

Stille Auftragserteilung (PayNow)

Überblick

- Überblick
- Zahlungsanfrage
 - [Webseite direkte](#)
 - Daten
 - [Beispiel HTML-Formular](#)
- [HTTP POST an URLSuccess /](#)

Eine **Stille Auftragserteilung** oder **Direkte Erteilung** ist eine Übertragungsmethode, bei der Formulardaten von einer Händler-Webseite direkt an einen Computop Paygate übergeben werden. Dies wird üblicherweise durch das Attribut **form action** erreicht, welches die URL angibt, wohin die Daten zu senden sind.

i Sensible Daten wie Kartendetails können innerhalb der Händler-Webseite erfasst werden, ohne dass diese vom Server des Händlers verarbeitet werden. Stattdessen werden die Daten im Computop Paygate für den Empfang von Anfragen der Stillen Auftragserteilung als **PayNow** bezeichnet.

```
<form action=".. /payNow.aspx" method="post">
```

[Hinweise zum Cookie-/session-Handling](#)

Dieser Ansatz ist sehr ähnlich zu den bei Computop gehosteten Zahlungsformularen und lässt dem Händler die volle Kontrolle über den Bezahlvorgang bereitgestellt werden.

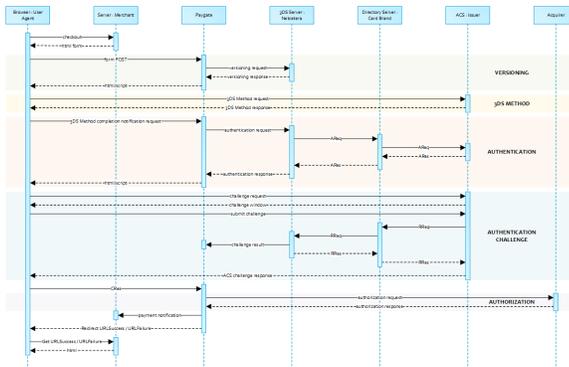
! PCI-DSS Betrachtungen

Händler, die Kartentransaktionen mit dem Modell der Stillen Erteilung verarbeiten, müssen den Fragebogen PCI DSS Self-Assessment Questionnaire (SAQ) A für Händler, die gehostete Zahlungsseiten verwenden. Händler sollten sich beraten, um das Maß der erforderlichen Compliance zu beurteilen und dabei die [PCI DSS Richtlinien](#) beachten. Das wirkt sich nicht auf die Verarbeitung ohne Einreichung des SAQ-Fragebogens möglich ist.

! Hinweis zum Cookie-/Session Handling

Bitte beachten Sie, dass einige Browser beim Rücksprung zu Ihrem Shop erforderliche Cookies blockieren könnten. [Hier](#) finden Sie weitere Informationen.

Sequenzdiagramm



Zahlungsanfrage

Bitte übermitteln Sie die Formulardaten per POST wie in der nachstehenden Tabelle dargestellt an <https://www.computop-paygate.com/payNow.aspx>.

Formularelemente

Data Element	Legacy Element	Beschreibung
MerchantID	--	HändlerID, die von Computop vergeben wird
Len	--	Die Länge des Originals verschlüsselt mit Blowfish
Data	--	Per Blowfish verschlüsselte Daten
number	CCNr	Kartenummer

securityCode	CCCVC	Kartenprüfnummer
expiryDate	CCEpiry	Kartenablaufdatum im Format JJJJMM
brand	CCBrand	Kartensystem
cardholder	CreditCardHolder	Name des Karteninhabers, wie er auf der Karte gedruckt ist. Hinweis: Alphanumerische Sonderzeichen gemäß EMV Book 4, „Anhang B“. Sonderzeichen wurden mit EMV 3DS Ver (Banken) unterstützen diesen Standard bereits.

(- Computop wird weiterhin die alten Formulardatenfelder unterstützen, die derzeit verwendet werden. -)

Daten

Key	Format	CND	Beschreibung
MerchantID	ans..30	M	HändlerID, die von Computop vergeben wird. Dieser Parameter ist zusätzlich auch unverschlüsselt zu übergeben.

