Debit Routing and EMV 3-D Secure

Version 1.0

Publication Date: March 2022

U.S. Payments Forum
191 Clarksville Road
Princeton Junction, NJ 08550

www.uspaymentsforum.org

About the U.S. Payments Forum

The U.S. Payments Forum is a cross-industry body focused on supporting the introduction and implementation of EMV chip and other new and emerging technologies that protect the security of, and enhance opportunities for payment transactions within the United States. The Forum is the only non-profit organization whose membership includes the entire payments ecosystem, ensuring that all stakeholders have the opportunity to coordinate, cooperate on, and have a voice in the future of the U.S. payments industry. Additional information can be found at http://www.uspaymentsforum.org.

EMV® is a registered trademark of EMVCo, LLC in the United States and other countries around the world.

Table of Contents

1. Introduction

EMV® 3-D Secure (EMV 3DS) is a protocol specification[1] that is designed to facilitate cardholder verification/authentication for card-not-present transactions with the goal of reducing fraud. The EMV 3DS specification is published and managed by EMVCo. The scope of this document is EMV 3DS (also known as 3DS 2.x) and not 3-D Secure 1.x.

Additional background information on the protocol can be found in the U.S. Payments Forum white paper, "EMV® 3-D Secure,"[2] published in March 2020. This previously published white paper contains information on authentication message types and transaction flows (among other topics) and discusses the key differences between 3-D Secure 1.x and EMV 3DS.

The "3-D" in the protocol name refers to three domains of security:

- Acquirer domain
- Interoperability domain
- Issuer domain

EMV 3DS is used to support three primary use cases:

- Payment authentication: Cardholder authentication during an e-commerce transaction
- Non-payment authentication: Identity verification
- Confirmation of account: Verification of account

All global payment networks support EMV 3DS-based solutions for both credit and debit cards. In each of their implementations, their networks function as the interoperability domain.

Multiple interoperability domains are of particular interest for debit card transaction routing. The EMV 3DS specification has no reference to its ability to support multiple interoperability domains. The specification neither prohibits more than one interoperability domain for a given card nor provides examples where more than one interoperability domain exists.

The intent of this document is to:

- Help educate payments industry stakeholders on technical options for routing debit transactions when EMV 3DS is being used.
- Propose a solution concept for facilitating merchant routing choice on transactions that include EMV 3DS.
- Describe issuer options for participating in either single or multiple interoperability domains.

Payment transactions involving 3DS authentication are conducted in two phases. The diagram in Figure 1 illustrates the relationship between the key concepts of 3DS authentication and transaction authorization.

- The first phase is the 3DS authentication process. The purpose of this phase is to authenticate the cardholder.
- The second phase is transaction authorization. Once the 3DS authentication phase is complete, the merchant sends an authorization request, including the results of 3DS authentication, for approval.

[1] https://www.emvco.com/emv-technologies/3d-secure/

[2] https://www.uspaymentsforum.org/emv-3-d-secure/

The text noted in red in Figure 1 represent a new proposed step that is further described in Section 4 of this document. The purpose of this step is to provide the merchants, acquirers and participating EMV 3DS server providers with a means of preserving routing choice.

