

# Programmiergrundlagen

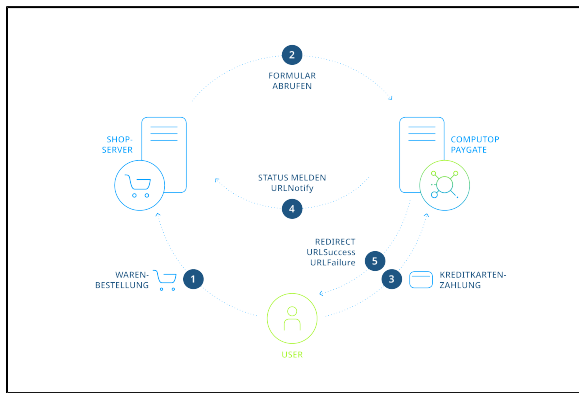
## Programmierung

### Varianten der Händler-Schnittstelle

Das Computop Paygate erlaubt drei Formen der Online-Kommunikation mit Händler-Systemen: Zum einen stellt das Computop Paygate Formulare für die Eingabe der Zahlungsdaten bereit, zum anderen können Sie die Formulare selbst gestalten und die Zahlungen über eine Server-zu-Server-Verbindung zwischen Shop und Computop Paygate-Server im Hintergrund abwickeln.

### Paygate-Formulare

Das Computop Paygate stellt Ihnen HTML-Formulare mit TLS-Verschlüsselung zur Verfügung. Ihr Shop braucht nur das HTML-Formular des Paygate aufzurufen, um den Kunden zur Zahlung mit dem Computop Paygate zu verbinden. Der Kunde gibt dann seine Zahlungsdaten im HTML-Formular des Computop Paygate ein, das ein SSL-Zertifikat von Computop verwendet. Das Computop Paygate führt die Zahlung aus und informiert den Shop über den Transaktionsstatus ([URLNotify](#), [URLSuccess](#), [URLFailure](#)). Formulare verursachen den geringsten Programmieraufwand.



Ablauf einer Zahlung mit Computop Paygate HTML-Formularen

Ein Vorteil ist, dass Kreditkartendaten und Kontoverbindungen nur auf dem Computop Paygate-Server gespeichert werden. So bleiben Sie von den Sicherheitsregularien wie PCI DSS (Payment Card Industry, ehemals VISA AIS MasterCard SDP Site Data Protection) verschont, weil keine Kreditkartendaten im Shop gespeichert werden. Eine Erklärung zu PCI finden Sie weiter unten im Text.

Computop

Kartenzahlung

Diese Seite ist mit SSL verschlüsselt, um Ihre Daten zu schützen.

Kartenmarke: [Auswahl]  
Kartennummer: [Eingabe]  
Gültig bis Monat / Jahr: [Auswahl]  
Kartenprüfnummer: [Eingabe]

