Google Pay™ 3DS-Ablauf für PAN_ONLY-Payload

Google Pay™ 3DS-Verarbeitung für PAN_ONLY-Payload

> Bitte beachten Sie, dass Zahlungen aufgrund der PSD2-Verordnung eine SCA (Starke Kundenautenrisierung) aufweisen müssen. Dies gilt auch für Google Pay™. Google Pay™ bietet im Allgemeinen zwei Arten von PAyloads mit Zahlungsdaten an.
>
> Bei der Payload CRYPTOGRAM_3DS ist die Zahlung bereits auf dem Kundengerät SCA-authentifiziert und die Payload enthält einen Authentifizierungsnachweis. Daher ist keine zusätzliche SCA in Form von 3-D Secure erforderlich.
>
> Bei der Payload PAN_ONLY sind die Zahlungsdaten nicht SCA-authentifiziert. Um Soft Declines zu vermeiden, ist daher eine 3-D Secure-Authentifizierung erforderlich.

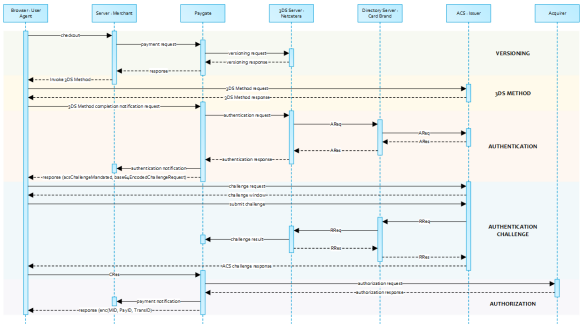
Nachstehende Anleitung beschreibt, wie 3-D Secure 2.0 für Google-Pay-Zahlungen angewendet werden kann.

Diese Anleitung kann für alle Google-Pay-Zahlungen angewendet werden, da Paygate PAN_ONLY-Nutzdaten dynamisch erkannt und der 3-D Secure-Prozess gestartet wird. Im Falle der CRYPTOGRAM_3DS-Nutzdaten wird 3-D Secure nicht gestartet.

Eine 3DS 2.0 Zahlungssequenz kann aus den folgenden verschiedenen Aktivitäten bestehen:

- Versionierung
  - Anfrage von ACS- und DS-Protokol-Version(en), die mit dem Kartenkontenbereich korrespondieren sowie einer optionalen 3DS Method URL
- 3DS Methode
  - Verbindet den Browser des Karteninhabers mit dem ACS des Issuers, um zusätzliche Browserdaten zu erhalten
- Authentisierung
  - Übermittlung der Authentisierungs-Anfrage an den ACS des Issuers
- Challenge
  - Challenge des Karteninhabers, falls angeordnet
- Autorisierung
  - Autorisierung der authentisierten Transaktion beim Acquirer

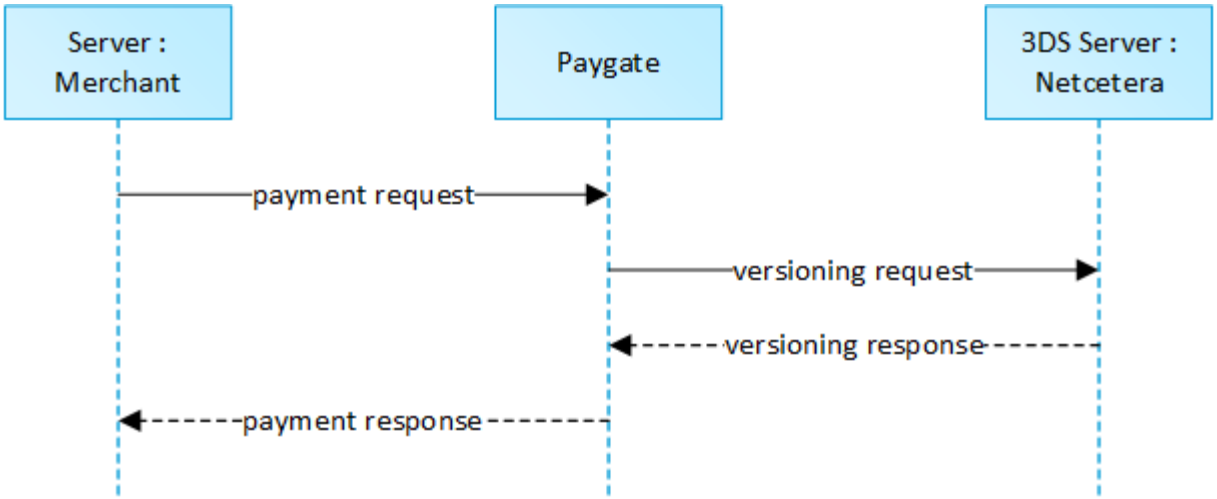
Server-2-Server Sequenzdiagramm



> Beachten Sie bitte, dass die Kommunikation zwischen Client und Access Control Server (ACS) über iFrames implementiert ist. Daher kommen die Antworten in einem HTML-Subdokument an und Sie können entsprechende Event-Listener in Ihrem Root-Dokument einrichten.
>
> Alternativ könnten Sie alleinig auf die asynchronen Benachrichtigungen an ihr Backend vertrauen. In jenen Fällen müssen Sie eventuell Methoden wie Long Polling, SSE oder Websockets zum Update des Clients in Betracht ziehen.

Initiierung der Zahlung

Die anfängliche Anfrage an das Computop Paygate ist unabhängig vom zugrundeliegenden 3DS-Protokoll gleich.



Um eine Server-zu-Server 3-D Secure Kartenzahlungssequenz zu starten, senden Sie bitte folgende Schlüssel-Wert-Paare an https://www.computop-paygate.com/direct.aspx.