Key	Format	CND	Beschreibung
TransID	ans..64	M	Ihre eigene TransaktionsID, die für jede Zahlung eindeutig sein muss

Key	Format	CND	Beschreibung
MsgVer	ans..5	M	Message-Version. Zulässige Werte: <ul style="list-style-type: none"> • 2.0
RefNr		O	Eindeutige Referenznummer des Händlers, welche als Auszahlungsreferenz in der entsprechenden Acquirer EPA-Datei angegeben wird eigenen Auszahlungsreferenz können Sie die EPA-Transaktionen nicht zuordnen, zusätzlich kann das Computop Settlement File (CTS)  Informationen zum unterstützten Format finden Sie weiter unten in der zahlartspezifischen Beschreibung. Es sind ausschließlich ASCII-Zeichen erlaubt. Sonderzeichen wie ("Umlaute", ...) sind nicht erlaubt und müssen ggf. durch ASCII-Zeichen ersetzt werden.

Key	Format	CND	Beschreibung
Amount	n..10	M	Betrag in der kleinsten Währungseinheit (z.B. EUR Cent). Bitte wenden Sie sich an den Computop Helpdesk , wenn Sie Beträge < 100 (K)

Key	Format	CND	Beschreibung
Currency	a3	M	Währung, drei Zeichen DIN / ISO 4217, z.B. EUR, USD, GBP. Hier eine Übersicht: A1 Währungstabelle

Key	Format	CND	Beschreibung								
Capture	an..6	OM	Bestimmt Art und Zeitpunkt der Buchung (engl. Capture). <table border="1" data-bbox="418 1402 1495 1581"> <thead> <tr> <th>Buchungsart</th> <th>Beschreibung</th> </tr> </thead> <tbody> <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. Leistung</td> </tr> <tr> <td><Zahl></td> <td>Verzögerung in Stunden bis zur Buchung (ganze Zahl; 1 bis 696).</td> </tr> </tbody> </table>	Buchungsart	Beschreibung	AUTO	Buchung sofort nach Autorisierung (Standardwert).	MANUAL	Buchung erfolgt durch den Händler - in der Regel die Buchung zum Zeitpunkt der Warenauslieferung bzw. Leistung	<Zahl>	Verzögerung in Stunden bis zur Buchung (ganze Zahl; 1 bis 696).
Buchungsart	Beschreibung										
AUTO	Buchung sofort nach Autorisierung (Standardwert).										
MANUAL	Buchung erfolgt durch den Händler - in der Regel die Buchung zum Zeitpunkt der Warenauslieferung bzw. Leistung										
<Zahl>	Verzögerung in Stunden bis zur Buchung (ganze Zahl; 1 bis 696).										

Key	Format	CND	Beschreibung
billingDescriptor	ans..22	O	Ein auf dem Kontoauszug des Karteninhabers zu druckender Beschreiber. Beachten Sie bitte auch die andernorts gemachten z Regeln und Vorschriften.
OrderDesc	ans..768	O	Beschreibung der Bestellung
AccVerify	a3	O	Indikator zur Anforderung einer Konto-Verifizierung (alias Nullwert-Autorisierung). Wenn eine Konto-Verifizierung angefordert wird die tatsächliche Zahlungstransaktion (d.h. Autorisierung) ignoriert. Zulässige Werte: <ul style="list-style-type: none"> • Yes
threeDSPolicy	JSON	O	Objekt, dass die Authentisierungs-Richtlinien und Strategien zur Behandlung von Ausnahmen angibt

