3DSV2 - Direct Interface - Authentication and Authorization

Content

These pages describe how the merchants request Payline for an authorization coupled with a 3DS V2 authentication.

Exchanges outlines

The exchanges consist in 3 steps:

1. Verify enrollment which tells the merchant how authenticate the buyer for the requested order
2. Challenge (optional), which represents the connection of the buyer to the ACS authentication page
3. Authorization

Verify Enrollment

This method tells the merchant how to authenticate the buyer according to the order he requested.

The ACS/Network may propose 3 possibilities depending on the payment card, the order and the buyer :

- to be authenticated with challenge (V2)
- authenticated in frictionless mode (V2)
- fallback in authentication V1

The merchant fills out the request with the following parameters:

1. merchant transaction identifier which is the 'correlation id' used up to the authorization;
2. Payment attributes (PAN, expiration, cvx, payment mode, ...);
3. The URL of the system that receives the `CRes` message or Error Message;
4. Buyer's and order's attributes;
5. The merchant indication related to the authentication. This is the way for the merchant to indicates whether a challenge is requested for this transaction.
6. The browser's or the sdk's attributes of the buyer;
7. The previous authentication's method of that buyer (optional);
8. The result of the 3DS method (refer to the description of that use case)

In response Payline returns:

1. the action to be carry out by the merchant to authenticate its buyer given by the '`returnCode`' parameter
2. The attributes of the call to the ACS (`HTTP_METHOD(get/post), URL, METHOD_FIELD_NAME, METHOD_FIELD_VALUE, MD_FIELD_NAME, MD_FIELD_VALUE, TERM_URL_FIELD_NAME, TERM_URL_FIELD_VALUE,...`);
3. The authentication result container in case of frictionless authentication
4. `transientData` used internally by Payline to process the transaction, this field must be sent back to subsequent call to the `verifyEnrollment` or `doAuthorization`

Processing screen requirements

EMVCo specifies that during the `AReq / ARes` message cycle initiated by the call of the `verifyEnrollment` web service, the merchant shall comply with the followings

The 3DS Requestor (merchant) website shall:

Seq 4.32 [Req 172] Create a Processing screen for display during the AReq/ARes message cycle.

Note: The Processing screen is displayed by the 3DS Requestor website during AReq message processing.

Seq 4.33 [Req 173] Display a graphical element (for example, a progress bar or a spinning wheel) that conveys to indicate to the Cardholder that processing is occurring.

Seq 4.34 [Req 174] Include the DS logo for display unless specifically requested not to include.

Seq 4.35 [Req 175] Not include any other design element in the Processing screen.

Seq 4.36 [Req 176] Display the Processing screen for a minimum of two seconds.

Challenge

Initiating the challenge

When the `verifyEnrollmentresponse` tells the merchant to connect the buyer to the ACS for authentication, the merchant shall

"[Req 267] Create a 3-D Secure challenge window by generating a CReq message, creating an HTML iframe in the Cardholder browser, and generating an HTTP POST through the iframe to the ACS URL that was received in the ARes message." (*EMVCo requirement*)

The merchant sets up the html form according to the response parameters of the `verifyEnrollment` web service as follows

Html code snippet of the challenge window

```
<!--...-->
<iframe id="<iFrameId>" name="<iFrameName>" style="width: <width>; height: <height>;" src="
javascript:false;" xmlns="http://www.w3.org/1999/xhtml">
<!--...-->
</iframe>
<!--...-->

<form id="webform0" name="" method="<HTTP_METHOD>" action="<URL>" accept_charset="UTF-8" target="
<iFrameName>">
<input type="hidden" name="_charset_" value="UTF-8"/>
<input type="hidden" name="<METHOD_FIELD_NAME>" value="<METHOD_FIELD_VALUE>"/>
<input type="hidden" name="<MD_FIELD_NAME>" value="<MD_FIELD_VALUE>"/>
<input type="hidden" name="<TERM_URL_FIELD_NAME>" value="<TERM_URL_FIELD_VALUE>"/>
</form>
<!--...-->
```

Authentication window design hints

The merchant designs the authentication window taking into account that the pre-configured sizes in pixels of the authentication windows the ACS shall renders are as follows (width x height):

- 250 x 400
- 390 x 400
- 500 x 600
- 600 x 400
- Full screen

The ACS shall reply with content that is formatted to appropriately render in this window to provide the best possible user experience. (*EMV Co requirement*)

Handling the challenge response

The consumer returns from the authentication to the `<TERM_URL_FIELD_VALUE>` that was included in the form. When the consumer returns, two parameters will be included: `<MD_FIELD_NAME>` and '`PaRes`' or '`CRes`'.

1. `<MD_FIELD_NAME>` contains the same reference number sent to the ACS. Should be used to look up the correct transaction in the merchant's system.
2. `PaRes` or `CRes` contains the Payment Authentication Response that must be sent in to the `doAuthorization` web service.

Authorization

To issue an authorization request after the buyer has been 3DS authenticated, the merchant shall fill out the following fields of the `authentication3DSecure` object:

- `md`
- `pares` if the ACS requested a challenge
- `resultContainer` if the ACS processed the authentication in frictionless mode

The cardBrand (ie. scheme) in the `doAuthorizaton` must be the same as in the authentication

JSON Container

The JSON container format is described here : 3DS V2 JSON container format

Authentification use cases

The merchant begins the authentication process by sending a `verifyEnrollmentRequest` to Payline.

