CARDNET

USING LLOYDS BANK ONLINE PAYMENTS WITH EMV 3D SECURE

LLOYDS BANK

Introduction

The e-commerce environment has evolved significantly over the last decade, prompting a refocus to reduce friction in the 3DS transaction experience.

EMVCo in cooperation with major international schemes defined new EMV 3DS / 2.0 specification for the benefit of the entire industry to collaboratively develop the next generation of 3D-Secure protocol. The new version promotes frictionless consumer authentication and enables consumers to authenticate themselves with their card issuer when making card-not-present e-commerce purchases.

EMV 3D-Secure protocol supports app-based authentication and integration with digital wallets, as well as traditional browser-based e-commerce transactions and delivers industry leading security features.

The purpose of this document is to provide you consolidated overview of the implementation in our Gateway.

Light Green text shows what is new compared to how it currently works or represents the elements of high importance.

We recommend to always check xsd files for further information about specific elements:

https://www.ipg-online.com/ipgapi/schemas/ipgapi.xsd

https://www.ipg-online.com/ipgapi/schemas/a1.xsd

https://www.ipg-online.com/ipgapi/schemas/v1.xsd

NOTE: In case you submit 'OrderId' element in your request, please make sure to include only allowed characters: A-Z, a-z, 0-9, "-" Please do not submit 'spaces' in your OrderId request.

SOAP API Authentication with external 3DS Service provider

In case you are using your own/external 3DS Service provider and plan to send authorisation request to the Gateway, you need to submit the authentication values obtained during the authentication you have obtained from your 3DS Service provider.

The following XML document represents an example of a sale transaction submitted to our Gateway after authenticated by external service provider:

```
<?xml version="1.0" encoding="UTF-8"?><ns4:IPGApiOrderRequest
xmlns:ns4="http://ipg-online.com/ipgapi/schemas/ipgapi"
xmlns:ns2="http://ipg-online.com/ipgapi/schemas/a1"
xmlns:ns3="http://ipg-online.com/ipgapi/schemas/v1">
  <ns3:Transaction>
    <ns3:CreditCardTxType>
      <ns3:Type>sale</ns3:Type>
    </ns3:CreditCardTxType>
    <ns3:CreditCardData>
      <ns3:CardNumber>403587XXXXXX4977</ns3:CardNumber>
      <ns3:ExpMonth>12</ns3:ExpMonth>
      <ns3:ExpYear>22</ns3:ExpYear>
      <ns3:CardCodeValue>XXX</ns3:CardCodeValue>
    </ns3:CreditCardData>
    <ns3:CreditCard3DSecure>
      <ns3:AuthenticationValue>jEET5Odser3oCRAyNTY5BVgAAAA=</ns3:AuthenticationValue>
      <ns3:XID>jHDMyjJJF9bLBCFT/YUbqMhoQ0s=</ns3:XID>
      <ns3:Secure3D2TransactionStatus>Y</ns3:Secure3D2TransactionStatus>
      <ns3:Secure3D2AuthenticationResponse>Y</ns3:Secure3D2AuthenticationResponse>
      <ns3:Secure3DProtocolVersion>2.1.0</ns3:Secure3DProtocolVersion>
      <ns3:DirectoryServerTransID>12345678</ns3:DirectoryServerTransID>
    </ns3:CreditCard3DSecure>
    <ns3:Payment>
      <ns3:ChargeTotal>1</ns3:ChargeTotal>
      <ns3:Currency>978</ns3:Currency>
    </ns3:Payment>
    <ns3:TransactionDetails>
      <ns3:OrderId>API-Test-Order123456789</ns3:OrderId>
    </ns3:TransactionDetails>
  </ns3:Transaction>
</ns4:IPGApiOrderRequest>
```

Transaction status values:

Y = Authentication Verification Successful

N = Not Authenticated /Account Not Verified; Transaction denied

U = Authentication/ Account Verification Could Not Be Performed; Technical or other problem, as indicated in ARes or RReq

A = Attempts Processing Performed; Not Authenticated/Verified, but a proof of attempted authentication/verification is provided

C = Challenge Required; Additional authentication is required using the CReq/CRes