Bestätigen

Standard-Paygate-Formular für Kreditkartenzahlungen

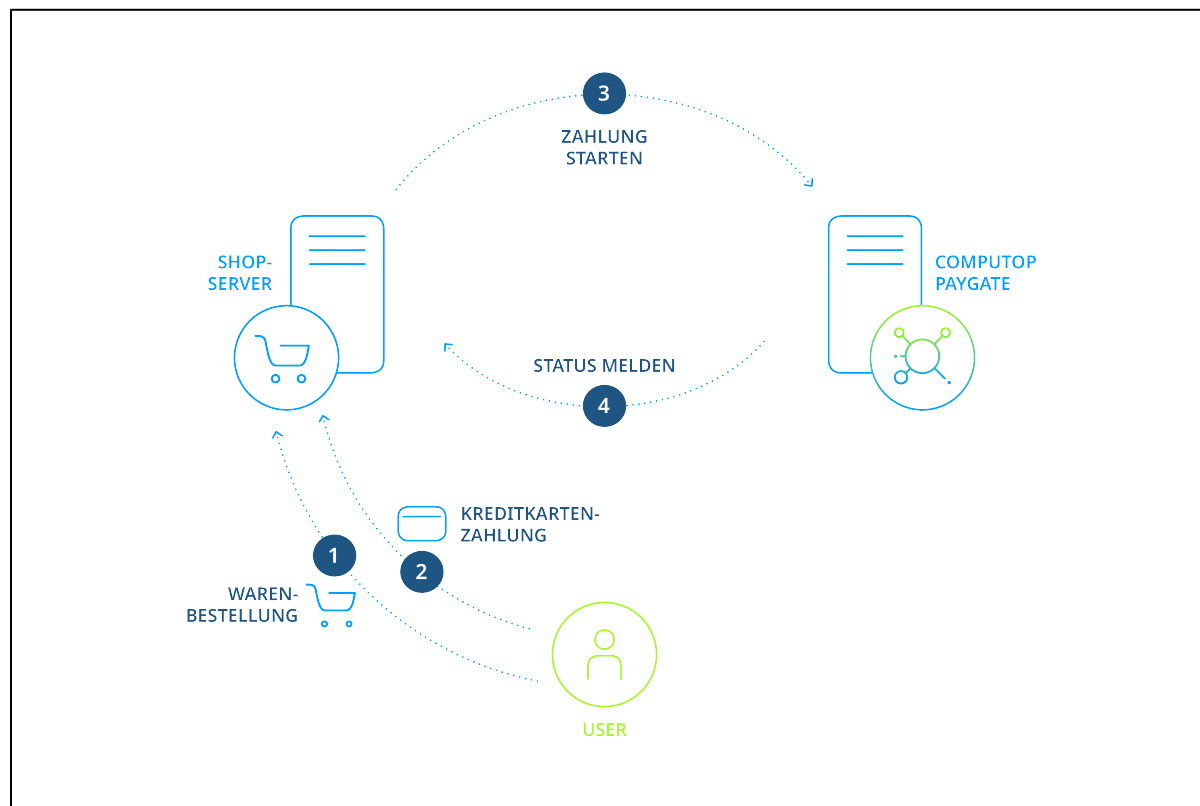
Die Formulare des Computop Paygate sind mehrsprachig konfigurierbar und erlauben die individuelle Auswahl von Farben, Bildern und Schriftformaten, damit die Seite zum Layout des Shops passt. Zusätzlich können für Kreditkartentransaktionen und SEPA-Lastschriften eigene Formulare passende zum Layout des Shops hinterlegt werden (siehe dazu den Abschnitt Corporate PayPage: XSLT-Layout für Formulare im betreffenden Handbuch).

### Zahlungsabwicklung von Server-zu-Server

- **Programmierung**
  - Varianten der Händler-Schnittstelle
    - Paygate-Formulare
    - Zahlungsabwicklung von Server-zu-Server
    - Zahlungsabwicklung über Batch
  - Sicherheit: Payment Card Industry (ehemals Visa AIS und MasterCard SDP)
    - 1) Paygate HTML-Formular
    - 2) Server-zu-Server-Zahlung
    - 3) Batch
    - 4) PayNow – der Silent Mode
  - Prinzipien der Paygate-Programmierung
  - Funktionsweise der Händler-Schnittstelle
- **Zahlungen über Paygate-Formulare**
  - Ablauf der Zahlung
  - Aufruf eines Paygate-Formulars
  - Hash MAC-Authentisierung in der Anfrage
  - Hash MAC-Authentisierung im Notify
  - Benachrichtigung des Shops
  - Weiterleitung des Kunden zum Shop
  - Richtig testen
    - Testfälle mit Timeout
- **Zahlungen per Server-zu-Server-Verbindung**
  - Ablauf einer Server-zu-Server-Zahlung

API Playground

Wenn Sie eigene Formulare für die Eingabe der Zahlungsdaten gestalten wollen, können Sie Ihre Transaktionen über eine Server-zu-Server-Verbindung im Hintergrund abwickeln. In diesem Fall speichert Ihr System Zahlungsdaten wie Kreditkartennummern oder Bankverbindungen und baut dann eine TLS-Socket-Verbindung zum Paygate-Server auf, um die Zahlung auszuführen. Bei dieser Variante steuert Ihr System die Kommunikation mit dem Computop Paygate, so dass mehr Programmieraufwand entsteht als bei Paygate-Formularen, welche die Zahlungen für Sie automatisch abwickeln.



Ablauf einer Server-zu-Server-Zahlung

**Hinweis:** Bitte beachten Sie, dass Buchungen, Gutschriften und Statusabfragen nur über die Server-zu-Server-Verbindung oder per Batch möglich sind.

## Zahlungsabwicklung über Batch

Der Batch-Manager erlaubt die Übertragung von Zahlungstransaktionen in Form von Dateien. Dabei sammeln Sie Transaktionsdaten wie Transaktions-ID, Betrag und Währung in einer Batch-Datei, die Sie später an das Computop Paygate übertragen. Das Paygate führt dann die Zahlungen aus und speichert den Transaktionsstatus in der Batch-Datei. Nach der Verarbeitung kann der Händler die Batch-Datei mit den Angaben zum Transaktionsstatus per Download wieder abrufen.

