In this Document:

EMV 3-D Secure General, Specification and Testing FAQs

This document contains information current as of December 2018. New and updated responses are highlighted and can also be searched for by keywords, (New) or (Updated).

EMV 3-D Secure—General FAQs

1. **This section provides information specific to EMVCo, and the purpose of EMV 3-D Secure. What is EMV 3-D Secure?**

   EMV 3-D Secure (3DS) is a messaging protocol developed by EMVCo to enable 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 protects the merchant from CNP exposure to fraud.

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

2. **What role does 3-D Secure play within the payments community?**

   The purpose of the 3DS protocol is to facilitate the exchange of data between stakeholders (merchant, cardholder and card issuer). 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. **3-D Secure is already used by the market. Why has an EMVCo specification been created?**

   To reflect current and future market requirements, 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 EMVCo's development of a new industry specification: *EMV® 3-D Secure—Protocol and Core Functions Specification* (EMV 3DS Specification) addresses these new payment channels and supports the delivery of industry leading security, performance and user experience.

4. **What does EMV 3-D Secure offer the marketplace?**

   The specification:

   - Supports specific app-based purchases on mobile and other consumer devices.

- Improves the consumer experience by enabling intelligent risk-based decisioning that encourages frictionless consumer authentication.
- Delivers industry leading security features.
- Specifies use of multiple options for step-up authentication, including one-time passcodes, as well as biometrics via out-of-band 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.

5. What are the benefits of EMV 3-D Secure to each of the ecosystem stakeholders?

Solutions developed on the EMV 3DS specification can bring many benefits to the marketplace as they will reflect the payment community's objective to secure consumer e-commerce transactions while optimising the user experience.

- **Merchants** will be able to implement a consistent approach across multiple platforms and digital media when confirming the authenticity of a transaction. EMV 3DS based solutions can achieve this during the purchasing process, minimising the risk of potential checkout abandonment.
- **Issuers** will be able to improve frictionless authentication 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, and 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.

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

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

7. **How will EMV 3-D Secure be adopted by payment stakeholders?**

   EMVCo provides a ‘tool box’ of specifications that facilitate the worldwide interoperability and acceptance of secure payment transactions by managing and evolving the EMV Specifications and related testing processes. 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. 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 market needs.

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

8. **What is the purpose of the EMV 3-D Secure Software Development Kit (SDK) Specification?**

   The *EMV 3-D Secure SDK Specification* details the SDK information and requirements for 3-D Secure app-based solutions. This technical document is intended to be utilised by parties interested in gaining a deeper understanding around the *EMV 3-D Secure Protocol and Core Functions 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.

9. **How does EMV 3-D Secure SDK Specification differ from the EMV 3-D Secure Specification?**

   The *EMV 3-D Secure -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 3-D Secure SDK Specification* focuses exclusively on the SDK and the specific role it plays in the 3DS flows and requirements.

10. **Does the release of 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 tokenisation, mobile payments, secure remote commerce and security initiatives. The collective goal is to advance the global interoperability of digital and e-commerce payments, while supporting cardholder authentication and enhancing transaction security.

11. **Who has provided input into the EMV 3DS specification and how will it be managed long-term?**

    EMVCo engages with several industry bodies, alliances and community stakeholders to receive feedback on its specifications and to ensure that they evolve in line with industry requirements.

    As part of EMVCo's work to create the EMV 3DS specification, the body commissioned user-testing in multiple countries to understand which mechanisms users preferred. External reviews of the draft specification 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 Business & Technical Associates.

12. **Does the EMV® 3-D Secure specification support multi-card brand processing?**

    Yes, the specification does support multi-card brand processing. Although the actual multi-card brand 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.

13. **How can I 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 3-D Secure Protocol and Core Specification effort to join its Associates Programme. See https://www.emvco.com/get-involved/ways-to-participate/ for additional information.

14. **Can I submit questions through EMVCo directly to the Payment Systems?**

    No, these questions must be submitted directly to the Payment System(s). Please note any question regarding Payment System(s) will be returned.

15. **Why was EMVCo selected to advance and manage this new industry specification?**

    EMVCo members recognised value in advancing the new EMV 3DS specification to authenticate cardholders through its specification setting process. Adopting this open specification approach encourages cooperation within the payments community to establish a more universally accepted 3DS specification. EMVCo has the strategic breadth, industry knowledge and technical depth to develop a universally interoperable specification that will support card-not-present authentication.

In addition to EMVCo's expertise, the global technical body has a governance framework that enables collaboration within the payments community, and a well-established track record of technical specification delivery. EMVCo receives significant input from its Business and Technical Associates, which consist of industry participants including issuers, acquirers, payment networks, merchants, manufacturers, technology providers and testing laboratories from numerous countries. EMVCo is dedicated to developing universally accessible and objective specifications as the risk landscape continues to evolve. EMVCo makes its specifications available on a royalty-free basis to all industry participants and to the public.