priorAuthenticationInfo	JSON	O	Das Objekt Prior Transaction Authentication Information enthält optionale Informationen über eine 3DS-Authentisierung eines K erfolgt ist.
browserInfo	JSON	M	Exakte Browserinformationen sind nötig, um eine optimierte Nutzererfahrung zu liefern. Erforderlich für 3DS 2.0 Transaktionen.
accountInfo	JSON	O	Die Kontoinformationen enthalten optionale Informationen über das Kundenkonto beim Händler.
billToCustomer	JSON	C	Der Kunde, dem die Waren und / oder Dienstleistungen in Rechnung gestellt werden. Erforderlich, sofern nicht Markt- oder regio beschränken.
shipToCustomer	JSON	C	Der Kunde, an den die Waren und / oder Dienstleistungen gesendet werden. Erforderlich, falls von billToCustomer abweichend.
billingAddress	JSON	C	Rechnungsadresse. Erforderlich (falls verfügbar), sofern nicht Markt- oder regionale Mandate das Senden dieser Informationen
shippingAddress	JSON	C	Lieferadresse. Falls abweichend von billingAddress, erforderlich (falls verfügbar), sofern nicht Markt- oder regionale Mandate da
credentialOnFile	JSON	C	Objekt, dass Art und Reihe der Transaktionen angibt, die unter Verwendung von beim Händler hinterlegten Zahlungsdaten (z.B. Verarbeitung künftiger Käufe eines Kunden erfolgen. Erforderlich, falls zutreffend.
merchantRiskIndicator	JSON	O	Der Händler-Risikoindikator enthält optionale Informationen über den bestimmten Einkauf des Kunden. Falls keine <code>shippingAddress</code> vorhanden ist, ist es dringend empfohlen, die Eigenschaft <code>shippingAddressIndicator</code> mit <code>dress</code> , <code>digitalGoods</code> oder <code>noShipment</code> auszufüllen.

Key	Format	CND	Beschreibung
URLSuccess	ans..256	M	Vollständige URL, die das Paygate aufruft, wenn die Zahlung erfolgreich war. Die URL darf nur über Port 443 aufgerufen werden. Diese I durchzureichen nutzen Sie stattdessen den Parameter UserData . i Allgemeine Hinweise: <ul style="list-style-type: none"> Wir empfehlen, den Parameter "response=encrypt" zu verwenden, um eine verschlüsselte Antwort von Paygate zu erhalten Betrüger könnten das verschlüsselte DATA-Element kopieren, welches an URLFailure gesendet wurde, und betrügerisch dasselbe daher unbedingt den "code"-Wert des DATA-Elements. Nur eine Antwort mit "code=00000000" sollte als erfolgreich angesehen we

Key	Format	CND	Beschreibung
URLFailure	ans..256	M	Vollständige URL, die das Paygateaufruft, wenn die Zahlung gescheitert ist. Die URL darf nur über Port 443 aufgerufen werden. Diese UI durchzureichen nutzen Sie stattdessen den Parameter UserData . i Allgemeine Hinweise: <ul style="list-style-type: none"> Wir empfehlen, den Parameter "response=encrypt" zu verwenden, um eine verschlüsselte Antwort von Paygate zu erhalten Betrüger könnten das verschlüsselte DATA-Element kopieren, welches an URLFailure gesendet wurde, und betrügerisch dasselbe Überprüfen Sie daher unbedingt den "code"-Wert des DATA-Elements. Nur eine Antwort mit "code=00000000" sollte als erfolgreich

Key	Format	CND	Beschreibung
URLNotify	ans..256	M	Vollständige URL, die das Paygate aufruft, um den Shop zu benachrichtigen. Die URL darf nur über Port 443 aufgerufen werden. Sie dar den Parameter UserData . i Allgemeine Hinweise: <ul style="list-style-type: none"> Wir empfehlen, den Parameter "response=encrypt" zu verwenden, um eine verschlüsselte Antwort von Paygate zu erhalten Betrüger könnten das verschlüsselte DATA-Element kopieren, welches an URLFailure gesendet wurde, und betrügerisch dasselbe Überprüfen Sie daher unbedingt den "code"-Wert des DATA-Elements. Nur eine Antwort mit "code=00000000" sollte als erfolgreich

Key	Format	CND	Beschreibung
MAC	an64	M	Hash Message Authentication Code (HMAC) mit SHA-256-Algorithmus. Details finden Sie hier: <ul style="list-style-type: none"> HMAC-Authentisierung (Anfrage) HMAC-Authentisierung (Notify)

Key	Format	CND	Beschreibung
UserData	ans..1024	O	Wenn beim Aufruf angegeben, übergibt das Paygate die Parameter mit dem Zahlungsergebnis an den Shop.