## Sicherheit: Payment Card Industry (ehemals Visa AIS und MasterCard SDP)

Für die Sicherheit der Kreditkartenzahlungen im Internet ist entscheidend, wo die Kreditkartendaten erfasst und gespeichert werden. Die Kartenorganisationen haben mit der PCI-Sicherheitszertifizierung (Payment Card Industry) ein Sicherheitsprogramm etabliert, um die sichere Speicherung der Kreditkartendaten zu gewährleisten. Bitte beachten Sie, dass die Teilnahme an PCI verpflichtend und kostenpflichtig ist, wenn Sie Kreditkartendaten selbst speichern oder weiterleiten. Entscheidend dafür ist die Variante der Händler-Schnittstelle:

### 1) Paygate HTML-Formular

Hier werden die Kreditkartendaten nur auf dem gesicherten Paygate-Server von Computop gespeichert. Optional stellt Ihnen das Paygate als Ersatz für die Kreditkartennummer eine Pseudo-Kartennummer (PKN) zur Verfügung, die wie die echte Kartennummer funktioniert.

### 2) Server-zu-Server-Zahlung

Die Speicherung der Kreditkartendaten erfolgt auf Ihren Systemen. Damit werden Sie unter Umständen verpflichtet, das PCI-Sicherheitsprogramm von MasterCard und VISA zu durchlaufen, welches mit jährlichen Zertifizierungskosten und Aufwand verbunden ist. Detaillierte Informationen dazu erhalten Sie bei Ihrer Kreditkartengesellschaft.

**Hinweis:** Bitte beachten Sie, dass Visa und MasterCard strenge Sicherheitsregularien zum Schutz der Kreditkartendaten erlassen haben. Wer Kreditkartennummern auf seinem System speichert oder auch nur durchleitet, muss seine Server einer regelmäßigen und kostenpflichtigen Sicherheitszertifizierung unterziehen. Sie sollten deshalb die Computop Paygate-Formulare einsetzen. Wenn Sie die Kreditkartennummern für wiederkehrende Abo-Zahlungen benötigen, erlaubt das Computop Paygate die Verwendung einer Pseudo-Kartennummer, die Sie anstelle der echten Kreditkartennummer für Autorisierungen, Buchungen und Gutschriften benutzen können.

### 3) Batch

Zahlungsdaten lassen sich als Batch-Datei beim Computop Paygate einreichen. Dabei gibt es die beiden Varianten über das Protokoll SFTP sowie per HTTPS über das Backoffice des Händlers in Computop Analytics. Im Batch-Verfahren sind nicht alle Funktionen verfügbar, die für die Online-Schnittstelle verfügbar sind.

### 4) PayNow – der Silent Mode

Bei der PayNow-Lösung erfolgt die Dateneingabe des Kunden ähnlich der Server-zu-Server-Lösung mit dem wesentlichen Unterschied, dass die Kreditkartendaten vom Browser (Client) des Endkunden direkt an Computop Paygate übermittelt werden. Das spart vor allem bei komplexen 3D-Verfahren wie Verified by Visa, MasterCard SecureCode und American Express SafeKey viel Aufwand. Weitere Details zur PayNow-Lösung finden Sie im Handbuch zu den Kreditkarten. Um diese Schnittstelle zu nutzen, muss der Händler die PCI Anforderung SAQ A-EP erfüllen ([https://www.pcisecuritystandards.org/documents/PCI-DSS-v3\\_2-SAQ-A\\_EP-rev1\\_1.pdf](https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2-SAQ-A_EP-rev1_1.pdf)).

## Prinzipien der Paygate-Programmierung

Die Händler-Schnittstelle dient ganz allgemein der Aufnahme von Transaktionen aus dem Internet. Diese Schnittstelle kann nicht nur von Shops sondern auch von Warenwirtschaftssystemen genutzt werden, um zum Beispiel nach der Warenlieferung die Buchung über das Paygate auszulösen.

Um die Kompatibilität mit Programmiersprachen und Betriebssystemen zu erreichen, verzichtet das Paygate auf die Installation von komplexer Software auf dem Shop-Server, weil Software-Installation in der Regel Probleme mit Betriebssystem-Versionen oder Sicherheitsbestimmungen verursachen. Stattdessen brauchen Sie nur Daten via HTML an das Paygate zu senden - das funktioniert in jeder Programmiersprache auf jedem Betriebssystem.

Die Kommunikation mit dem Paygate erfolgt über TCP/IP und HTTP (HyperText Transfer Protocol) mit 128 / 256 Bit TLS-Verschlüsselung (HTTPS). Um eine Transaktion auszuführen, wird je nach Zahlungsmethode eine bestimmte Internet-Seite aufgerufen.

Bitte beachten Sie, dass das Paygate als eingehenden und ausgehenden Datenverkehr ausschließlich TLS 1.2 oder höher akzeptiert.