16. What documentation has EMVCo published in support of EMV 3DS? (Updated)

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

- *EMV® 3-D Secure—Protocol and Core Functions Specification*
- *EMV® 3-D Secure—SDK Device Information*
- *EMV® 3-D Secure—SDK Specification*
- *EMV® 3-D Secure—SDK Technical Guide*
- *EMV 3-D Secure Approval Administrative Process*
- *EMV® 3-D Secure JSON Message Samples*
- *EMV® 3-D Secure App-based Cryptographic Worked Samples*

Additionally, EMVCo has published the following 3-D Secure related Bulletins:

- *3DSTA 01 3-D Secure Approval Fees*
- *SB 204 EMV® 3-D Secure Updates, Clarifications & Errata for v2.1.0*
- *SB 205 EMV® 3-D Secure SDK and Device Information Updates, Clarifications & Errata for v2.1.0*
- *SB 207 EMV® 3-D Secure Key Features for v2.2.0*
- *SB 211 EMV® 3-D Secure SDK Features for v2.2.0*
- *SB 213 EMV® 3-D Secure Device Information Key Features for v2.2.0*

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

EMV 3-D Secure—Specification FAQs

This section provides information specific to the usage of the 3-D Secure specification.

1. **What ACS Reference Number and ACS Transaction ID should be used when the Directory Server (DS) creates the ARes message?**

   When the DS creates the ARes message, (including when the DS submits a Transaction Status = A, indicating Attempts Processing Performed), the ACS Reference Number provided in the ARes message will be the DS Reference Number, and the ACS Transaction ID will be the DS Transaction ID.

2. **How will the Directory Server public keys be shared with the 3-D Secure Vendors?**

   There are no processes defined within the *EMV 3-D Secure Protocol and Core Functions Specification* around sharing public keys. Each 3-D Secure vendor will need to work with their appropriate Directory Servers and determine how those public keys will be shared prior to implementation.

3. **How should a 3DS Requestor use the Address Match Indicator?**

   The Address Match Indicator allows the 3DS Requestor to indicate to the ACS whether the cardholder's billing and shipping address are the same.

   3DS Requestors can use the Address Match Indicator to identify that the cardholder selected a checkbox indicating that the shipping address is the same as the billing address. This could be helpful in regions that have privacy mandates that prohibit providing billing and shipping address details.

   3DS Requestors should still provide billing and shipping address information (assuming no privacy mandates exist within the region), even when the Address Match Indicator has been provided.

4. **Can a DS issue both EC and RSA keys to an SDK for Device Information encryption?**

   A DS can issue either an EC or RSA key to an SDK. The type of the key issued will be determined by the DS program rules. SDKs are required to support both key types per the specification requirements.

5. **To what extent does an EMV 3-D Secure user interface (UI) need to follow the UI requirements shown in Chapter 4 of the *EMV 3-D Secure Protocol and Core Functions Specification*? (Updated)**

   It is EMVCo's intention that the 3-D Secure user interface be globally consistent across all 3DS transactions. This consistent appearance is one of the benefits of the new protocol and contributes to an enhanced user experience. Therefore, that the UI templates (the layout, the position of the logos and different text elements, etc.) must be implemented as shown in the specification per the requirements.

The user interface templates contained in Chapter 4 are an output of EMVCo's usability studies for understanding what constitutes a 3DS user interface.

UI or requirements template questions can be addressed to EMVCo or to the payment systems.

6. **Can you provide additional information about supporting the "fall-back method" mentioned in Step 10 of the Browser-based requirements?**

   This is meant to indicate that the implementation must support an alternative approach/solution for environments that do not support JavaScript. This fall-back method could be some sort of HTTP POST that may require consumer participation, such as a click of a button. For example: a consumer may be provided a button to enable a submit if JavaScript is not supported.

7. **How do 3DS Servers verify the authenticity as defined in [Req 7] of the *EMV 3-D Secure Protocol and Core Functions Specification*?**

   The requirement is on the 3DS Server to ensure that the 3DS SDK is authentic. How that is done—and who does what—depends on the integration model chosen by the 3DS Integrator for the components in the 3DS Requestor Environment (as outlined in section 2.1.1), thus the actual methods to verify the authenticity is outside the scope of EMVCo's specification.

   One possible model could be a 3DS Server outsourcing the authenticity of the 3DS SDK to the 3DS Requestor, assuming that the 3DS Server has a way to trust the 3DS Requestor as well as the relationship between 3DS SDK and 3DS Requestor. Other models are equally possible.

8. **Some of the security algorithms required by EMV 3-D Secure specification (RSA-OAEP-256 and PS256 algorithms) are not supported by the operating system version (iOS) that I am working on. How should I proceed?**

   You may find third-party libraries that implement the required algorithms or you may implement algorithms yourself. For example, the RSA-OAEP-256 algorithms is not supported in iOS-8 however there is a third-party library: GMEllipticCurveCrypto that supports the RSA-OAEP-256 algorithm.

9. **In the specification section 5.9, Message Error Handling, the sentence "If a specific transaction can be identified, …" is used numerous places. Which data element are used to identify a transaction? (New)**

   It depends on the specific error situation and the specific implementation. In some situations, one or more of the identification data elements (SDK Transaction ID, 3DS Server Transaction ID, DS Transaction ID, or ACS Transaction ID) may be recoverable and could be used to identify a specific transaction.

