

# Integration Guide 3D Secure

## Integration Guide 3D Secure

Zum 01.01.2021 wird die Zwei-Faktor-Authentifizierung verpflichtend für alle Zahlungsvorgänge im Internet eingeführt. Um dieser Verpflichtung nachzukommen verwenden die Betreiber der Kreditkartennetzwerke das sogenannte 3D Secure Verfahren. Für Sie als Händler ist es ab dem 01.01.2021 zwingend erforderlich dieses Verfahren für Ihre Kunden durchführen zu können. Im Folgenden finden Sie eine Beschreibung über die unterschiedlichen Integrationsmöglichkeiten und wie das 3D Secure Verfahren für diese durchzuführen ist.

Bitte wählen Sie das von Ihnen verwendete Integrationsverfahren

- Verwenden Sie das Checkout-Formular hCO?
- Verwenden Sie das Checkout-Formular hPF?
- Wickeln Sie Zahlungen ohne Verwendung eines vom Unzer System gestellten Formulars ab?

**Bitte beachten Sie:** Hierbei ist wichtig in welcher Form Belastungen oder Authorisierungen (Reservierungen) vorgenommen werden. Auch wenn sie für die Registrierung der Kartendaten ein Formular der Unzer GmbH verwenden, wird der 3D Secure Prozess erst bei der ersten Belastung oder Authorisierung dann ohne Checkout-Formular erfolgen, also der dritte Integrationsweg beschritten.

### 3D Secure Verfahren bei Einsatz des hCO Checkout-Formulares

Das hCO Checkout Formular ist bereits für das 3D Secure Verfahren ausgelegt. Es entstehen auf Ihrer Seite grundsätzlich keine zusätzlichen Aufwände für die Implementierung des Verfahrens. Sie müssen jedoch sicherstellen, dass Ihr System mit den entsprechenden Antworten unseres Payment Systems umgehen kann, wenn es zu einer Ablehnung aufgrund der gescheiterten Authentifizierung der Zahlung kommt. In der asynchronen Antwort des Payment Systems an Ihren Server wird das Ergebnis der Transaktion übermittelt und muss dort ausgewertet werden, bevor eine Rückleitungs-URL an das Payment System übertragen wird.

Dazu müssen folgende Parameter ausgelesen werden.

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

Erklärung: Der Status der Transaktion ist "Pending", der Parameter `PROCESSING.RESULT` stellt nur ein vorläufiges Ergebnis dar.

Das endgültige Ergebnis der Transaktion ist dann entweder:

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

oder

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

Im ersten Fall ist die Transaktion erfolgreich abgeschlossen, im zweiten Fall insgesamt gescheitert. Letzteres kann unterschiedliche Gründe haben, unter anderem auch eine Ablehnung der Authentifizierung. Sie erhalten detailliertere Informationen über die Parameter "PROCESSING.RETURN" und "PROCESSING.RETURN.CODE".

Wir empfehlen einen Test für beide Meldungen durchzugehen. Weitere Informationen für einen Test und Informationen dazu welche Kreditkartendaten Sie für einen Test verwenden können, finden Sie weiter unten.

### 3D Secure Verfahren bei Einsatz des hPF-Checkout-Formulares

Auch das hPF Checkout Formular ist bereits für die Verwendung des 3DS Verfahrens ausgelegt. Es entstehen auf Ihrer Seite auch hier keine zusätzlichen Aufwände für die Implementierung des Verfahrens. Es gilt auch hier, dass die Antwort des Payment Systems in zwei Schritten erfolgt, analog zum hCO Formular, weshalb Ihr System den Parameter PROCESSING.RETURN.CODE bei der weiteren Verarbeitung der Antwort berücksichtigen muss.

Dazu müssen folgende Parameter ausgelesen werden.

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

Erklärung: Der Status der Transaktion ist "Pending", der Parameter PROCESSING.RESULT stellt nur ein vorläufiges Ergebnis dar.