The message's snippet below explains how to fill up that request.

verifyEnrollmentRequest

```
<verifyEnrollmentRequest xmlns="http://impl.ws.payline.experian.com" xmlns:ns2="http://obj.ws.payline.
experian.com" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <ns1:version>22</ns1:version>
  <ns1:card>
    <ns2:number>453304XXXXXX8423</number>
    <ns2:type>VISA</ns2:type>
    <ns2:expirationDate>0319</expirationDate>
    <ns2:cvx xsi:nil="true"/>
    <ns2:ownerBirthdayDate/>
    <ns2:password/>
    <ns2:cardPresent/>
  </ns1:card>
  <ns1:payment>
    <ns2:amount>16230</ns2:amount>
    <ns2:currency>978</ns2:currency>
    <ns2:action>100</ns2:action>
    <ns2:mode>CPT</ns2:mode>
```

```
    <ns2:contractNumber>CB_3DS</ns2:contractNumber>
    <ns2:differedActionDate xsi:nil="true"/>
    <ns2:method xsi:nil="true"/>
    <ns2:softDescriptorxsi:nil="true"/>
    <ns2:cardBrand xsi:nil="true"/>                          <!-- Optionnal; by default: scheme defined in
the Payline Payment method contract  -->
    <ns2:registrationToken xsi:nil="true"/>
  </ns1:payment>
  <ns1:order>
    <ns2:ref>47960539</ns2:ref>
    <ns2:origin xsi:nil="true"/>
    <ns2:country>FR</ns2:country>
    <ns2:taxes xsi:nil="true"/>
    <ns2:amount>16230</ns2:amount>
    <ns2:currency>978</ns2:currency>
    <ns2:date>27/01/2019 11:01</ns2:date>
    <ns2:details xsi:nil="true"/>
    <ns2:deliveryTime>6</ns2:deliveryTime>                   <!-- Strongly recommended for frictionless.
(same day dhipping,overnight shipping, ... -->
    <ns2:deliveryMode>7</ns2:deliveryMode>                   <!-- Strongly recommended for frictionless -->
                                                             <!-- Ship to cardholder’s billing address,
locker delivery, travel or event ticket, ... -->
    <ns2:deliveryExpectedDate xsi:nil="true"/>               <!-- In case of pre-order    -->
    <ns2:deliveryExpectedDelay xsi:nil="true"/>
    <ns2:deliveryCharge>2490</ns2:deliveryCharge>
    <ns2:orderExtended>
      <ns2:giftCardAmount>0</ns2:giftCardAmount>             <!-- If gift cards are used for payment,
partial or not   -->
      <ns2:giftCardCount>0</ns2:giftCardCount>               <!-- If gift cards are used for payment,
partial or not -->
      <ns2:reorderIndicator>01</ns2::reorderIndicator>       <!-- Indicates whether the cardholder is
reordering previously purchased merchandise -->
                                                             <!-- Strongly recommended for frictionless -->
    </ns2:orderExtended>
 </ns1:order>
  <ns1:buyer>
    <ns2:title>4</ns2:title>
    <ns2:lastName>Dupont</ns2:lastName>                      <!-- Strongly recommended for frictionless -->
    <ns2:firstName>Jean</ns2:firstName>                      <!-- Strongly recommended for frictionless -->
    <ns2:email>jean.dupont@monext.net</ns2:email>            <!-- Strongly recommended for frictionless -->
    <ns2:shippingAdress>                                     <!-- Strongly recommended for frictionless -->
      <ns2:title>4</ns2:title>                               <!-- Strongly recommended for frictionless -->
      <ns2:name xsi:nil="true"/>
      <ns2:createDate>05/11/2011</ns2:createDate>            <!-- Strongly recommended for frictionless -->
      <ns2:firstName>Jean</ns2:firstName>                    <!-- Strongly recommended for frictionless -->
      <ns2:lastName>Dupont</ns2:lastName>                    <!-- Strongly recommended for frictionless -->
      <ns2:street1>260, rue Claude Nicolas Ledoux</ns2:street1>     <!-- Strongly recommended for
frictionless -->
      <ns2:street2>CS 60507</ns2:street2>                          <!-- Strongly recommended for
frictionless -->
      <ns2:cityName>Aix-en-Provence cedex 3</ns2:cityName>         <!-- Strongly recommended for
frictionless -->
      <ns2:zipCode>13593</ns2:zipCode>                             <!-- Strongly recommended for
frictionless -->
      <ns2:country>FR</ns2:country>                                <!-- Strongly recommended for
frictionless -->
      <ns2:email></ns2:email>                                 <!-- In case of digital good sended by email;
Strongly recommended for frictionless -->
      <ns2:phone>0442251515</ns2:phone>
      <ns2:state>13</ns2:state>
      <ns2:county xsi:nil="true"/>
      <ns2:phoneType xsi:nil="true"/>
    </ns2:shippingAdress>
    <ns2:billingAddress>
      <ns2:title>4</ns2:title>
      <ns2:name xsi:nil="true"/>
      <ns2:firstName>Jean</ns2:firstName>
      <ns2:lastName>Dupont</ns2:lastName>
      <ns2:street1>260, rue Claude Nicolas Ledoux</ns2:street1>        <!-- Strongly recommended for
frictionless -->
      <ns2:street2>CS 60507</ns2:street2>                              <!-- Strongly recommended for
```

