REST API 3D Secure

3D Secure (3DS) ist eine Authentifizierungsmethode, die zusätzlichen Schutz vor Betrug bei Online-Kartenzahlungen bietet. Wenn Sie Zahlungen innerhalb des Europäischen Wirtschaftsraums akzeptieren, ist die Authentifizierung der Transaktionen mit 3D Secure zwingend erforderlich, um die Anforderungen der PSD2 SCA (Strong Customer Authentication) zu erfüllen.

3D Secure Integrationsoptionen

Computop Paygate ermöglicht die 3DS-Authentifizierung für alle Integrationsarten:

Hosted Payment Page oder gehostete Formulare

Wenn Sie die Hosted Payment Page oder gehostete Formulare des Computop Paygate nutzen, sind für die Implementierung von 3DS keine weiteren Schritte erforderlich. Das Computop Paygate übernimmt den gesamten Authentifizierungsprozess automatisch für Sie und stellt die Einhaltung der PSD2-SCA-Anforderungen sicher.

Direkte Integration

Für Händler, die die direkte Integration verwenden, hängt die Implementierung von 3DS davon ab, wie Sie den Authentifizierungsprozess handhaben:

Vom Händler verwaltete 3DS-Authentifizierung

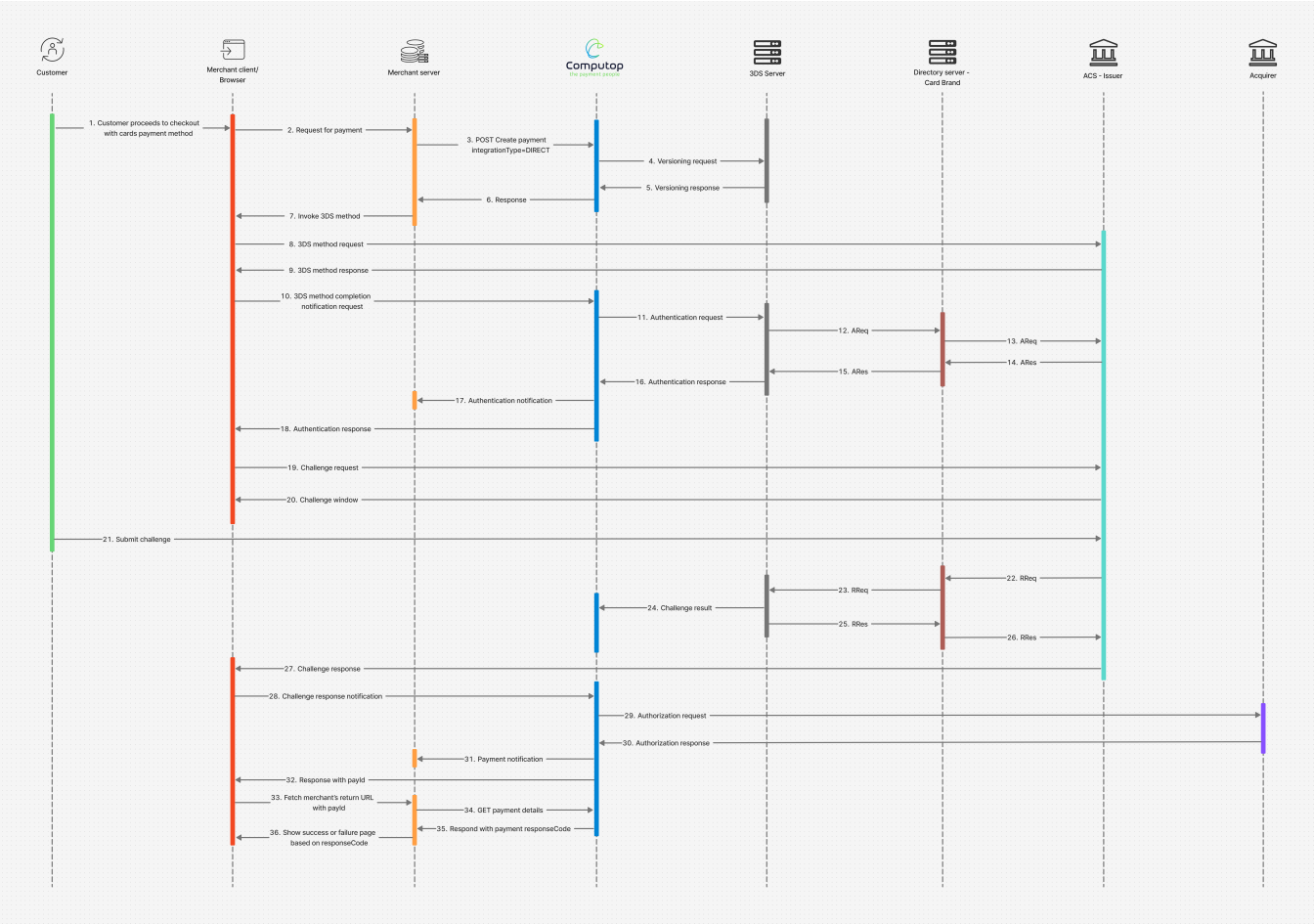
Wenn Sie den 3DS-Authentifizierungsprozess unabhängig verwalten, bevor Sie die Zahlungsanforderung an Computop senden, stellen Sie sicher, dass alle relevanten Authentifizierungsdaten im Objekt `paymentMethods.card.threedsdata` innerhalb der Zahlungsanfrage enthalten sind.

```
{
    "acsProtocolVersion": "2.2.0",
    "authenticationValue": "AAABBIcWERFgUFgUQklFQRE=",
    "eci": "02",
    "threeDSServerTransID": "55570cf-bt5b-43fe-bd0d-2trr3427401c",
    "acsXID": "34565040-e95d-4f55-9aa1-d48d1234acd4",
    "dsTransID": "4347f607-d631-4ad5-34564533cadce558",
    "intermediateStatus": "Y",
    "finalStatus": "Y",
    "challengeRequestInd": "01"
}
```

