VISA

Visa Secure using EMV 3DS

Best Practices for Merchants

Version 1.0

06 October 2021

Important Information on Confidentiality and Copyright

Note: This document is not part of the Visa Rules. In the event of any conflict between any content in this document, any document referenced herein, any exhibit to this document, or any communications concerning this document, and any content in the Visa Rules, the Visa Rules shall govern and control.

THE INFORMATION HEREIN IS PROVIDED ON AN "AS IS," "WHERE IS," BASIS, "WITH ALL FAULTS" KNOWN AND UNKNOWN. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, VISA EXPLICITLY DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, REGARDING THE INFORMATION HEREIN, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT.

These materials and best practice recommendations are provided for informational purposes only and should not be relied upon for marketing, legal, regulatory, or other advice. The information herein should be independently evaluated considering your specific business needs and any applicable laws and regulations. Visa is not responsible for your use of these materials, best practice recommendations, or other information, including errors of any kind.

Contents

Tables

Introduction

The purpose of this best practice guide is to provide Merchants with the necessary tools and knowledge to successfully use EMV® 3-D Secure (EMV 3DS).

Related Publications

Table 1: Related Publications

Title	Description
Visa Secure - Merchant/Acquirer Implementation Guide for EMV 3-D Secure	This document provides detailed guidance for Merchants and acquirers implementing EMV 3DS.
Visa Secure Program Guide	This document is a supplement of the Visa Core Rules and Visa Product and Service Rules and provides additional requirements for Visa Secure
EMV® 3-D Secure Protocol and Core Functions Specification Version 2.2.0	This document describes the EMV 3-D Secure infrastructure and components, and to specify the requirements for each component within the infrastructure and their interaction.
VisaNet Authorization-Only Online Messages Technical Specifications	This document provides detailed information on technical specifications related VIP (VisaNet Integrated Payment).

Contact Information

Visa Secure Program

Visa regional support teams are available to answer your questions about Visa Secure. Contact the team for your region using the email address below:

- North America: esupport@visa.com
- Latin America, and Caribbean (LAC): Visa's Account Support Center (ASC) through the Visa Client Support Application (VCSA), available via Visa Online
- Asia Pacific (AP): isupport@visa.com
- Central Europe, Middle East, and Africa (CEMEA): csupport@visa.com
- European Region: customersupport@visa.com

1 Merchant Best Practices

1.1 EMV 3-D Secure Implementation

Merchants should:

- Create an EMV 3DS strategy prior to implementation that includes defining the objectives and key performance indicators (KPIs) upfront to drive implementation.
  - Examples of objectives include combatting fraud or gaining compliance to local or regional regulations.
  - Examples of KPIs include a lift in sales or increase in authorization rates.
- Define the primary objectives for implementation upfront to drive the crucial solution design. Inventory all checkout flows and purchase journeys available to your consumers to understand the various checkout experiences so the implementation of EMV 3DS can be optimized across each one.
- Work with their acquirers to ensure proper monitoring is in place. Acquirers may provide Issuer-reported fraud data that can give insight to important KPIs (fraud to sales rations or approval rates on EMV 3DS vs non-3DS transactions). In evaluating this data, Merchants can adjust their strategy and performance as needed.
- If participating in EMV 3DS, Merchants should send their transactions to EMV 3DS first before deferring to version 1.0.2.
  - Merchants should use the highest available version of 3DS in order to ensure authentication is carried out on the best-supported protocol. They are strongly encouraged to only send EMV 3DS authentication request messages (AReq) to account ranges that actively support EMV 3DS authentication. For account ranges that do not support authentication under EMV 3DS, it is recommended to use 3DS protocol version 1.0.2 to maximize the number of successful authentications and authorization approvals. To know if the Issuer BIN is enrolled for EMV 3DS, check for the PReq/PRes data.
  - After the quasi-sunset of 1.0 is in effect on 16 October 2021, if an Issuer is no longer supporting 1.0, then a Merchant can only receive fraud protection through EMV 3DS. To know who is participating in 1.0, Merchants should look to pull the CRReq/Res.
  - Merchants are recommended to protect their future ecommerce business from being impacted by the changes to 3DS 1.0.2 by enabling their authentication solution on EMV 3DS ahead of 16 October 2021. EMV 3DS penetration of overall 3DS continues to grow at pace with strong Issuer adoption, as well as optimal authorization approval rates.
  - In mandated regions that need fully authenticated transactions, Merchants that would like fully authenticated transactions, need to view the PReq/Res to know who is participating. Then they use 3DS protocol version 1.0, PReq/Res.