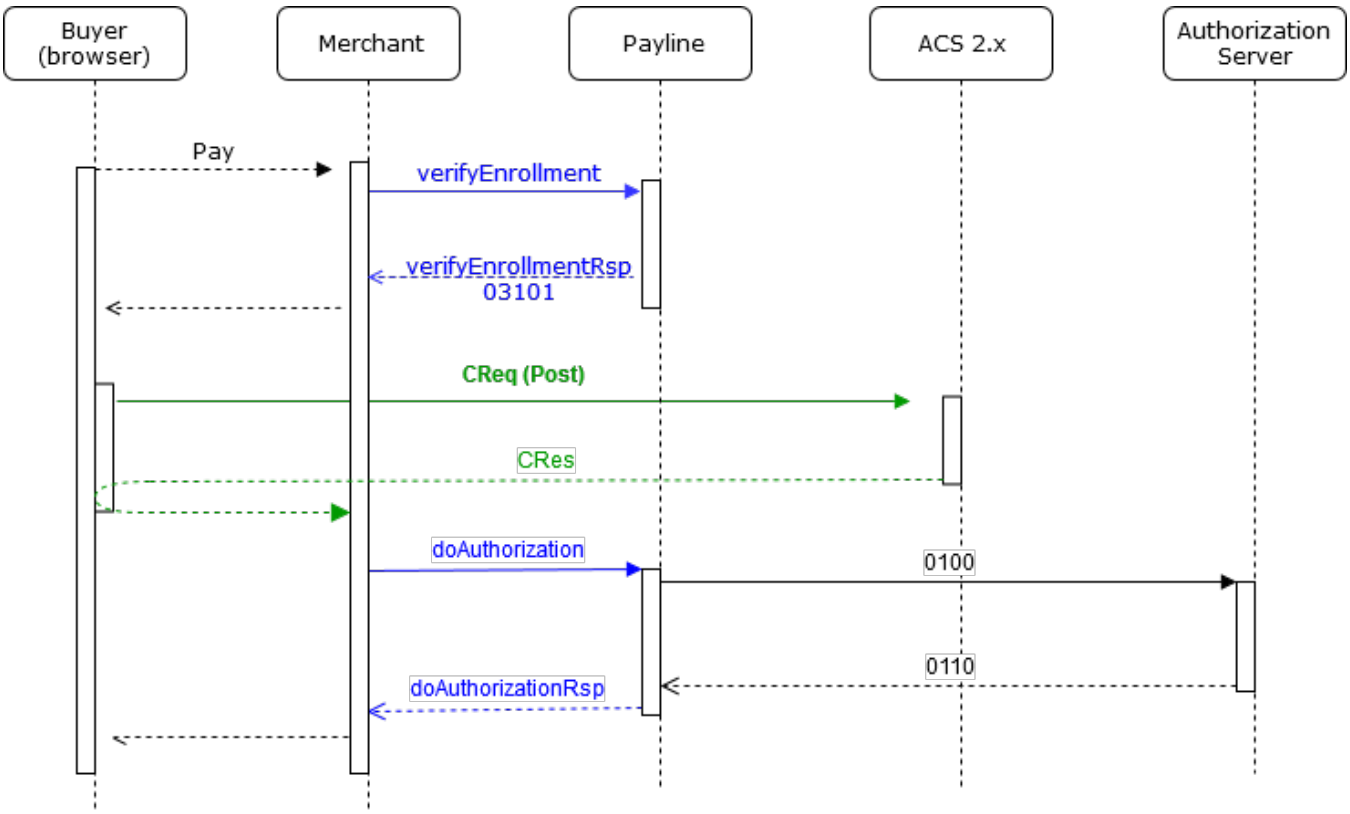
```
frictionless -->
      <ns2:cityName>Aix-en-Provence cedex 3</ns2:cityName>             <!-- Strongly recommended for
frictionless -->
      <ns2:zipCode>13593</ns2:zipCode>                                 <!-- Strongly recommended for
frictionless -->
      <ns2:country>FR</ns2:country>                                    <!-- Strongly recommended for
frictionless -->
      <ns2:phone>0442251515</ns2:phone>                                <!-- Strongly recommended for
frictionless -->
      <ns2:state>13</ns2:state>
      <ns2:county xsi:nil="true"/>
      <ns2:phoneType xsi:nil="true"/>
    </ns2:billingAddress>
    <ns2:accountCreateDate>05/11/11</ns2:accountCreateDate>            <!-- Strongly recommended for
frictionless -->
    <ns2:accountAverageAmount xsi:nil="true"/>
    <ns2:accountOrderCount>0</ns2:accountOrderCount>
    <ns2:walletId xsi:nil="true"/>
    <ns2:walletDisplayed xsi:nil="true"/>
    <ns2:walletSecured xsi:nil="true"/>
    <ns2:walletCardInd xsi:nil="true"/>
    <ns2:ip>90.37.101.225</ns2:ip>                     <!-- mandatory if browser based authentication  --
>
    <ns2:mobilePhone>0627720695</ns2:mobilePhone>
    <ns2:customerId>4805157</ns2:customerId>
    <ns2:legalStatus>1</ns2:legalStatus>
    <ns2:legalDocument xsi:nil="true"/>
    <ns2:birthDate xsi:nil="true"/>
    <ns2:fingerprintID xsi:nil="true"/>
    <ns2:deviceFingerprint xsi:nil="true"/>
    <ns2:isBot xsi:nil="true"/>
    <ns2:isIncognito xsi:nil="true"/>
    <ns2:isBehindProxy xsi:nil="true"/>
    <ns2:isFromTor xsi:nil="true"/>
    <ns2:isEmulator xsi:nil="true"/>
    <ns2:isRooted xsi:nil="true"/>
    <ns2:hasTimezoneMismatch xsi:nil="true"/>
    <ns2:merchantAuthentication>
        <ns2:method>02</ns2:method>                        <!-- Recommended for frictionless -->
        <ns2:date>27/01/2019 12:01</ns2:date>              <!-- Recommended for frictionless -->
    </ns2:merchantAnthentication>

    <ns2:buyerExtended><ns2:buyerExtendedHistory>                       <!-- Strongly recommended for
frictionless -->
        <ns2:suspiciousActivity>01</ns2:suspiciousActivity> <!-- Strongly recommended for frictionless -->
                                                            <!-- Indicates whether the merchant has
experienced suspicious activity -->
                                                            <!--(including previous fraud) on the cardholder
account. -->
        <ns2:lastChange>07/12/2018 10:40</ns2:lastChange>   <!-- Date that the cardholder’s account with the
merchant was last changed -->
        <ns2:lastPasswordChange>07/12/2018 10:40</ns2:lastPasswordChange>   <!-- Date that cardholder’s
account with the merchant -->
                                                                            <!-- had a password change or
account reset. -->
        <ns2:orderCount6Months>15</ns2:orderCount6Months>                   <!-- Number of purchases with
this cardholder account during
                                                                            <!-- the previous  six months.-->
        <ns2:provisionAttemptsDay>0</ns2:provisionAttemptsDay>              <!-- Number of Add Card attempts
in the last 24 hours.-->
        <ns2:transactionCountDay>0</ns2:transactionCountDay>                <!-- Number of transactions
(successful and abandoned) for this cardholder -->
                                                                            <!-- account with the merchant
across all payment accounts in the previous 24 hours. -->
        <ns2:transactionCountYear>38</ns2:transactionCountYear>             <!-- Number of transactions
(successful and abandoned) for this cardholder -->
                                                                            <!-- account with the 3DS
Requestor across all payment accounts in the previous year. -->
        <ns2:paymentAccountAge>14/11/2018</ns2:paymentAccountAge>           <!-- Date that the payment
account was enrolled in the -->
                                                                            <!-- cardholder’s account with
```

```
the merchant. -->
    </ns2:buyerExtendedHistory></ns2:buyerExtended>

  </ns1:buyer>
  <ns1:subMerchant xsi:nil="true">
  <ns1:userAgent/>                                                    <!-- Deprecated, use   browser.
userAgent instead -->

                                                                      <!-- The URL of the system that
receives the CRes message or Error Message -->
  <ns1:returnURL>https://merchant.com/notification/3DSresult.do;orderId=47960539</ns1:returnURL>
  <ns1:threeDSInfo>
    <ns2:challengeInd>02</ns2:challengeInd>        <!-- Optional: This is the way for the merchant to
indicates whether a challenge is requested for this transaction. -->

                                                <!-- optional information about a 3DS cardholder
authentication that occurred prior to the current transaction. -->
    <ns2:threeDSReqPriorAuthData/>                              <!-- For future usage -->
    <ns2:threeDSReqPriorAuthMethod>02</ns2:threeDSReqPriorAuthMethod>
    <ns2:threeDSReqPriorAuthTimestamp>12/01/2017 11:59</ns2:threeDSReqPriorAuthTimestamp>

    <ns2:browser>                                                                    <!-- mandatory for
browser based authentication -->
        <ns2:acceptHeader> xyz....tre </ns2:acceptHeader>
        <ns2:javaEnabled>true</ns2:javaEnabled>
        <ns2:language>fr</ns2:language>
        <ns2:colorDepth>32</ns2:colorDepth>
        <ns2:screenHeight>420</ns2:screenHeight>
        <ns2:screenWidth>400</ns2:screenWidth>
        <ns2:timeZoneOffset>+60</ns2:timeZoneOffset>
        <ns2:javascriptEnabled>true</ns2:javascriptEnabled>
        <ns2:userAgent>Mozilla/5.0 (Windows NT 6.1; WOW64; rv:64.0) Gecko/20100101 Firefox/64.0</ns2:
userAgent>
    </ns2:browser>
    <ns2:sdk/>

<!-- in case the ACS requires the 3DS method -->
    <ns2:threeDSMethodNotificationURL>https://merchant.com/3DSMethodNotif;
threeDSSessionData=2F04CC56F968373D0114AD4B6BB4E4F1 </ns2:threeDSMethodNotificationURL>
        <ns2:threeDSMethodResult>Y</ns2:threeDSMethodResult>  <!-- in case the 3DS method has been called
before and rendered a completion notification-->
  </ns1:threeDSInfo>
  <ns1:mdFieldValue>60c19577-b902-43b9-9033-2eb366551228<ns1:mdFieldValue> <!-- merchant transaction
identifier which is the 'correlation id' used up to the authorization --
>
  <ns1:transientData>{JSON}</ns1:transientData>        <!-- required if present in the response of previous
calls -->
  <ns1:merchantScore/>                                 <!-- For CB scoring only -->
  <ns1:walletId/>
  <ns1:walletCardInd/>
  <ns1:generateVirtualCvx/>
</ns1:verifyEnrollmentRequest>
```

