Visa DAF

Visa Digital Authentication Framework delivers the security benefits of authentication with a low friction checkout experience. Merchants can store payment credentials for Visa cardholders while helping streamline authentication at checkout by passing enhanced data with the Visa Secure DAF extension.

DAF Flow (non-registered credentials)

Steps

1. The cardholder initiates a first DAF EMV 3DS transaction with a stored credential or PAN at a participating merchant.
2. The participating merchant sends an AReq with the required DAF EMV 3DS data elements and the DAF Extension.
3. Visa confirms that the required data elements are present as outlined in DAF Authentication Request Requirement section; the merchant's VMID is active for the DAF EMV 3DS program.
4. Visa passes the authentication request to the issuer ACS.
5. The issuer ACS performs authentication of the cardholder and issues a CAVV and ECI value 05 or no CAVV and ECI value 07, indicating an unsuccessful authentication.
6. If authentication is successful, Visa saves the PAN, VMID & Cardholder Account Requestor ID combination as an approved Authenticated Payment Credential (APC).
7. Visa passes the authentication results back to the merchant, along with a Cardholder Authentication Verification Value (CAVV).
8. The merchant submits the CAVV + authorization request to VisaNet via their acquirer for authorization processing.
9. The issuer receives the CAVV + authorization request with Field 34, Dataset ID 01, Tag C010 set to 1 (DAF Indicator) to indicate that the transaction is a DAF transaction.

The participating merchant sends an AReq with the required DAF Extension and EMV 3DS data elements. Visa confirms the data and merchant's VMID are valid then passes the request to the issuer ACS. Issuer ACS performs authentication of the cardholder and issues a CAVV and ECI value 05 or no CAVV and ECI value 07, indicating an unsuccessful authentication. Visa saves the PAN, VMID and Cardholder Account Requestor ID combination as an approved Authenticated

Copyright ©2019 GPayments Pty Ltd. All rights reserved.

Payment Credential (APC). The merchant submits the authorisation request with CAVV and request Field 34, Dataset ID 01, Tag C010 set to 1 (DAF Indicator).

DAF Flow (registered credentials)

Steps

1. The cardholder initiates a DAF EMV 3DS transaction with a stored credential or PAN that has been previously authenticated under the DAF EMV 3DS program at a participating merchant.
2. The participating merchant sends an AReq with the required DAF EMV 3DS data elements and the DAF Extension.
3. Visa confirms that the required data elements are present, the merchant's VMID is active for the DAF EMV 3DS program and obtains a risk score. For Europe acquired transactions, a separate check is completed to ensure the VMID is activated for DAF in Europe.
4. Based on the authentication fraud risk, Visa assigns a `DAF Advice` to the transaction. The `DAF Advice` can either be `Must Approve` or `Issuer Decision`
5. Visa passes the authentication request to the issuer ACS.

   a. If DAF Advice = `Must Approve` : The issuer must perform successful frictionless authentication of the cardholder.
   b. If DAF Advice = `Issuer Decision` : The issuer has the choice of declining or approving the authentication request.

EMV 3DS DAF authentication requests for registered Authenticated Payment Credentials will proceed without challenge, regardless of authentication result. When an issuer fails an authentication request, the merchant has the option to either resubmit the transaction as an EMV 3DS authentication without the DAF extension or proceed to authorization without the DAF indicator.

The participating merchant sends an AReq with the required DAF Extension and EMV 3DS data elements. Visa confirms the data and merchant's VMID are valid, obtains a risk score and passes the request to the issuer ACS with `DAF Advice` set to either `Must Approve` or `Issuer decision` . DAF authentication requests for registered APCs will proceed without challenge, regardless of authentication result. When the authentication request fails, the merchant can resubmit the transaction a 3DS authentication without the DAF extension or proceed to authorisation without the DAF indicator.

Copyright ©2019 GPayments Pty Ltd. All rights reserved.

Enabling DAF

To enable DAF, the merchant must contact their acquirer to sign up for the program and receive a Visa Merchant ID (VMID). The merchant should inform their acquirer if they wish to support DAF Everywhere except Europe, Europe, or Everywhere. The merchant's 3DS Requestor ID in the Merchant Profile must then be updated with the approved VMID. The VMID can be used for DAF and non-DAF transactions.

Using DAF

ActiveServer supports the Message Extension field in the API request. To utilise DAF, the 3DS Requestor must populate and send the Message Extension data with the appropriate program requirements.

- messageExtension
  - criticalityIndicator: `false`
  - id: `A000000003-003`
  - name: `DAF Extension`
  - data:
    - chAccReqID: The 3DS Requestor assigned account identifier of the transacting cardholder. This identifier is a unique representation of the account identifier for the 3DS Requestor. This identifier is coded as the SHA-256 + Base64 of the Cardholder Account Requestor ID and is provided as a String.
      - Length: Variable, maximum 64 characters
      - JSON Data Type: String
      - Values accepted: Base64 encoded value provided as a string
    - authPayProcessReqInd: Indicates whether the purpose of the transaction is to process as a DAF transaction or to inquire on the Authenticated Payment Credential Status.
      - Length: 2 characters
      - JSON Data Type: String
      - Values accepted:
        - 01 = DAF transaction (default value)

Copyright ©2019 GPayments Pty Ltd. All rights reserved.

        - 02 = Credential Status Check
    - version: `1.0`
- In addition to 3DS required data, the following accurate data must be provided in the normal body of the 3DS request:
    - 3DS Requestor ID: VMID
    - Cardholder Billing Address City
    - Cardholder Billing Address Country
    - Cardholder Billing Address Line 1
    - Cardholder Billing Address Postal Code
    - Cardholder Billing Address State
    - Cardholder email address
    - Cardholder Mobile Phone Number
    - Common Device Identification Parameters Available in All Platforms – C010 - IP Address (for SDK transactions) (APP device channel only)
    - Browser IP Address (BRW device channel only)
    - DAF Extension fields must be present (Message Extension)

Copyright ©2019 GPayments Pty Ltd. All rights reserved.