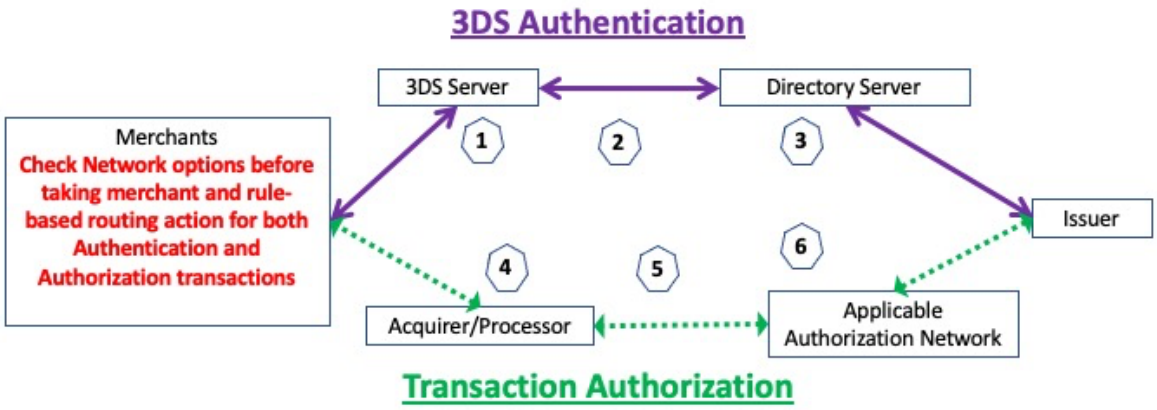

Figure 1. EMV 3DS Authentication and Transaction Authorization Processes

During the proposed EMV 3DS process, the following steps occur:

1. The merchant makes the initial authentication request.
2. The 3DS server provider reviews Directory Server and network options.
3. The Directory Server submits the request to the issuer for the designated network. The issuer sends a response back to the Directory Server provider where the merchant receives the response.
4. The merchant creates the transaction authorization message with applicable authentication information and submits the request to the acquirer/processor.
5. The acquirer/processor converts the merchant message, determines network routing options, and submits the transaction to the applicable network in its required format.
6. The authorization network then routes the transaction to the issuer, who responds back via the authorization network to the acquirer/processor, where the merchant receives the response.

2. EMV 3-D Secure Domains

The EMV 3DS protocol incorporates cardholder authentication into the financial authorization process. This additional authentication is based on the three-domain model:

- Acquirer domain
  - Contains the systems and functions of the 3DS requestor environment and, optionally, the acquirer.
- Interoperability domain
  - Facilitates the transfer of information between the issuer domain and acquirer domain systems.
- Issuer domain
  - Contains the systems and functions of the issuer and its customers (cardholders).

2.1 EMV 3DS Components

3DS Server

A 3DS Server, referred to in earlier versions of 3DS as a merchant plug-in or a MPI, is designed to facilitate EMV 3DS authentications. The 3DS Server identifies the account number and queries the Directory Server(s) to determine if it is enrolled in EMV 3DS.

Directory Server (DS)

The Directory Server is responsible for handling request and response authentication messages between participating merchants and issuers in a payment network's 3DS program. The Directory Server is designed to receive authentication requests for card numbers from merchants, determine if the card numbers are in an enrolled issuer BIN range, direct a request for cardholder authentication to the appropriate Access Control Server (ACS), and then respond back to the 3DS Server indicating whether payment authentication is available for the queried card number.

To provide this service, the Directory Server is configured with card ranges to determine participation in the EMV 3DS program.

Access Control Server (ACS)

In the EMV 3DS protocol, the ACS is controlled by the issuer. The ACS is responsible for verifying whether a card number is eligible for EMV 3DS, determining risk thresholds, and authenticating the cardholder. Currently, most card issuers outsource ACS responsibilities to a third party.

3. EMV 3DS – Current Implementations in the U.S.

In the U.S., a specific global payment-network-based Directory Server (DS) is available for a given card (i.e., the payment network brand that is associated with the card). The EMV 3DS specification allows for the identification of the Directory Server based on the BIN and other criteria. However, EMVCo has not specified a process for the identification of and selection between multiple Directory Servers for a given account number. This document was developed to propose a solution that includes multiple Directory Servers. Depending on the business benefits, merchants may currently attempt EMV 3DS authentication for cards that do not participate in EMV 3DS. Directory Servers may respond to the 3DS Server even when issuers do not participate or when the issuer ACS is unavailable.

Figure 2 illustrates the current flow of the EMV 3DS authentication process.

