Integration Guide 3D Secure

Unzer E-Com GmbH, Vangerowstraße 18, D 69115 Heidelberg, Registergericht: Amtsgericht Mannheim, HRB 337681, Geschäftsführer: Mirko Hüllemann, Dr. Axel Rebien, Fatih Bektas, zuständige Aufsichtsbehörde: Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Graurheindorfer Str. 108, 53117 Bonn
www.unzer.com

Integration Guide 3D Secure

From 01.01.2021 on two-factor authentication will be implemented as a mandatory requirement for all ecommerce card payment transactions. In order to comply with this obligation, the operators of credit card networks will use the so called 3D Secure procedure. For you as a merchant it is mandatory to be able to carry out this procedure for your customers from 01.01.2021. In the following you will find a description of the different ways of integration and how the 3D Secure procedure has to be implemented for them.

Please select the integration method you use

- Are you using the checkout form hCO?
- Are you using the checkout form hPF?
- Do you process payments without using a form provided by the Unzer system?

Please note: It is also important in which way debits or preauthorisations (reservations) are made. Even if you use a payment form from Unzer GmbH for the registration of card data, the 3D Secure process will be carried out without a checkout form when the card data are first debited or authorised for the first time. In this case the third way of integration without a form provided by Unzer applies.

Please note also:
If you use recurring payments (subscription payments), be sure to read the section "3D Secure and Recurring Payment".

3D Secure procedure when using the hCO checkout form

The hCO checkout form is already designed for the 3D Secure procedure. There is no additional action from your side needed for the implementation of the procedure. However, you have to make sure that your system can handle the corresponding answers of our payment system in case the 3D Secure process is started. In the asynchronous response from the payment system to your server, the result of the transaction is transmitted and must be evaluated there before a return URL is transmitted to the payment system.

For this purpose the following parameters must be evaluated.

- PROCESSING.RETURN.CODE = 000.200.000
- PROCESSING.RETURN = Transaction+pending
- PROCESSING.RESULT = ACK

Explanation: The status of the transaction is "pending", the parameter PROCESSING.RESULT represents only a preliminary result. As long as the 3D Secure process is carried out, the status remain pending.

The final result of the transaction is then either

- PROCESSING.RETURN.CODE = 000.000.000
- PROCESSING.RESULT = ACK

or

- PROCESSING.RETURN.CODE = irgendein Wert ungleich 000.000.000 oder 000.200.000
- PROCESSING.RESULT = NOK

In the first case the transaction has been successfully completed, in the second case it has failed overall. The latter can have various reasons, including a refusal to authenticate. You will

receive more detailed information in the parameters "PROCESSING.RETURN" and "PROCESSING.RETURN.CODE".

We recommend that you run a test for both messages. For more information on how to do a test and which credit card details you can use for a test, please see below.

3D Secure procedure when using the hPF checkout form

The hPF checkout form is also designed to use the 3DS procedure already. There is no additional action from your side needed for the implementation of the procedure. As described for the hCO implementation the response from the payment system takes place in two steps, which is why your system must check the value of the PROCESSING.RETURN.CODE parameter when processing the response.

For this purpose the following parameters must be evaluated.

- PROCESSING.RETURN.CODE = 000.200.000
- PROCESSING.RETURN = Transaction+pending
- PROCESSING.RESULT = ACK

Explanation: The status of the transaction is "pending", the parameter PROCESSING.RESULT represents only a preliminary result. As long as the 3D Secure process is carried out, the status remain pending.

The final result of the transaction is then either

- PROCESSING.RETURN.CODE = 000.000.000
- PROCESSING.RESULT = ACK

or

- PROCESSING.RETURN.CODE = irgendein Wert ungleich 000.000.000 oder 000.200.000
- PROCESSING.RESULT = NOK

In the first case the transaction has been successfully completed, in the second case it has failed overall. The latter can have various reasons, including a refusal to authenticate. You will receive more detailed information in the parameters "PROCESSING.RETURN" and "PROCESSING.RETURN.CODE".

We recommend that you run a test for both messages. For more information on how to do a test and which credit card details you can use for a test, please see below.

