EMV® 3-D Secure

Frequently Asked Questions (FAQ)

1. What is EMV® 3-D Secure?

EMV 3-D Secure (3DS) is a messaging protocol that promotes frictionless consumer authentication and enables consumers to authenticate themselves with their card issuer when making card-not-present (CNP) e-commerce purchases. The additional security layer helps prevent unauthorised CNP transactions and helps protect the merchant from exposure to CNP fraud.

The three domains consist of the merchant / acquirer domain, issuer domain, and the interoperability domain (e.g., payment systems).

2. What role does EMV 3DS play within the payments community?

The purpose of the EMV 3DS protocol is to facilitate the exchange of data between the merchant using 3DS and a card issuer to authenticate a cardholder, help increase authorisation approval rates as well as reduce the risk of fraud. The objective is to benefit each of these parties by providing the ability to authenticate cardholders during a CNP e-commerce purchase, reducing the likelihood of fraudulent usage of payment cards.

3. 3DS is already used within the payments industry. Why did EMVCo create a specification?

3DS was initially developed by Visa to provide additional security to online purchases through standard web browsers by providing authentication between the cardholder and the issuer.

To reflect the current and future requirements of marketplaces around the globe, the payments industry recognised the need to create a new specification that would support app-based authentication and integration with digital wallets, as well as traditional browser-based e-commerce transactions. This led to the development of a new specification, EMV 3DS by EMVCo. The first EMV 3-D Secure – Protocol and Core Functions Specification (v2.0.0) was released in 2016. This was followed by the publication of v2.1.0 in 2017, v2.2.0 in 2018, and v2.3.0 in 2021. EMV 3DS takes into account payment channels and supports the delivery of industry leading security, performance and user experience.

4. What are key enhancements in version 2.3.0?

The current version of the specification is version 2.3.0, published in 2021. Key enhancements in version 2.3.0 include:

© 2021 EMVCo, LLC. All rights reserved.

Greater flexibility to support different technical environments

- New Split-SDK model with multiple variants makes it easier to implement EMV 3DS across both traditional and non-traditional e-commerce payment channels and devices, such as smart speakers and other IoT devices.

Additional authentication approaches to enhance security and fraud prevention

- EMVCo has collaborated with the World Wide Web Consortium (W3C) and the FIDO Alliance to include support for WebAuthn (Web Authentication) and SPC (Secure Payment Confirmation) that issuers and merchants can use within the EMV 3DS flow to better determine the legitimacy of a transaction in order to reduce the risk of fraud.

Streamlined consumer authentication

- Support for device binding, which enables the consumer to be remembered on their device and can reduce the need for an authentication challenge.
- Automated out-of-band (OOB) transitions, which help the consumer to switch seamlessly between a merchant application and an authentication application.
- Additional recurring transaction data and EMV Payment Token data, which help issuers to better identify the transaction and can simplify the authentication experience for future purchases.

5. What does EMV 3DS offer marketplaces globally?

The specification:

- Supports browser and app-based authentication on mobile and other consumer devices.
- Promotes an improved consumer experience by enabling intelligent risk-based decisioning that encourages frictionless consumer authentication.
- Allows for the delivery of enhanced security features.
- Specifies use of multiple options for step-up authentication, including onetime passcodes, as well as biometrics via out-of-band authentication flows and FIDO based consumer authentication.
- Enhances functionality that enables merchants to integrate the authentication process into their checkout experiences, for both app and browser-based implementations.
- Offers performance improvements for end-to-end message processing.
- Adds a non-payment message category to provide cardholder verification details to support various non-payment activities, such as adding a payment card to a digital wallet.
- Enables merchant-initiated transactions.
- Supports WebAuthn (Web Authentication) and SPC (Secure Payment Confirmation) within the 3DS flow for FIDO based consumer authentication.
- Provides multiple 3DS SDK (Software Development Kit) models for different merchant technical environments.

6. What are the benefits of EMV 3DS to each of the ecosystem stakeholders?

Solutions developed on the EMV 3DS Specification bring many benefits to marketplaces as they reflect the payment community's objective to enhance the security of consumer e-commerce transactions while optimising the user experience.

- **Merchants** will be able to implement a consistent approach across multiple platforms and digital channels for cardholder authentication or account

© 2021 EMVCo, LLC. All rights reserved.

verification. EMV 3DS-based solutions can achieve this during the purchasing process, minimising the risk of potential checkout abandonment.