Das endgültige Ergebnis der Transaktion ist dann entweder:

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

oder

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

Im ersten Fall ist die Transaktion erfolgreich abgeschlossen, im zweiten Fall insgesamt gescheitert. Letzteres kann unterschiedliche Gründe haben, unter anderem auch eine Ablehnung der Authentifizierung. Sie erhalten detailliertere Informationen über die Parameter "PROCESSING.RETURN" und "PROCESSING.RETURN.CODE".

Wir empfehlen einen Test für beide Meldungen durchzugehen. Weitere Informationen für einen Test und Informationen dazu welche Kreditkartendaten Sie für einen Test verwenden können, finden Sie weiter unten.

### 3D Secure Verfahren bei direkter Anbindung

Wenn Sie kein Formular von Unzer (ehemals heidelpay) verwenden um Kreditkarten-Zahlungen abzuwickeln, oder wenn Sie lediglich die Registrierung einer Karte über eines der Formulare durchführen und die Authorisierung (Reservierung) oder Belastung als Referenz auf die Registrierung als direkte Kommunikation mit dem Payment System abwickeln, müssen Sie den 3D Secure Ablauf implementieren.

#### *Asynchroner Transaktionsablauf:*

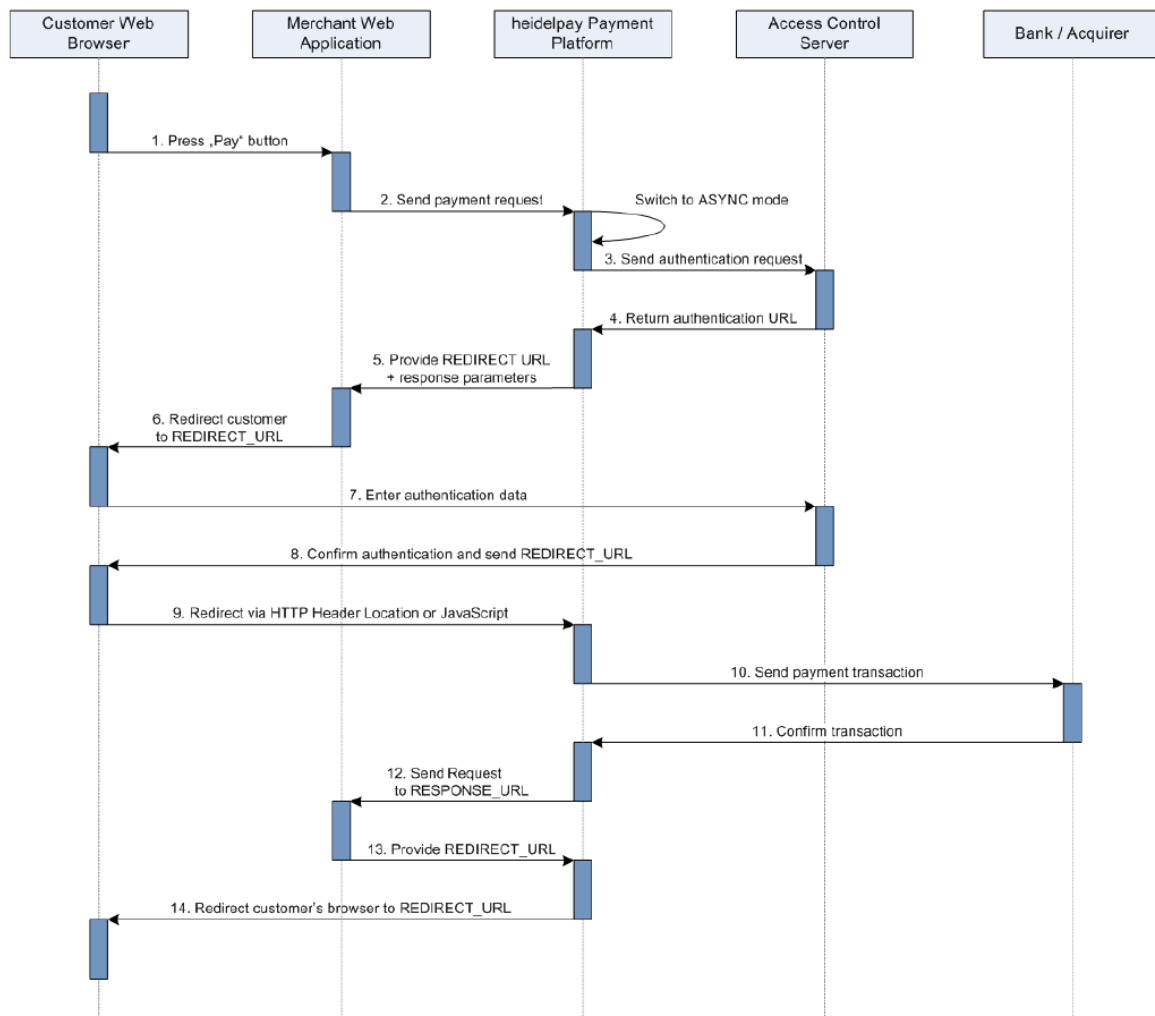
Dies ist ein asynchroner Ablauf bei welchem Ihr Server von unserem Payment System eine Weiterleitungs-URL (Redirect URL) erhält. An diese URL muss Ihr Server den Käufer weiterleiten, damit dieser dort die Authentifizierung per 3D Secure Verfahren durchführen kann.