3D Secure procedure with direct connection

If you do not use a payment form provided by Unzer (formerly heidelpay) to process credit card payments, or if you simply register a card using one of the forms and process the preauthorisation (reservation) or debit as a reference to the registration as a direct communication with the payment system, you must implement the 3D Secure process.

Asynchronous transaction flow:
This is an asynchronous process in which your server receives a forwarding URL (Redirect URL) from our payment system. Your server must forward the customer to this URL so that he can carry out the authentication via 3D Secure procedure. The result of this 3D Secure authentication is reported directly to Unzer by the card issuing bank.

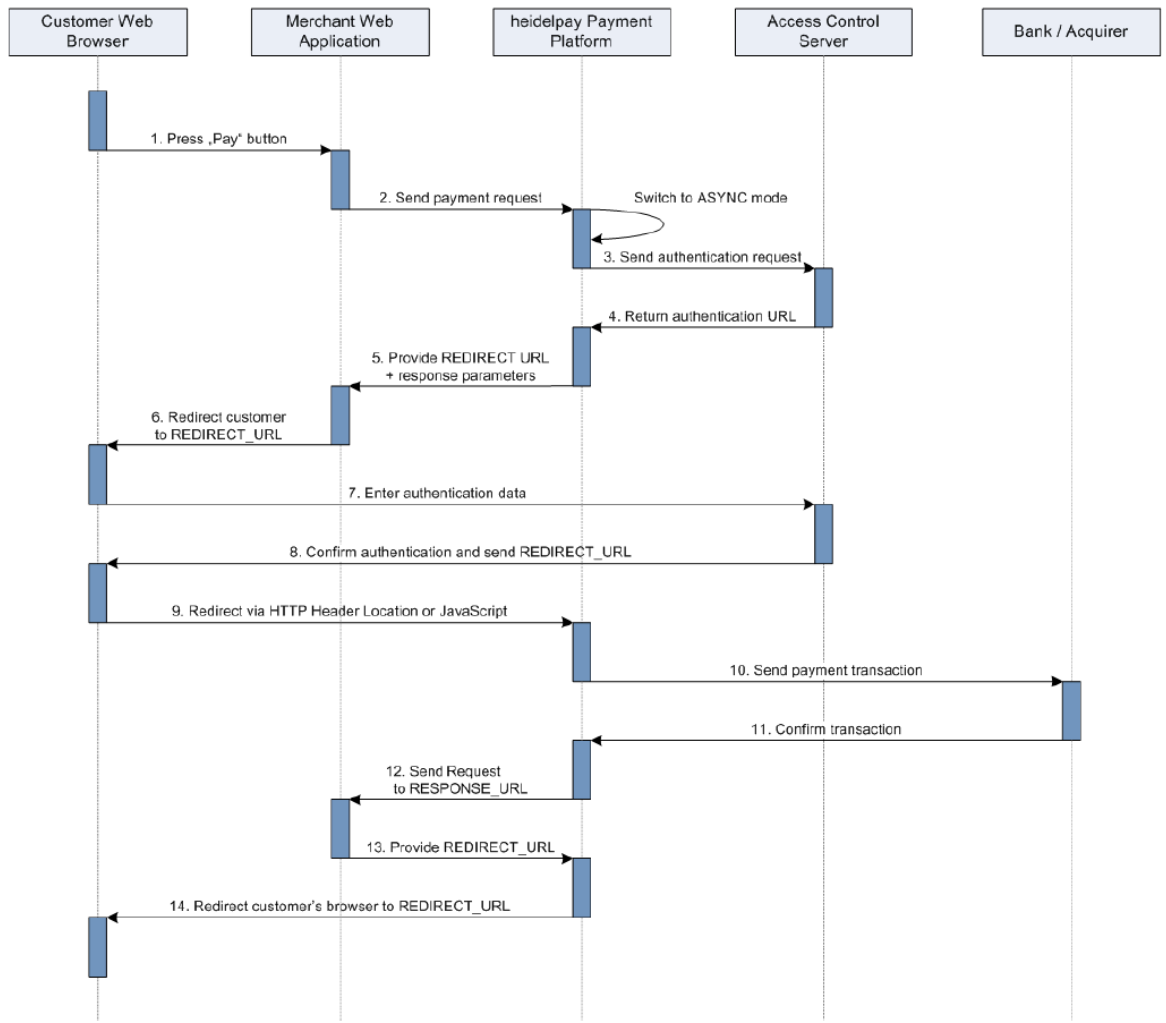
After successful authentication, the transaction is further processed in the Unzer system in the way you already know by sending your system an overall result at the end, to which you reply with a redirect URL. The payment system will then redirect the customer back to your system using this redirect URL from your system