Aufruf der Schnittstelle: allgemeine Parameter

Um eine Zahlung mit Google Pay über eine Server-zu-Server-Verbindung auszuführen, verwenden Sie bitte folgende URL:

https://www.computop-paygate.com/googlepay.aspx

Aufruf-Elemente

Hinweis: Aus Sicherheitsgründen lehnt das Paygate alle Zahlungsanfragen mit Formatfehlern ab. Bitte übergeben Sie deshalb bei jedem Parameter den korrekten Datentyp.

Die folgende Tabelle beschreibt die verschlüsselten Übergabeparameter:

Key	Format	CND	Beschreibung
MerchantID	ans..30	M	HändlerID, die von Computop vergeben wird. Dieser Parameter ist zusätzlich auch unverschlüsselt zu übergeben.
msgver	ans..5	M	Computop Paygate Message-Version. Zulässige Werte: **Wert** / **Beschreibung** 2.0 – Mit 3-D Secure 2.x wurde eine Vielzahl zusätzlicher Daten (Browser-Information, Rechnungs-/Versand-Adresse, ...) erforderlich, um den Authentifizierungs-Prozess zu optimieren. Um diese Informationen zu handhaben, wurden die JSON-Objekte eingeführt. Der Parameter MsgVer zeigt an, dass diese Daten verwendet werden.
TransID	ans..64	M	Ihre eigene TransaktionsID, die für jede Zahlung eindeutig sein muss
ReqId	ans..32	O	Um Doppelzahlungen (z.B. durch ETM) zu vermeiden, übergeben Sie einen alphanumerischen Wert, der Ihre Transaktion oder Aktion identifiziert und nur einmal vergeben werden darf. Falls die Transaktion oder Aktion mit derselben ReqID erneut eingereicht wird, führt das Computop Paygate keine Zahlung oder weitere Aktion aus, sondern gibt nur den Status der ursprünglichen Transaktion oder Aktion zurück. Bitte beachten Sie, dass das Computop Paygate für die erste initiale Aktion (Authentifizierung/Autorisierung) einen abgeschlossenen Transaktionsstatus haben muss. Dies gilt nicht für 3-D Secure Authentifizierungen, die durch einem Timeout beendet werden. Der Status 3-D Secure Timeout gilt nicht als abgeschlossener Status, bei dem ReqID-Funktionalität am Paygate nicht greift. Einreichungen mit identischer ReqID auf einen offenen Status werden regulär verarbeitet. **Hinweis:** Bitte beachten Sie, dass eine ReqID nur 12 Monate gültig ist, danach wird sie vom Paygate gelöscht.
RefNr		O	Eindeutige Referenznummer des Händlers, welche als Auszahlungsreferenz in der EPA-Datei des Acquirers dient. Bitte beachten Sie, dass ohne die eigene Shop-Referenzlieferung die EPA-Transaktion nicht ausgelesen werden kann und wir die zusätzlichen Zahlungsdaten nicht in die zusätzliche Computop Abrechnungsdatei (CTSF) aufnehmen können. Einzelheiten zum unterstützten Format finden Sie weiter unten im zahlungsspezifischen Abschnitt. Es sind ausschließlich ASCII-Zeichen erlaubt. Sonderzeichen wie ("Umlaute", ...) sind nicht erlaubt und müssen ggf. durch ASCII-Zeichen ersetzt werden (z.B. ü ue, é e, ...).

<table>
<tr><td>Amount</td><td>n..10</td><td>M</td><td>Betrag in der kleinsten Währungseinheit (z.B. EUR Cent). Bitte wenden Sie sich an den Computop Helpdesk, wenn Sie Beträge < 100 (kleinste Währungseinheit) buchen möchten.</td></tr>
<tr><td>Currency</td><td>a3</td><td>M</td><td>Währung, drei Zeichen DIN / ISO 4217, z.B. EUR, USD, GBP. Hier eine Übersicht: A1 Währungstabelle</td></tr>
<tr><td>Capture</td><td>an..6</td><td>OM</td><td>Bestimmt Art und Zeitpunkt der Buchung (engl. Capture).
<table><tr><th>Buchungsart</th><th>Beschreibung</th></tr><tr><td>AUTO</td><td>Buchung sofort nach Autorisierung (Standardwert).</td></tr><tr><td>MANUAL</td><td>Buchung erfolgt durch den Händler - in der Regel die Buchung zum Zeitpunkt der Warenauslieferung bzw. Leistungserbringung.</td></tr><tr><td><Zahl></td><td>Verzögerung in Stunden bis zur Buchung (ganze Zahl; 1 bis 696).</td></tr></table></td></tr>
<tr><td>OrderDesc</td><td>ans..768</td><td>O</td><td>Beschreibung der Bestellung</td></tr>
<tr><td>browserInfo</td><td>JSON</td><td>M</td><td>Exakte Browserinformationen sind nötig, um eine optimierte Nutzererfahrung zu liefern. Erforderlich für 3-D Secure 2.0 Transaktionen.</td></tr>
<tr><td>billToCustomer</td><td>JSON</td><td>C</td><td>Der Kunde, dem die Waren und / oder Dienstleistungen in Rechnung gestellt werden. Erforderlich, sofern nicht Markt- oder regionale Mandate das Senden dieser Informationen beschränken.</td></tr>
<tr><td>URLNotify</td><td>ans..256</td><td>C</td><td>Vollständige URL, die das Paygate aufruft, um den Shop zu benachrichtigen. Die URL darf nur über Port 443 aufgerufen werden. Sie darf keine Parameter enthalten: Nutzen Sie stattdessen den Parameter UserData.

Im Falle einer vom Händler initiierten wiederkehrenden Transaktion sind die JSON-Objekte (außer credentialOnFile und card), URLNotify und TermURL keine obligatorischen Parameter, da kein 3-D Secure und keine Risikobewertung durch die kartenausgebende Bank erfolgt und das Zahlungsergebnis direkt erfolgt innerhalb der Antwort zurückgegeben.