D = Challenge Required; Decoupled Authentication confirmed

R = Authentication/ Account Verification Rejected; Issuer is rejecting

The following XML document represents an example of a response:

```
<?xml version="1.0" encoding="UTF-8"?><ipgapi:IPGApiOrderResponse
xmlns:ipgapi="http://ipg-online.com/ipgapi/schemas/ipgapi"
xmlns:a1="http://ipg-online.com/ipgapi/schemas/a1"
xmlns:v1="http://ipg-online.com/ipgapi/schemas/v1">
   <ipgapi:ApprovalCode>Y:282266:8385028528:PPXM:3056131932</ipgapi:ApprovalCode>
   <ipgapi:AVSResponse>PPX</ipgapi:AVSResponse>
   <ipgapi:Brand>VISA</ipgapi:Brand>
   <ipgapi:Country>USA</ipgapi:Country>
   <ipgapi:CommercialServiceProvider>TELECASH</ipgapi:CommercialServiceProvider>
   <ipgapi:OrderId>API-Test-Order123456789</ipgapi:OrderId>
   <ipgapi:IpgTransactionId>8385028528</ipgapi:IpgTransactionId>
   <ipgapi:PaymentType>CREDITCARD</ipgapi:PaymentType>
   <ipgapi:ProcessorApprovalCode>282266</ipgapi:ProcessorApprovalCode>
   <ipgapi:ProcessorReceiptNumber>1932</ipgapi:ProcessorReceiptNumber>
   <ipgapi:ProcessorCCVResponse>M</ipgapi:ProcessorCCVResponse>
   <ipgapi:ProcessorReferenceNumber>55063291</ipgapi:ProcessorReferenceNumber>
   <ipgapi:ProcessorResponseCode>00</ipgapi:ProcessorResponseCode>
   <ipgapi:ProcessorResponseMessage>Function performed error-free</ipgapi:ProcessorResponseMessage>
   <ipgapi:ProcessorTraceNumber>305613</ipgapi:ProcessorTraceNumber>
   <ipgapi:TDate>1553773696</ipgapi:TDate>
   <ipgapi:TDateFormatted>2019.03.28 12:48:16 (CET)</ipgapi:TDateFormatted>
   <ipgapi:TerminalID>54000668</ipgapi:TerminalID>
   <ipgapi:TransactionResult>APPROVED</ipgapi:TransactionResult>
   <ipgapi:TransactionTime>1553773696</ipgapi:TransactionTime>
   <ipgapi:Secure3DResponse>
         <v1:ResponseCode3dSecure>1</v1:ResponseCode3dSecure>
   </ipgapi:Secure3DResponse>
</ipgapi:IPGApiOrderResponse>
```

SOAP API Authentication with Lloyds Bank Online Payments Gateway as 3DS Service provider

In case you use the Gateway for 3DS web based authentication, in the first step you need to submit a verification request with an 'AuthenticateTransaction' parameter set to "true" and indicate which URL the result of the authentication should be sent to with using 'TermUrl' parameter.

If you wish to be notified about 3DSMethod form display completion, you need to submit also optional element "ThreeDSMethodNotificationURL" in your transaction request. The URL should be uniquely identifiable, so when there is a notification received on this URL, you should be able to map it with the corresponding transaction. This eliminates any dependency on the ThreeDSServerTransID, which you will receive with the 3DSMethod form response. An easy way how to ensure correct transaction mapping is to is to pass a transaction reference as a query string. For example:

https://www.mywebshop.com/process3dSecureMethodNotification?transactionReferenceNumber=ffffffff-ba0b-539f-8000-016b2343ad7e

Note: The purpose of 3DSMethod is explained below under Sale transaction example.

In case you would like to influence which authentication flow should be used, you can submit optional "Challenge Indicator" element with one of the values listed below. In case Challenge Indicator is not sent within your transaction request, the Gateway will populate the value "01" – No preference.

Challenge indicator available values for 3DS protocol version 2.1 are:

"01" = No preference (You have no preference whether a challenge should be performed. This is the default value)

"02" = No challenge requested (You prefer that no challenge should be performed.)

"03" = Challenge requested: 3DS Requestor Preference (You prefer that a challenge should be performed)

"04" = Challenge requested: Mandate (There are local or regional mandates that mean that a challenge must be performed)

Note: It is highly recommended to include also Billing and Shipping details in your transaction request to lower the risk of authentication declines. The description of all related optional parameters you can find in the SOAP API Integration Guide, which can be found here – **https://www.lloydsbankcardnet.com/payment-services/online-payments/**

In case you would like to define the size of the challenge window displayed to your customers during authentication process, you can submit optional "Challenge Window Size" element with one of the values listed below.

01 = 250 x 400

02 = 390 x 400

03 = 500 x 600

04 = 600 x 400

05 = Full screen

Note: Based on the payment schemes' observation it is highly recommended to use the value "05 - Full screen" only for browser-based flows. Using full screen mode in app-based flows where the authentication of the cardholder happens on a smartphone or tablet might cause time-outs and trigger an error on issuer/ACS side.

The following XML document represents an example of a Sale transaction request with minimal set of elements:

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope
   xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
   <SOAP-ENV:Header/>
   <SOAP-ENV:Body>
      <ns4:IPGApiOrderRequest
         xmlns:ns4="http://ipg-online.com/ipgapi/schemas/ipgapi"
         xmlns:ns2="http://ipg-online.com/ipgapi/schemas/v1"
         xmlns:ns3="http://ipg-online.com/ipgapi/schemas/a1">
         <ns2:Transaction>
            <ns2:CreditCardTxType>
               <ns2:StoreId>120995000</ns2:StoreId>
               <ns2:Type>sale</ns2:Type>
            </ns2:CreditCardTxType>
            <ns2:CreditCardData>
               <ns2:CardNumber>542606XXXXXX4979</ns2:CardNumber>
               <ns2:ExpMonth>12</ns2:ExpMonth>
               <ns2:ExpYear>24</ns2:ExpYear>
               <ns2:CardCodeValue>XXX</ns2:CardCodeValue>
            </ns2:CreditCardData>
            <ns2:CreditCard3DSecure>
               <ns2:AuthenticateTransaction>true</ns2:AuthenticateTransaction>
               <ns2:TermUrl>https://www.mywebshop.com/process3dSecure...</ns2:TermUrl>
               <ns2:ThreeDSMethodNotificationURL>https://www.mywebshop.com/process3dSecureMethodNotification?transactionReferenceNumber=ffffffff-ba0b-539f-8000-016b2343ad7e</ns2:ThreeDSMethodNotificationURL>
               <ns2:ThreeDSRequestorChallengeIndicator>01</ns2:ThreeDSRequestorChallengeIn dicator>
               <ns2:ThreeDSRequestorChallengeWindowSize>01</ns2:ThreeDSRequestorChallengeWindowSize>
            </ns2:CreditCard3DSecure>
            <ns2:Payment>
               <ns2:ChargeTotal>13.99</ns2:ChargeTotal>
               <ns2:Currency>978</ns2:Currency>
            </ns2:Payment>
         </ns2:Transaction>
      </ns4:IPGApiOrderRequest>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

The response from the Gateway contains '3DSMethod' element, which generates hidden iframe that helps to collect the browser data for the issuers. This information adds to the overall consumer profile and helps in identifying potentially fraudulent transactions.