Please note: In this workflow your system receives two answers from the payment system:

- One with the status "pending" (PROCESSING.RETURN.CODE=000.200.000 and PROCESSING.RETURN=Transaction+pending) and the redirect parameters to the card-issuing bank of the customer

- One with the final result of the debit or reservation.

There are also two redirect URLs mentioned in this process, one from the payment system to which the customer has to be redirected to authenticate at his card issuing bank und one from your system, when receiving the final result, to redirect the customer back into your system.



The following changes will be made to the regular procedure. Please note that due to the implementation of other asynchronous payment methods, such as Paypal, some of these processes may already exist in your implementation.

1. Response URL

In the first call (no.2 in the diagram) to the payment system, a "Response URL" must be passed in the **frontend group**.

```
REQUEST.VERSION=1.0
SECURITY.SENDER=31HA07BC8142C5A171745D00AD63D182
USER.LOGIN=31ha07bc8142c5a171744e5aef11ffd3
USER.PWD=93167DE7
TRANSACTION.MODE=CONNECTOR_TEST
TRANSACTION.RESPONSE=SYNC
...
PAYMENT.CODE=CC.DB
...
IDENTIFICATION.REFERENCEID=31HA07BC8127506676A52C2CD2B1C85C
...
FRONTEND.ENABLED=true
FRONTEND.MODE=WHITELABEL
FRONTEND.RESPONSE_URL=https://myshop.com/payment/result.php
```

```
<?xml version="1.0" encoding="UTF-8"?>
  <Request version="1.0">
    <Header>
      <Security sender="123a456b789c123d456e789f012g345" />
    </Header>
    <Transaction mode="CONNECTOR_TEST" channel="678a456b789c123-D456e789f012g432">
      ...
    <Frontend>
      <ResponseUrl>https://myshop.com/payment/result.php</ResponseUrl>
      <SessionID>12abcd34abc56cdefg9876</SessionID>
    </Frontend>
  </Transaction>
</Request>
```

Please note: The IDENTIFICATION.REFERENCEID parameter is only relevant if you refer to a registration or other already existing transaction.