Zugelassene Cipher:

TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256  
TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384

Bei dieser homogenen Schnittstelle werden unabhängig von der Zahlungsmethode in der Regel dieselben Parameter an diese Internet-Seiten übergeben, so dass alle Zahlungsmethoden prinzipiell gleich funktionieren und keinen Zusatzaufwand verursachen.

Die wichtigsten Parameter für den Aufruf der Internet-Seiten sind:

- HändlerID (engl. MerchantID)
- Betrag (engl. Amount) und Währung (engl. Currency)
- URLs für Status-Meldungen

Die **MerchantID** ist ein alphanumerischer Wert, die den Händler eindeutig identifiziert und von uns vergeben wird. Die Parameter **Amount** und **Currency** bestimmen die Höhe der Zahlung. Außerdem geben Sie eine Internet-Seite des Shops an, die das Ergebnis der Zahlung entgegennimmt: Nach Durchführung der Zahlung bestätigt das Paygate erfolgreiche Zahlungen durch den Aufruf der **URLSuccess** und gescheiterte Zahlungen durch den Aufruf der **URLFailure**.

Das folgende Listing zeigt ein typisches Beispiel mit Parametern für die Durchführung einer Zahlung:

```
MerchantID=IhreHaendlerID&TransID=ab123456&Amount=9000&Currency=EUR&URLSuccess=https://www.shop.de/ok.  
cgi&URLFailure=https://www.shop.de/failed.cgi&URLNotify=https://www.shop.de/notify.cgi
```

**Hinweis:** Je nach Implementierung erfolgt der Aufruf von **URLSuccess** und **URLFailure** über ein Redirect (HTTP Status 302 Object Moved) und ist dann vom Browser des Kunden abhängig. Um sicher zu gehen, dass der Shop über den korrekten Status der Zahlung informiert wurde, sendet das Paygate eine weitere Bestätigung über eine direkte Server-zu-Server-Verbindung zum Shop (**URLNotify**).

## Funktionsweise der Händler-Schnittstelle

Um Zahlungsaufträge an die Paygate Händler-Schnittstelle zu senden, verbindet sich ein Shop via Internet mit dem und übergibt die benötigten Zahlungsdaten in einem definierten homogenen Format, welches auf Name-Value-Paaren (NVP) beruht. Die Händler-Schnittstelle des Paygate arbeitet mit HTML und ist deshalb zu allen gängigen Firewalls, Betriebssystemen (Linux, Unix, Windows) und Shop-Systemen kompatibel. Auch bei selbst programmierten Shops lässt sich die Paygate-Schnittstelle einfach integrieren.

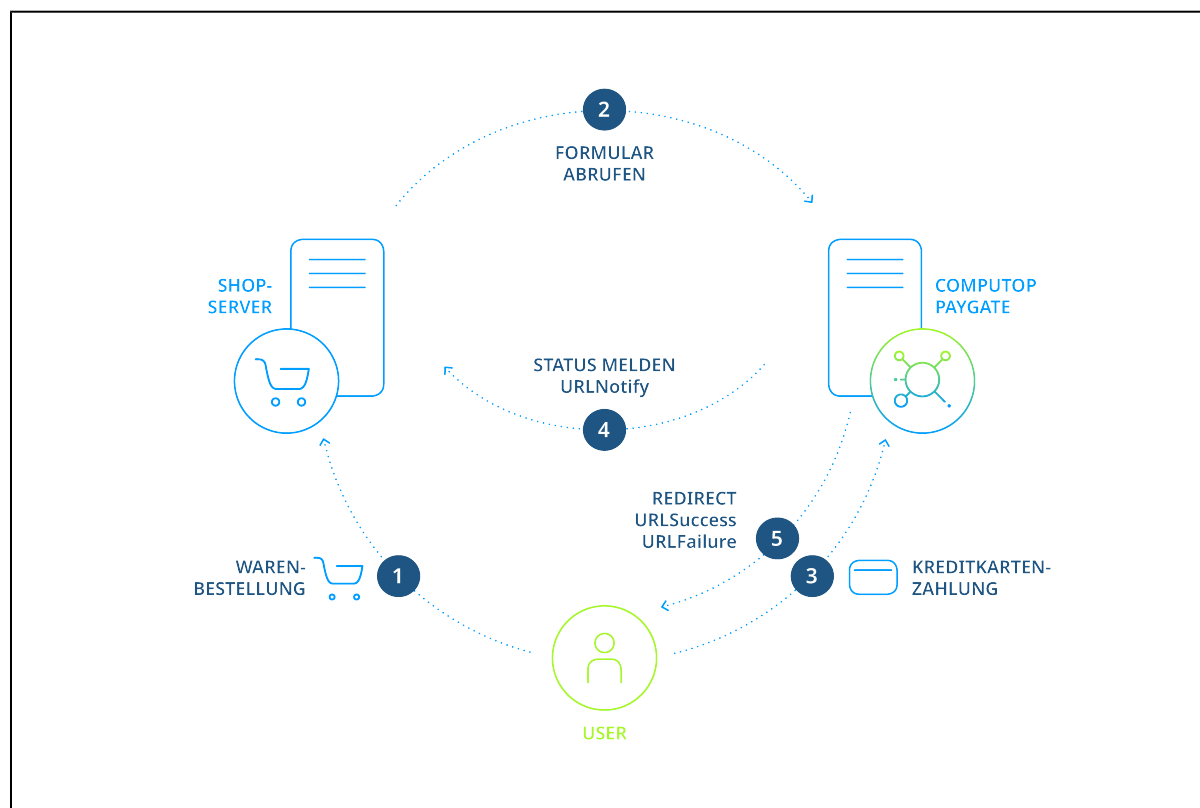
Ein Bezahlvorgang sieht im Prinzip so aus:

- 1 Der Käufer wählt im Shop die Zahlungsmethode und klickt auf die Schaltfläche **Bezahlen**.
- 2 Der Shop generiert eine Zeichenkette (String) mit Händlernummer, Betrag und Warenkorb:  
"HAENDLER=IhreHaendlerID&BETRAG=49&WARENKORB=Blumen"
- 3 Je nach Zahlungsmethode wird die Zeichenkette an die entsprechende Internet-Seite übergeben: <https://www.computop-paygate.com/paySSL.aspx?HAENDLER=123&BETRAG=49&WARENKORB=Blumen>

Die simple Übermittlung einer Zeichenkette hat den Vorteil, dass auf dem Shop-Server keine Software installiert werden muss. Außerdem funktioniert die Schnittstelle mit allen gängigen Zahlungsmethoden, so dass eine Verbindung zum Paygate ausreicht, um mehrere Zahlungs-methoden anzubieten.

## Zahlungen über Paygate-Formulare

Bei Zahlungen über die Paygate-Formulare verbindet der Shop den Kunden mit dem HTML-Formular des Paygate, damit er dort die Zahlungsdaten eingibt. Das Paygate führt dann die Zahlung durch und informiert den Shop über das Zahlungsergebnis.



Ablauf einer Zahlung mit Paygate-HTML-Formularen

## Ablauf der Zahlung

Um Zahlungen über Paygate-Formulare auszuführen, rufen Sie eine Internet-Seite mit HTTPS GET oder HTTPS POST auf. Die entsprechende URL finden Sie jeweils im Handbuch zur betreffenden Zahlungsmethode.

Alle Daten, die für eine Zahlungsabwicklung notwendig sind, werden als Parameter übergeben. Damit weder der Kunde noch ein Dritter die Daten manipulieren kann, werden die Parameter mit Blowfish verschlüsselt und durch eine HMAC-Authentisierung (siehe nachfolgend) geschützt.

Beim Aufruf des Formulars entschlüsselt das Paygate die Parameter und zeigt die HTML-Seite mit den Eingabefeldern der entsprechenden Zahlungsart an. Dort gibt der Kunde seine Daten ein und startet den Zahlungsprozess per Mausklick auf die Schaltfläche **Bezahlen**.

Nach Durchführung der Zahlung leitet das Paygate den Kunden per HTTPS GET oder HTTPS POST auf eine Shop-Seite zurück (**URLSuccess**, **URLFailure**) und übergibt dabei das Zahlungsergebnis als Blowfish-verschlüsselte Parameter. Zusätzlich übermittelt das Paygate das Ergebnis per HTTPS POST an die Notify-Seite des Shops (**URLNotify**). Der Shop nimmt das Zahlungsergebnis entgegen und entschlüsselt die Daten, um den Kunden über den Status zu informieren.

**Hinweis:** Bitte beachten Sie, dass der Händler sowohl HTTPS GET als auch HTTPS POST verarbeiten können muss. Ob GET oder POST verwendet wird, hängt von der Zahlungsart und Implementierung ab.

## Aufruf eines Paygate-Formulars

Der Aufruf eines Paygate-Formulars beginnt mit der korrekten Zusammenstellung der Parameter, die aus einem Schlüssel und einem Wert bestehen und durch ein Gleichheitszeichen (=) getrennt sind. Es handelt sich hier um sogenannte Name-Value-Paare (NVP):

```
MerchantID=IhreHaendlerID
```

Alle Parameter werden in einer Zeichenkette aneinandergereiht und durch das Zeichen & getrennt:

```
Amount=100&Currency=EUR&TransID=12345
```

**Hinweis:** Da die Zeichen "=" und "&" als Trennzeichen verwendet werden, können diese Zeichen nicht als Wert übergeben werden. Alle Werte, die Sie ohne Blowfish-Verschlüsselung übergeben, müssen URL-encoded sein.