Even if Merchants and 3DS Servers do not support EMV 3DS, they should still check the PReq/PRes data to get additional information.

- Use the 3DS Requestor Challenge Indicator in the Authentication Request to indicate the challenge preference.
- Submit authentication requests with as much additional data as possible, which will provide Issuers with more data to improve their risk models and risk assessment, and lead to more frictionless authentications. Use EMV 3DS for:
  - Authenticating the cardholder for guest checkout transactions as consumer is not known to the Merchant
  - First time use or subsequent higher value and/or out of pattern purchase transaction
  - Suspected account take over scenarios (i.e., address change, user id /password updates)
- Continually monitor their check-out process and work with their 3DS Server provider to make adjustments as needed to improve checkout experience.
- Implement monitoring on Fraud-to-Sales Ratio, and Approval rates on 3DS vs. non 3DS transactions and make adjustments to risk strategies and implementation approaches accordingly.

1.1.1 Visa Secure Program Participation

Merchants should work with their 3DS Server provider to:

- Ensure they are using the latest version of EMV 3DS and are keeping up to date with Visa's updates.
- Test any major enhancements prior to deploying the updates in production to ensure the changes work effectively.

1.2 Performance Monitoring

Merchants should:

- Monitor step-up rates by Issuer and report high challenge issuers to Visa. Visa can work with Issuers to help them optimize performance.
- Track authentication (and subsequent authorization) rates on high-risk transactions vs low-risk transactions. There should be a noticeable difference in the rates.
- Monitor abandonment rates and ensure that they optimize their website / educate their shoppers about Visa Secure so that good transactions continue to get through, even when stepped-up by Issuers.
- Monitor how many transactions they send to EMV 3DS, 3DS 1.0.2, and no authentication. They then should track approval rates in authorization for the three authentication types.
- Monitor what percentage of their transactions go to some type of authentication vs. none at all.

- Track the percentage of AReq's with at least three valid PII elements. There should be a very high proportion of transactions with at least three valid elements (>95%).
- Monitor the number of transactions where Method URL successfully completes.

1.2.1 Merchant Data

Merchants should ensure that the data sent into authorization is accurate and consistent with the data sent into authentication.

The more, accurate/high quality data Merchants can provide to Issuers the better. The more information Issuers have to feed their risk engines will be a driver in frictionless/challenge outcomes so any Merchant interested in driving down challenge rates should be looking to supply as much data as they can.

1.2.1.1 Merchant Data Consistency

Merchants should be aware that there are two types of data:

1. Systemic data (i.e. transaction amount, IP address and device) that is captured systemically
2. Manually entered data that are customer input fields

Customer input fields have been found to result in a higher rate of error at approximately 3%. When possible, implementing a drop-down menu of required fields for consumers to select their information, and ensuring card-on-file is present can greatly reduce the rate of human error.

For billing and shipping addresses, not every country has the same address conventions (i.e. provinces, states, territories). Whenever possible, Merchants should use a dropdown feature to improve accuracy and reduce human error in manually entered data.

As a best practice, Merchants should allow card-on-file and consumer pre-filled data to ensure consistent entries for returning customers. This also improves consumer experience as the checkout process will be faster.

1.2.1.2 Merchant Data Quality

Merchants should avoid overwriting blank fields with generic data. It is preferable to present blank fields than to provide fake Merchant IDs or pre-filled data. When pre-filled or generic (spam) data is provided, this leads to a negative impact on the Issuer's risk model, rule set and final risk decision.

Reasons why this has a negative impact:

- It is not the consumer's true data which leads to false assumptions.
- Repeated, pre-filled data fields result in significant elevation of velocity risk triggers in the model and the Issuer's rules.

- Pre-filled, generic field entries hamper the ability of risk models and Issuers to identify true fraud activity.

1.2.2 3DS Method URL

Merchants are required to invoke the 3DS Method URL every time one is present for an Issuer. The 3DS Method URL allows Issuers to obtain additional device data that helps Issuers in making better decisions. Merchants should launch the 3DS Method URL as early as possible in the checkout process. This will be driven by how soon Merchants know which card is being used. As soon as the PAN is identified, that should allow the URL to be invoked.