Vom Computop Paygate verwaltete 3DS-Authentifizierung

Dieser Abschnitt beschreibt den Prozessablauf für Händler, die den 3DS-Authentifizierungsprozess von Computop durchführen lassen möchten.

Prozessablauf



1. Der Kunde geht mit Kartenzahlung als bevorzugter Zahlungsmethode in Ihrem Webshop zur Kasse und übermittelt alle Kartendaten.

2. Ihr Frontend stellt eine Zahlungsanforderung an Ihr Backend.

3. Ihr Backend machte einen Aufruf Zahlung anlegen an das Computop Paygate.

Versionierung:

4. Das Computop Paygate sendet eine Versionierungsanfrage an den 3DS-Server, um die Protokollversionen des Access Control Servers (ACS) und des Directory Servers (DS) abzurufen, die dem Kartenkontobereich entsprechen, sowie optional eine URL der 3D-Secure-Methode.

5. Das Computop Paygate erhält die Versionierungsantwort mit den ACS- und DS-Protokollversionen.

6. Das Computop Paygate antwortet mit einem HTTP 201-Antwortcode an Ihr Backend mit Versionsdaten in `paymentMethods.card.versioningData`

```
{
    "threeDSServerTransID": "f049e8fb-5d93-1234-b995-3eaf05cef06a",
    "acsStartProtocolVersion": "2.2.0",
    "acsEndProtocolVersion": "2.2.0",
    "dsStartProtocolVersion": "2.2.0",
    "dsEndProtocolVersion": "2.2.0",
    "threeDSMethodURL": "https://testacsserver.com/3ds-method",
    "threeDSMethodDataForm":
"eyJ0aHJlZURTTWV0aG9kTm90aWZpY2F0aW9uVVJMIjoiaHR0cHM6Ly93d3cuY29tcHV0b3AtcGF5Z2F0ZS5jb20vY2JUaHJlZURTLmFzcHg_
YWN0aW9uPW10aGROdGZuIiwidGhyZWVEU1NlcnZlclRyYW5zSUQiOiJmMDQ5ZThmYi01ZDkzLTQ2MTAtYjk5NS0zZWFmMDVjZWYwNmEifQ",
    "threeDSMethodData": {
        "threeDSMethodNotificationURL": "https://www.computop-paygate.com/cbThreeDS.aspx?action=mthdNtfn",
        "threeDSServerTransID": "f049e8fb-5d93-4610-b995-3eaf05cef06a"
    }
}
```