Allgemeine Hinweise:
Bevor Folgeaktionen (Buchung / Gutschrift / Storno) auf eine bestehende Transaktion ausgeführt werden, muss zuvor das erste Notify durch den Shop beantwortet worden sein.
Betrüger könnten das verschlüsselte DATA-Element kopieren, welches an URLFailure gesendet wurde, und betrügerisch dasselbe DATA an URLSuccess/URLNotify senden. Überprüfen Sie daher unbedingt den "code"-Wert des DATA-Elements. Nur eine Antwort mit "code=00000000" sollte als erfolgreich angesehen werden.</td></tr>
<tr><td>MAC</td><td>an64</td><td>M</td><td>Hash Message Authentication Code (HMAC) mit SHA-256-Algorithmus. Details finden Sie hier:
HMAC-Authentisierung (Anfrage)
HMAC-Authentisierung (Notify)</td></tr>
<tr><td>TokenExt</td><td>ans..1024</td><td>M</td><td>Google Pay Token als JSON-String im Base64-Format
Beispiel für TokenExt
<pre>{
 "signature": "MEQCIC4z
/QHSrzekRkkuk3vGYxBTBdNgEQl5XFHx0Wk5fFLIUAiB3+q227havAJdagfGZaMXbefhatdJE7Df2qrIoKDv
1Og==",
 "protocolVersion": "ECv1",
 "signedMessage": "{\"encryptedMessage\":\"
bOYRmExGeCsBrFqESt7kd9O1FN+vQZf2KG0UNYC8jNA+VVf9nQeK7lDvU8k37cH+LOziJQkHNL2OxDHIk6Go
RV1BrXprwBnAJR0O2VnCUH8lsqq0ELwemeqW364Ir8cU
/hDFzWNp+38H25JVDAMExZBKodMMTzUXXgyO+s5jOyAl8jUhnAw3fTRPkefuYsE8NFK5tvcs4L29h87Zo7ot
0/8XrUhXt9b
/Fld1LEthkuPSN+K1eEFP7bseB6jjRdHnwYAdqiE3iOmh71pcDmNIyrlWRj74UJaszeerZW7DoZNx11oN7fo
uq/8fe1vklsr/e+y/RSG2nQMWg5yR/fMTfqCyabTDhJMvMM1Zhe91+dQ0/xi
/zKRgsIhiongJUjYtoSNIjUHnMLRuVTKdjX50CCI1QOiBtr9h0bOLePhxw9cLYeU1KwCfYJyt28DBKCvaWFS
bCl+dzNcZ9B83kv\",\"ephemeralPublicKey\":\"BFUju73/IT/KqnB
/nc0W3BaL3BXFybrbYaPiMCKXIcg78PbslwV7MRUq3SpWEDEJT6pakLCvf34412HbDGCpsa4\\u003d\",\"
tag\":\"xIuCUWB2U6yWEfidsJpQaa+leU/kqS522JLOnrnk42g\\u003d\"}"
}</pre></td></tr>
<tr><td>Channel</td><td>a..10</td><td>C</td><td>Kanal, über den die Bestellung abgewickelt wird. Erlaubt sind die Werte WEBSITE und MOBILE_APP.

Der Parameter Channel ist für RedSys obligatorisch. Bitte geben Sie ihn an, wenn Ihr Prozessor RedSys ist. Für andere Prozessoren ist die Angabe dieser Information nicht obligatorisch.</td></tr>
</table>

Allgemeine Parameter für Kreditkartenzahlungen über Socket-Verbindungen

Beachten Sie bitte die zusätzlichen Parameter für eine spezifische Kreditkartenintegration im Abschnitt „Spezifische Parameter“

Antwort-Elemente (Authentisierung)

Die folgende Tabelle beschreibt die Parameter, die das Paygate als Antwort zurückgibt:

es können jederzeit neue Parameter hinzugefügt bzw. die Reihenfolge geändert werden

die Parameter (z.B. mid, RefNr) sollten nicht auf Groß-/Kleinschreibung geprüft werden

Key	Format	CND	Beschreibung
mid	ans..30	M	HändlerID, die von Computop vergeben wird
PayID	an32	M	Vom Paygate vergebene ID für die Zahlung; z.B. zur Referenzierung in Batch-Dateien sowie im Capture- oder Credit-Request.
XID	an32	M	Vom Paygate vergebene ID für alle einzelnen Transaktionen (Autorisierung, Buchung, Gutschrift), die für eine Zahlung durchgeführt werden
TransID	ans..64	M	Ihre eigene TransaktionsID, die für jede Zahlung eindeutig sein muss
refnr		O	Referenznummer wie im Request angegeben
Status	a..20	M	Status der Transaktion. Zulässige Werte: • **`AUTHENTICATION_REQUEST`** • **`PENDING`** • **`FAILED`**
Description	ans..1024	M	Nähere Beschreibung bei Ablehnung der Zahlung. Bitte nutzen Sie **nicht** den Parameter **Description, sondern** Code für die Auswertung des Transaktionsstatus!
Code	an8	M	Fehlercode gemäß Paygate Antwort-Codes (A4 Fehlercodes)
UserData	ans..1024	O	Wenn beim Aufruf angegeben, übergibt das Paygate die Parameter mit dem Zahlungsergebnis an den Shop.
card	JSON	M	Kartendaten
versioningdata	JSON	M	Das Datenelement Card Range Data enthält Informationen, welche die jüngste vom ACS, der den Kartenbereich hostet, unterstützte EMV 3-D Secure-Version angeben. Es kann optional auch die ACS URL für die 3-D Secure Methode enthalten, falls vom ACS unterstützt, sowie die DS Start- und End-Protokoll-Versionen, die den Kartenbereich unterstützen.
threeDSLegacy	JSON	C	Objekt, dass die erforderlichen Datenelemente für die Konstruktion der Anfrage zur Zahler-Authentisierung im Falle eines **Fallbacks** auf 3-D Secure 1.0 enthält.

versioningData

Das Objekt **`versioningData`** gibt die EMV 3DS Protokoll-Versionen (d.h. 2.1.0 oder höher) an, die vom Access Control Server des Issuers unterstützt werden.