You need to include the 3DSMethod in your website as hidden iframe. No user interface screen is presented to the cardholder.

The following XML document represents an example of a response:

```
<?xml version="1.0" encoding="UTF-8"?>
  <SOAP-ENV:Envelope
  xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
      <ipgapi:IPGApiOrderResponse
          xmlns:ipgapi="http://ipg-online.com/ipgapi/schemas/ipgapi"
          xmlns:a1="http://ipg-online.com/ipgapi/schemas/a1"
          xmlns:v1="http://ipg-online.com/ipgapi/schemas/v1">
          <ipgapi:ApprovalCode>?:waiting 3dsecure method</ipgapi:ApprovalCode>
          <ipgapi:Brand>MASTERCARD</ipgapi:Brand>
          <ipgapi:CommercialServiceProvider>RESELLER</ipgapi:CommercialServiceProvider>
          <ipgapi:OrderId>A-4b9804e6410b84475809e59e1b26</ipgapi:OrderId>
          <ipgapi:IpgTransactionId>8383394827</ipgapi:IpgTransactionId>
          <ipgapi:PaymentType>CREDITCARD</ipgapi:PaymentType>
          <ipgapi:TDate>1493130774</ipgapi:TDate>
          <ipgapi:TDateFormatted>2017.04.25 16:32:54(CEST)</ipgapi:TDateFormatted>
          <ipgapi:TransactionTime>1493130774</ipgapi:TransactionTime>
          <ipgapi:Secure3DResponse>
              <v1:Secure3DMethod>
                  <v1:Secure3DMethodForm>
&lt;!DOCTYPE iframe SYSTEM "about:legacy-compat"&gt;
&lt;iframe id="tdsMmethodTgtFrame" name="tdsMmethodTgtFrame" style="width: 1px;
height: 1px; display:
none;" src="javascript:false;" xmlns="http://www.w3.org/1999/xhtml"&gt;
&lt;!--.--&gt;
&lt;/iframe&gt;&lt;form id="tdsMmethodForm" name="tdsMmethodForm"
action="https://localhost.modirum.com:8543/dstests/ACSEmu2" method="post"
target="tdsMmethodTgtFrame"
xmlns="http://www.w3.org/1999/xhtml"&gt;
&lt;input type="hidden" name="3DSMethodData"
value="eyAidGhyZWVEU1NlcnZlclRyYW5zSUQiIDogIjAwMDAwMDAwLTU2NzYtNTY2My04MDAwLTAwMDA
w&amp;#10;MDAwNDFhOSIsICJ0aHJlZURTTWV0aG9kTm90aWZpY2F0aW9uVVJMIiA6ICJodHRwczovL2xvY
2Fs&amp;#10;aG9zdC5tb2RpcnVtLmNvbTo4NTQzL21kcGF5bXBpL01lcmNoYW50U2VydmVyP21uPVkmd
HhpZD0x&amp;#10;NjgwOSZkaWdlc3Q9aSUyQnhhUEF5NWFOcVJRbllqNmozbWFDZlFJbTdFdjJYTmkwNn
h6YmZNJTJG&amp;#10;R3MlM0QiIH0"/&gt;
&lt;input type="hidden" name="threeDSMethodData"
value="eyAidGhyZWVEU1NlcnZlclRyYW5zSUQiIDogIjAwMDAwMDAwLTU2NzYtNTY2My04MDAwLTAwMDA
w&amp;#10;MDAwNDFhOSIsICJ0aHJlZURTTWV0aG9kTm90aWZpY2F0aW9uVVJMIiA6ICJodHRwczovL2xvY
2Fs&amp;#10;aG9zdC5tb2RpcnVtLmNvbTo4NTQzL21kcGF5bXBpL01lcmNoYW50U2VydmVyP21uPVkmd
HhpZD0x&amp;#10;NjgwOSZkaWdlc3Q9aSUyQnhhUEF5NWFOcVJRbllqNmozbWFDZlFJbTdFdjJYTmkwNn
h6YmZNJTJG&amp;#10;R3MlM0QiIH0"/&gt;
&lt;/form&gt;&lt;script type="text/javascript" xmlns="http://www.w3.org/1999/xhtml"&gt;
document.getElementById("tdsMmethodForm").submit();
&lt;/script&gt;
                  </v1:Secure3DMethodForm>
          <v1:ThreeDSServerTransID>3ac7caa7-aa42-2663-791b-2ac05a542c4a</v1:ThreeDSServerTransID>
              </v1:Secure3DMethod>
          </ipgapi:Secure3DResponse>
      </ipgapi:IPGApiOrderResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Frictionless Flow

When a transaction is considered to be a low risk transaction or an exemption is requested, a frictionless flow is applied. In such case the Gateway proceeds with the authorisation without additional authentication of the cardholder.

Once the 3DS Method call has been completed, you need to notify the Gateway that the authentication process can continue by submitting the '**Secure3DMethodNotificationStatus**' element with the values based on corresponding conditions:

- **Secure3DMethodNotificationStatus** = "RECEIVED" in case you have submitted the element ThreeDSMethodNotificationURL in the initial Sale transaction request and have received the notification from ACS within 10 seconds, you will receive HTTP POST message from ACS, which will contain a unique transaction identifier represented by threeDSServerTransID
- **Secure3DMethodNotificationStatus** = "EXPECTED_BUT_NOT_RECEIVED" in case you have submitted the element ThreeDSMethodNotificationURL in the initial Sale transaction request and **have not** received the notification from ACS within 10 seconds

- **Secure3DMethodNotificationStatus** = "NOT_EXPECTED" in case you have NOT submitted the element ThreeDSMethodNotificationURL in the initial Sale transaction request.

The following XML document represents an example of a request to be sent after 3DSMethod form display:

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope
  xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
      <ns4:IPGApiOrderRequest
            xmlns:ns4="http://ipg-online.com/ipgapi/schemas/ipgapi"
            xmlns:ns2="http://ipg-online.com/ipgapi/schemas/v1"
            xmlns:ns3="http://ipg-online.com/ipgapi/schemas/a1">
            <ns2:Transaction>
                  <ns2:CreditCardTxType>
                        <ns2:StoreId>120995000</ns2:StoreId>
                        <ns2:Type>sale</ns2:Type>
                  </ns2:CreditCardTxType>
                  <ns2:CreditCard3DSecure>
                        <ns2:Secure3DMethodNotificationStatus>RECEIVED</ns2: Secure3DMethodNotificationStatus>
                  </ns2:CreditCard3DSecure>