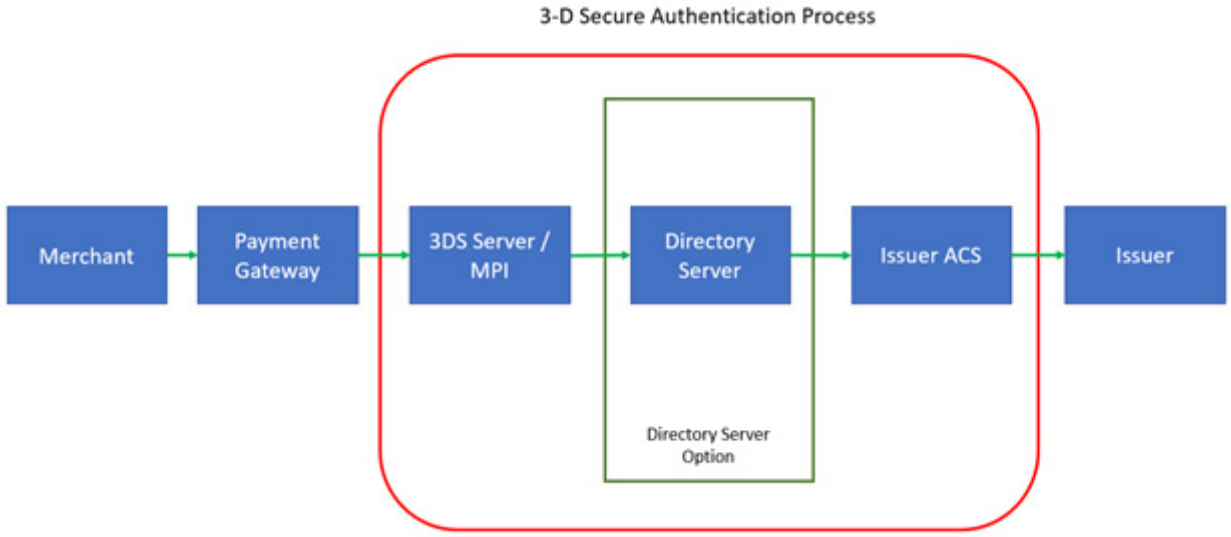

Figure 2. Current U.S. Implementations of EMV 3DS

4. EMV 3DS – Solution Concept for Multiple Directory Servers

The solution concept defined in this document assumes that two or more Directory Servers are available for a given account number, thus introducing a new Directory Server discovery/selection process.

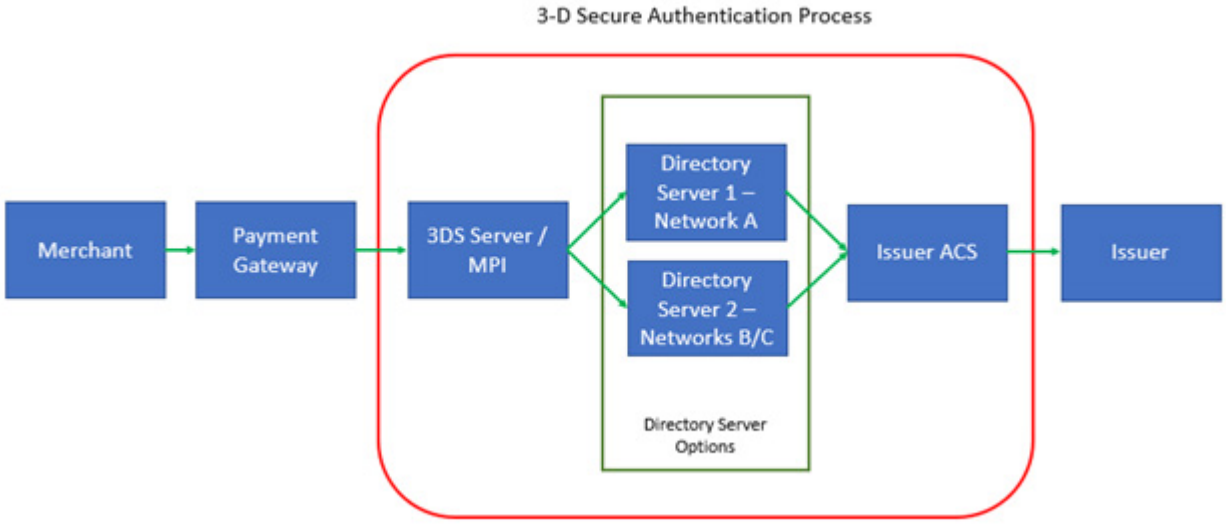

Figure 3. Solution Concept for Multiple Directory Servers

4.1 EMV 3DS – Solution Concept Pre-Step: Discovery Process

Prior to authentication, the solution concept executes a discovery process. The 3DS Server uses PReq/PRes messages to identify the card ranges and other applicable information, along with other data supported by each Directory Server (Figure 4).

