Visa Business News

E-Commerce & Authentication

12 September 2019

Visa Secure Processing Requirements and Reminders

Global | *Acquirers, Issuers, Processors, Agents*

Visa, Interlink, Plus Networks; V PAY; Europe Processing

Overview: Visa has compiled several processing requirements and reminders for processing 3-D Secure (3DS) 1.0.2 and EMV® 3DS transactions with Visa Secure.

The 3-D Secure (3DS) standard is a messaging protocol that enables consumer authentication for e-commerce transactions by allowing the exchange of data between the merchant, card issuer and, when necessary, consumer. Visa currently offers its 3DS service through the Visa Secure program, which supports the existing 3DS 1.0.2 and EMV® 3DS (formerly known as 3DS 2.0) specifications for consumer authentication.

Identifying Issuers That Actively Support Visa Secure Using EMV 3DS

Issuers, acquirers and merchants are actively enabling EMV 3DS globally. Though full deployment of EMV 3DS is underway, not all issuers yet support EMV 3DS. To help ensure the best overall payment experience, merchants are strongly encouraged to submit authentication requests to issuers that are actively participating in EMV 3DS. When an issuer does not actively support EMV 3DS, the merchant should proceed with a 3DS 1.0 transaction. This approach is particularly important in regions such as Europe, where authentication is a regulatory requirement.

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 from the Directory Server (DS) the issuer account ranges set up for EMV 3DS authentication services.

The format and layout of the PRes message vary between EMV 3DS protocol versions 2.1.0 and 2.2.0. In protocol version 2.1.0, the PRes information only indicates availability of 3DS authentication service and there is no distinction between issuers that are actively participating in 3DS authentication with an access control server (ACS) versus issuers that are not actively participating in EMV 3DS. In protocol version 2.2.0, the PRes message contains more information about services supported by the issuer, and indicates if the issuer is actively supporting EMV 3DS authentication.

Clients, processors and agents should be aware that once the region's EMV 3DS activation date has passed, Visa will enable all non-participating issuer account ranges for the Visa Attempts Server functionality. This means that a PRes in protocol version 2.1.0 will return all account ranges for that region even though full authentication may not be available for every issuer.

Identifying Issuers That Support Authentication

To obtain information on which issuer account ranges support authentication, the 3DS Server needs to send a PReq message with message version number 2.2.0. This will prompt the Visa DS to return a PRes message under

protocol version number 2.2.0, which contains the necessary information on issuer participation. This option is also available to 3DS servers that are only certified for protocol version 2.1.0.

Within the 2.2.0 PRes message the 3DS Server will receive the issuer ACS Information Indicator (acsInfoInd) and Action Indicators (actionInd) fields, which provides the following additional information to the 3DS Server:

ACS Information Indicator:

- 01 = Authentication Available at ACS
- 02 = Attempts Supported by ACS or DS

Action Indicator:

- A = Add the card range to the cache (default value)
- D = Delete the card range from the cache
- M = Modify the card range data (new value in version 2.2.0)

Best Practices

Visa strongly recommends that 3DS servers use the PRes supported in EMV 3DS 2.2.0 to identify issuers that are actively supporting EMV 3DS, particularly for markets with regulations that require authentication. This approach will allow 3DS servers and merchants to optimize authentication according to market needs.

3DS servers can verify if an account range is supporting authentication at the ACS by checking the ACS Information Indicator data element, which needs to be set to '01.'

Account ranges that have the ACS Information Indicator value only set to '02' mean the issuer does not support EMV 3DS and Visa will provide an attempted authentication response (e.g., electronic commerce indicator [ECI] 06 and Cardholder Authentication Verification Value [CAVV]) on behalf of the issuer. An ACS Information Indicator value with both '01' and '02' means the account range supports authentication at the ACS and the Visa Attempts Server is available as a backup when the ACS is not available.

3DS servers are strongly encouraged to only send EMV 3DS authentication request messages (AReq) to account ranges that support authentication at the ACS, particularly in regulated markets.

Clients should be aware that the PRes for EMV 3DS version 2.2.0 contains additional ACS Information Indicator data (e.g., whitelisting, decoupled authentication) than what is listed above. Clients should disregard the additional information if not applicable or until their product / system is ready for those functionalities. For more details on the PRes message please refer to the *EMV 3-D Secure Protocol and Core Functions Specification, Version 2.2.0*.

Global Reminders

Visa has compiled the following reminders for processing 3DS 1.0.2 and/or EMV 3DS transactions.