Use case examples for invoking the method URL include:

- For registered users with the Merchant and card-on-file consumers who have set and stored a preferred card, the preferred card will be the default card used for method URL.
- For guest checkout, the method URL should be invoked immediately after the consumer enters their card account number.

1.3 EMV 3DS Data[1]

Merchants should provide as much data as possible (including required, conditional, and optional data elements). Issuers use this data to analyze the risk of the transaction, which can reduce the number of challenges that occur.

To provide better decision making for Issuers, the data fields below are most effective. For a definitive list of fields and their requirements, refer to the *Visa Secure Program Guide*.

addrMatch
acctInfo
billAddrCity
billAddrCountry
billAddrLine1
billAddrLine2
billAddrPostCode
billAddrState
browserIP
browserScreenHeight
browserScreenWidth
cardholderName
deviceInfo
deviceChannel
homePhone
MerchantCountryCode
MerchantName
MerchantRiskIndicator
mobilePhone
shipAddrCity
shipAddrCountry
shipAddrLine1
shipAddrLine2
shipAddrPostCode
shipAddrState
wprkPhone

[1] Providing EMV 3DS data is subject to regional and country regulations.

Merchant or 3DS Server providers should ensure they are following the EMV 3DS specification (including any subsequent bulletins) and using the correct encoding when directed to do so.

1.3.1 Merchant 3DS Requestor Challenge Indicator

Use the 3DS Requestor Challenge Indicator to flag to Issuer challenge preference[2].

1.3.2 3DS Optimal Field Completion

EMV 3DS transactions are experiencing increased step-up/challenge rates as compared to 3DS 1.0.2. Inconsistencies in certain data fields have resulted in issuers incorrectly identifying certain transactions as fraudulent. Three key data fields have caused a significant number of errors with EMV 3DS. To avoid declines, the following data must be captured and submitted correctly:

- The 3DS Method URL
- Three key data fields:
  - Browser IP (Field 21)
  - Shipping & Billing Post Code (Field 11 & 26)
  - Address Match Indicator (Field 27)
- Additional optional fields, if provided consistently and accurately, can also reduce mischaracterization of legitimate transactions.

Please refer to the UK Finance SCA Managed Rollout Programme—3DS testing approach and guidance document[3], pages 8-10, for further information.

1.3.3 Cardholder Information Text

An Issuer can use the Cardholder Information Text (cardholderInfo) field in the Authentication Response (ARes) to communicate important information to the cardholder as to why a transaction has not been successful (e.g., enrollment required, card suspended, contact Issuer etc.). Although this field is optional for Merchants to display in EMV 3DS 2.1 is it highly recommended that whenever this field is populated by the Issuer it is displayed to cardholder. In EMV 3DS 2.2 it becomes mandatory for Merchants to display this field if populated by Issuers.

[2] Merchants can put flags in, but Visa cannot require Issuers to support challenge methods. If a Merchant sets this value, they may still receive a frictionless transaction, especially where Issuers do not support challenge methods.

[3] SCA Managed Rollout Programme – 3DS testing approach and guidance document, available at https://www.ukfinance.org.uk/system/files/Redacted%20-%20UK%20Finance%20SCA%20Programme%20-%20Testing%20Approach%20and%20Guidance%20Nov%2020.pdf, at pages 8-10.

1.3.4 1.10 ACS Signed Content

If the ACS determines that a challenge is required for an in-app authentication using a 3DS SDK, for the secure channel setup the ACS must use the sdkEphemPubKey that the ACS received from the 3DS SDK in the AReq message. An incorrect value of the key may lead to transaction failure at the 3DS SDK side.

The 3DS SDK should verify that the sdkEphemPubKey: Qc present in the signature (acsSignedContent) is the same as generated by the 3DS SDK and provided for inclusion in the AReq message.

3DS SDKs should monitor for issues validating the acsSignedContent returned from the ACS in the ARes message (challenge flow). If the 3DS SDK cannot validate the acsSignedContent, the merchant cannot execute the challenge.

1.4 Recurring, Installment and Unscheduled Transactions

Merchants that perform recurring, installment, or unscheduled transactions should ensure they are using the Merchant Initiated Transaction (MIT) framework for subsequent transactions.