The returnCode present in the `verifyEnrollmentResponse` message tells the merchant how to continue:

- `03101` : The ACS requires a challenge to authenticate the buyer description
- `03102`: The ACS authenticated the buyer in frictionless mode description
- `03000`: The buyer shall authenticated using 3DS V1 description
- `03100`: The ACS requires the 3DS Method to be called description

Authentification with challenge



The merchant receives the following `verifyEnrollmentResponse`

Authentication with challenge

```
<impl:verifyEnrollmentResponse xmlns:impl="http://impl.ws.payline.experian.com" xmlns:obj="http://obj.ws.
payline.experian.com">
   <impl:result>
      <obj:code>03101</obj:code> <!-- The ACS requires a challenge -->
      <obj:shortMessage>ACCEPTED</obj:shortMessage>
      <obj:longMessage>Transaction accepted - Challenge requested</obj:longMessage>
   </impl:result>
<!------------------------------ Attributes for the CReq message  Beginning  -->
   <impl:actionUrl>https://dsx.modirum.com:443/dstests/ACSEmu2</impl:actionUrl>
   <impl:actionMethod>POST</impl:actionMethod>
   <impl:pareqFieldName>creq</impl:pareqFieldName>
   <impl:pareqFieldValue>ewogICAiYWNzVHJhbnNJRCIgOi......jIgp9</impl:pareqFieldValue>
   <impl:mdFieldName>MD</impl:mdFieldName>
   <impl:mdFieldValue>CixYXysxxvCVaEvolWXq</impl:mdFieldValue>
<!------------------------------ Attributes for the CReq message  End-->
  <mpiResult>C</mpiResult>
  <authentication3DSecure\>
  <transientData>{JSON}</transientData> <!-- Important : must be sent in subsequent calls -->
</impl:verifyEnrollmentResponse>
```

The merchant creates a 3-D Secure challenge window by generating a `CReq` message, creating an HTML iframe in the Cardholder browser, and generating an `HTTP POST` through the iframe to the ACS URL that was received in the `ARes` message."

