuer Validation of FIDO® Authentication Data," Version 2.0, EMVCo, November 2023, https://www.emvco.com/resources/emv-3-d-secure-white-paper-use-of-fido-data-in-3-d-secure-messages/.

- **Streamlined EMV 3DS step-up/challenge flow.** SPC helps transform the often-problematic EMV 3DS challenge flow into a simpler, more efficient process. By leveraging passkeys, SPC helps reduce the friction that traditionally caused users to abandon their purchases, thereby increasing authentication success rates.
- **Industry collaboration**. The development of SPC through W3C, EMVCo, and FIDO Alliance collaboration demonstrates a unified industry effort to create a universal and robust standard for secure online payments. This collaborative approach helps ensure broad adoption and interoperability across the payment ecosystem.

Securing Agentic Commerce with EMV 3DS

Agentic commerce, encompassing autonomous transactions driven by artificial intelligence (AI) for human-in-the-loop purchases to full agent-to-agent negotiations, is rapidly advancing. Gartner forecasts that 40% of enterprise applications will integrate task-specific AI agents by 2026 (up from less than 5% in 2025).[2] However, the integration of EMV 3DS authentication in agentic commerce remains an evolving frontier requiring industry alignment on definitions and use cases. Merchants and issuers must prioritize synchronizing protocols to balance security and seamlessness, which is especially critical since traditional EMV 3DS challenges may disrupt agentic flows that lack direct human oversight. As of this publication, no standardized framework fully optimizes EMV 3DS for partial or fully agentic scenarios.

Close monitoring of the EMV 3DS approaches described in this brief, along with future innovations, is important as merchants consider how agentic commerce fits within their broader authentication and fraud management strategies. Examples such as requestor-initiated flows, data-only frictionless exchanges, and emerging trusted agent frameworks illustrate different ways EMV 3DS could be applied depending on transaction context and risk. Issuers should also remain aware of these evolving models to ensure their decisioning and risk engines can appropriately ingest and interpret the data provided. Taken together, these approaches highlight how agentic commerce may evolve over time, from automated transactions that are indistinguishable from traditional checkouts to more transparent, agent-aware processes that incorporate EMV 3DS safeguards to address emerging fraud risks, including agent impersonation.

Payment Network Fraud Monitoring Programs

Each payment network has monitoring programs to identify individual parties whose fraud, chargebacks, or a combination of both, exceed a tolerance threshold. These programs may measure both acquirer and merchant fraud and dispute rates for card-not-present (CNP) transactions (domestic and cross-border) or may be used to detect merchants with unusually high levels of CNP fraud-related chargebacks.

Depending on the applicable network and program rules:

- Exceeding certain thresholds within these programs may result in imposition of financial penalties or other requirements, including loss of chargeback protection; and
- By using EMV 3DS, merchants may be less likely to cross the program thresholds where penalties may be assessed and chargeback protections lost.

[2] "Gartner Predicts 40% of Enterprise Apps Will Feature Task-Specific AI Agents by 2026, Up from Less Than 5% in 2025," Gartner Group press release, August 26, 2025, https://www.gartner.com/en/newsroom/press-releases/2025-08-26-gartner-predicts-40-percent-of-enterprise-apps-will-feature-task-specific-ai-agents-by-2026-up-from-less-than-5-percent-in-2025.

Merchants should contact applicable networks or acquirers for specific information.

Summary

EMV® 3-D Secure continues to evolve to address emerging commerce models, modern authentication methods, and changing fraud dynamics. Advanced EMV 3DS capabilities, including decoupled authentication, SPC, and the use of FIDO® authentication data, illustrate how the protocol can be applied across a range of emerging use cases and transaction contexts. Key implementation considerations and adoption challenges are also highlighted, reinforcing that EMV 3DS supports multiple approaches, with implementation and use-case selection shaped by merchant and issuer strategies, risk tolerance, and fraud management objectives.

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 mini-series of short summaries specific to EMV 3DS. This is the fourth and final brief in the mini-series;[3] additional topics the working committee explored in previous briefs include EMV 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.

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