- For recurring, installment and unscheduled transactions, Merchants should authenticate the consumer on the initial transaction (with the cardholder present) and submit the Visa Secure transactions in authorization with the ECI and CAVV values received. Visa Secure does not provide fraud liability protection for subsequent transactions. For subsequent transactions, Merchants should use the Merchant Initiated Transaction (MIT) framework so that the subsequent authorization messages can tie back to the initial authorization. This allows Issuers to make better decisions.
- For transactions that include a free trial period to consumers, Merchants are recommended to authenticate the consumer with a $0.00 charge and send a $0.00 authorization with the ECI and CAVV values received in authentication. When the Merchant is ready to bill the consumer, they may use the MIT framework requirement so that the subsequent authorization messages can tie back to the initial authorization. This allows Issuers to make better decisions.
  - Visa recommends charging $0.00 as a payment authentication. Non-payments can only be used for adding a card to a wallet, maintain a card, or ID&V for tokens.

1.5 Cardholder Authentication Verification Values (CAVV)

1.5.1 CAVV Results Code—Field 44.13

Field 44.13 contains the results of CAVV verification. See the *VIP Technical Manual* for detailed values.

For Token Transactions with a CAVV

- Field 126.8 will contain the TAVV
- Field 126.9 will contain the CAVV Data
- Field 44.13 will contain the CAVV Result

1.5.2 CAVV Data—Field 126.9

Account Verification Transactions

Merchant/acquirers can submit an account verification request with a CAVV value in Field 126.9 (CAVV Data).

V.I.P. will process the CAVV verification in the account verification request based on the Issuer's CAVV verification settings. The same CAVV verification settings are used for CAVV verification for both Account Verification transactions and Authorization Transactions. Field 44.13 is used for the CAVV Result.

For Token Transactions with a CAVV

- Field 126.8 will contain the TAVV
- Field 126.9 will contain the CAVV Data
- Field 44.13 will contain the CAVV Result

1.6 Visa Secure Badge & Guidelines

Merchants should review the Visa Secure Badge and Logo Assets and Visa Secure Guidelines available at: https://Merchantsignage.visa.com/brand_guidelines.

This document provides a guide on how to communicate the launch of EMV 3-D Secure to customers along with the brand updates for Visa Secure to better align the offering name to the Visa master brand strategy by leading with Visa. Educating your shoppers with Visa Secure messaging raises awareness that you are a Visa Secure-enabled Merchant, and enhances the comfort level of your customers. The guide provides consumer-facing communications to emphasize that Visa's EMV 3-D Secure service helps prevent the unauthorized use of cardholder's Visa card – helping to protect their online transactions from fraud. Example website content, FAQs, and messaging are provided.

The Visa Secure Badge and Logos are also available for download to include on the Merchant's website.

1.7 In-App Native Challenge

As a best practice, merchants should build quality templates with their SDKs to support in-app native mobile experiences.

In-app native challenges create more streamlined experiences that match the merchant's user interface whereas HTML mobile in-app experiences may not be optimized to the user screen. In-app native challenges experience lower abandonment rates and create a better user experience for the customer since there is improved integration and proper sizing displayed on the challenge screen.

It is important to note that it is ultimately the Issuer's decision whether they would like to return a native mobile in-app challenge or a HTML mobile in-app challenge.

1.8 Travel and Multi-party Merchants

Merchants making multi-party bookings or transaction requests on behalf of multiple suppliers who will subsequently submit authorization request(s) and collect payment(s), should ensure that they support 3RI requests to obtain individual CAVVs for the subsequent authorization requests submitted by the travel providers.

1.9 Digital Certificates and Product Certification Renewals

The Merchant/Acquirer must have a 3DS Server that can connect to the Visa Secure EMV 3DS Directory Server (DS).