Eine korrekte Parameter-Zeichenkette für das Paygate enthält grundsätzlich drei Parameter: **MerchantID**, **Len** und **Data**. Die Parameter **MerchantID** und **Len** sind unverschlüsselt. Nur der Parameter **Data** wird Blowfish-verschlüsselt:

```
MerchantID=IhreHaendlerID&Len=67&Data=0A67FE96a65d384350F50FF1
```

Der Parameter **Data** enthält die sensiblen Zahlungsdaten wie Betrag und Währung. Die verschlüsselten Bytes sind Hex-codiert und auf zwei Zeichen von links mit einer Null aufgefüllt. Die Verschlüsselung erfolgt über Blowfish ECB und steht Ihnen als Source-Code und Komponente zur Verfügung.

Für die Entschlüsselung ist der Parameter **Len** sehr wichtig, der die Länge der unverschlüsselten(!) Zeichenkette im Parameter **Data** enthält. Da bei der Verschlüsselung mit Blowfish die zu verschlüsselnde Datenmenge auf ein Vielfaches von 8 vergrößert wird, muss bei der Entschlüsselung die korrekte Länge der Zeichenkette bekannt sein. Andernfalls tauchen am Ende der Zeichenkette zufällige Zeichen auf.

Die Übergabe der Parameter erfolgt per HTTPS POST oder HTTPS GET. Die empfohlene Übertragungsmethode ist HTTPS POST, weil die Parameterzeichenkette bei GET an die URL angehängt wird, die je nach Browser auf 2048 Bytes begrenzt ist.

**Hinweis:** Bitte beachten Sie, dass die maximale Länge einer Zahlungsanfrage auf 5120 Zeichen begrenzt ist. Wenn Sie längere Zeichenketten benötigen, melden Sie sich bitte beim [Computop Helpdesk](#).

Die folgenden Listings zeigen die Entwicklung eines Zahlungsaufrufs. Das erste Listing ist die unverschlüsselte Parameterzeichenkette:

```
MerchantID=IhreHaendlerID&TransID=100000001&Amount=11&Currency=EUR&URLSuccess=https://www.shop.de/ok.html&URLFailure=https://www.shop.de/failed.html&URLNotify=https://www.shop.com/notify.cgi&OrderDesc=Mein Einkauf
```

**Hinweis:** Bitte beachten Sie, dass jedem Parameter ein Wert zugewiesen wird. Leere Parameter dürfen nicht übergeben werden, da andernfalls die Zahlung scheitern kann.

Diese Zeichenkette wird verschlüsselt und als Parameter **Data** übergeben, so dass der HTTPS GET Aufruf des Paygate-Formulars für Kreditkartenzahlungen so aussieht:

```
<A href="https://www.computop-paygate.com/payssl.aspx?MerchantID=YourMerchantID&Len=162&Data=E98D40FFFD622C5FE7414F73539A1852C2CE7C8B09D34DF217E27FA2E194B9968DE9ABAE3B1F44B5485EFE3EF2597C7395BADBAD4340CDFD00DD57129EEFAA0BE904A7E2339DCF9363DA6ACDBE5EF98E169FC3092B160252A037135421FD0CE092C174A7D1D63517BD45099AC2B682F5E3CD2C942A6F0E741A833C0&Background=https://www.meinshop.de/grafik/hintergrundbild.jpg">Zahlen</A>
```

**Hinweis:** Bitte beachten Sie, dass die Parameter zum Layout des Formulars unverschlüsselt übergeben werden.

Für HTTPS POST wird ein HTML-Formular erstellt und alle Parameter als Hidden Fields übergeben. Nur die Schaltfläche **Zahlen** ist für den Kunden sichtbar:

```
<FORM method="POST" action="https://www.computop-paygate.com/payssl.aspx">
  <INPUT type="hidden" name="MerchantID" value="YourMerchantID">
  <INPUT type="hidden" name="Len" value="162">
  <INPUT type="hidden" name="Data"
value="
E98D40FFFD622C5FE7414F73539A1852C2CE7C8B09D34DF217E27FA2E194B9968DE9ABAE3B1F44B5485EFE3EF2597C7395BADBAD4340C
DFD000DD57129EEFAA0BE904A7E2339DCF9363DA6ACDBE5EF98E169FC3092B160252A037135421FD0CE092C174A7D1D63517BD45099AC
2B682F5E3CD2C942A6F0E741A833C0">
  <INPUT type="hidden" name="Background" value="https://www.meinshop.de/grafik/hintergrundbild.jpg">
  <INPUT type="submit" name="Pay" value="Zahlen">
</FORM>
```