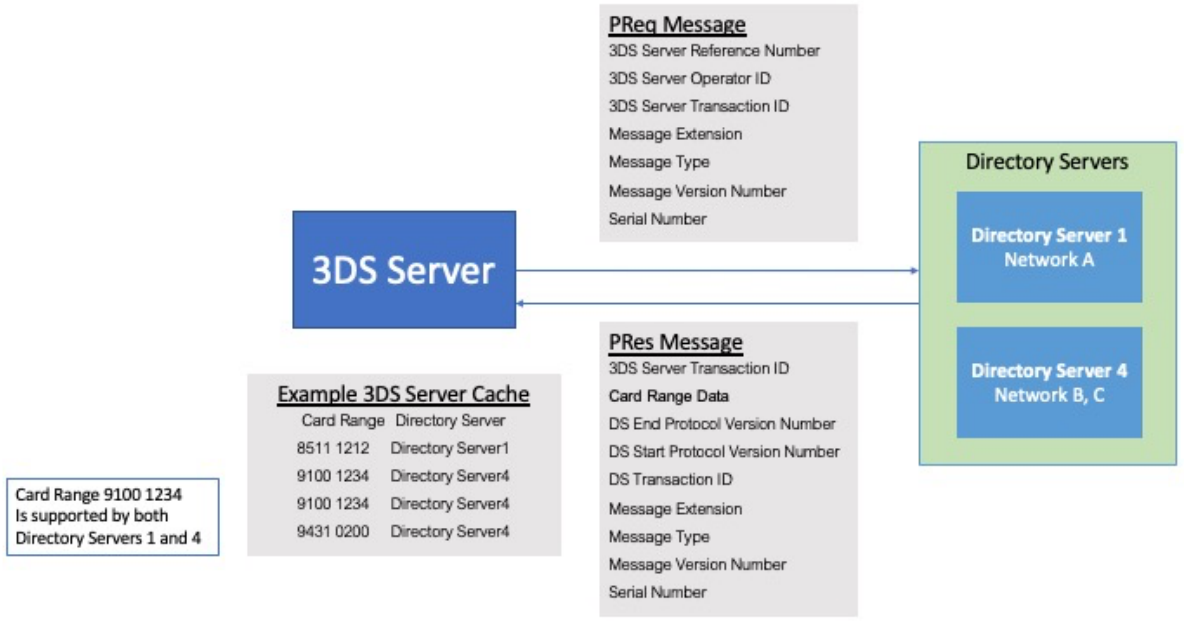

Figure 4. Solution Concept Pre-Step: Discovery Process

4.2 EMV 3DS – Solution Concept Step 1: Directory Server Selection and 3DS Authentication

Figure 5 illustrates the Directory Server selection and EMV 3DS authentication process.

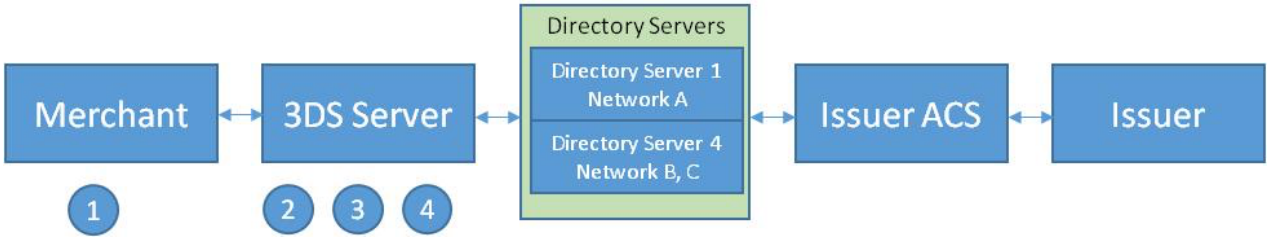

Figure 5. Solution Concept Step 1: Directory Server Selection and 3DS Authentication