Das Ergebnis dieser 3D Secure Authentifizierung wird von der kartenausgebenden Bank direkt an Unzer zurückgemeldet.

Nach der erfolgreichen Authentifizierung erfolgt die weitere Verarbeitung der Transaktion im Unzer System so wie bereits bekannt, indem Ihrem System am Ende ein Gesamtergebnis mitgeteilt wird, auf welches Sie mit einer Rückleitungs-URL (Redirect URL) antworten. Das Payment System wird den Käufer dann über diese Rückleitungs-URL in Ihr System zurückführen.

**Bitte beachten Sie:** Ihr System erhält bei diesem Workflow also zwei Antworten des Payment Systems:

- Eine mit dem Status "pending" (PROCESSING.RETURN.CODE=000.200.000 und PROCESSING.RETURN=Transaction+pending) und den Redirect Parametern zur kartenausgebenden Bank des Kunden
- Eine mit dem finalen Ergebnis der Belastung oder Reservierung.



Folgende Änderungen ergeben sich zum regulären Ablauf. Bitte beachten Sie, dass aufgrund der Implementierung anderer asynchroner Zahlarten, wie beispielsweise Paypal, diese Prozesse bereits vorhanden sein können.

## 1. Response URL

Im ersten Aufruf (Nr.2 im Diagramm) an das Payment System muss eine "Response URL" in der Frontend Group übergeben werden.

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <Request version="1.0">
3   <Header>
4     <Security sender="123a456b789c123d456e789f012g345" />
5   </Header>
6   <Transaction mode="CONNECTOR_TEST" channel="678a456b789c123-D456e789f012g432">
7     ...
8     <Frontend>
9       <ResponseUrl>https://myshop.com/payment/result.php</ResponseUrl>
10      <SessionID>l2abcd34abc56cdefg9876</SessionID>
11    </Frontend>
12  </Transaction>
13 </Request>
```