Wenn die entsprechenden Felder der Protokoll-Version NULL sind, bedeutet dies, dass der BIN-Bereich des Karten-Issuers nicht für 3DS 2.0 registriert ist und ein Fallback auf 3DS 1.0 für Transaktionen erforderlich ist, die unter den Geltungsbereich der PSD2 SCA fallen.

Achten Sie beim Zerlegen von **`versioningData`** bitte auch auf das Subelement **`errorDetails`**, das den Grund angibt, falls einige Felder nicht ausgefüllt sind (z.B. Ungültige Kontonumber des Karteninhabers übergeben, nicht verfügbare Kartenbereichsdaten, Fehler beo Codieren/Serialisieren der 3DS Methoden-Daten usw.)

BASEURL= https://www.computop-paygate.com/


```
{
        "threeDSServerTransID": "14dd844c-b0fc-4dfe-8635-366fbf43468c",
        "acsStartProtocolVersion": "2.1.0",
        "acsEndProtocolVersion": "2.1.0",
        "dsStartProtocolVersion": "2.1.0",
        "dsEndProtocolVersion": "2.1.0",
        "threeDSMethodURL": "http://www.acs.com/script",
        "threeDSMethodDataForm":
"eyJ0aHJlZURTTWV0aG9kTm90aWZpY2F0aW9uVVJMIjoiaHR0cHM6Ly93d3cuY29tcHV0b3AtcGF5Z2F0ZS5jb20vY2JUaHJlZURTLmFzcHg_
YWN0aW9uPW10aGROdGZuIiwidGhyZWVEU1NlcnZlclRyYW5zSUQiOiIxNGRkODQ0Yy1iMGZjLTRkZmUtODYzNS0zNjZmYmY0MzQ2OGMifQ=="
,
```

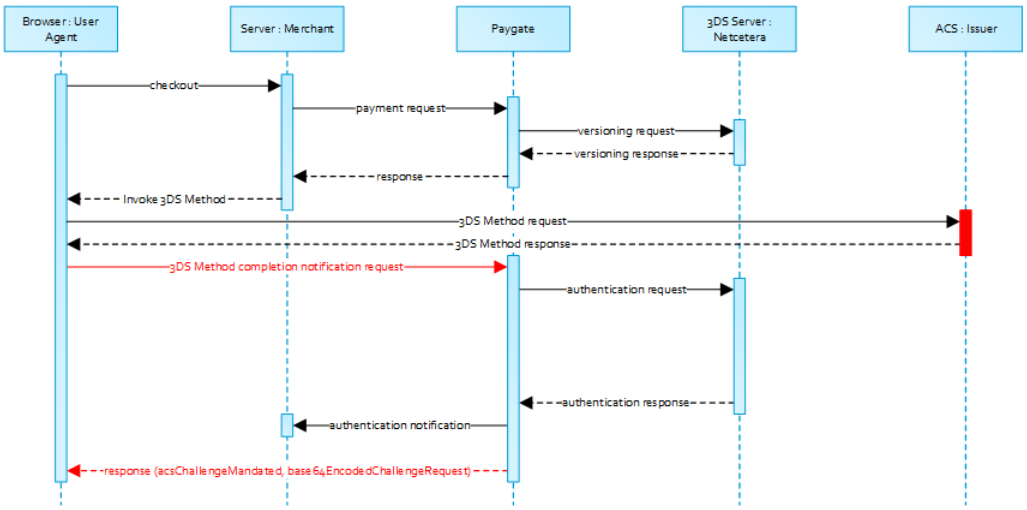
```
        "threeDSMethodData": {
                "threeDSMethodNotificationURL": "BASEURL/cbThreeDS.aspx?action=mthdNtfn",
                "threeDSServerTransID": "14dd844c-b0fc-4dfe-8635-366fbf43468c"
        }
}
```

3-D Secure-Methode

Die 3DS Methode ermöglicht das Erfassen zusätzlicher Browserinformationen durch einen ACS vor Erhalt der Authensisierungsanfrage (AReq), um die Risikobeurteilung der Transaktion zu erleichtern. Die Unterstützung der 3DS Methode ist optional und liegt im Ermessen des Issuers.

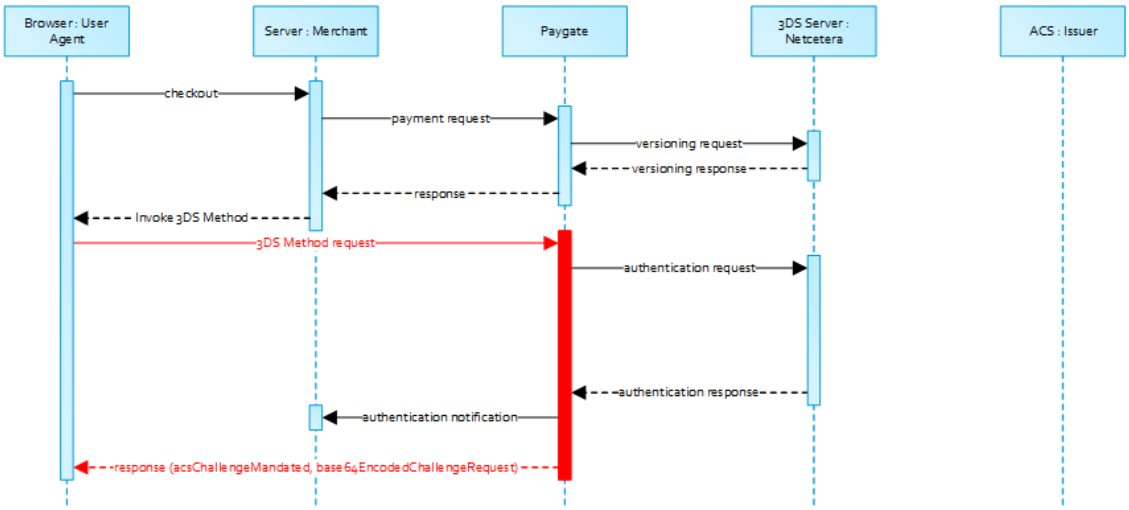
Das Objekt **`versioningData`** enthält einen Wert für **`threeDSMethodURL`**. Der Händler sollte die 3DS Methode über einen versteckten HTML-iFrame im Browser des Karteninhabers aufrufen und ein Formular mit einem Feld namens **`threeDSMethodData`** über HTTP POST an die ACS 3DS Methoden-URL senden.