- **ACS Must Support Own Failover Processing:** An issuer supporting Visa Secure using EMV 3DS can only register a single URL for Visa Secure using EMV 3DS DS to connect to the issuer's ACS. Issuers' ACS providers must support failover processing on the back end; this includes not supporting an Attempt ACS as a backup. Best practice is to implement system redundancy of critical production components ideally

located in physically separate data centers. This helps to enforce the Visa timeout rule of five seconds response to the AReq.

- **New CAVV Version:** Visa has released an updated version of the CAVV. There are three CAVV-supported formats:
    - CAVV Usage 3, Version 0
    - CAVV Usage 3, Version 1
    - CAVV Usage 3, Version 7

Version 0 and Version 7 applies to both 3DS 1.0.2 and EMV 3DS while Version 1 only applies to 3DS 1.0.2, as highlighted in the following table:

3DS Specification	CAVV Usage 3, Version 0	CAVV Usage 3, Version 1	CAVV Usage 3, Version 7[1, 2]
3DS 1.0.2	✓	✓	✓
EMV 3DS	✓	Not supported	✓

[1] CAVV Usage 3, Version 7 applies to 3DS 1.0 and EMV 3DS and its subsequent versions.

[2] CAVV Usage 3, Version 7 includes the authentication amount, currency code and authentication date, etc.

- **Non-Reloadable Prepaid Cards:** Merchants and acquirers should be aware that Visa Secure using EMV 3DS transactions will receive an ARes = N response with a Transaction Status Reason Code 87—Excluded from Attempts Processing for Non-Reloadable Prepaid Cards. This response may also be provided for other excluded transactions.
- **3DS Requestor ID and Name:** Visa requires a unique 3DS Requestor ID (threeDSRequestorID), and 3DS Requestor Name (threeDSREquestorName) be assigned to each merchant and sent in the Authentication Request (AReq) using a self-assignment process. Details on this process can be found on the Visa 3-D Secure 2.0 page at the Visa Technology Partner website.
- **Visa Secure Supports Visa Token Transactions:** When Visa Secure is invoked using Visa Token Service, the Visa Secure DS will decrypt the token, obtain the full primary account number (PAN) and route the transaction to the appropriate issuer for authentication. The authorization may contain a Token Authentication Verification Value (TAVV) and CAVV in Fields 126.8 and 126.9, respectively.
- **Verify Enrollment Response (VERes) = N Definition (Visa Secure using 3DS 1.0.2 only):** Prior to the requirement for all Visa Secure transactions to contain a CAVV, a VERes = N response means the cardholder or issuer did not participate and the merchant can send in the transaction for authorization as an ECI 06 with no CAVV. Post the CAVV requirement, if a VERes = N response is received, the merchant must send for authorization as an ECI 07.
- **International Organization for Standardization (ISO) Country Code:** Issuers should use the ISO country code-approved list located in the VisaNet technical documentation to determine what ISO country code is valid in the Verify Enrollment Request.

Reminders for Processing Transactions Associated with Europe

As clients prepare to meet regulatory requirements, the following considerations and solutions can help with strong customer authentication (SCA) compliance and optimization:

- **Issuers outside of Europe should expect more Visa Secure transactions:** Non-European issuers should expect an increase in Visa Secure volume from European merchants and should make the following necessary changes in the authentication request:
    - For merchants that request a challenge (mandate), the issuer should adhere to this request if they support challenges or perform risk-based authentication with the cardholder.
    - Instead of out-right failing risky transactions, it is a best practice to challenge the cardholder instead.
    - Issuers must respond with an ECI 05 only for fully authenticated transactions (including risk-based authentication).
- **SCA implementation for regions located outside the European Economic Area (EEA):** Depending on local law, SCA may apply to transactions in some markets that are not part of the EEA, such as those that are associated with countries within the EEA. Markets that may need to apply SCA include **micro-states and city-states in Europe**, along with **territories of EEA countries that are located outside of Europe**. Clients in those regions should contact their local regulator and Visa representative to determine if SCA applies, and if so, how to comply with the upcoming requirements and optimize SCA.
- Acquirers are reminded that Field 19 (which identifies the country of the acquiring institution for the merchant) must be populated with the correct acquirer country code, as issuers will use this field to determine if a transaction is in or out of scope for SCA. If a country code is incorrect, the issuer may not be able to determine whether SCA is required. This could lead to regulatory non-compliance or transaction declines.

For More Information

Merchants and third party agents should contact their acquirer.