Beispiel HTML-Formular

i BASEURL= <https://www.computop-paygate.com/schemas>

```

<!DOCTYPE html>
<html>
  <head>
    <title>Merchant Checkout</title>
  </head>
  <body>
    <form name="card form" action="BASEURLpayNow.aspx" method="post">
      <input type="hidden" name="MerchantID" value="MerchantID">
      <input type="hidden" name="Len" value="Length of the Blowfish encrypted data">
      <input type="hidden" name="Data" value="Blowfish encrypted data">
      Cardholder:
      <input type="text" name="cardholder"><br>
      Card number:
      <input type="text" name="number"><br>
      Expiry date:
      <input type="text" name="expiryDate"><br>
      CVV2:
      <input type="text" name="securityCode"><br>
      Card brand:
      <input type="text" name="brand"><br>
      <input type="submit" value="Submit">
    </form>
  </body>
</html>

```

Wenn die Zahlung abgeschlossen ist, sendet das Computop Paygate eine Benachrichtigung an den Händler-Server (d.h. **URLNotify**) und leitet den Browser zum **Failure** weiter.

Die in der folgenden Tabelle genannten per Blowfish verschlüsselten Datenelemente werden per **HTTP POST** Anfragemethode an URLNotify und URLSuccess



Hinweis: Bitte beachten Sie, dass der Aufruf der URLSuccess oder URLFailure bei einem Fallback zu 3-D Secure 1.0 mit GET stattfindet. Ihre Server können GET als auch per POST entgegennehmen können.

HTTP POST an URLSuccess / URLFailure / URLNotify

Key	Format	CND	Beschreibung		
mid	ans..30	M	HändlerID, die von Computop vergeben wird		
msgver	ans..5	M	Computop Paygate Message-Version. Zulässige Werte: <table border="1" style="margin-left: 20px;"> <tr> <td>2.0</td> <td>Mit 3-D Secure 2.x wurde eine Vielzahl zusätzlicher Daten (Browser-Information, Rechnungs-/Versand-Adresse, ...) erforderlich optimieren. Um diese Informationen zu handhaben, wurden die JSON-Objekte eingeführt. Der Parameter MsgVer zeigt an, ob</td> </tr> </table>	2.0	Mit 3-D Secure 2.x wurde eine Vielzahl zusätzlicher Daten (Browser-Information, Rechnungs-/Versand-Adresse, ...) erforderlich optimieren. Um diese Informationen zu handhaben, wurden die JSON-Objekte eingeführt. Der Parameter MsgVer zeigt an, ob
2.0	Mit 3-D Secure 2.x wurde eine Vielzahl zusätzlicher Daten (Browser-Information, Rechnungs-/Versand-Adresse, ...) erforderlich optimieren. Um diese Informationen zu handhaben, wurden die JSON-Objekte eingeführt. Der Parameter MsgVer zeigt an, ob				
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		
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 Autorisierung Pflicht: CredentialOnFile – initial false – unschedule MIT / recurring schemeReferenceID wird bei 3DS2-Zahlungsvorgängen zurückgegeben. Bei einem Fallback auf 3DS1 prüfen Sie bitte zusätzlich auf Die SchemeReferenceID ist eine eindeutige Kennung, die von den Kartenmarken generiert wird. In der Regel können Computop-Händlerübergreifend verwenden, welche unter Verwendung eines anderen PSP / separater Paygate-MerchantID / separater Acquirer Contract		
refnr		O	Referenznummer vom Request		

Status	a..20	M	Status der Transaktion. Zulässige Werte: <ul style="list-style-type: none"> • Authorized • OK (Sale) • 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 Auswe
Code	n8	M	Fehlercode gemäß Paygate Antwort-Codes (A4 Fehlercodes)
card	JSON	M	Kartenantwortdaten
ipinfo	JSON	C	Objekt mit IP-Informationen. Das Vorhandensein hängt von der Konfiguration des Händlers ab.
threedsdata	JSON	M	Authentisierungsdaten
resultsresponse	JSON	C	Falls der Authentisierungsprozess eine Challenge des Karteninhabers enthalten hat, werden zusätzliche Informationen über das Erg
externalPaymentData	JSON	O	Optionale Daten des Acquirers/Issuers/externen Dienstleisters für eine Autorisierung
UserData	ans..1024	O	Wenn beim Aufruf angegeben, übergibt das Paygate die Parameter mit dem Zahlungsergebnis an den Shop.
MAC	an64	M	Hash Message Authentication Code (HMAC) mit SHA-256-Algorithmus. Details finden Sie hier: <ul style="list-style-type: none"> • HMAC-Authentisierung (Anfrage) • HMAC-Authentisierung (Notify)