The window contains :

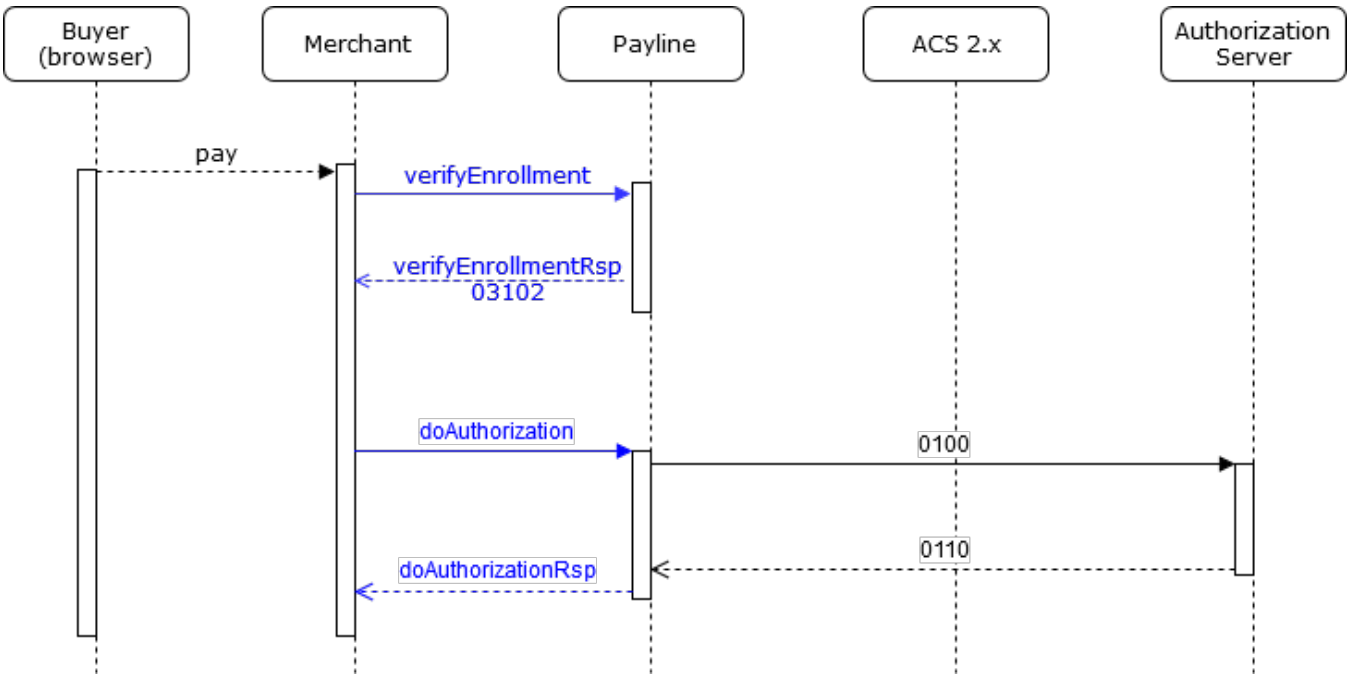
Html code snippet of the challenge window

```
<!--...-->
<iframe id="idIframeChallenge" name="challenge" style="width: 390; height: 400;" src="javascript:false;"
xmlns="http://www.w3.org/1999/xhtml">
```

```
<!--...-->
</iframe>
<!--...-->
<form id="webform0" name="" method="POST" action="https://localhost.modirum.com:8543/dstests/ACSEmu2"
accept_charset="UTF-8" target="challenge">
<input type="hidden" name="_charset_" value="UTF-8"/>
<input type="hidden" name="creq" value="ewogICAiYWNzVHJhbnNJRCIgOi....lmLTgwMDAtMDAwMDAwMDJmYTk5Igp9"/>
</form>
<!--...-->
```

When the buyer is done with the authentication, the merchant retrieves the `CRes` message base64 encoded posted by the ACS to the `termURL`.