                  <ns2:TransactionDetails>
                        <ns2:IpgTransactionId>8383394827</ns2:IpgTransactionId>
                  </ns2:TransactionDetails>
            </ns2:Transaction>
      </ns4:IPGApiOrderRequest>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

The following XML document represents an example of a response you receive from the Gateway indicating, that the authorisation has been successful:

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope
  xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
      <ipgapi:IPGApiOrderResponse
            xmlns:ipgapi="http://ipg-online.com/ipgapi/schemas/ipgapi"
            xmlns:a1="http://ipg-online.com/ipgapi/schemas/a1"
            xmlns:v1="http://ipg-online.com/ipgapi/schemas/v1">
            <ipgapi:ApprovalCode>Y:416502:0014750513:PPXM:4625106408</ipgapi:ApprovalCode>
            <ipgapi:AVSResponse>PPX</ipgapi:AVSResponse>
            <ipgapi:Brand>VISA</ipgapi:Brand>
            <ipgapi:OrderId>A-52421c39-69c4-4b2d-959d-9fdcd3a9420a</ipgapi:OrderId>
            <ipgapi:PaymentType>CREDITCARD</ipgapi:PaymentType>
            <ipgapi:ProcessorApprovalCode>416502</ipgapi:ProcessorApprovalCode>
            <ipgapi:ProcessorReceiptNumber>6408</ipgapi:ProcessorReceiptNumber>
            <ipgapi:ProcessorCCVResponse>M</ipgapi:ProcessorCCVResponse>
            <ipgapi:ProcessorTraceNumber>462510</ipgapi:ProcessorTraceNumber>
            <ipgapi:ReferencedTDate>1407373209</ipgapi:ReferencedTDate>
            <ipgapi:TDate>1407373209</ipgapi:TDate>
            <ipgapi:TDateFormatted>2014.08.07 03:00:09 (CEST)</ipgapi:TDateFormatted>
            <ipgapi:TerminalID>54000666</ipgapi:TerminalID>
            <ipgapi:Secure3DResponse>
                  <v1:ResponseCode3dSecure>1</v1:ResponseCode3dSecure>
            </ipgapi:Secure3DResponse>
      </ipgapi:IPGApiOrderResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Challenge Flow

This flow is triggered, when the transaction is not considered as low risk or in case the issuer requires additional authentication of the cardholder. The whole process starts with initial Sale transaction request (page 3) until the step where 3DS Method is displayed.

Once the 3DS Method call has been completed, you need to notify the Gateway that the authentication process can continue by submitting the 'Secure3DMethodNotificationStatus' element with the values based on corresponding conditions:

- **Secure3DMethodNotificationStatus** = "**RECEIVED**" in case you have submitted the element ThreeDSMethodNotificationURL in the initial Sale transaction request (page 3) and have received the notification from ACS within 10 seconds, you will receive HTTP POST message from ACS, which will contain a unique transaction identifier represented by threeDSServerTransID
- **Secure3DMethodNotificationStatus** = "**EXPECTED_BUT_NOT_RECEIVED**" in case you have submitted the element ThreeDSMethodNotificationURL in the initial Sale transaction request (page 3) and **have not** received the notification from ACS within 10 seconds
- **Secure3DMethodNotificationStatus** = "**NOT_EXPECTED**" in case you have NOT submitted the element ThreeDSMethodNotificationURL in the initial Sale transaction request (page 3)

The following XML document represents an example of a request:

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope
  xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
      <ns4:IPGApiOrderRequest
            xmlns:ns4="http://ipg-online.com/ipgapi/schemas/ipgapi"
            xmlns:ns2="http://ipg-online.com/ipgapi/schemas/v1"
            xmlns:ns3="http://ipg-online.com/ipgapi/schemas/a1">
                  <ns2:Transaction>
                  <ns2:CreditCardTxType>
                        <ns2:StoreId>120995000</ns2:StoreId>
                        <ns2:Type>sale</ns2:Type>
                  </ns2:CreditCardTxType>
                  <ns2:CreditCard3DSecure>
                        <ns2:Secure3DMethodNotificationStatus>RECEIVED</ns2: Secure3DMethodNotificationStatus>
                  </ns2:CreditCard3DSecure>
                  <ns2:TransactionDetails>
                        <ns2:IpgTransactionId>8383394827</ns2:IpgTransactionId>
                  </ns2:TransactionDetails>
            </ns2:Transaction>
      </ns4:IPGApiOrderRequest>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Our Gateway verifies the response and provides the result back to you, including the challenge result data.

The following XML document represents an example of a response:

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope
  xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
      <ipgapi:IPGApiOrderResponse
            xmlns:ipgapi="http://ipg-online.com/ipgapi/schemas/ipgapi"
            xmlns:a1="http://ipg-online.com/ipgapi/schemas/a1"
            xmlns:v1="http://ipg-online.com/ipgapi/schemas/v1">
            <ipgapi:ApprovalCode>?:waiting 3dsecure</ipgapi:ApprovalCode>
            <ipgapi:Brand>MASTERCARD</ipgapi:Brand>
            <ipgapi:CommercialServiceProvider>AIBMS</ipgapi:CommercialServiceProvider>
            <ipgapi:OrderId>A-4b9804e6410b84475809e59e1b26</ipgapi:OrderId>
