EMVCo 3-D SECURE v2

QUICK GUIDE

Version 1.0

VERSION CONTROL

Ver.	Date	Author	Update information
1.00	04/05/22	J Blurton	New guide to supplement the existing Gateway Integration Guide

CONTENTS

1. About this Guide

Welcome to our explainer on EMVCo 3-D Secure v2 (known herein throughout as EMV 3-D Secure v2). This document has been produced to give a simplified description of the new authentication flow, and to give context to each step of the process.

Throughout this *Quick Guide*, we reference technical implementation details within the existing *Gateway Integration Guide (Integration Guide)*.

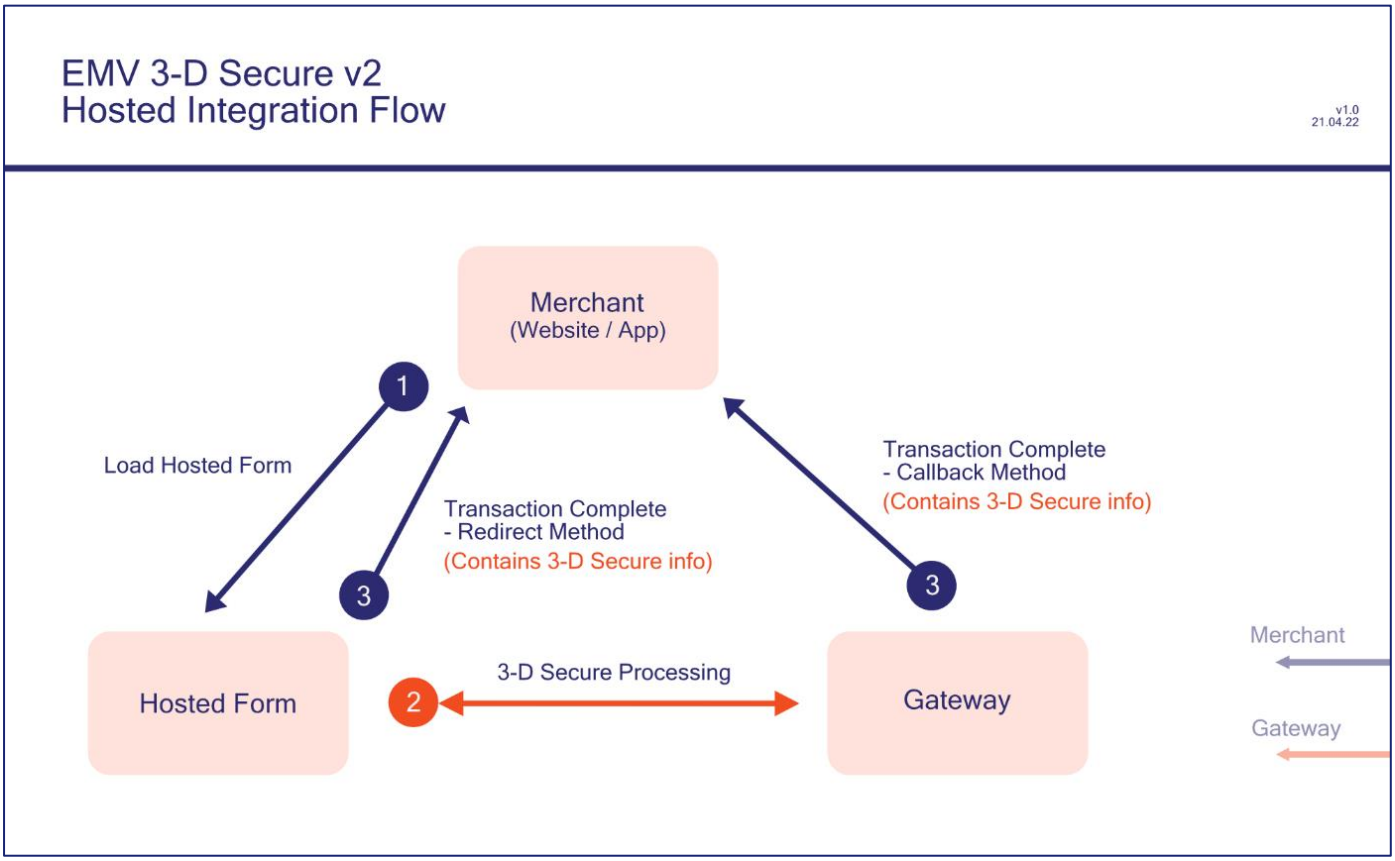
2. Testing

To ensure proper compliance with the new authentication flow, we recommend that you test the integration thoroughly using your test account. If for any reason you do not have a test account, please request one.

