EMV v2.2.0 migration

This guide outlines the technical migration guide from the EMV 3DS 2.1.0 specification to the v2.2.0 specification. From **ActiveServer** version 2.0.0 onwards, EMV v2.2.0 authentication requests are supported by specifying the `messageVersion` field in the API requests.

Change summary

- There are no breaking changes included in the EMV v2.2.0 specifications or **ActiveServer** v2.0.0. Your existing 3DS Requestor implementation can continue sending authentication requests using EMV v2.1.0 messages after the upgrade is complete.
- A number of new fields were added and new values were added to current fields in the Authentication API to support the EMV v2.2.0 specifications. The new fields and values added were marked with a `[From v2.2.0]` tag in the authentication API document. However, all newly added v2.2.0 fields are optional, having been introduced to enhance existing procedures such as SCA.
- A new optional `messageVersion` field was added to the following endpoints: `/api/v2/auth/brw`, `/api/v2/auth/3ri` and `/api/v2/auth/app`. This field is optional and is used to override the message version. For more details refer to upgrade guide below.
- If v2.2.0 fields are specified in a v2.1.0 request, **ActiveServer** will ignore the fields when forming the AReq. For example, if field `threeDSDecReqInd` was sent in the authentication API request, but the ACS card range only supports EMV v2.1.0 messages, then **ActiveServer** will try to downgrade the request to v2.1.0 and ignore the field. However, if v2.2.0 only values such as `challengeInd=07` are provided for the v2.1.0 field `challengeInd` in a v2.1.0 request, then it will result in error code `203` as per EMV specification requirements.
- The 3DS Server Reference number and PReq process was updated for EMV 2.2.0 processes. For more details, refer to the ActiveServer changes section below.
- The `/api/v2/auth/enrol` API was updated to include the ACS supported message versions (`supportedMessageVersions`) and ACS Information Indicator (`acsInfoInd`). For more details refer to the Enrol API section below.
- The new Decoupled Authentication flow was introduced in EMV v2.2.0. For more details refer to the Decoupled Authentication section below.

Copyright ©2019 GPayments Pty Ltd. All rights reserved.

- The new merchant whitelisting feature was introduced in EMV v2.2.0. For more details refer to the Merchant whitelisting section below.
- The `/api/v2/auth/3ri/result` API endpoint was added to allow the 3DS Requestor to obtain the result for decoupled authentications.
- GPayments TestLabs supports v2.2.0 messages.

3DS Requestor v2.2.0 upgrade guide

The 3DS Requestor code should be upgraded to send the v2.2.0 fields and values. If you want to utilise message version v2.2.0 fields, then the `messageVersion` field must be set to `2.2.0`, as **ActiveServer** will utilise the highest common `messageVersion` by default if no message version field is provided.

As such, the 3DS Requestor should be updated to request and process the new field `supportedMessageVersions` in the Enrol API. If the response field `supportedMessageVersions` contains `2.2.0`, then the card range supports the v2.2.0 protocol and a 2.2.0 authentication request can be sent by using the `messageVersion` field in the API request.

Message version is downgraded if not supported

If the message version is specified to be v2.2.0 but the Enrol API's `supportedMessageVersions` only supports `2.1.0` for that account number, then **ActiveServer** will downgrade the `messageVersion` to v2.1.0. This is for maximum compatibility so that authentications won't fail when the 3DS Requestor sends a message version that the ACS does not support.

If the message version is specified to be v2.2.0 and no card range is found, **ActiveServer** will attempt to send a v2.2.0 message to the Directory Server.

ActiveServer Changes

3DS Server Reference number

After **ActiveServer** completes EMV compliance testing, it is issued with a 3DS Server Reference number, which is included in all AReq's sent to the Directory Server. For backward compatibility, by default **ActiveServer** uses the 3DS Server Reference number issued by EMVco during v2.1.0 certification in the 2.0.0 release. The default reference number is only valid for sending v2.1.0

Copyright ©2019 GPayments Pty Ltd. All rights reserved.

requests and the card scheme Directory Servers will likely reject the v2.2.0 requests using this reference number.

During card scheme compliance testing, it may be required to overwrite the 2.1.0 reference number with the new 2.2.0 reference number. It will also be required to overwrite the 2.1.0 reference number with the new 2.2.0 reference number on your production instance, **although this should only be done after compliance testing is completed**. For more information on 3DS Server Reference number overriding, refer to the section in the Quickstart guide.