            <ipgapi:IpgTransactionId>8383394827</ipgapi:IpgTransactionId>
            <ipgapi:PaymentType>CREDITCARD</ipgapi:PaymentType>
            <ipgapi:TDate>1493130774</ipgapi:TDate>
            <ipgapi:TDateFormatted>2017.04.25 16:32:54(CEST)</ipgapi:TDateFormatted>
            <ipgapi:TransactionTime>1493130774</ipgapi:TransactionTime>
            <ipgapi:Secure3DResponse>
                  <v1:Secure3DVerificationResponse>
                        <v1:VerificationRedirectResponse>
                              <v1:AcsURL>https://3ds-acs.test.modirum.com/mdpayacs/pareq</v1:AcsURL>
                              <v1:CReq>ewogICAiYWNzVHJhbCIgOiA...wMDAtMDAwMDAwMDA0MWE5Igp9</v1:CReq>
                              <v1:TermUrl>https://www.mywebshop.com/process3dSecure/</v1:TermUrl>
                              <v1:ThreeDSSessionData>50F2156E03083CA665BCB4..</v1:ThreeDSSessionData>
                        </v1:VerificationRedirectResponse>
                  </v1:Secure3DVerificationResponse>
            </ipgapi:Secure3DResponse>
      </ipgapi:IPGApiOrderResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

In the next step you need to POST the data to the indicated URL usually implemented as auto-submit form. This needs to be implemented within your website. The cardholders will be redirected to the ACS and presented with the UI to collect the authentication details – for example enter one-time-password or perform authentication using their banking app (out-of-band authentication). After authentication completion the consumer is redirected back to your webpage.

After you receive the data from the ACS you need to submit them to the Gateway in 'CRes' element together with the reference to the original transaction.

The following XML document represents an example of a request with CRes element:

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope
  xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
      <ns4:IPGApiOrderRequest
            xmlns:ns4="http://ipg-online.com/ipgapi/schemas/ipgapi"
            xmlns:ns2="http://ipg-online.com/ipgapi/schemas/v1"
            xmlns:ns3="http://ipg-online.com/ipgapi/schemas/a1">
            <ns2:Transaction>
                  <ns2:CreditCardTxType>
                        <ns2:StoreId>120995000</ns2:StoreId>
                        <ns2:Type>sale</ns2:Type>
                  </ns2:CreditCardTxType>
                  <ns2:CreditCard3DSecure>
                        <ns2:Secure3DRequest>
                              <ns2:Secure3DAuthenticationRequest>
                        <ns2:AcsResponse>
                              <ns2:CRes>ewogICAiYWNzUmVmZX...Fuc1N0YXR...IKfQ==</ns2:CRes>
                         </ns2:AcsResponse>
                  </ns2:Secure3DAuthenticationRequest>
                  </ns2:Secure3DRequest>
            </ns2:CreditCard3DSecure>
            <ns2:TransactionDetails>
                  <ns2:IpgTransactionId>8383394827</ns2:IpgTransactionId>
            </ns2:TransactionDetails>
      </ns2:Transaction>
      </ns4:IPGApiOrderRequest>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Since this transaction was initiated as Sale, the authorisation is performed as part of this step if the authentication was successful.

The following XML document represents an example of a response you receive from the Gateway indicating, that the authorisation has been successful:

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope
  xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
      <ipgapi:IPGApiOrderResponse
            xmlns:ipgapi="http://ipg-online.com/ipgapi/schemas/ipgapi"
            xmlns:a1="http://ipg-online.com/ipgapi/schemas/a1"
            xmlns:v1="http://ipg-online.com/ipgapi/schemas/v1">
            <ipgapi:ApprovalCode>Y:416502:0014750513:PPXM:4625106408</ipgapi:ApprovalCode>
            <ipgapi:AVSResponse>PPX</ipgapi:AVSResponse>
            <ipgapi:Brand>VISA</ipgapi:Brand>
            <ipgapi:OrderId>A-52421c39-69c4-4b2d-959d-9fdcd3a9420a</ipgapi:OrderId>
            <ipgapi:PaymentType>CREDITCARD</ipgapi:PaymentType>
            <ipgapi:ProcessorApprovalCode>416502</ipgapi:ProcessorApprovalCode>
            <ipgapi:ProcessorReceiptNumber>6408</ipgapi:ProcessorReceiptNumber>
            <ipgapi:ProcessorCCVResponse>M</ipgapi:ProcessorCCVResponse>
            <ipgapi:ProcessorTraceNumber>462510</ipgapi:ProcessorTraceNumber>
            <ipgapi:ReferencedTDate>1407373209</ipgapi:ReferencedTDate>
            <ipgapi:TDate>1407373209</ipgapi:TDate>
            <ipgapi:TDateFormatted>2014.08.07 03:00:09 (CEST)</ipgapi:TDateFormatted>
            <ipgapi:TerminalID>54000666</ipgapi:TerminalID>
            <ipgapi:Secure3DResponse>
                  <v1:ResponseCode3dSecure>1</v1:ResponseCode3dSecure>
            </ipgapi:Secure3DResponse>
      </ipgapi:IPGApiOrderResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Fallback to 3DS 1.0 protocol

For cases, where issuers do not support 2.x 3DS protocol version yet, the Gateway provides an option to "downgrade" to 3DS 1.0 authentication instead.

In the first step you submit Sale transaction request as for 2.x version:

