Back-end implementation (v1)

In this section, we will show the implementation details for the back-end side of the merchant application using our sample code based on the **Auth API version 1**.

> **Important**
>
> GPayments strongly recommends all new implementations of **ActiveServer** to integrate with version 2 of the Auth API from the beginning, as version 1 will be deprecated in a future release. Refer to the API migration from v1 to v2 guide for a summary of the changes and migration process from **v1** to **v2**. To check the new **API v2** implementation, refer here.

For the back-end, we need to implement a **3DS Requestor**. The **3DS Requestor** receives information from the **3ds-web-adapter** and sends the requests to **ActiveServer**. It also receives the authentication results from **ActiveServer** and forwards the results to the **3ds-web-adapter**.

The demo **3DS Requestor** code provides the backend implementation with the following server side languages:

- **Java**: The java version is implemented based on the Springboot framework. For details of Springboot, check out https://spring.io/projects/spring-boot
- **C#**: The C# version is implemented based on ASP.net.
- **PHP**: The PHP version is implemented based on PHP 7.2 with cURL (Client URL Library).
- **Go**: The Go version is implemented based on Go 1.12 with Go Module support. All dependencies are listed in `go.mod` file.

> **Why we need to implement a backend?**
>
> As defined by EMVCo's 3DSecure 2.0 specification, when the 3DS Server and the 3DS Requestor environment is separated, the communication between these two components must be mutual authenticated:
>
> > [Req 300] If the 3DS Requestor and 3DS Server are separate components, ensure that data transferred between the components is protected at a level that satisfies Payment System security requirements with mutual authentication of both servers.

Before starting the authentication process with **ActiveServer**, the **3DS Requestor** needs to establish a mutual TLS connection with **ActiveServer**. Make sure you have the **client certificate** and configure it with the **3DS Requestor**. If not, follow the Get client certificate and Configure 3DS Requestor details instructions found on the Introduction page.

> **Tip**
>
> The implementation of TLS configuration for the HTTP Client can be found as follows:
>
> - Java: The TLS configuration and client certificate loading can be found in class `RestClientConfig.java`.
> - C#: The TLS configuration and client certificate loading can be found in class `RestClientHelper.cs`.
> - PHP: The TLS configuration and client certificate loading can be found in file `RestClientConfig.php`.
> - Go: The TLS configuration and client certificate loading can be found in file `https.go`.

Next, we will describe the details of the back-end implementation based on the authentication processes and authentication sequence.

Process 1: Initialise the Authentication

To initialise authentication, the **3DS Requestor** needs to:

- Receive the `Initialise authentication` request from the **3DS-web-adapter** (Step. 2).
- Forward the request to **ActiveServer** (Step. 3).
- Receive the response data from **ActiveServer** (Step. 4).
- Return the response data to the **3DS-web-adapter** (Step. 5).

Java C# PHP Go

```java
//AuthControllerV1.java
/**
 * Receives the initialise authentication request from the 3DS-web-adapter
(Step 2)
 * Send data to ActiveServer to Initialise Authentication
 */
  @PostMapping("/v1/auth/init/{messageCategory}")
  public Message initAuth(@RequestParam(value = "trans-type", required = false)
String transType,
      @RequestBody Message request,
      @PathVariable(value = "messageCategory") String messageCategory) {

    //Generate requestor trans ID
    String transId = UUID.randomUUID().toString();
    request.put("threeDSRequestorTransID", transId);
    //Fill the event call back url with requestor url + /3ds-notify
    String callBackUrl = config.getBaseUrl() + "/3ds-notify";
    request.put("eventCallbackUrl", callBackUrl);

    //ActiveServer url for Initialise Authentication
    String initAuthUrl = config.getAsAuthUrl() + "/api/v1/auth/brw/init/" +
messageCategory;

    //Add parameter trans-type=prod in the initAuthUrl to use prod DS,
otherwise use TestLabs DS
    //For example, in this demo, the initAuthUrl for transactions with prod DS
is https://api.as.testlab.3dsecure.cloud:7443/api/v1/auth/brw/init?trans-
type=prod
    //For more details, refer to: https://docs.activeserver.cloud
    if ("prod".equals(transType)) {
      initAuthUrl = initAuthUrl + "?trans-type=prod";
    }

    logger.info("initAuthRequest on url: {}, body: \n{}", initAuthUrl, request);

    //Send data to ActiveServer to Initialise authentication (Step 3)
    //Get the response data from ActiveServer (Step 4)
    Message response =
        sendRequest(initAuthUrl, request, HttpMethod.POST);
    logger.info("initAuthResponseBRW: \n{}", response);

    //Return data to 3ds-web-adapter (Step 5)
    return response;
}
```

Note

We set the `eventCallbackUrl` to `{baseUrl}/3ds-notify`. This allows **ActiveServer** to make a notification when the browser information collection (Step. 7) is done. The `baseUrl` is set here.