```
1 REQUEST.VERSION=1.0
2 SECURITY.SENDER=31HA07BC8142C5A171745D00AD63D182
3 USER.LOGIN=31ha07bc8142c5a171744e5aef11ffd3
4 USER.PWD=93167DE7
5 TRANSACTION.MODE=CONNECTOR_TEST
6 TRANSACTION.RESPONSE=SYNC
7 ...
8 PAYMENT.CODE=CC.DB
9 ...
10 IDENTIFICATION.REFERENCEID=31HA07BC8127506676A52C2CD2B1C85C
11 ...
12 FRONTEND.ENABLED=true
13 FRONTEND.MODE=WHITELABEL
14 FRONTEND.RESPONSE_URL=https://myshop.com/payment/result.php
```

**Bitte beachten Sie:** Der Parameter IDENTIFICATION.REFERENCEID ist nur relevant, wenn Sie auf eine Registrierung oder eine andere Transaktion referenzieren.

## 2. Verarbeitung Redirect URL

Im Fall einer notwendigen Authentifizierung wird in der Antwort des Systems eine Redirect URL nebst weiteren Parametern in der Redirect Gruppe übergeben (Nr. 5 im Diagramm).

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <Response version="1.0">
3   <Transaction mode="CONNECTOR_TEST" response="ASYNC" channel="678a456b789c123-D456e789f012g432">
4     ...
5     <Processing code="CC.DB.80.00">
6       ...
7       <Redirect url="https://www.mybank.com/3-D_validation">
8         <Parameter name="TermUrl">https://heidelpay.hpcgw.net/TransactionCore/mpiReceiver</Parameter>
9         <Parameter name="MD">31HA07BC8127506676A51CCF56ECFD38</Parameter>
10        <Parameter
11          name="PaReq">eJxVUstuwjAQ/JWIO7GdB8FosUQbpHLgIaAf4DpWSWkccJwG+vW1QwL0EG137MnOzBr2ByllupOilpLBU1YV/
12          5Renk0H0YhiSuiYJCEdMNjMtvLM4EfgKi8Viz72A0B9a51aHLgYDLg4vYxWLEpGGBNAXQuF1IuUEYzDgBAYAnQDQPPFCsoBS6m3
13          KynxwdQTUYiDKWhl9ZUFkb/cN1PqbHYw5TRBqmsZ3TF+UBSB3A0ihY107qrI/uuQZw6azpVvW6uvYrPfzeJ3Ow+WvmAJyNyDjx
14          irBAb6Ag8nE0InkXY4sALp8CKifwQe/P3rbV2g+DkJs3u5yEG9AyBzVZLJa6MJmPrp09AXk61ko4E6F5DJivBXPi+S9+38Sc
15          eiWk43BmuMq6z4V5WZtgb9axAxwD0MPz65tYgTbt4QoJxGLEbaBE3Nnexxjhg57oGk0Ogbsmoewe2+vc+/gAdOrKc</Paramet
16        er>
17      </Redirect>
18    </Processing>
19  </Transaction>
20 </Response>
```

```

1 ...
2 PROCESSING.RETURN.CODE = 000.200.000
3 PROCESSING.RETURN = Transaction+pending
4 PROCESSING.RESULT = ACK
5 ...
6 PROCESSING.REDIRECT.PARAMETER.TermUrl=https://heidelpay.hpcgw.net/TransactionCore/mpiReceiver
7 PROCESSING.REDIRECT.PARAMETER.MD=31HA07BC8127506676A51CCF56ECFD38
8 PROCESSING.REDIRECT.PARAM.PaReq=eJxVUstuwjAQ/JWIO7GdB8FosUQbpHLgIaAf4DpWSWkccJwG+vWlQwL0EG137MnOzBr2By1lup
  OilpLBULYV/5Renk0H0YhiSuiYJCEdMjMtvLM4EfQKi8Viz72A0B9a51aHLgyDLg4vyxWLEpGGBNAXQuFlIuUEYzDgBAyAnQDQPFcsoBS
  6m3KynxwdTUYiDKWhl9ZUFkb/cN1PqbHYw5TRBqmsZ3TF+UBSB3AOihY1O7qrI/uuQZw6azpvvw6uvYrPfzeJ3Ow+WvmAJyNyDjxirBAb
  b6Ag8nE0InkfXY4sAlp8CKifwQe/P3rbV2g+DkJs3u5yEG9AyBzVZLJa6MjMPrpO9AXk6lko4E6F5DJivBXPi+S9+38SceiWk43BmuMq6z
  4V5WZtgb9axAxwD0MPz65tYgTbt4QoJxGLEbaBE3Nnexxjhg57oGkO0gbsmoewe2+yc+/gAdOrKc
9 PROCESSING.REDIRECT.URL=https://secure.bank.de/acs-pa-service/pa/paRequest
10 ...