```
<?xml version="1.0" encoding="UTF-8"?><SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/">
   <SOAP-ENV:Header/>
   <SOAP-ENV:Body>
         <ns3:IPGApiOrderRequest
xmlns:ns3="http://ipg-online.com/ipgapi/schemas/ipgapi"
xmlns:ns2="http://ipg-online.com/ipgapi/schemas/v1"
xmlns:ns4="http://ipg-online.com/ipgapi/schemas/a1">
                  <ns2:Transaction>
                        <ns2:CreditCardTxType>
                              <ns2:StoreId>120995000</ns2:StoreId>
                              <ns2:Type>sale</ns2:Type>
                        </ns2:CreditCardTxType>
                        <ns2:CreditCardData>
                              <ns2:CardNumber>542606XXXXXX4979</ns2:CardNumber>
                              <ns2:ExpMonth>12</ns2:ExpMonth>
                              <ns2:ExpYear>33</ns2:ExpYear>
                              <ns2:CardCodeValue>XXX</ns2:CardCodeValue>
                              </ns2:CreditCardData>
                        <ns2:CreditCard3DSecure>
                              <ns2:AuthenticateTransaction>true</ns2:AuthenticateTransaction>
                              <ns2:TermUrl>https://www.mywebshop.com/process3dSecure</ns2:TermUrl>
                              <ns2:ThreeDSMethodNotificationURL>https://www.mywebshop.com/process3dSecureMethodNotification</ns2:
                              ThreeDSMethodNotificationURL>
                              <ns2:ThreeDSRequestorChallengeIndicator>1</ns2:ThreeDSRequestorChallengeIndicator>
                        </ns2:CreditCard3DSecure>
                        <ns2:Payment>
                              <ns2:ChargeTotal>13.99</ns2:ChargeTotal>
                              <ns2:Currency>978</ns2:Currency>
                        </ns2:Payment>
                  </ns2:Transaction>
         </ns3:IPGApiOrderRequest>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