The `initAuth` request will be sent to `{ActiveServer auth url}/api/v1/auth/brw/init/{messageCategory}`. To check the data structure of `initAuth` request, refer to the API document.

Important: By default, the URL above will send the authentication request to GPayments TestLabs for testing purposes. When moving into production, to send the API request to the card scheme directory server, the *trans-type query parameter* must be appended to this API URL. See API description for further information on usage.

HTTP header for Master Auth API client certificate

If you are using a Master Auth API client certificate to authenticate a **Business Admin** user on behalf of a merchant, the back-end needs to add a HTTP Header in the HTTP Request with a field of `AS-Merchant-Token`, which should be set to the merchantToken from the merchants profile.

Java C# PHP

```
//Note: the sendRequest() function will send the request to ActiveServer.
//If this is groupAuth, the request should include a HTTP Header with the field
of AS-Merchant-Token.
private Message sendRequest(String url, Message request, HttpMethod method) {

    HttpEntity<Message> req;
    HttpHeaders headers = null;

    if (config.isGroupAuth()) {
      //the certificate is for groupAuth, work out the header.
      headers = new HttpHeaders();
      headers.add("AS-Merchant-Token", config.getMerchantToken());
    }

    switch (method) {
      case POST:
        req = new HttpEntity<>(request, headers);
        return restTemplate.postForObject(url, req, Message.class);
      case GET:
        if (headers == null) {
          return restTemplate.getForObject(url, Message.class);
        } else {
          req = new HttpEntity<>(headers);
          return restTemplate.exchange(url, HttpMethod.GET, req,
Message.class).getBody();
        }
      default:
        return null;
    }
  }
}
```

```Go tab= //Note: the callASAPI() function will send the request to ActiveServer. //If this is groupAuth, the request should include a HTTP Header with the field of AS-Merchant-Token. func callASAPI(message map[string]interface{}, url string, c *gin.Context, httpClient *http.Client, config *Config, rHandler respHandler) { //add ActiveServer base URL callASAPIWithUrl(message, config.GPayments.AsAuthUrl+url, c, httpClient, config, rHandler) } func callASAPIWithUrl( message map[string]interface{}, url string, c *gin.Context, httpClient *http.Client, config *Config, rHandler respHandler) {
```

```
var r *http.Request
var err error

if message == nil {
    r, err = http.NewRequest("GET", url, nil)
    if err != nil {
        c.JSON(http.StatusInternalServerError, gin.H{"error": err.Error()})
        return
    }
} else {
    var data []byte
    data, err = json.Marshal(message)
    if err != nil {
        c.JSON(http.StatusInternalServerError, gin.H{"error": err.Error()})
        return
    }

    r, err = http.NewRequest("POST", url, bytes.NewBuffer(data))
    if err != nil {
        c.JSON(http.StatusInternalServerError, gin.H{"error": err.Error()})
        return
    }
    r.Header.Set("Content-Type", "application/json;charset=utf-8")

}

//if this is groupAuth
if config.GPayments.GroupAuth {
    r.Header.Set("AS-Merchant-Token", config.GPayments.MerchantToken)
}

response, err := httpClient.Do(r)
if err != nil {
    c.JSON(http.StatusInternalServerError, gin.H{"error": err.Error()})
    return
}
defer response.Body.Close()

contentType := response.Header.Get("Content-Type")
responseBody, err := ioutil.ReadAll(response.Body)

if err != nil {
    c.JSON(http.StatusInternalServerError, gin.H{"error": err.Error()})
    return
}

if rHandler != nil {

    if err = rHandler(responseBody); err != nil {
```

```
        c.JSON(http.StatusInternalServerError, gin.H{"error": err.Error()})
        return
```