- **Issuers** will be able to increase the proportion of frictionless authentications due to richer data exchanges. By supporting new devices / channels, solutions compatible to the EMV 3DS Specification will encourage cardholders to make purchases using their preferred medium without compromising on security.
- **Consumers** seek increased convenience and security during e-commerce payments. Solutions based on the EMV 3DS Specification will offer these benefits, adding efficiency with minimal to no impact on the applications and payment flows that consumers are using and experiencing today.

7. Does Non-Payment Authentication mean that the EMV 3DS protocol can use other consumer credentials (e.g., Driver's License, Bank Account Number, Social Security Number) as the basis for performing a consumer authentication?

The EMV 3DS protocol currently supports cardholder authentication using a Primary Account Number (or Payment Token) as the core data element and does not support the use of other consumer credentials to initiate an authentication. Authentication can happen during an e-commerce transaction (Payment Authentication) or for provisioning and verification activities (Non-Payment Authentication) such as adding a card to a digital wallet or confirming an account is in good standing. Non-payment authentications may add further confidence to related payments at a future time.

8. Is EMV 3DS consistent with consumer privacy principles?

An EMV 3DS transaction utilises consumer data for the purposes of evaluating risk in order to prevent fraud. Merchants and issuers using this data for this purpose are responsible for complying with applicable privacy laws.

9. Is the specification available to all parties without charge?

Yes. Like other EMV Specifications, the EMV 3DS Protocol and Core Specification is available on a royalty-free basis for anyone to download from the EMVCo website. EMVCo has an established system for delivering payment-related specifications through open and transparent processes in consultation with industry stakeholders.

10. How will EMV 3DS be adopted by payment stakeholders?

EMVCo manages and evolves a range of specifications and related testing processes that facilitate the worldwide interoperability and acceptance of secure payment transactions. Adoption of EMV Specifications and associated approval and certification processes promotes a unified international payments framework that supports an advancing range of payment methods, technologies, and acceptance environments. The specifications are designed to be flexible and can be adapted regionally to meet national payment requirements and accommodate local regulations.

© 2021 EMVCo, LLC. All rights reserved.

EMVCo does not mandate the use of its specifications and industry stakeholders are free to choose from any or all of the related EMV Specifications to address their customer and industry needs.

Accordingly, EMVCo expects the EMV 3DS Specification will be used primarily by parties to develop and implement EMV 3DS-compliant products and services.

To learn more about the role EMVCo plays within the payments ecosystem, read its Operating Principles.

11. What is the purpose of the EMV 3DS Software Development Kit (SDK) Specification?

The EMV 3DS SDK Specification details the SDK information and requirements for EMV 3DS app-based solutions. This technical document is intended to be utilised by parties interested in gaining a deeper understanding around the EMV 3DS Protocol and Core Specification and its functions. In addition to the EMV 3DS SDK Specification, EMVCo has developed a specification that focuses on device information and an SDK technical guide (EMV 3-D Secure SDK—Device Information and EMV 3-D Secure SDK Technical Guide). Collectively, these documents provide practical insight on how to create an EMV 3DS SDK and how this can be integrated into an EMV-compliant 3DS Requestor App.

12. How does the EMV 3DS SDK Specification differ from the EMV 3DS Core Specification?

The EMV 3DS - Protocol and Core Specification provides the requirements for all EMV 3DS components, such as 3DS Requestor, 3DS SDK, 3DS Server, Directory Server and Access Control Server, and details all of the flows and data elements. In contrast, the EMV 3DS SDK Specification focuses exclusively on the SDK and the specific role it plays in the 3DS flows and requirements.

13. What is the purpose of the EMV 3DS Split-SDK Specification?

The EMV 3DS Split-SDK Specification details the Split-SDK information, requirements and model variants. The Split-SDK functions much like the 3DS Default SDK described in the EMV 3-D Secure—SDK Specification. The distinction of the Split-SDK is that some client functionality does not run on the device, but on a server component, thus implementing a model that splits the functionality between a Split-SDK Client (client side) and a Split-SDK Server (server side).

14. Does the release of the EMV 3DS Specification have an impact on other areas of EMVCo activity / work?

The EMVCo 3DS Working Group works in close alignment with the technical body's payment tokenisation, secure remote commerce, mobile and security related initiatives. The collective goal is to advance the global interoperability of digital and e-commerce

© 2021 EMVCo, LLC. All rights reserved.

payments, while supporting cardholder authentication and enhancing transaction security.