During the authentication process the following steps occur:

1. The cardholder initiates checkout and the merchant invokes EMV 3DS using a specific account number.
2. The 3DS Server performs Directory Server discovery, identifies that there are two or more available Directory Servers available for the card, and creates a candidate list of the Directory Servers.
3. The 3DS Server applies Directory Server selection logic to determine which Directory Server to choose. This process includes:
    a. Performing a BIN file inquiry to determine network participation for the card number.
    b. Comparing Directory Server network participation to merchant network routing preferences.

c. Selecting the Directory Server that provides access to the preferred combination of network and Directory Server or abandoning EMV 3DS authentication.

4. The Directory Server Selection is complete. The 3DS Server initiates the remaining EMV 3DS authentication steps with the selected Directory Server until authentication is complete.

4.3 EMV 3DS – Solution Concept Step 2: Transaction Authorization

Figure 6 illustrates the transaction authorization process.

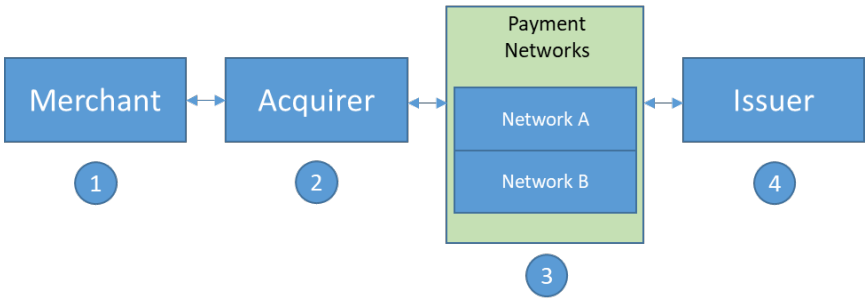

Figure 6. Solution Concept Step 2: Transaction Authorization

During the authorization process, the following steps occur:

1. The process begins upon receipt of either: (1) a final EMV 3DS authentication response (ARes) message, or (2) in cases where the issuer invokes the Challenge Flow, a final EMV 3DS Result Response (RRes) message. The data should also include the Directory Server ID for the Directory Server utilized.
2. The merchant generates a transaction authorization request and submits authorization data, including the Directory Server ID, to the acquirer.
3. The acquirer receives the authorization request, determines the network routing choice, and routes the transaction authorization request to the chosen network. Network routing choice is based on the networks supported for both BIN and EMV 3DS Directory Server business requirements and is determined by the merchant or acquirer.
4. The authorization request is routed to issuer. The issuer authorizes the transaction and the resulting authorization response is passed back to merchant via the network and acquirer.

5. Solution Considerations

5.1 Merchant/Acquiring Processor

In addition to consulting with EMV 3DS Server providers, merchants should consult with their acquirers/processors and determine what would be necessary to support multiple Directory Servers. The decision may include considering transaction authorization routing choices. Another topic to consider is whether the authorization message to the acquirers can accommodate Directory Server identification to allow the acquirer to follow the business policies of the chosen Directory Server. After consultations with EMV 3DS Server providers and acquirers/processors, merchants should be in a better position to identify other considerations before making a final decision. For more in-depth information on EMV 3DS, please see the U.S. Payments Forum white paper, "EMV 3-D Secure."

5.2 3DS Server Providers

The 3DS Server provider is the primary facilitator for routing choice on EMV 3DS transactions. The Directory Server they choose on behalf of the merchant may limit the networks that a transaction authorization request can be routed to once EMV 3DS authentication has been performed. The proposed solution assumes that participating 3DS Server providers support multiple Directory Server providers and build the Directory Server selection logic as defined in Section 4.