3-D Secure-Methode: `threeDSMethodURL`



Beachten Sie bitte, dass die **`threeDSMethodURL`** vom Computop Paygate ausgefüllt wird, falls der Issuer die 3DS Methode nicht unterstützt. Der 3DS Methoden-Formular-Post wie unten dargestellt muss unabhängig davon ausgeführt werden, ob dies vom Issuer unterstützt wird. Das ist notwending, um die direkte Kommunikation zwischen dem Browser und dem Computop Paygate im Falle einer angeordneten Challenge oder eines reibungslosen Ablaufs zu erleichtern.

3-D Secure-Methode: Keine Issuer `threeDSMethodURL`



3-D Secure-Methode Form Post

```
<form name="frm" method="POST" action="Rendering URL">
    <input type="hidden" name="threeDSMethodData" value="
eyJ0aHJlZURTU2VydmVyVHJhbnNJRCI6IjNhYzdjYWE3LWFhNDItMjY2My03OTFiLTJhYzA1YTU0MmM0YSIsInRocmVlRFNNZXRob2ROb3RpZ
mljYXRpb25VUkwiOiJ0aHJlZURTTWV0aG9kTm90aWZpY2F0aW9uVVJMIn0">
</form>
```

Der ACS interagiert mit dem Browser des Karteninhabers über den HTML-iFrame und speichert dann die zutreffenden Werte mit der 3DS Server Transaction ID für die Verwendung, wenn eine nachfolgende Authentisierungs-Nachricht empfangen wird, welche die gleiche 3DS Server Transaction ID enthält.

Netcetera 3DS Web SDK

Sie können nach eigenem Ermessen die Operationen **`init3DSMethod`** oder **`createIframeAndInit3DSMethod`** vom nca3DSWebSDK verwenden, um die 3DS Methode zu initialisieren. Bitte beachten Sie dazu das Integrations-Handbuch unter https://mpi.netcetera.com/3dsserver/doc/current/integration.html#Web_Service_API.

Nachdem die 3DS-Methode abgeschlossen ist, weist der ACS den Browser des Karteninhabers über das iFrame-Antwortdokument an, **`threeDSMethodData`** als ein verstecktes Formularfeld an die 3DS Method Notification URL zu übermitteln.

ACS Response-Dokument

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8"/>
    <title>Identifying...</title>
</head>
<body>
<script>
    var tdsMethodNotificationValue =
'eyJ0aHJlZURTU2VydmVyVHJhbnNJRCI6ImUxYzFlYmViLTc0ZTgtNDNiMi1iMzg1LTJlNjdkMWFhY2ZhMiJ9';

    var form = document.createElement("form");
    form.setAttribute("method", "post");
    form.setAttribute("action", "notification URL");

    addParameter(form, "threeDSMethodData", tdsMethodNotificationValue);

    document.body.appendChild(form);
    form.submit();

    function addParameter(form, key, value) {
        var hiddenField = document.createElement("input");
        hiddenField.setAttribute("type", "hidden");
        hiddenField.setAttribute("name", key);
        hiddenField.setAttribute("value", value);
        form.appendChild(hiddenField);
    }
</script>
</body>
</html>
```

3-D Secure-Methode Benachrichtigungs-Formular