3. Hosted Flow

Please choose this route if you integrate with the Gateway using a form provided by us as a redirect, embedded in your web page, or if you are using our Pay Button Integration. This information is relevant whether you are using v1 or v2 of our Hosted Form.

Note
If you are using Hosted Fields in your integration, you should follow the Direct Flow below.



Step 1: Load the Gateway's Hosted Form

Load the Hosted Form on your web page using your Gateway Integration URL. This must be loaded over HTTPS.

Step 2: The Gateway Processes EMV 3-D Secure v2 Transactions

Let the Gateway handle the complexities of the 3-D Secure process for you.

Step 3: Transaction Complete

Two ways of receiving the final transaction status response are available: via the *Redirect URL* and the *Callback URL*. Extra 3-D Secure transaction data is available in this response and can be used by your application for analytical purposes. This holds no sensitive Cardholder information.

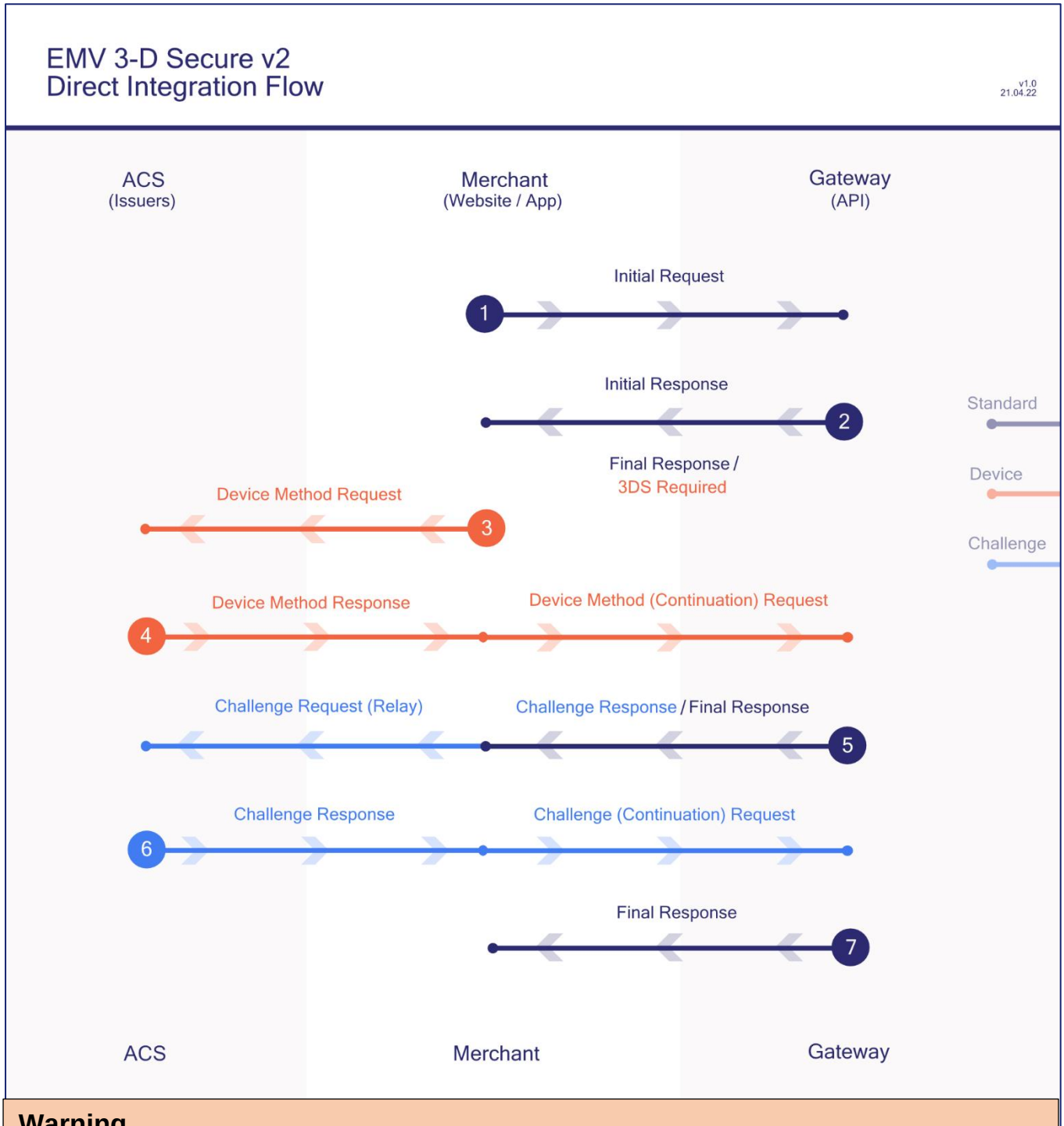
To use 3-D Secure on your Hosted Form, you must enable this support and fully configure your account in the MMS (Merchant Management System). Further details of this process are included in a dedicated guide (MMS Settings for SCA) – please contact your support representative to receive a copy.