15. **As EMVCo has now published its EMV Secure Remote Commerce (SRC) Specification, do stakeholders need to wait for EMV SRC solutions rather than utilise the EMV 3DS Specification?**

EMV 3DS can be implemented independently of EMV SRC and EMV SRC is not a replacement for EMV 3DS. The EMV SRC Specification will provide integration options for the EMV 3DS Specification. EMVCo therefore encourages stakeholders to continue developing solutions based on EMV 3DS.

16. **Who has provided input into the EMV 3DS Specifications and how will they be managed long-term?**

EMVCo engages and collaborates with hundreds of organisations, technical bodies and industry associations to develop EMV Specifications that support innovation and address the needs of marketplaces globally.

As part of EMVCo's work to create the EMV 3DS Specifications, the body commissioned user-testing in multiple countries to understand which mechanisms users preferred. External reviews of the draft specifications were also completed, including usability studies, academic analyses, and detailed review of the security design. This is in addition to extensive input and guidance from EMVCo Associates.

17. **Do the EMV 3DS Specifications support co-badge processing?**

Yes, the specification does support co-badge processing. Although the actual co-badge processing logic resides outside of the specification, the specification will support the routing of that transaction to the appropriate Directory Server as indicated by the 3DS Server.

18. **How can interested parties get involved?**

EMVCo has an established Associates Programme that is open to all industry stakeholders. EMVCo engages with its Associates to collect industry input to develop and refine its specifications. This serves to solidify EMVCo's understanding of industry requirements to support global interoperability, security and cardholder authentication. EMVCo will be seeking input from its Associates, at both a technical and business level, on an ongoing basis to ensure current and future global requirements are addressed.

EMVCo welcomes new participants who are interested in contributing to the EMV 3DS Specifications effort to join its Associates Programme or to become a Subscriber to access advance EMV 3DS information.

19. **What documentation has EMVCo published in support of the EMV 3DS Specifications?**

© 2021 EMVCo, LLC. All rights reserved.

EMVCo has published the following final specifications and related education materials to the industry in support of EMV 3DS:

a. *EMV® 3-D Secure—Protocol and Core Functions Specification*
b. *EMV® 3-D Secure—SDK Device Information*
c. *EMV® 3-D Secure—SDK Specification*
d. *EMV® 3-D Secure—Split-SDK Specification*
e. *SB 255 EMV® 3-D Secure Specification Version Configuration*
f. *EMV® 3-D Secure—SDK Technical Guide*
g. *EMV 3-D Secure Approval Administrative Process*
h. *EMV® 3-D Secure JSON Message Samples*
i. *EMV® 3-D Secure App-based Cryptographic Worked Samples*
j. *EMV® 3-D Secure Browser Flow Best Practices*
k. *EMV® 3-D Secure Payment Token Message Extension*
l. *EMV® 3-D Secure UI/UX Design Guidelines*
m. *EMV® 3-D Secure Travel Industry Message Extension*
n. *EMV® 3-D Secure Device Acknowledgement Message Extension*
o. *EMV® 3-D Secure Version Number Management Protocol Versions*

Additionally, EMVCo has published the following EMV 3DS related Bulletins:

a. *3DSTA 01 3-D Secure Approval Fees*
b. *SB 204 EMV® 3-D Secure Updates, Clarifications & Errata for v2.1.0*
c. *SB 205 EMV® 3-D Secure SDK and Device Information Updates, Clarifications & Errata for v2.1.0*
d. *SB 207 EMV® 3-D Secure Key Features for v2.2.0*
e. *SB 211 EMV® 3-D Secure SDK and Device Information Key Features for v2.2.0*
f. *SB 214 EMV® 3-D Secure Updates, Clarifications & Errata for v2.2.0*
g. *SB 225 EMV® 3-D Secure SDK—Device Information Updates Data Version 1.5*
h. *SB 227 EMV® 3-D Secure Key Features v2.3.0.0*
i. *SB 228 EMV® 3-D Secure SDK Specification version, Updates for 2.3.0.0*

All EMV 3DS documentation can be accessed, viewed, and downloaded from https://www.emvco.com/emv-technologies/3d-secure.

© 2021 EMVCo, LLC. All rights reserved.

EMV® is a registered trademark in the U.S. and other countries and an unregistered trademark elsewhere. The EMV trademark is owned by EMVCo, LLC.

© 2021 EMVCo, LLC. All rights reserved.