As soon as our 3DServer identifies, that used credit card is not eligible for 2.x protocol, the Gateway automatically initiate fallback request and redirect to the dedicated DS and ACS.

The Gateway then checks the card participation from the 3D Secure directory and returns the redirection URL of the card issuer's Access Control Server (ACS).

If the card is enrolled in 3D Secure 1.0, the response contains the following key values:

- PaReq: The Payer Authentication Request, required to initiate the authentication
- ACS URL: The target of 3D Secure redirection
- Term URL: The URL, that the ACS should send the outcome to in your application
- MD: Merchant Data which have to be sent to ACS URL

Please note, that there might be cases, when MD element is not present in the response and its presence does not have to be validated in the next step.

The following represents an example of a response:

```
<?xml version="1.0" encoding="UTF-8"?>
<ipgapi:IPGApiOrderResponse
xmlns:ipgapi="http://ipg-online.com/ipgapi/schemas/ipgapi"
xmlns:a1=http://ipg-online.com/ipgapi/schemas/a1
xmlns:v1="http://ipg-online.com/ipgapi/schemas/v1">
   <ipgapi:ApprovalCode>?:waiting 3dsecure</ipgapi:ApprovalCode>
   <ipgapi:Brand>MASTERCARD</ipgapi:Brand>
   <ipgapi:Country>DEU</ipgapi:Country>
   <ipgapi:CommercialServiceProvider>TELECASH
   </ipgapi:CommercialServiceProvider>
   <ipgapi:OrderId>A-9278d36a-0cb1-4b6a-918b-34c723c41c6a</ipgapi:OrderId>
   <ipgapi:IpgTransactionId>84514040874</ipgapi:IpgTransactionId>
   <ipgapi:PaymentType>CREDITCARD</ipgapi:PaymentType>
   <ipgapi:TDate>1505997548</ipgapi:TDate>
   <ipgapi:TDateFormatted>2017.09.21 14:39:08 (CEST)
   </ipgapi:TDateFormatted>
   <ipgapi:TransactionTime>1505997548</ipgapi:TransactionTime>
   <ipgapi:Secure3DResponse>
         <v1:Secure3DVerificationResponse>
               <v1:VerificationRedirectResponse>
                     <v1:AcsURL>https://3ds-acs.test.modirum.com/mdpayacs/pareq</v1:AcsURL>
                     <v1:PaReq>
               eJxVUslugzAQZUodzA2iCWaWEqzNaraRoFeenPMqFAFQgxk+fvahCz1xfPe2M8zbwxJphBnMcpW3rGvxg4M8HQ8nVsSCMHV9YTlySy1vq6OIhlv
               L9WTAXOlR6YtqyGE92eCBwxFVne9LTm3HZkBuUIsqmYmy4SDk4WX1wWm3gPQQClSrGS/
               y9Ja4ElCKAvlqvRwk8zgZxMnnZg6kI0Hu27JRF84CH8gNQKt2PGuaqh4Rcjqd7AZ3KEWd2SkCMUkgj2LWrVlqLXbOUx691d/L33N8PLDjbHoJg1KxxeLrNVqEYy
               DmBKSiQc4cGjgRowPKRm40ckIgHQ+iMFVwyhxHd3YFUJk3Js+ZZwa06QpLeeFRoHXuCPBc7UvUJ7SN9xhSrKXuoN8e5U9fjbOy0Zax0Pc8XZ3xtiOMVG588uh
               VywAg5grpx0b6oevo32f4A8WErtw=
                     </v1:PaReq>
                     <v1:TermUrl> https://www.mywebshop.com/process3dSecure</v1:TermUrl>
                     <v1:MD>MD_120020170921123.....f1f3-4768-998f </v1:MD>
               </v1:VerificationRedirectResponse>
         </v1:Secure3DVerificationResponse>
   </ipgapi:Secure3DResponse>
</ipgapi:IPGApiOrderResponse>
```

After you have redirected the cardholder for authentication and have received the payer authentication response (PARes) from the card issuer, you submit the PARes and MD (if present) in your next request to our API:

```
<?xml version="1.0" encoding="UTF-8"?>
<ipg:IPGApiOrderRequest xmlns:ipg="http://ipg-online.com/ipgapi/schemas/ipgapi">
   <v1:Transaction xmlns:v1="http://ipg-online.com/ipgapi/schemas/v1">
         <v1:CreditCardTxType>
               <v1:StoreId>120995000</v1:StoreId>
               <v1:Type>sale</v1:Type>
         </v1:CreditCardTxType>
         <v1:CreditCard3DSecure>
               <v1:Secure3DRequest>
                     <v1:Secure3DAuthenticationRequest>
                           <v1:AcsResponse>
                                 <v1:MD>MD_1200201709211deP2Yur.....8b64-f1f3-4768-998f</v1:MD>
                                 <v1:PaRes>eJzVWE.....v9/X/LjJebtlfrsCf70Y/flq/P8ARjWe/A==</v1:PaRes>
                           </v1:AcsResponse>
                     </v1:Secure3DAuthenticationRequest>
               </v1:Secure3DRequest>
   </v1:CreditCard3DSecure>
         <v1:TransactionDetails>
               <v1:IpgTransactionId>84514043377</v1:IpgTransactionId>
         </v1:TransactionDetails>
   </v1:Transaction>
</ipg:IPGApiOrderRequest>
```

Our Gateway verifies the response and provides the result back to you:

```
<?xml version="1.0" encoding="UTF-8"?><ipgapi:IPGApiOrderResponse
xmlns:ipgapi="http://ipg-online.com/ipgapi/schemas/ipgapi"
xmlns:a1="http://ipg-online.com/ipgapi/schemas/a1"
xmlns:v1="http://ipg-online.com/ipgapi/schemas/v1">
<ipgapi:ApprovalCode>Y:282266:8385028528:PPXM:3056131932</ipgapi:ApprovalCode>
<ipgapi:AVSResponse>PPX</ipgapi:AVSResponse>
<ipgapi:Brand>VISA</ipgapi:Brand>
<ipgapi:Country>USA</ipgapi:Country>
<ipgapi:CommercialServiceProvider>TELECASH</ipgapi:CommercialServiceProvider>
<ipgapi:OrderId>API-Test-Order123456789</ipgapi:OrderId>
<ipgapi:IpgTransactionId>8385028528</ipgapi:IpgTransactionId>
<ipgapi:PaymentType>CREDITCARD</ipgapi:PaymentType>
<ipgapi:ProcessorApprovalCode>282266</ipgapi:ProcessorApprovalCode>
<ipgapi:ProcessorReceiptNumber>1932</ipgapi:ProcessorReceiptNumber>
<ipgapi:ProcessorCCVResponse>M</ipgapi:ProcessorCCVResponse>
<ipgapi:ProcessorReferenceNumber>55063291</ipgapi:ProcessorReferenceNumber>
<ipgapi:ProcessorResponseCode>00</ipgapi:ProcessorResponseCode>
<ipgapi:ProcessorResponseMessage>Function performed error-free</ipgapi:ProcessorResponseMessage>
<ipgapi:ProcessorTraceNumber>305613</ipgapi:ProcessorTraceNumber>
<ipgapi:TDate>1553773696</ipgapi:TDate>
<ipgapi:TDateFormatted>2019.03.28 12:48:16 (CET)</ipgapi:TDateFormatted>
<ipgapi:TerminalID>54000668</ipgapi:TerminalID>
<ipgapi:TransactionResult>APPROVED</ipgapi:TransactionResult>
<ipgapi:TransactionTime>1553773696</ipgapi:TransactionTime>
<ipgapi:Secure3DResponse>
  <v1:ResponseCode3dSecure>1</v1:ResponseCode3dSecure>
</ipgapi:Secure3DResponse>
</ipgapi:IPGApiOrderResponse>
```

Authentication with Lloyds Bank Online Payments Gateway as 3DS Service provider via Connect

The Connect solution includes the ability to authenticate transactions using Verified by Visa and MasterCard Identity Check programs. If your credit card agreement includes 3D Secure and your Merchant ID has been activated to use this service, you do not need to modify your payment page.