PReq process message version

ActiveServer v2.0.0 updates the PReq process for 2.2.0, by sending PReq's with message version 2.2.0 for Visa, Mastercard and American Express, as these Directory Servers handle this version by default. JCB and Discover require card scheme compliance testing and registration of the 3DS Server Reference number to be completed before 2.2.0 PReq's can be sent, so these card schemes will still send 2.1.0 PReq's by default.

During card scheme compliance testing, it may be required to send either 2.1.0 or 2.2.0 PReq messages. It will also be required to update all card schemes to use 2.2.0 PReq's on your production instance, **although this should only be done after compliance testing is completed**. To assist with this, a PReq message overriding setting has been added to the application-prod.properties file. For more information on PReq message overriding, refer to the section in the Quickstart guide.

Enrol API

As mentioned above, the Enrol API has been updated to proved the `supportedMessageVersions` field so that the 3DS Requestor knows what message version is supported for an account number before making an authentication request.

It will also provide the ACS Information Indicator (`acsInfoInd`) field, which describes the functions available on the ACS side:

- 01 = Authentication Available at ACS - normal 3DS authentication supported and available by the cardholders issuing bank.
- 02 = Attempts Supported by ACS or DS - authentication not available for cardholder, however an attemps response can be provided by the ACS or the DS for liability shift. Some card schemes may encourage falling back to 3DS v1.0 if possible to minimise fraud.

Copyright ©2019 GPayments Pty Ltd. All rights reserved.

- 03 = Decoupled Authentication Supported
- 04 = Whitelisting Supported

Additionally, there are some card scheme specific values, for full information on these and API usage refer to the Enrol API documentation.

Decoupled Authentication

Decoupled authentication is authentication performed outside the 3DS flow. For example, a cardholder authenticating directly with their banking app through biometrics.

Following is the general flow for a decoupled authentication:

1. In order to check if the ACS supports decoupled authentication, the 3DS Requestor can call the Enrol API. If the ACS supports decoupled authentication, the `acsInfoInd` field will contain value `03` (decoupled authentication supported). Note that **ActiveServer** does not do strict validation in accordance with `acsInfoInd`, i.e. even if `acsInfoInd` does not have the value `03` but `threeDSDecReqInd` is provided, it does not throw an error.
2. If the ACS supports decoupled authentication, the 3DS Requestor sets the `threeDSDecReqInd=Y` and `threeDSDecMaxTime`.
3. `transStatus=D` and `acsDecConInd=Y` will be returned in the authentication response if the ACS agrees to perform decoupled authentication. The 3DS Requestor should display the content of `cardholderInfo` in the UI which contains instructions for the cardholder to perform for authentication outside 3DS, for example, the message may direct the cardholder to open a banking app.
4. After the cardholder performs decoupled authentication or the `threeDSDecMaxTime` is exceeded the ACS sends the RReq to the 3DS server through the DS.
5. The 3DS Requestor can check the final authentication result availability by making polling requests to the `resultMonUrl`. When the RReq is received by the 3DS server, the event is set to `event=AuthResultReady`, which allows the 3DS Requestor to get the final result through the `/api/v2/auth/**/result` endpoint.

For the detailed flow refer to the authentication sequence diagram, which has been updated to include decoupled authentication. For the requestor implementation for decoupled authentication, refer to the integration guide.

Copyright ©2019 GPayments Pty Ltd. All rights reserved.

Merchant whitelisting

Whitelisting has been introduced in the EMV v2.2.0 specifications, which is the process of an ACS enabling the cardholder to place the merchant on their trusted beneficiaries list. This allows the issuer to exempt transactions in the future from SCA requirements such as PSD2.

The new field `whiteListStatus` was added to support this feature. Refer to the Authentication API document for more information.

In order to check if the ACS supports whitelisting, the 3DS Requestor can call the Enrol API. If the ACS supports whitelisting, the `acsInfoInd` field will contain value `04`. Note that **ActiveServer** does not do strict validation in accordance with `acsInfoInd`, i.e. even if `acsInfoInd` does not have the value `04` but `whiteListStatus` is provided by the 3DS Requestor, it does not throw an error.

Copyright ©2019 GPayments Pty Ltd. All rights reserved.