Die Gründe für fehlende Parameter in versioningData finden Sie im Objekt `paymentMethods.card.versioningData.errorDetails`.

3DS-Methode: Die 3DS-Methode ist ein optionaler Schritt im 3DS-Authentifizierungsablauf. Sie ermöglicht es dem ACS des Kartenausstellers, zusätzliche Browser-/Geräteinformationen zu erfassen, bevor die eigentliche Authentifizierungsanfrage (AReq) gesendet wird. Diese Daten ermöglichen dem ACS eine genauere Risikobewertung der Transaktion.

7. Basierend auf der erhaltenen Versionierungsantwort sollte der Prozess 3DS-Methode aufgerufen werden. Dazu muss Ihr Backend Ihrem Frontend die aus der Versionierungsantwort erhaltenen `threeDSMethodData` und `threeDSMethodURL` bereitstellen. Ihr Frontend sollte einen versteckten Iframe mit einem Formular mit einem versteckten Eingabefeld für `threeDSMethodData` erstellen und an `threeDSMethodURL` übermitteln. Die `threeDSMethodData` sollten Base64-kodiert gesendet werden und können direkt aus `threeDSMethodDataForm` in der Versionierungsantwort abgerufen werden. Nachfolgend sehen Sie ein Beispiel für die Implementierung:

```
<form name="threeDSMethodForm" method="POST" action="https://testacsserver.com/3ds-method">
  <input type="hidden" name="threeDSMethodData" value="
eyJ0aHJlZURTU2VydmVyVHJhbnNJRCI6IjNhYzdjYWE3LWFhNDItMjY2My03OTFiLTJhYzA1YTU0MmM0YSIsInRocmVlRFNNZXRob2ROb3RpZ
mljYXRpb25VUkwiOiJ0aHJlZURTTWV0aG9kTm90aWZpY2F0aW9uVVJMIn0">
</form>
```

Wenn der Issuer den Prozess 3DS-Methode nicht untestützt, füllt das Computop Paygate `threeDSMethodURL` aus, damit der Prozess 3DS-Methode zum Senden des versteckten Formulars trotzdem durchgeführt werden kann. Dies ist notwendig, um die direkte Kommunikation zwischen dem Browser und Computop Paygate im 3DS-Prozessablauf zu ermöglichen.

> Sie können nach eigenem Ermessen die Operationen `init3DSMethod` oder `createIframeAndInit3DSMethod` aus dem netcetra3DS WebSDK verwenden, um die 3-D Secure-Methode zu initiieren.

8. Ihr Frontend sendet das versteckte Formular an die ACS 3DS Method URL, die es ACS ermöglicht, alle erforderlichen Informationen zu erfassen.

9. ACS antwortet auf die Anfrage 3DS-Methode mit einen HTML-Dokument.

10. Das HTML-Dokument enthält JavaScript, das automatisch ein verstecktes Formular mit den `threeDSMethodData` erzeugt und an die `threeDSMethodNotificationURL` sendet, die vom Computop Paygate gehostet wird.

Authentifizierung:

11. Nach Erhalte der 3DS-Abschlussbenachrichtigung sendet das Computop Paygate eine Authentifizierungsanfrage an den 3DS-Server.