Frictionless authentication

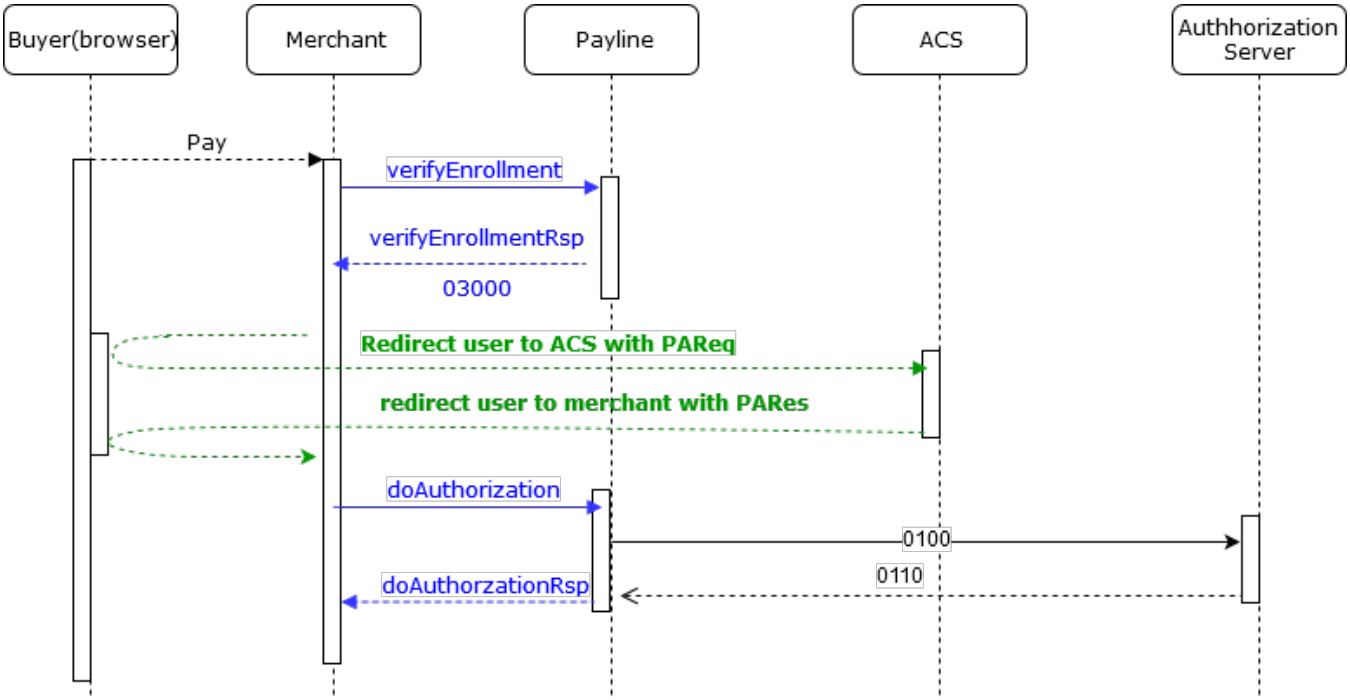


The merchant receives the following `verifyEnrollmentResponse`

Frictionless authentication

```
<impl:verifyEnrollmentResponse xmlns:impl="http://impl.ws.payline.experian.com" xmlns:obj="http://obj.ws.
payline.experian.com">
  <impl:result>
    <obj:code>03102</obj:code> <!-- The ACS accept a frictionless -->
    <obj:shortMessage>ACCEPTED</obj:shortMessage>
    <obj:longMessage>Transaction accepted - Cardholder authenticated</obj:longMessage>
  </impl:result>
  <impl:mdFieldName>MD</impl:mdFieldName>
  <impl:mdFieldValue>JikRUglPzWGYfPllKpPW</impl:mdFieldValue>
  <impl:mpiResult>Y</impl:mpiResult>
  <impl:authentication3DSecure>
  <obj:resultContainer>eyJjb250YWluZXJWZXJzaW9uIjoiMSIsIm.....W9uIjoiMi4xLjAifQ==</obj:resultContainer>
  </impl:authentication3DSecure>
  <transientData>{JSON}</transientData> <!-- must be sent in subsequent call -->
</impl:verifyEnrollmentResponse>
```

3DS V1 fallback



The merchant receives the following `verifyEnrollmentResponse`

Authentication with challenge

```
<verifyEnrollmentResponse xmlns="http://impl.ws.payline.experian.com" xmlns:obj="http://obj.ws.payline.
experian.com" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <result>
    <obj:code>03000</obj:code> <!-- The ACS requires a fallback in 3DS V1 -->
    <obj:shortMessage>ACCEPTED</obj:shortMessage>
    <obj:longMessage>Transaction accepted</obj:longMessage>
  </result>
<!------------------------------ Attributes for the Pareq message  Beginning  -->
  <actionUrl>https://ssl-prd-u7f-fo-acs-pa-casa.wlp-acs.com/acs-pa-service/pa/paRequest</actionUrl>
  <actionMethod>POST</actionMethod>
  <pareqFieldName>PaReq</pareqFieldName>
  <pareqFieldValue>eJxVUl1vgjAU/SvG99EPaAVzbeJwycyCOpQl28vC...GUY8y9ux4x1+U2M9F3PcY9MxES7HX2BgAyLqh/VdQ
/vK7+fYhfHAOuMA==</pareqFieldValue>
  <termUrlName>TermUrl</termUrlName>
  <termUrlValue>https://merchant.fr/authentV1Result</termUrlValue>
  <mdFieldName>MD</mdFieldName>
  <mdFieldValue>60c19577-b902-43b9-9033-2eb366551228</mdFieldValue>
<!------------------------------ Attributes for the PaReq message  End-->
  <mpiResult>Y</mpiResult>
  <virtualCvx></virtualCvx>
  <token></token>
  <authentication3DSecure\>
  <transientData>{JSON}</transientData> <!-- must be sent in subsequent call -->
</verifyEnrollmentResponse>
```

The merchant acts as for a regular **3DS V1 authentication**.
The merchant creates a 3-D Secure authentication window by generating a PaReq message.
When the buyer is done with the authentication, the merchant retrieves the PaRes message base64 encoded posted by the ACS to the termURL.