Additionally, an implementation-specific “session ID” created when the connection between two 3DS components is established can be used to identify the transaction. This “session ID” could be used even in situations where the Transaction ID’s from the 3DS messages are not recoverable.

The 3-D Secure specification does not mandate a specific method to identify a transaction, that will be up to each implementation.

10. What is the Base64 encoding used in the 3DS specification? (New)

RFC 7515 (JWS) is the reference for Base64 encoding. This means no padding: all trailing ’=’ characters omitted and do not include any line breaks, whitespace, or other additional characters.

The RFC 7515 refers to the RFC 4648, and also specifies options in this RFC for base64url encoding in the below note (extract from RFC 7515, Chapter 2 Terminology).

> "Base64 encoding using the URL- and filename-safe character set defined in Section 5 of RFC 4648 [RFC4648], with all trailing ’=’ characters omitted (as permitted by Section 3.2) and without the inclusion of any line breaks, whitespace, or other additional characters. Note that the Base64url encoding of the empty octet sequence is the empty string. (See Annex C for notes on implementing Base64url encoding without padding.)".

11. How does EMV 3DS define “conditional” within the specifications? (New)

The EMV 3DS specifications use the term "conditional" for three separate scenarios:

Scenario 1 is when the value present is based on conditions of other data elements within the transaction or conditions based on data elements across messages. For example, ACS Challenge Mandated Indicator must be present in the ARes message if Transaction Status = C.

Scenario 2 is when the value present is based on the DS program rules. For example, 3DS Server Operator ID is present in the AReq message due to a DS program rule stating that the 3DS Server Operator ID must be present for all transactions sent to that DS.

Scenario 3 is when the value is present because the local market allows such values to be sent between 3DS components. For example, Cardholder Billing Address City must be present in the AReq message unless regional mandates restrict sending such information.

12. How should a 3DS Server route a co-badge card? (New)

The EMV 3DS protocol allows Issuers to enroll their co-badge account ranges onto the DS and for the 3DS Server to obtain those account ranges for authentication routing. If a 3DS Server obtains multiple DS URLs for the same account ranges, the 3DS Server can choose to how to route that transaction for authentication.

The EMV 3DS specification does not specify how a 3DS Server routes co-badge cards. The choice of which DS the transaction is routed to will be implementation-specific based on the local market conditions.

13. Does the Data Device Version number need to align specifically to an EMV 3DS protocol version number? (New)

No. EMVCo has recently changed the version format of the SDK Device Information to indicate the most recent Data Device Version. The previous SDK Device Information version format indicated the EMV 3DS specification version number. This update reconfirms that the most recent Data Version Number is backwards compatible to previous EMV 3DS specification version(s). Please refer to Table 1.5 within the SDK Device Information for reference.

ACS Providers are urged to support all announced SDK Data Device Versions to help avoid step-up authentication.

EMVCo

EMV 3-D Secure—Testing FAQs

1. **Will there be a testing framework for EMV 3-D Secure compatible solutions?**

   Yes. EMVCo is working to support the functional testing of EMV 3DS solutions to confirm that they are compliant to the *EMV 3DS Protocol and Core Functions Specification*.

   Additionally, the PCI Security Standards Council will use the functional specification created by EMVCo, to deliver data security requirements, testing procedures, assessor training and reporting templates to address the environmental security.

   These related documents were released in 2017. Learn more about this collaboration.

2. **What is the expected launch date of the EMVCo test platform? (Updated)**

   The EMV 3DS test platform is now live and available for EMV 3DS v2.1.0 product testing and approval. Progress updates regarding testing support for EMV 3DS v2.2.0 will be posted on the EMVCo website.

3. **What type of testing does the EMV 3DS Approval Administrative Process describe?**

   The *EMV 3DS Approval Administrative Process* describes the functional testing process to ensure a Product Provider's software is compliant with EMV 3DS specifications. This document is available on https://www.emvco.com.

4. **Do the fees described in the EMV 3DS Product Approval Fees bulletin include Test Laboratory or Test Platform fees?**

   The *EMV 3-D Secure Approval Bulletin No. 001* (Product Approval Fees) describes EMVCo's fees for EMV's 3DS Approval Administrative Process. Other fees would be described by the Test Laboratory and/or test platform provider.

5. **Where can I locate the forms described in the EMV 3DS Approval Administrative Process document?**

   The forms described in the EMV 3DS Approval Administrative Process document are hosted on the EMVCo website using the following URL: https://www.emvco.com/processes-forms/product-approval/authentication/3ds/.

6. **Are Product Providers required to support EMV 3DS Specification v2.1.0? Are EMVCo 3DS 2.2.0 certified products automatically EMVCo 3DS 2.1.0 compliant? (New)**

   EMV 3DS specification v2.2.0 builds upon the current specification v2.1.0. Development/Support of v2.1.0 is required in order to implement v2.2.0 support. Products submitted for EMV 3DS v2.2.0 compliance testing will also be tested against EMV 3DS v2.1.0 to receive an EMV 3DS v2.2.0 Letter of Approval (LOA).