2. Processing Redirect URL

If authentication is required, a redirect URL and other parameters in the **redirect group** are transferred in the response from the payment system (No. 5 in the diagram).

```
...
PROCESSING.RETURN.CODE = 000.200.000
PROCESSING.RETURN = Transaction+pending
PROCESSING.RESULT = ACK
...
PROCESSING.REDIRECT.PARAMETER.TermUrl=https://heidelpay.hpcgw.net/TransactionCore/mpiReceiver
PROCESSING.REDIRECT.PARAMETER.MD=31HA07BC8127506676A51CCF56ECFD38
PROCESSING.REDIRECT.PARAM.PaReq=eJxVUstuwjAQ/JWIO7GdB8FosUQbpHLgIaAf4DpWSWkccJwG+vWlQwL0EGl37MnOzBr2Bylup
Oi1pLBUlYV/5Renk0H0YhiSuiYJCEdMNjMtvLM4EfqKi8VIz72A0B9a5laHLgyDLg4vyxWLEpGGBNAXQuFlIuUEYzDgBAyAnQDQPFCsoBS
6m3KynxwdQTUYiDKWhl9ZUFkb/cNlPqbHYw5TRBqmsZ3TF+UBSB3AOihYlO7qrI/uuQZW6azpvvw6uvYrPfzeJ3Ow+WvmAJyNyDjxirBAb
b6Ag8nE0InkfXY4sALp8CKifwQe/P3rbV2g+DkJs3u5yEG9AyBzVZLJa6MJmPrpO9AXk6lko4E6F5DJivBXPi+S9+38SceiWk43BmuMq6z
4V5WZtgb9axAxwD0MPz65tYgTBt4QoJxGLebaBE3Nnexxjhq57oGkOOgbsmoewe2+vc+/gAdOrKc
PROCESSING.REDIRECT.URL=https://secure.bank.de/acs-pa-service/pa/paRequest
...
```

```
<?xml version="1.0" encoding="UTF-8"?>
  <Response version="1.0">
    <Transaction mode="CONNECTOR_TEST" response="ASYNC" channel="678a456b789c123-D456e789f012g432">
    ...
    <Processing code="CC.DB.80.00">
    ...
      <Redirect url="https://www.mybank.com/3-D_validation">
        <Parameter name="TermUrl">https://heidelpay.hpcgw.net/TransactionCore/mpiReceiver</Parameter>
        <Parameter name="MD">31HA07BC8127506676A51CCF56ECFD38</Parameter>
        <Parameter
        name="PaReq">eJxVUstuwjAQ/JWIO7GdB8FosUQbpHLgIaAf4DpWSWkccJwG+vW1QwL0EGl37MnOzBr2By1lupOi1pLBUlYV/
        5Renk0H0YhiSuiYJCEdMNjMtvLM4EfqKi8VIz72A0B9a5laHLgyDLg4vyxWLEpGGBNAXQuF1IuUEYzDgBAyAnQDQPFCsoBS6m3
        KynxwdQTUYiDKWhl9ZUFkb/cN1PqbHYw5TRBqmsZ3TF+UBSB3AOihY1O7qrI/uuQZW6azpvvw6uvYrPfzeJ3Ow+WvmAJyNyDjx
        irBAbb6Ag8nE0InkfXY4sALp8CKifwQe/P3rbV2g+DkJs3u5yEG9AyBzVZLJa6MJmPrpO9AXk6lko4E6F5DJivBXPi+S9+38Sc
        eiWk43BmuMq6z4V5WZtgb9axAxwD0MPz65tYgTBt4QoJxGLebaBE3Nnexxjhq57oGkOOgbsmoewe2+vc+/gAdOrKc</Paramet
        er>
      </Redirect>
    ...
    </Processing>
  </Transaction>
</Response>
```

3. Forwarding of the customer to the redirect URL

If the redirect group is responding with a redirect URL, the customer's browser must be redirected to this URL (No. 6 in the diagram) to perform authentication. The additional parameters from the redirect group have to be transferred to the external website as POST parameters.

Please note: Additional parameters are returned in the "PROCESSING.REDIRECT.xxx" group only with 3D Secure Version 1 (even there the number and naming may vary), whereas with 3D Version 2 only a PROCESSING.REDIRECT.URL as displayed below is returned:

https://heidelpay.hpcgw.net/AuthService/v1/auth/public/2258_2863FFA4C5241C12E39F37CCF/run

This means that regardless of the type and number of parameters, the client browser must redirect to the PROCESSING.REDIRECT.URL.

Below you will find a simple code example of how such a redirect can be executed. The <noscript> part is intended to inform end customers whose systems do not support Javascript or have it disabled. We strongly recommend that the redirect is done within the customer's active browser window and not to use pop up windows or new browser windows, as this could irritate customers and lead them to close the page they are redirected to.

```
html>
   <head>
      <title>Redirect to 3-D Authentication</title>
   </head>
   <body OnLoad="OnLoadEvent();">
      <form name="downloadForm" action="REDIRECT URL HERE" method="POST">
         <input type="hidden" name="PaReq"
                value="BASE-64_ENCODED_PAREQ_HERE" />
         <input type="hidden" name="TermUrl" value="TERM_URL_HERE" />
         <input type="hidden" name="MD" value="MERCHANT_DATA_HERE" />
         <noscript>
            <h1>Processing your 3-D Secure Payment Transaction</h1>
            <h2>JavaScript is currently disabled or is not supported
                by your browser. </h2>
            <h3>Please click Submit to continue the processing of your
               3-D Secure Payment transaction. </h3>
            <input type="submit" value="Submit" />
         </noscript>
      </form>
      <SCRIPT LANGUAGE="Javascript">
         <!--
            function OnLoadEvent() { document.downloadForm.submit(); } //
         -->
      </SCRIPT>
   </body>
</html>
```

4. Asynchronous result check

The result of the authentication is sent asynchronously to your server. The payment system expects a valid URL as response. (No. 12 & 13 in the diagram). For successful or rejected payments, a different URL can be responded here by your system.