```
<form name="frm" method="POST" action="3DS Method Notification URL">
    <input type="hidden" name="threeDSMethodData" value="
eyJ0aHJlZURTU2VydmVyVHJhbnNJRCI6ImUxYzFlYmViLTc0ZTgtNDNiMi1iMzg1LTJlNjdkMWFhY2ZhMiJ9">
</form>
```

⚠ Beachten SIe bitte, dass die **`threeDSMethodNotificationURL`** wie sie in den Base64-codierten **`threeDSMethodData`** eingebettet ist, auf das Computop Paygate weist und nicht verändert werden darf. Die Händler-Benachrichtigung wird an die URLNotify geliefert, wie sie in der Originalanfrage übermittelt oder für die MerchantID im Computop Paygate konfiguriert ist.

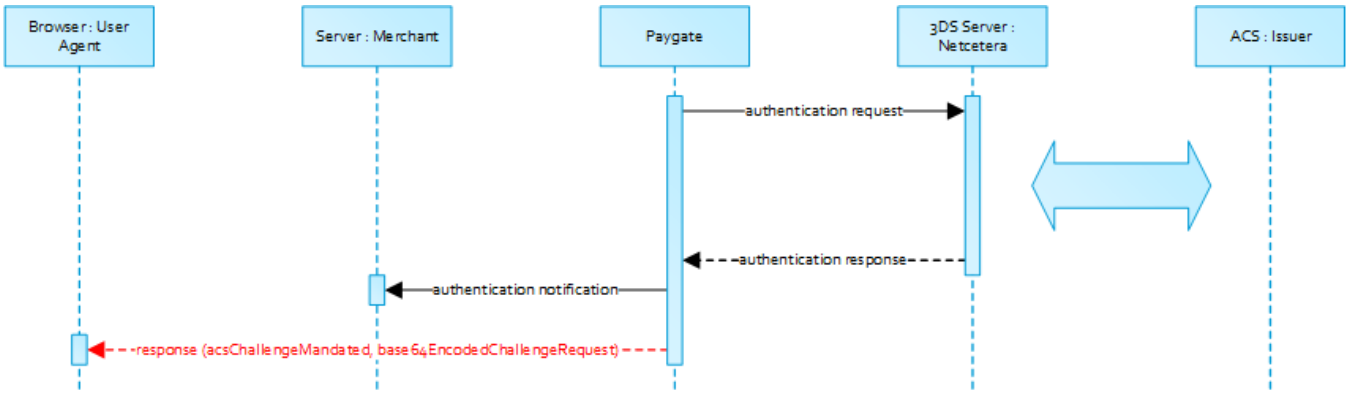
Authentisierung

Wenn die 3DS-Methode vom ACS des Issuers unterstützt wird und vom Händler aufgerufen wurde, setzt das Computop Paygate automatisch mit der Authentisierungsanfrage fort, nachdem die 3DS-Methode abgeschlossen ist (d.h. 3DS Methoden-Benachrichtigung).

Das Ergebnis der Authentisierung wird per HTTP POST an die **`URLNotify`** übertragen. Es kann anzeigen, dass der Karteninhaber authentisiert worden ist oder dass eine weitere Interaktion des Karteninhabers (d.h. Challenge) für den Abschluss der Authentisierung erforderlich ist.

Falls für den Karteninhaber eine Challenge für nötig angesehen ist, überträgt das Computop Paygate ein JSON-Objekt im Body der HTTP Browser-Antwort mit den Elementen **`acsChallengeMandated`**, **`challengeRequest`**, **`base64EncodedChallengeRequest`** und **`acsURL`**. Anderenfalls setzt das Computop Paygate in einem reibungslosen Ablauf automatisch fort und antwortet dem Browser des Karteninhabers, sobald die Autorisierung abgeschlossen ist.

Karteninhaber-Challenge: Browser-Antwort



Browser Challenge-Antwort

Datenelemente

Key	Format	CND	Beschreibung
acsChallengeMandated	boolean	M	Zeigt an, ob eine Challenge für die Autorisierung einer Transaktion wegen lokaler/regionaler Vorschriften oder anderer Variablen nötig ist: • true Challenge ist obligatorisch wegen lokaler/regional Vorschriften • false Challenge ist nicht obligatorisch wegen lokaler/regional Vorschriften, wird aber von ACS als **nötig angesehen**
challengeRequest	object	M	Objekt Challenge-Anfrage
base64EncodedChallengeRequest	string	M	Base64-codiertes Objekt Challenge-Anfrage
acsURL	string	M	Vollständige URL des ACS, die für das Posten der Challenge-Anfrage verwendet werden soll

Schema: Browser Challenge-Antwort

```
{
        "$schema": "http://json-schema.org/draft-07/schema#",
        "type": "object",
        "properties": {
                "acsChallengeMandated": {"type": "boolean"},
                "challengeRequest": {"type": "object"},
                "base64EncodedChallengeRequest": {"type": "string"},
                "acsURL": {"type": "string"}
        },
```

```
        "required": ["acsChallengeMandated", "challengeRequest", "base64EncodedChallengeRequest", "acsURL"],
        "additionalProperties": false
}
```

Beispiel: Browser Challenge-Antwort

```
{
        "acsChallengeMandated": false,
        "challengeRequest": {
                "threeDSServerTransID": "8a880dc0-d2d2-4067-bcb1-b08d1690b26e",
                "acsTransID": "d7c1ee99-9478-44a6-b1f2-391e29c6b340",
                "messageType": "CReq",
                "messageVersion": "2.1.0",
                "challengeWindowSize": "01",
                "messageExtension": [
                        {
                                "name": "emvcomsgextInChallenge",
                                "id": "tc8Qtm465Ln1FX0nZprA",
                                "criticalityIndicator": false,
                                "data": "messageExtensionDataInChallenge"
                        }
                ]
        },
        "base64EncodedChallengeRequest": "base64-encoded-challenge-request",
        "acsURL": "acsURL-to-post-challenge-request"
}
```

Authentisierungs-Benachrichtigung

Die Datenelemente der Authentisierungs-Benachrichtigung stehen in folgender Tabelle.

Key	Format	CND	Beschreibung
mid	ans..30	M	HändlerID, die von Computop vergeben wird
PayID	an32	M	Vom Paygate vergebene ID für die Zahlung; z.B. zur Referenzierung in Batch-Dateien sowie im Capture- oder Credit-Request.
TransID	ans..64	M	Ihre eigene TransaktionsID, die für jede Zahlung eindeutig sein muss
Code	an8	M	Fehlercode gemäß Paygate Antwort-Codes (A4 Fehlercodes)
MAC	an64	M	Hash Message Authentication Code (HMAC) mit SHA-256-Algorithmus. Details finden Sie hier: • HMAC-Authentisierung (Anfrage) • HMAC-Authentisierung (Notify)
authenticationResponse	JSON	M	Antwort-Objekt als Rückgabe zur Authentisierungs-Anfrage beim ACS

Browser Challenge

Wenn eine Challenge für nötig angesehen wird (siehe challengeRequest), erfolgt die Browser Challenge im Browser des Karteninhabers. Zum Erzeugen einer Challenge ist es erforderlich, den Wert **`base64EncodedChallengeRequest`** über ein HTML-iFrame an die ACS URL zu posten.

Challenge-Anfrage