Authentication's exception handling

Return code	Meaning	Action to be taken
03001	The bin card range not taken into account by any ACS.	Up to the merchant continuing with the authorization or to refuse and request for another card.
03002	The ACS handling the bin card range doésn't know the cardholder	
03003	Athentication refused	Refer to the transstatusInfo present in the resultContainer to determine the cause of refusal and adapt the response.
03006	Invalid Pares	The authentication response message given by the merchant has been altered.
03007	Technical error on the ACS side	Refer to the transstatusInfo present in the resultContainer to determine the cause of refusal and adapt the response.
03008	Authentication attempted	Due to an incident the ACS doesn't finalize the authentication but certifies the authentication has been issued by the merchant. According the trust levef of the transaction, the merchant may either refuse the payment or issue the authorization Request.
All other return code or no response	Payline technical error	According the trust levef of the transaction, the merchant may either refuse the payment or issue an authorization Request with authentication exemption due to technical outage doAuthorizationRequest with authentication3DSecure.pares parameter set to '3DS_UNAVAILABLE'

Error during the challenge

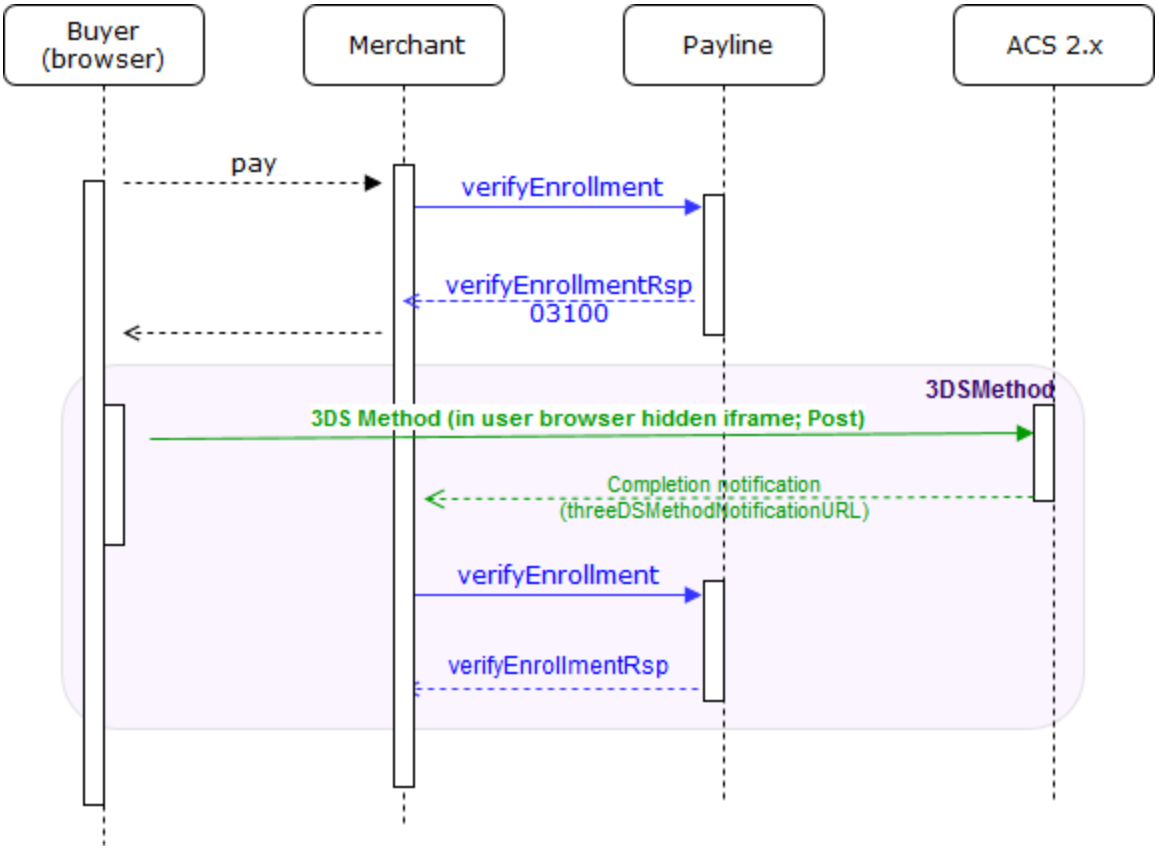
Error	Meaning	Action to be taken
The merchant doesn't receive the challengeResponse message	Network error or ACS error	According the trust levef of the transaction, the merchant may either refuse the payment or issue an authorization Request with authentication exemption due to technical outage doAuthorizationRequest with authentication3DSecure.pares parameter set to '3DS_UNAVAILABLE'

3DS error during the authorization

Error	Meaning	Action to be taken
03006 03022	Authentication result cannot be retrieve.	According the trust levef of the transaction, the merchant may either refuse the payment or issue an authorization Request with authentication exemption due to technical outage doAuthorizationRequest with authentication3DSecure.pares parameter set to '3DS_UNAVAILABLE'

The ACS requires the 3DS Method to be called

The ACS may require that before anything the buyer's browser to be redirected to it.



In that case, Payline renders a `returnCode` set to `03100`.

The merchant receives the following `verifyEnrollmentResponse`

ACS requires the 3DS method to be called

```
<impl:verifyEnrollmentResponse xmlns:impl="http://impl.ws.payline.experian.com" xmlns:obj="http://obj.ws.
payline.experian.com">
  <impl:result>
    <obj:code>03100</obj:code> <!-- The ACS requires the 3DS method to be called -->
    <obj:shortMessage>ACCEPTED</obj:shortMessage>
    <obj:longMessage>3DS method requested before enrollment</obj:longMessage>
  </impl:result>
<!------------------------------ Attributes for the 3DS Method  Beginning  -->
  <impl:actionUrl>https://dsx.modirum.com/dstests/ACSEmu2?handshake=1</impl:actionUrl>
  <impl:actionMethod>post</impl:actionMethod>
  <impl:pareqFieldName>threeDSMethodData</impl:pareqFieldName>
  <impl:pareqFieldValue>eyAidGhy.......NvbSIgfQ</impl:pareqFieldValue>
  <impl:mdFieldName>MD</impl:mdFieldName>
  <impl:mdFieldValue>bJZgiqZulMTZCrKyOzJn</impl:mdFieldValue>
<!------------------------------ Attributes for the 3DS Method  End-->
  <transientData>{JSON}</transientData> <!-- Important : must be sent in subsequent call -->
</impl:verifyEnrollmentResponse>
```

The merchant renders a hidden HTML iframe in the Cardholder browser and sends a form with a field named `threeDSMethodData`.