Merchants should work with their 3DS Server provider to:

- Ensure digital certificates are in compliance to the Visa Secure program and stay up-to-date with any Certificate Authority (CA) updates or migrations
- Ensure their 3DS Server product is valid and remains valid/does not expire.
  - To confirm whether the Visa 3DS product is still valid, ACS endpoints should refer to the Visa EMV 3DS Compliant Vendor Product List, available on the Visa Technology Partners (VTP) site. If you have any questions in relation to your Visa product certification, please visit VTP or contact Global Client Testing (GCT) 3DS Support.
- Renew certificates before they expire. 3DS Server providers will not be able to renew their certificate(s) if their Visa product certification has expired.
- Ensure there is monitoring and reporting of connections to the Visa Secure DS.
- If a 3DS SDK is used, monitor for any issues that are indicative of certificate incompatibility, such as the 3DS SDK is unable to validate the acsSignedContent or the Visa DS is unable to decrypt the sdkEncData/deviceInfo. These types of issues could cause a service disruption for In-App transactions.

1.11 Risk Management

Merchants and acquirers need to ensure they have risk management policies and procedures in place for ecommerce activities. Visa Secure is not a stand-alone solution for dealing with ecommerce fraud; rather, it should be used in combination with other risk management tools for a layered approach to address the risks associated with e-commerce transactions.

Merchants should have a layered approach to fraud prevention. EMV 3DS is NOT the only fraud prevention tool available for Merchants to leverage. Although EMV 3DS may help in the decline of fraud rates, it does not eliminate fraud entirely. Merchants should implement other practices to protect against fraud.

1.11.1 Data Models

For data models to work properly and for Issuers to make better decisions, Merchants should send substantial volume (at least 25–50% of total CNP volume) through 3DS. This is when virtuous cycle comes into effect and leads to higher authentication rates and lower fraud.

Additionally, Visa recommends that Merchants send almost all Global Collection Only (GCO) volume (as Merchant does not know consumer) and some card on file (COF) transactions, where the Merchant suspects account take over (e.g., first time card add, user or password change, shipping address change etc.).

1.11.2 Abandonment Rates

It’s important for Merchants to understand that some level of abandonment is normal. This is related to fraudsters being unable to beat the authentication challenges that are presented. High abandonment rate on higher-risk transactions indicates that fraud is getting stopped, and is therefore a good outcome.

1.11.3 Failed Authentication

Merchants that receive a failed authentication should not proceed to authorization. If Merchants in non-mandated regions would like to proceed to authorization, it is recommended that the Merchant find a way to follow up with the customer or do additional risk analysis.

1.12 Use of Messages to Identify BINs

1.12.1 Use of CRReq/CRRes messages to Identify BINs in 3DS 1.0

The CRReq message is sent from the MPI to the DS to request the list of participating 3DS 1.0.2 card ranges in order to update the MPI's internal cache information and the CRRes is sent from the DS to the MPI in response to a CRReq messages.

MPI providers are advised to refer to the 3DS 1.x specification *3-D Secure Protocol Specification Core Functions Version 1.0.2* for additional details about the contents of these messages, validation requirements, edit criteria and the processing of the message pair. The DS will also support the partial cache updates as noted in the specification (MPI has to include the serial number from the most recently processed CRRes message and the DS will share the changes since the previous CRRes message).

1.12.2 Use of PReq/PRes messages to Identify BINS in EMV 3DS[4]

The EMV 3DS specification includes a message pair called the Preparation Request Message / Preparation Response Message (PReq / PRes) that allows Merchants' 3DS servers to request the Issuer account ranges set up for EMV 3DS authentication services from the Visa Directory Server.

To obtain information on which Issuer account ranges support authentication, the Merchant's 3DS server must send a PReq message with Message Version Number "2.1.0" or "2.2.0." This prompts the Visa Directory Server to return a PRes message under the respective protocol version number, which contains the necessary information on Issuer participation.

In protocol version 2.2, the PRes message contains more information about services supported by the Issuer, including the Access Control Server (ACS) Information Indicator, where "01" means the account range is supporting authentication at the ACS, and "02" means the Issuer does not support EMV 3DS at the ACS.

[4] For CEMEA, AP, and Europe, Visa only returns participating ranges in version 2.1.

A Related Links

Use the following links to access documents described in this guide.

Table A–1: Related Links

Link	Description
Visa 3-D Secure 2.0	Includes program documentation including Visa Secure Implementation Guides.
Visa Online (VOL)	• Includes certificate request forms and directions for requesting certificates. • Includes quick reference guides (QRG), and certification requirements and user guides. • Includes information and documentation for the Visa Secure Root Certificate Update (Vendor bulletin and FAQs documents).