```

### 3. Weiterleitung des Käufers zur Redirect URL

Wenn die Redirect Gruppe mit der Redirect URL übergeben wird, muss der Browser des Kunden an diese URL geleitet werden (Nr. 6 im Diagramm) um die Authentifizierung durchzuführen. Dabei werden die übrigen Parameter als POST an die aufgerufene Seite übergeben.

**Bitte beachten Sie:** Einzelnen Parameternamen in der Redirect Gruppe können variieren, daher sollten Sie alle Parameter, die mit "PROCESSING.REDIRECT.xxx" zurückgegeben werden, bzw. sich in der Redirect Gruppe befinden an die Redirect URL weitergeben, unabhängig davon, wie diese konkret genannt werden.

Anbei finden Sie ein einfaches Codebeispiel, wie eine solcher Redirect ausgeführt werden kann. Der <noscript> Teil soll dabei Endkunden informieren, deren Systeme Javascript nicht unterstützen oder deaktiviert haben. Wir empfehlen ausdrücklich den Redirect innerhalb des aktiven Fensters des Kunden zu machen und keine Pop-Ups oder neue Browserfenster zu verwenden, denn das könnte Kunden irritieren und zum wegklicken der aufgerufenen Seite verleiten.

```

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. Asynchrone Ergebnisprüfung

Das Ergebnis der Authentifizierung wird asynchron an Ihren Server übermittelt. Das Payment System erwartet als Antwort eine gültige URL zurück. (Nr. 12 & 13 im Diagramm). Im Beispiel eine erfolgreiche Authentifizierung und Abwicklung der Zahlung. Für erfolgreiche oder abgelehnte Zahlungen kann hier eine jeweils andere URL übergeben werden.

#### 5. Rückleitung des Käufers

Das Payment System leitet den Käufer nach Abschluss des Authentifizierungsvorganges und der Transaktion insgesamt an die vom Händlersystem übergebene URL zurück.

**Bitte beachten Sie:** Die Schritte 4.) und 5.) laufen genauso ab, wie Sie es von den bestehenden NONE 3D Secure Transaktionen bereits gewohnt sind.

### Testen der 3D Secure Anbindung

Sie können die 3D Secure Anbindung jederzeit über unser Payment System testen. Verwenden Sie dazu, wie in den Beispielen oben gezeigt, den Modus "CONNECTOR\_TEST" für eine Transaktion.

Anbindungsdaten für diesen Test:

SECURITY.SENDER	31HA07BC8142C5A171745D00AD63D182
USER.LOGIN	31ha07bc8142c5a171744e5aef11ffd3
USER.PWD	93167DE7
TRANSACTION.CHANNEL	31HA07BC8142C5A171749A60D979B6E4
Währungen	EUR, USD, GBP, CZK, CHF, SEK

Kartendaten für diesen Test:

Brands	Kartenummer	CVV	Ablaufdatum	Anmerkung
MasterCard	5453010000059543	123	Datum in der Zukunft	3D - Passwort: secret3
MasterCard	5453010000059675	123	Datum in der Zukunft	3DS Auth schlägt immer fehl
Visa	4711100000000000	123	Datum in der Zukunft	3DS - Passwort: secret!33
Visa	4012001037461114	123	Datum in der Zukunft	Kein 3D – Card not enrolled