The merchant constructs the iframe for the 3DS method in a very similar way than for the challenge.

The window contains :

Iframe code snippet for the 3DS method

```
<!--...-->
<iframe id="idIframe3DSMethod" name="threeDSMethod" style="width: 0; height: 0; style="visibility: hidden;"
```

```
src="javascript:false;" xmlns="http://www.w3.org/1999/xhtml">
<!--...-->
</iframe>
<!--...-->
<form id="webform0" name="" method="POST" action="https://nspk-ds.test.modirum.com/ds/DDF/1" accept_charset="
UTF-8" target="threeDSMethod">
<input type="hidden" name="_charset_" value="UTF-8"/>
<input type="hidden" name="threeDSMethodData" value="eyAidGhyZWVEU1NlcnZlclRyYW5zSUQiIDo...
JbTdFdjJYTmkwNnh6YmZNJTJGR3MlM0QiIH0"/>
</form>
<!--...-->
```

After having redirected the buyer's browser iframe to the ACS, the merchant wait for the notification of the completion of the 3DS method.

The ACS POST to the result to threeDSInfo.`threeDSMethodNotificationURL` parameter of the `verifyEnrollmentRequest` .

If the merchant receives the notification within the next 10 secondes he issues a second time the `verifyEnrollmentRequest` after having added the threeDSInfo.`threeDSMethodResult` parameter set to 'Y'

Otherwise he adds the `threeDSMethodResult` parameter set to 'N' in the second `verifyEnrollmentRequest`

Authorization

New Request data

When the authentication process is done the merchant issues a doAuthorizationRequest message enhanced with the result of the authentication.

Request fields updates

In order to handle 3DS V2, new fields are required in Authorization

Payline Field Name	Format	Mandatory	Comment
`authentication3DSecure.md`	string	Conditional	Either (md, `pares`) or `resultContainer` must be present. Commonly: • if frictionless, the resultContainer is used, • if challenge, md and pares are used If the merchant didn't provide the md the verifyEnrollment response returned the value determined by Payline.
`authentication3DSecure.pares`	string	Conditional	Either (md, `pares`) or `resultContainer` must be present. Commonly: • if frictionless, the resultContainer is used, • if challenge, md and pares are used **In case of challenge in 3DS V2**, the pares field shall be valued with the content of the CRes received from the ACS
`authentication3DSecure.resultContainer`	string	Conditional	Either (md, `pares`) or `resultContainer` must be present. Commonly: • if frictionless, the resultContainer is used, • if challenge, md and pares are used **In case of frictionless**, this field is constructed from 3DS V2 data by Payline. It contains all data required by Payline to format and process the Authorization. This field is base64 encoded.
`payment.action`	string	Mandatory	This value depends on the payment case the merchant issues.

Other fields has not been modified and should be used as previously.

In the response, two very important fields are added :

Payline Field Name	Format	Mandatory	Comment
linkedTransactionID	string	Conditional	Issuer transaction ID to be used on subsequent Authorization
authentication3DSecure.resultContainer	string	Mandatory	**In case of frictionless**, the field is echoing the request field **In case of challenge**, this field is constructed from 3DS V2 data by Payline. It contains all data required by Payline to format and process the subsequent Authorization.

Other fields has not been modified and should be used as previously.

The message snippet below describes the parameters to be added:

doAuthorizationRequest message snippet : how to valuate the authentication3DSecure object

```
...
<transientData>{JSON}</transientData> <!-- from previous verifYEnrollement call -->
...
<authentication3DSecure>
  <md>2F04CC56F968373D0114AD4B6BB4E4F1</md>

  <!-- In case of challenge, the pares field shall be valued with the content of the CRes received from the
ACS -->
  <!-- In case of 3DS V1, this field shall be valued with the content of the PaRes received from the ACS -->
  <!-- In other cases, this field is left empty -->
  <pares>eJxVUl1vgjAU/SvG99EPaAVzbeJwycyCOpQl28vC...GUY8y9ux4x1+U2M9F3PcY9MxES7HX2BgAyLqh/VdQ
/vK7+fYhfHAOuMA==</pares>

  <!-- In case of frictionless, the resultContainerfield shall be valued with the content of the
resultContainer -->
  <!-- present in the verifyEnrollmentResponse-->
  <!-- In other cases, this field is left empty -->
  <resultContainer>eyAidGhyZWVEU1NlcnZlclRyYW5z....QVTc4MUpiOVZnbHhVZnA1Z0Q4JTNEIiB9</resultContainer>
</authentication3DSecure>
...
```

New response code

Payline will respond with some new codes related to 3DSV2

Code	Comment
01131	Authorization refused, SCA required. Should happened only on "direct to auth"
01132	Recurring payments on the currently used MID are revoked, SCA required.
01133	Recurring payments on all MID are revoked, SCA required.

Linked pages

- 3D Secure 2.0 - Comply with DSP2
- 3DSV2 - Direct Interface - Authentication and Authorization
- 3DSV2 - Functionalities
- 3DSV2 - La liste des impacts Codes retour
- 3DSV2 - La liste des impacts de l'API Payline
- Codes - ChallengeInd
- Codes - threeDSReqPriorAuthMethod
- Object - address

- Object - authentication3DSecure
- Object - browser
- Object - buyer
- Object - merchantAuthentication
- Object - sdk
- Object - threeDSInfo
- Webservice - doAuthorizationRequest