There should be no need for you to change your code to enable 3-D Secure support, unless you wish to use the data returned here in step 3.

4. Direct Flow

Please choose this route if you integrate with the Gateway directly using our Direct Integration method.

The device flow and the challenge flow are optional, depending on the Cardholder's bank.



Warning
At no point should you hardcode 3-D Secure response fields as these will vary between ACSs.

4.1 Diagram Legend

Step 1: Initial Request

Your Cardholder has just pressed 'submit' on your payment form. You now start the payment process with a SALE request to the Gateway.

See Integration Guide section 5.5.1.

Step 2: Initial Response

We check basic factors relating to the card being charged and respond with a determination of whether 3-D Secure is needed on this transaction.

Note: this process is influenced by third parties and not totally within the Gateway's control.

If no 3-D Secure challenge is required, the Gateway will respond with a transaction completion status using one of our standard codes (a Final Response, see Integration Guide section 5.6.2).

However, if 3-D Secure challenge is required, the Gateway will respond with a `responseCode` of `65802`, and the response will include a transaction reference called `threeDSRef`, an array of data called `threeDSRequest`, and the URL for the Access Control Server (ACS) called `threeDSURL` (a Challenge Response, see Integration Guide section 5.6.1)

You will need to save the `threeDSRef` as it will be needed in step 4**.**

Step 3: Device Method Request

If 3DS device fingerprinting is required, send the contents of the `threeDSRequest` to the `threeDSURL` as received in step 2. This should be done in the Cardholder's browser using an HTTP POST method.

See Integration Guide section 5.4.6

Step 4: Method (Continuation) Request

The ACS will respond with method data. The Gateway now needs this data to continue with the transaction.

Please relay this data to the Gateway, including the relevant `threeDSRef` provided in step 2.

If the method response was sufficient to allow the card to be authorised without a challenge, you will receive a transaction complete response, with an authorisation code.

See Integration Guide section 5.5.3.

Step 5: Challenge Response / Final Response

If the Gateway responds with a further `responseCode` of `65802`, send the contents of the `threeDSRequest` to the `threeDSURL` as explained in step 2. This should be done in the Cardholder's browser using an HTTP POST method.

See Integration Guide section 5.4.5.

Step 6: Challenge (Continuation) Request

Once you have received a Challenge Response from the ACS, please relay this data to the Gateway, including the relevant `threeDSRef` provided in step 5.

See Integration Guide section 5.6.1.

Step 7: Final Response

You might have noticed that steps 3-6 were remarkably similar. It is in fact the same implementation, repeated. We recommend creating a loop to handle these similar messages as continuations of the same process, then simply ending the loop when you receive a Final Response.

See Integration Guide section 5.6.2.

Explainer

*Our Gateway Integration Guide refers to steps 4 and 6 as **Continuation Request** because you continue passing the 3DS requests and responses back-and-forth between the Gateway and the ACS until the transaction is complete. The full flow is described in Integration Guide section 5.4.1*