The following represents an example of a 'Sale' transaction request with minimum set of fields including optional "Challenge Indicator" element, which can be used to request an exemption:

```
<!-- #include file="ipg-util.asp"-->
<html>
<head><title>IPG Connect Sample for ASP</title></head>
<body>
<p><h1>Order Form</h1></p>

<form method="post" action=" https://test.ipg-online.com/connect/gateway/processing ">
        <input type="hidden" name="txntype" value="sale">
        <input type="hidden" name="timezone" value="Europe/Berlin"/>
        <input type="hidden" name="txndatetime" value="<% getDateTime() %>"/>
        <input type="hidden" name="hash_algorithm" value="SHA256"/>
        <input type="hidden" name="hash" value="<% call createHash( "13.00","978" ) %>"/>
        <input type="hidden" name="storename" value="110995000" />
        <input type="hidden" name="mode" value="payonly"/>
        <input type="hidden" name="paymentMethod" value="V"/>
        <input type="text" name="chargetotal" value="13.00" />
        <input type="hidden" name="currency" value="978"/>
        <input type="hidden" name="authenticateTransaction" value="true"/>
        <input type="text" name="threeDSRequestorChallengeIndicator" value="1"/>
        <input type="submit" value="Submit">
</form>
</body>
</html>
```

Challenge indicator available values for 3DS protocol version 2.1 are:

01 = No preference (You have no preference whether a challenge should be performed. This is the default value)

02 = No challenge requested (You prefer that no challenge should be performed)

03 = Challenge requested: 3DS Requestor Preference (You prefer that a challenge should be performed)

04 = Challenge requested: Mandate (There are local or regional mandates that mean that a challenge must be performed)

In case you have not used billing and shipping details in your authentication request before, please consider to include below listed optional parameters to lower the 3D Secure authentication declines.

Field name	Possible values	Description
bname	Alphanumeric characters, spaces and dashes	Customers Name
bcity	Limit of 96 characters, including spaces	Billing City
bcountry	2 Letter Country Code	Country of Billing Address
baddr1	Limit of 96 characters, including spaces	Customer Billing Address 1
baddr2	Limit of 96 characters, including spaces	Customer Billing Address 2
bzip	Limit of 24 characters, including spaces	Zip or Postal Code
bstate	Limit of 96 characters, including spaces	State, Province or Territory
email	Limit of 254 Characters	Customers Email Address
phone	Limit of 32 Characters	Customers Phone Number
cellphone	Limit of 32 Characters	Customers Phone Number
scity	Limit of 96 characters, including spaces	Shipping City
scountry	2 Letter Country Code	Country of Shipping Address
saddr1	Limit of 96 characters, including spaces	Shipping Address Line 1
saddr2	Limit of 96 characters, including spaces	Shipping Address Line 2
szip	Limit of 24 characters, including spaces	Zip or Postal Code
sstate	Limit of 96 characters, including spaces	State, Province or Territory

The result of the transaction will be sent back to the defined 'responseSuccessURL' or 'responseFailURL' as hidden fields:

{txndate_processed=12/04/10 13:37:33,

ccbin=542606,

timezone=CET,

oid=C-2101f68a-45e9-4f3c-a6da-1337d5574717,

cccountry=N/A,

expmonth=12,

currency=978,

chargetotal=13.99,

approval_code=Y:ECI2/5:Authenticated,

hiddenSharedsecret=sharedsecret,

hiddenTxndatetime=2019:04:10-13:37:08,

expyear=2024,

response_hash=927d3c3108d596c593f74fd79184ece7c33103fe,

response_code_3dsecure=1,

hiddenStorename=12345678,

transactionNotificationURL=https://test.ipg-online.com/webshop/transactionNotification,

tdate=1554903428,

ignore_refreshTime=on,

ccbrand=VISA,

txntype=sale,

paymentMethod=V,

txndatetime=2019:04:10-13:37:08,

cardnumber=(VISA) ... 4979,

ipgTransactionId=84120276797,

status=APPROVED}

Contact us

New Customers

0345 60 44 635
Lines are open 9am to 5pm Monday to Friday

cardnetsalescentre@lloydsbanking.com

Trade Associations

0345 60 44 635
Lines are open 9am to 5pm Monday to Friday

Existing Customers

01268 567 100
Lines are open 8am to 5pm Monday to Saturday

cardnet_sales@lloydsbanking.com

By Post

Cardnet Merchant Services
Phoenix House, Christopher Martin Road
Basildon, Essex SS14 3EZ

Important information

Please remember we cannot guarantee the security of messages sent by email.

Lloyds Bank plc is covered by the Financial Ombudsman Service. (Please note that due to the eligibility criteria of this scheme not all Lloyds Bank customers will be covered.)

This information is correct as of August 2020.

LLOYDS BANK

CRD00155 (08/20)