## Hash MAC-Authentisierung in der Anfrage

Zum Schutz vor unbefugter Manipulation Ihrer Zahlungstransaktionen prüft das Computop Paygate mit Hilfe eines Hash Message Authentication Code (HMAC), ob Ihre Zahlungsanfrage echt ist und nicht manipuliert wurde. Dazu übergeben Sie bei jeder Transaktion im Parameter MAC einen HMAC-Wert an das Paygate.

Hintergrund: Im Gegensatz zum HMAC-Verfahren hat jedes Codiervorhaben den Nachteil, dass es ein passendes Decodierverfahren gibt. Jeder, der den richtigen Schlüssel besitzt oder die Verschlüsselung knackt, kann die Daten lesen und manipulieren. Daher ist keine Verschlüsselungsmethode jemals 100% sicher. Beim Hash-Verfahren ist hingegen keine Dekodierung möglich, so dass ein Hash-Wert die Authentizität der Nachricht zweifelsfrei bestätigen kann.

Das Computop Paygate nutzt einen Hash Message Authentication Code (HMAC), um die Authentizität Ihrer Zahlungen zu prüfen. Dazu wird der MAC SHA-256-Algorithmus mit einer 32-stelligen Schlüssellänge (256 Bit) verwendet. Das zusätzliche Kennwort macht das HMAC-Verfahren besonders sicher.

Folgende Tabelle beschreibt, wie Sie die Hash-Werte für Ihre Zahlung erzeugen:

Schritt	Aufgabe
1	Melden Sie sich bitte beim <a href="#">Computop Helpdesk</a> an, der Ihnen das Hash-Kennwort mitteilt.

2

Der HMAC-Wert wird mit Hilfe des Kennworts und mehrerer Parameterwerte berechnet. Zur Berechnung werden die Parameter PayID, TransID, MerchantID, Amount and Currency verwendet und mit Sternchen getrennt:

PayID\*TransID\*MerchantID\*Amount\*Currency

Key	Wert	Anmerkungen
PayID	Referenzierte PayID	Kann leer sein, z.B. zum Erstellen eines anfänglichen Zahlungsvorgangs oder einer Risikomanagement-Anfrage; wird bei nachfolgenden Anfragen wie Erfassung /Erstattung verwendet.
TransID	Ihre Transaktions-ID zur Referenzierung / Identifikation Ihrer Anfrage	Ihre eigene Referenz zur Identifikation jeder Anfrage / jedes Zahlungsvorgangs.
MerchantID	Ihre von Computop vergebene MerchantID	Ihre MerchantID zur Identifikation dieser Anfrage.
Amount	Betrag in der kleinsten Währungseinheit, z.B.123=1,23	Betrag dieser Anfrage; kann leer sein, falls der Wert z.B. für Statusanfragen nicht verwendet wird.
Currency	Währung des Zahlungsvorgangs gemäß ISO 4217, z.B. EUR, USD, GBP	Währung dieser Anfrage; kann leer sein, falls der Wert z.B. für Statusanfragen nicht verwendet wird.
YourHmacPassword	Ihr von Computop zugeteiltes HMAC-Kennwort	Ihr zu einer bestimmten MID zugeordnetes HMAC-Kennwort; falls Sie mehrere MIDs haben, haben Sie auch verschiedene HMAC-Kennwörter.

Hinweis:

Falls eine Transaktion nicht alle diese Parameter unterstützt, können Sie die fehlenden Werte einfach weglassen.

Beispielsweise liegt bei der ersten Transaktion noch keine PayID vor, sodass Sie diese nicht übertragen müssen. Die PayID ist Bestandteil der Hash-Berechnung bei nachfolgenden Transaktionen:

Beispiele zur MAC-Berechnung	Formel	Ergebnis
ohne PayID, mit Betrag/Währung	HmacSHA256 ( " *TID-4453732122167114558*YourMerchantID*1234*EUR" , "mySecret" )	0522F1AF6A88597D396A5A877499F3C9087EBCF103B1B47D7E4D13421CC7EA36
ohne PayID, ohne TransID, mit Betrag /Währung	HmacSHA256 ( " **YourMerchantID*1234*EUR" , "mySecret" )	1427748D983478080F22BE0878BD99AF7BE3E1C4B19C07AFD1B372BA552ADC08
mit PayID, ohne Betrag/Währung	HmacSHA256 ( " fe3f002e19814eea8aa733ec4fdacafe*TID-4453732122167114558*YourMerchantID**" , "mySecret" )	6ED0CFDCE92CE13399552C4221B44E5B036DE943D7F84E33D1E73DF9871AE7C8

3

Verwenden Sie den HMAC SHA-256-Algorithmus, den fast alle Programmiersprachen unterstützen, um den Hash-Wert mit dem Kennwort und den Parameterwerten zu berechnen.