5. Return path of the customer

The payment system redirects the customer to the URL provided by the merchant's system after the authentication process and the payment transaction have been completed.

Please note: Steps 4.) and 5.) proceed in exactly the same way as you are already familiar with in existing NONE 3D Secure transactions.

3D Secure and Recurring Payment

From the 1st of January 2021, 3D Secure will be mandatory for all e-commerce card transactions. However, since this is hardly applicable for recurring payments, the banking systems have a separate workflow for this.

For this purpose, the banks distinguish between

- CIT = customer initialised transactions
- MIT = merchant initialised transactions

The first transaction of a card in your merchant account must be authenticated with 3D Secure from 01.01.2021 onwards. Such a successful authentication is a mandatory requirement in order to be able to subsequently submit further bookings on the same card without 3D Secure. The customer must therefore be forwarded to his card-issuing bank for the first debit in

accordance with the procedure described above and authenticate himself there as the cardholder.

If a debit is not planned at the time of the order, for example due to a trial period, a reservation (pre-authorisation) of at least one euro must be made with 3D Secure in the presence of the customer instead. Capturing of this reservation is not necessary.

For existing customers, however, no 3D Secure authentication needs to be made up. If the first successful debit took place before 01.01.2021, the customer record can also be assumed to have been successfully authenticated.

For new customers as of 01.01.2021, on the other hand, 3D Secure authentication is mandatory for the first debit or reservation (pre-authorisation).

Please note: In this respect, the banking system looks at the card data, not the customer data. So if an existing customer uses a new card after 01.01.2021, for example because the previous one has expired or because he has changed his card-issuing bank, this is a new recurring cycle from the banks' point of view and must be authenticated with 3D Secure for the first booking.

Once this initial authentication has been successfully carried out, all further transactions are exempt from the obligation to use 3D Secure

The prerequisites for recurring payment without 3D Secure are therefore:

- There is at least one successful debit or reservation (pre-authorisation) which was either **carried out with 3D Secure or took place before 01.01.2021**.
- it is referenced to an existing registration and debit upon submission

To let the payment system know, that this is a recurring payment, the parameter RECURRENCE.MODE=REPEATED must be sent as well. This signals to the system that a recurring payment is to be reported to the banking systems.

Please note: If the parameter RECURRENCE.MODE=REPEATED is entered when a new card is loaded for the first time, 3D Secure forwarding will be carried out despite this parameter.

Testing the 3D Secure implementation

You can test the 3D Secure connection at any time via our payment system. To do so, use the "CONNECTOR_TEST" mode for a transaction, as shown in the examples above.

Connection data for this test:

SECURITY.SENDER	31HA07BC8142C5A171745D00AD63D182
USER.LOGIN	31ha07bc8142c5a171744e5aef11ffd3
USER.PWD	93167DE7
TRANSACTION.CHANNEL	31HA07BC8142C5A171749A60D979B6E4
Currencies configured for 3D Version 2	EUR, USD, SEK
Currencies configured for 3D Version 1	GBP, CZK, CHF

System gateway endpoint is either
SGW gateway:
- *https://test-heidelpay.hpcgw.net/sgw/gtw* - Latin-15 encoded
- *https://test-heidelpay.hpcgw.net/sgw/gtwu* - UTF-8 encoded

NGW gateway:
- *https://test-heidelpay.hpcgw.net/ngw/post*

Credit card data for this test:

brands	card numbers	CVV	expiry date	note
MasterCard	5453010000059543	123	future date	3D - password: **secret3**
Visa	4711100000000000	123	future date	3DS - password: **secret!33**

Please note: For 3D Secure Version 2, you do not need to enter a password, but simply click on the link ”*Click here to complete authentication.”*

The only way to simulate an error with 3D Secure Version 2 is to let the page with the link time out (approx. 18 minutes).