12. Der 3DS-Server sendet eine Authentifizierungsanforderung an den Directory-Server.

13. Der Directory-Server sendet eine Authentifizierungsanforderung an ACS

14. ACS sendet eine Authentifizierungsantwort an den Directory-Server zurück

15. Der Directory-Server leitet die Antwort an den 3DS-Server weiter

16. Der 3DS-Server leitet die Antwort an das Computop Paygate weiter. Falls die Authentifizierungsantwort keine Challenge erfordert, springt der Prozess zu Schritt 29, andernfalls beginnt der nachfolgende Challenge-Prozess.

17. Computop Paygate sendet eine Benachchtigung mit der `payId` im Text an to `urls.webhook`, den Sie in der ursprünglichen Anfrage übermittel haben (Schritt 3). Sie können Zahlungsdetails abfragen with `payId` aufrufen, um alle Daten der Authentisierungs-Antwort abzurufen.

18. Computop Paygate sendet zusätzlich die Authentifizierungsantwort (base64-kodiert) als Antwort auf die Benachrichtigungsanfrage zum 3DS-Methodenabschluss (Schritt 10) an den Browser. Der iframe verwendet window.postMessage(), um die Base64-kodierte JSON-Nutzlast an die übergeordnete Seite zu senden. Nachfolgend ein Ausschnitt der dekodierten Authentifizierungsantwort, die an den Browser gesendet wurde.

ChallengeWindowSize wird anhand der in browserInfo bereitgestellten Viewport-Abmessungen berechnet. Wenn der Händler kleinere Abmessungen angibt, werden diese an das ACS übermittelt. Obwohl die meisten ACS für ihre SCA/OTP-Ansichten ein responsives Design verwenden, gibt es keine Garantie dafür, dass jede Größe funktioniert oder optisch ansprechend dargestellt wird.


```
{
  "threeDSServerTransID": "f049e8fb-5d93-1234-b995-3eaf05cef06a",
  "acsChallengeMandated": true,
  "acsDecConInd": false,
  "acsOperatorID": "10024942",
  "acsReferenceNumber": "3DS_LOA_ACS_HIIN_020200_00553",
  "acsTransID": "70283ff7-df85-44be-b157-3bc6f8a31b89",
  "acsURL": "https://testacsserver.com/3ds-method",
  "dsReferenceNumber": "VISA.V 17 0003",
  "dsTransID": "2f15b09e-b915-4d5e-9f04-239ed985f3bb",
  "messageType": "ARes",
  "messageVersion": "2.2.0",
  "transStatus": "C",
  "challengeRequest": {
      "threeDSServerTransID": "f049e8fb-5d93-1234-b995-3eaf05cef06a",
      "acsTransID": "70283ff7-df85-44be-b157-3bc6f8a31b89",
      "challengeWindowSize": "04",
      "messageVersion": "2.2.0",
      "messageType": "CReq"
  },
  "base64EncodedChallengeRequest":
"eyJtZXNzYWdlVHlwZSI6IkNSZXEiLCJ0aHJlZURTU2VydmVyVHJhbnNJRCI6ImYwNDllOGZiLTVkOTMtNDYxMC1iOTk1LTNlYWYwNWNlZjA2
YSIsImFjc1RyYW5zSUQiOiI3MDI4M2ZmNy1kZjg1LTQ0YmUtYjE1Ny0zYmM2ZjhhMzFiODkiLCJjaGFsbGVuZ2VXaW5kb3dTaXplIjoiMDQiL
CJtZXNzYWdlVmVyc2lvbiI6IjIuMi4wIn0"
}
```


Challenge:

19. Basierend auf der erhaltenen Authentifizierungsantwort sollte Ihr Frontend eine Challenge-Anfrage erzeugen. Dazu dekodieren Sie die Authenfizierungsantwort und erfassen die in `base64EncodedChallengeRequest` und `acsURL` vorhandenen Werte. Senden Sie `base64EncodedChallengeRequest` über einen Iframe der Größe x (entweder challengeWindowSize oder go 05; 100%*100%). Nachfolgend sehen Sie ein Beispiel für die Implementierung:


```
<form name="challengeRequestForm" method="POST" action="https://testacsserver.com/3ds-method">
  <input type="hidden" name="creq" value="
eyJtZXNzYWdlVHlwZSI6IkNSZXEiLCJ0aHJlZURTU2VydmVyVHJhbnNJRCI6ImYwNDllOGZiLTVkOTMtNDYxMC1iOTk1LTNlYWYwNWNlZjA2Y
SIsImFjc1RyYW5zSUQiOiI3MDI4M2ZmNy1kZjg1LTQ0YmUtYjE1Ny0zYmM2ZjhhMzFiODkiLCJjaGFsbGVuZ2VXaW5kb3dTaXplIjoiMDQiLC
JtZXNzYWdlVmVyc2lvbiI6IjIuMi4wIn0">
</form>
```


> Sie können nach eigenem Ermessen die Operationen `init3DSChallengeRequest` oder `createIFrameAndInit3DSChallengeRequest` aus dem netcetra3DSWebSDK verwenden, um eine Challenge-Anfrage zu senden.

20. ACS rendert das Challenge-Fenster im Browser.

21. Der Kunde absolviert die Challenge.

22. ACS benachrichtigt den Directory-Server über das Ergebnis der Challenge mittels Ergebnisanforderungsnachricht (RReq).

23. Der Directory-Server leitet die RReq an den 3DS-Server weiter.

24. Der 3DS-Server leitet das Challenge-Ergebnis an das Computop Paygate weiter.

25. Der 3DS-Server bestätigt RReq mit einer Ergebnisantwort (RRes) an den Directory-Server.

26. Der Directory-Server leitet RRes an ACS weiter.

27. ACS stellt dem Browser zusätzlich die Challenge-Antwort als Antwort auf „Challenge senden“ (Schritt 21) zur Verfügung. Ihr Frontend sollte die an das Iframe zurückgegebene Challenge-Antwort abhören.

28. Sobald die Challenge-Antwort eingegangen ist, sendet Ihr Frontend eine Challenge-Antwort-Benachrichtigungsanforderung an das Computop Paygate. Nachstehend sehen Sie das dekodierte JSON-Beispiel:

```
{
  "messageType": "CRes",
  "messageVersion": "2.2.0",
  "threeDSServerTransID": "f049e8fb-5d93-1234-b995-3eaf05cef06a",
  "acsTransID": "70283ff7-df85-44be-b157-3bc6f8a31b89",
  "challengeCompletionInd": "Y",
  "transStatus": "Y"
}
```


Autorisierung:

29. Computop Paygate führt die Autorisierung beim Acquirer durch.

30. Der Acquirer übermittelt die Autorisierungsantwort an Computop Paygate.

31. Computop Paygate sendet eine Benachrichtigung mit `payId` im Nachrichtentext an `urls.webhook`, den Sie ursprünglich übermittelt haben (Schritt 3). Sie können Zahlungsdetails abfragen mit `payId` aufrufen, um alle Daten der Autorisierungsantwort zu erhalten.

32. Computop Paygate antwortet dem Browser zusätzlich mit der `payId` im Nachrichtentext als Antwort auf Schritt 28. Der Iframe verwendet window.postMessage(), um das zu senden.

33. Ihr Frontend ruft die Rücksprung-URL Ihres Shops mit `payId` von Ihrem Backend auf.

34. Ihr Backend führt Zahlungsdetails abfragen mit `payId` am Computop Paygate aus, um den endgültigen responseCode der Transaktion abzurufen.

35. Computop Paygate antwortet mit dem responseCode der Transaktion.

36. Ihr Backend rendert je nach responseCode der Transaktion eine Erfolgs- oder Fehlerseite.