```
<form name="challengeRequestForm" method="post" action="acsChallengeURL">
        <input type="hidden" name="creq" value="
ewogICAgInRocmVlRFNTZXJ2ZXJUcmFuc0lEIjogIjhhODgwZGMwLWQyZDItNDA2Ny1iY2IxLWIwOGQxNjkwYjI2ZSIsCiAgICAiYWNzVHJhb
nNJRCI6ICJkN2MxZWU5OS05NDc4LTQ0YTYtYjFmMi0zOTFlMjljNmIzNDAiLAogICAgIm1lc3NhZ2VUeXBlIjogIkNSZXEiLAogICAgIm1lc3
NhZ2VWZXJzaW9uIjogIjIuMS4wIiwKICAgICJjaGFsbGVuZ2VXaW5kb3dTaXplIjogIjAxIiwKICAgICJtZXNzYWdlRXh0ZW5zaW9uIjogWwo
JCXsKCQkJIm5hbWUiOiAiZW12Y29tc2dleHRJbkNoYWxsZW5nZSIsCgkJCSJpZCI6ICJ0YzhRdG00NjVMbjFGWDBuWnByQSIsCgkJCSJjcml0
aWNhbGl0eUluZGljYXRvciI6IGZhbHNlLAoJCQkiZGF0YSI6ICJtZXNzYWdlRXh0ZW5zaW9uRGF0YUluQ2hhbGxlbmdlIgoJCX0KICAgIF0Kf
Q==">
</form>
```

Sie können die Operationen **`init3DSChallengeRequest`** oder **`createIFrameAndInit3DSChallengeRequest`** aus dem nca3DSWebSDK verwenden, um die Challenge-Nachricht an den Browser des Karteninhabers zu übermitteln.

3DS Challenge-Anfrage initialisieren - Beispiel

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <script src="nca-3ds-web-sdk.js" type="text/javascript"></script>
    <title>Init 3-D Secure Challenge Request - Example</title>
</head>
<body>
<!-- This example will show how to initiate Challenge Reqeuests for different window sizes. -->
<div id="frameContainer01"></div>
<div id="frameContainer02"></div>
<div id="frameContainer03"></div>
<div id="frameContainer04"></div>
<div id="frameContainer05"></div>
<iframe id="iframeContainerFull" name="iframeContainerFull" width="100%" height="100%"></iframe>

<script type="text/javascript">
    // Load all containers
    iFrameContainerFull = document.getElementById('iframeContainerFull');
    container01 = document.getElementById('frameContainer01');
    container02 = document.getElementById('frameContainer02');
    container03 = document.getElementById('frameContainer03');
    container04 = document.getElementById('frameContainer04');
    container05 = document.getElementById('frameContainer05');


    // nca3DSWebSDK.init3DSChallengeRequest(acsUrl, creqData, container);
    nca3DSWebSDK.init3DSChallengeRequest('http://example.com', 'base64-encoded-challenge-request',
iFrameContainerFull);

    // nca3DSWebSDK.createIFrameAndInit3DSChallengeRequest(acsUrl, creqData, challengeWindowSize, frameName,
rootContainer, callbackWhenLoaded);
    nca3DSWebSDK.createIFrameAndInit3DSChallengeRequest('http://example.com', 'base64-encoded-challenge-
request', '01', 'threeDSCReq01', container01);
    nca3DSWebSDK.createIFrameAndInit3DSChallengeRequest('http://example.com', 'base64-encoded-challenge-
request', '02', 'threeDSCReq02', container02);
    nca3DSWebSDK.createIFrameAndInit3DSChallengeRequest('http://example.com', 'base64-encoded-challenge-
request', '03', 'threeDSCReq03', container03);
    nca3DSWebSDK.createIFrameAndInit3DSChallengeRequest('http://example.com', 'base64-encoded-challenge-
request', '04', 'threeDSCReq04', container04);
    nca3DSWebSDK.createIFrameAndInit3DSChallengeRequest('http://example.com', 'base64-encoded-challenge-
request', '05', 'threeDSCReq05', container05, () => {
        console.log('Iframe loaded, form created and submitted');
    });
</script>

</body>
</html>
```

Sobald die Challenge des Karteninhabers abgeschlossen, abgebrochen oder per Zeitüberschreitung beendet ist, weist der ACS den Browser an, die Ergebnisse per Post an die in der Challenge-Anfrage angegebene Benachrichtigungs-URL zu senden und eine Ergebnis-Anfrage (RReq) über den Directory Server an den 3DS Server zu senden.

Beachten Sie bitte, dass die in der Challenge-Anfrage übergebene Benachrichtigungs-URL auf das Computop Paygate zeigt und nicht verändert werden darf.

Autorisierung

Nachdem die erfolgreiche Authentisierung des Karteninhabers oder der Nachweis der versuchten Authentisierung/Verifizierung bereitgestellt ist, setzt das Computop Paygate die Zahlungsautorisierung automatisch fort.

Falls die Authentisierung des Karteninhabers nicht erfolgreich war oder der Nachweise der versuchten Authentisierung/Verifizierung nicht bereitgestellt werden kann, setzt das Computop Paygate nicht mit einer Autorisierungsanfrage fort.

In beiden Fällen liefert das Paygate eine Benachrichtigung mit dem Ergebnis der Authentifizierung an die vom Händler angegebene **`URLNotify`** mit den Datenelementen gemäß nachstehender Tabelle.