3DS Server providers that choose to expand their processing capabilities may be required to do the following in addition to what they already do today:

- Receive and process network BIN files.
- Implement system configuration logic and rules that enable merchants to designate their network routing and Directory Server preference hierarchy.
- Establish system logic and rules that facilitate Directory Server selection logic before EMV 3DS authentication, including:
  - Identifying all Directory Servers available for a given card to create a 3DS Directory Server candidate list. This is achieved by comparing the card data received in an EMV 3DS authentication transaction against the card ranges supported by each supported Directory Servers.
  - Identifying all available network options for a given card. This is achieved by comparing the card data received in a EMV 3DS authentication transaction with the network participation data received in network BIN files.
  - Ranking the available Directory Servers in the candidate list by the merchant's designated preference hierarchy.
  - Initiating EMV 3DS authentication with the selected Directory Server.
- Report to the merchant which 3DS Directory Server was selected for a given transaction.

5.3 Payment Networks

Some payments networks may need to enhance technical specifications to support EMV 3DS data, including the Directory Server ID, in transaction processing where applicable and establish processing rules related to EMV 3DS authentication. Payment networks may need to enroll card ranges in their supported Directory Servers for both: (1) issuers that participate in EMV 3DS authentication, and (2)

issuers whose card ranges are not enabled for EMV 3DS authentication but where the payment network supports EMV 3DS attempts processing.

5.4 Issuer/Issuer Processor

Issuers may need to enroll card ranges enabled for participation in EMV 3DS authentication with each supported payment network and Directory Server(s). System changes may be needed to verify specific elements (e.g., Authentication Value, specific e-commerce indicators).

6. Conclusion

This white paper has described a solution concept that allows merchants to determine which EMV 3DS Directory Server to use, where the selection will consider transaction authorization routing choices. The EMVCo "EMV 3-D Secure Protocol and Core Functions Specification" has no limitations that prohibit issuer domains and acquirer domains from interacting with multiple interoperability domains for a given authentication transaction. This document has proposed a solution for identifying and deciding which of multiple Directory Servers to use for an EMV 3DS authentication transaction. This solution is intended to allow a merchant to use a Directory Server, or none, that best satisfies the merchant's business decisions. This proposed solution consists of the following steps:

- Discovery of multiple Directory Servers for a given card
- Directory Server selection and EMV 3DS authentication, including routing considerations
- Transaction authorization

The proposed solution concept described in this document allows merchants to decide which Directory Server to use for a given transaction, while taking into consideration which networks are eligible given each Directory Server's business policies.

Each step discussed in this document may require modifications by the relevant stakeholders. Industry stakeholders are encouraged to evaluate this proposed solution, especially as it relates to understanding the routing options available with the Directory Server choice.

7. Appendix A: References

"EMV® EMV 3-D Secure Protocol and Core Functions Specification," Version 2.3.0.0, EMVCo, September 2001, https://www.emvco.com/emv-technologies/3d-secure/

"EMV® 3-D Secure," U.S. Payments Forum white paper, March 2020, https://www.uspaymentsforum.org/emv-3-d-secure/

8. Legal Notice

This document is provided solely as a convenience to its readers, for purposes of considering a proposed solution concept that may facilitate merchant routing choice on transactions using EMV 3-D Secure. This document provides only a high-level description of the solution concept, and stakeholders interested in implementing such a solution will therefore need to develop their own specifications. Consideration of the solution concept does not and should not be construed to obligate or commit any person or entity to adopt the proposal or any particular solution or approach described herein or element thereof. While great effort has been made to ensure that the information provided in this document is accurate and current, this document does not constitute legal or technical advice, should not be relied upon for any legal or technical purpose, and all warranties of any kind, whether express or implied, relating to this document, the information herein, or the use thereof are expressly disclaimed, including but not limited to warranties as to the accuracy, completeness or adequacy of such information, all implied warranties of merchantability and fitness for a particular purpose, and all warranties regarding title or non-infringement. Any person that uses or otherwise relies on the information set forth herein does so at his or her sole risk. This document is not intended to be exhaustive; EMV 3-D Secure implementations, circumstances and considerations may differ, as may corresponding stakeholder security and business needs, requirements, capabilities, and results, any of which may impact or be impacted by specific facts and circumstances. Accordingly, stakeholders interested in implementing EMV 3-D Secure are strongly encouraged to consult with the relevant payment networks, acquirers, processors, issuers, 3DS Server providers and other stakeholders, as well as appropriate professional and legal advisors, prior to any implementation decisions.