Zahlungs-Benachrichtigung

Bei Verwendung der Key-Value-Pair-API

Die folgende Tabelle beschreibt die Ergebnis-Parameter, die das Paygate an Ihre **URLSuccess, URLFailure** und **URLNotify** übergibt. Wenn Sie den Parameter **Response=encrypt** angegeben haben, werden die folgenden Parameter mit Blowfish verschlüsselt an Ihr System übergeben:

es können jederzeit neue Parameter hinzugefügt bzw. die Reihenfolge geändert werden

die Parameter (z.B. mid, RefNr) sollten nicht auf Groß-/Kleinschreibung geprüft werden

Key	Format	CND	Beschreibung
mid	ans..30	M	HändlerID, die von Computop vergeben wird
msgver	ans..5	M	Computop Paygate Message-Version. Zulässige Werte: **Wert** / **Beschreibung** 2.0 – Mit 3-D Secure 2.x wurde eine Vielzahl zusätzlicher Daten (Browser-Information, Rechnungs-/Versand-Adresse, ...) erforderlich, um den Authentifizierungs-Prozess zu optimieren. Um diese Informationen zu handhaben, wurden die JSON-Objekte eingeführt. Der Parameter MsgVer zeigt an, dass diese Daten verwendet werden.
PayID	an32	M	Vom Paygate vergebene ID für die Zahlung; z.B. zur Referenzierung in Batch-Dateien sowie im Capture- oder Credit-Request.
XID	an32	M	Vom Paygate vergebene ID für alle einzelnen Transaktionen (Autorisierung, Buchung, Gutschrift), die für eine Zahlung durchgeführt werden
TransID	ans..64	M	Ihre eigene TransaktionsID, die für jede Zahlung eindeutig sein muss
schemeReferenceID	ans..64	C	Spezifische Transaktions-ID des Kartenschemas, die für nachfolgende Zahlungen mit gespeicherten Zugangsdaten, verzögerte Autorisierungen und Wiedereinreichungen erforderlich ist. Pflicht: CredentialOnFile – initial false – unschedule MIT / recurring schemeReferenceID wird bei 3DS2-Zahlungsvorgängen zurückgegeben. Bei einem Fallback auf 3DS1 prüfen Sie bitte zusätzlich auf TransactionId. Die SchemeReferenceID ist eine eindeutige Kennung, die von den Kartenmarken generiert wird. In der Regel können Computop-Händler die SchemeReferenceIDs für Abonnements übergreifend verwenden, welche unter Verwendung eines anderen PSP / separater Paygate-MerchantID / separater Acquirer ContractID / Acquirer erstellt wurden.
TrxTime	an21	M	Zeitstempel der Transaktion im Format TT.MM.JJJJ HH:mm:ssff
Status	a..20	M	Status der Transaktion. Zulässige Werte: • **`Authorized`** • **`OK`** (Sale) • **`PENDING`** • **`FAILED`** Im Falle von **nur Authentisierung** ist der **Status** entweder **`OK`** oder **`FAILED`** .
Description	ans..1024	M	Nähere Beschreibung bei Ablehnung der Zahlung. Bitte nutzen Sie **nicht** den Parameter **Description, sondern** Code für die Auswertung des Transaktionsstatus!
Code	an8	M	Fehlercode gemäß Paygate Antwort-Codes (A4 Fehlercodes)
MAC	an64	M	Hash Message Authentication Code (HMAC) mit SHA-256-Algorithmus. Details finden Sie hier: • HMAC-Authentisierung (Anfrage) • HMAC-Authentisierung (Notify)
card	JSON	M	Kartendaten
ipinfo	JSON	O	Objekt mit IP-Informationen
threedsdata	JSON	M	Authentisierungsdaten
resultsresponse	JSON	C	Falls der Authentisierungsprozess eine Challenge des Karteninhabers enthalten hat, werden zusätzliche Informationen über das Ergebnis der Challenge bereitgestellt

externalPaymentData	JSON	O	Optionale Daten des Acquirers/Issuers/externen Dienstleisters für eine Autorisierung
PCNr	n16	O	Pseudo Card Number: Vom Computop Paygate generierte Zufallszahl, die eine reale Kreditkartennummer repräsentiert. Die Pseudokartennummer (PKN) beginnt mit 0, und die letzten 3 Stellen entsprechen denen der realen Kartennummer. Die PKN kann wie eine Kreditkartennummer für Autorisierung, Buchung und Gutschriften verwendet werden. PCNr ist ein **Antwortwert** von Computop Paygate und kann ebenfalls als CCNr im Request oder als Teil von card-JSON verwendet werden.

Browser Zahlungs-Antwort

Zusätzlich werden nachstehende Datenelemente im JSON-Format im Body der HTTP-Antwort zum Browser des Karteninhabers übertragen. Beachten Sie bitte, dass die Datenelemente (d.h. **`MID`**, **`Len`**, **`Data`**) base64-codiert sind.

Datenelemente

Key	Format	CND	Beschreibung
mid	ans..30	M	HändlerID, die von Computop vergeben wird
Len	integer	M	Länge des unverschlüsselten Strings **`Data`**
Data	string	M	Blowfish-verschlüsselter String, der ein JSON-Objekt mit **`MID`** , **`PayID`** und **`TransID`** enthält

Schema

```
{
        "$schema": "http://json-schema.org/draft-07/schema#",
        "type": "object",
        "properties": {
                "MID": {
                        "type": "string"
                },
                "Len": {
                        "type": "integer"
                },
                "Data": {
                        "type": "string"
                }
        },
        "required": ["MID", "Len", "Data"],
        "additionalProperties": false
}
```

Händler sollten diese Datenelemente zur Entschlüsselung und für den Abgleich mit der Zahlungs-Benachrichtigung am ihren Server weiterleiten. Basierend auf dem Zahlungsergebnis kann der Händler-Server eine entsprechende Antwort an den Browser des Karteninhabers senden (z.B. Erfolgsseite).

Entschlüsseltes Objekt Data

Key	Format	CND	Beschreibung
mid	ans..30	M	HändlerID, die von Computop vergeben wird
PayID	an32	M	Vom Paygate vergebene ID für die Zahlung; z.B. zur Referenzierung in Batch-Dateien sowie im Capture- oder Credit-Request.
TransID	ans..64	M	Ihre eigene TransaktionsID, die für jede Zahlung eindeutig sein muss

Beispiel für entschlüsseltes Objekt Data

```
MID=YourMID&PayID=PayIDassignedbyPlatform&TransID=YourTransID
```