4

Verwenden Sie den Parameter MAC, um den hexadezimal codierten Hash-Wert bei jeder Transaktion im codierten Datenfeld an das Paygate zu übertragen.

### Ihre Implementierung prüfen

Eine einfache Anwendung zur Überprüfung der Umsetzung Ihrer HMAC-Berechnung finden Sie hier: <https://computop.com/paygate-test>

Mit der Anwendung können Sie mit unserer Paygate API spielen – verwenden Sie einfach Ihre MerchantID und Ihr Blowfish-Kennwort, die Sie bereits erhalten haben.

 **Hinweis:** Beachten Sie, dass der Parameter MAC für alle nachfolgenden Transaktionen (z. B. Buchung, Gutschrift) obligatorisch ist, wenn er mit der ersten Transaktion (z. B. Autorisierung) übertragen wurde.



**Wichtig:** Das Paygate lehnt Transaktionen mit falschen oder fehlenden HMAC-Werten sofort ohne weitere Verarbeitung ab, weil das ein Hinweis auf Hackerangriffe ist. Deshalb erscheinen Transaktionen, die das Paygate mit den Fehlercodes 20100044 oder 20120044 ablehnt, nicht in Computop Analytics.



**Wichtig:** Die MerchantID, welche in der HMAC Berechnung verwendet wird, muss identisch mit der MerchantID im unverschlüsselten Request sein (Parameter MerchantID). Bei der Verarbeitung der "MerchantID" muss die Groß- und Kleinschreibung beachtet werden. "YourMerchantId" und "YourMerchantID" dürfen nicht vermischt werden.

#### Listing mit HMAC-Beispielen

##### Anfrage ohne PayID:

MerchantID=YourMerchantID&TransID=100000001&Amount=11&Currency=EUR&URLSuccess=<https://www.shop.de/ok.html>&URLFailure=<https://www.shop.de/failed.html>&OrderDesc=My purchase

String zur MAC-Erzeugung:

\*100000001\*YourMerchantID\*11\*EUR

Anfrage mit MAC-Parameter (Secret: "mySecret"):

MerchantID=YourMerchantID&TransID=100000001&Amount=11&Currency=EUR&URLSuccess=<https://www.shop.de/ok.html>&URLFailure=<https://www.shop.de/failed.html>&OrderDesc=My purchase&MAC=0A125E070BD4D7AE614BCB2D5A48FB80E1C4441E262A1024AE7F2A1819052A6F

##### Anfrage ohne TransID:

MerchantID=YourMerchantID&PayID=8ee4e922c39446ac9ee66095a4a4b475&Amount=100&Currency=USD

String zur MAC-Erzeugung:

8ee4e922c39446ac9ee66095a4a4b475\*\*YourMerchantID\*100\*USD

Anfrage mit MAC-Parameter (Secret: "mySecret"):

MerchantID=YourMerchantID&PayID=8ee4e922c39446ac9ee66095a4a4b475&Amount=100&Currency=USD&MAC=4016FD6C705399A024D8B4CCB0018814E05A5490DDEBEC04909E6DA138CB5AF8

## Hash MAC-Authentisierung im Notify

Der Shop muss überprüfen, ob eine Benachrichtigungsanfrage wirklich von Computop Paygate stammt. Anderenfalls kann ein Angreifer eine Transaktion initialisieren und dann diese Benachrichtigung fälschen. Ein Shop-Betreiber wird nicht manuell prüfen, ob in jedem Fall eine entsprechende Transaktion durchgeführt wurde. Deshalb muss das Modul dies automatisch machen.

Derzeit ist die Benachrichtigungsanfrage nur verschlüsselt. Diese Verschlüsselung garantiert jedoch nicht die Authentizität einer Nachricht. Sie garantiert nur, dass eine Nachricht nicht mitgehört werden kann. Daher ist diese Sicherheitsmaßnahme unzureichend.

Deshalb wird der Antwortparameter MAC verwendet, der mit demselben Algorithmus wie der [MAC](#) in der Anfrage gebildet wird. Nur die Datenparameter unterscheiden sich.

Für die Hash-Generierung gilt hier folgendes Datenmuster: `PayID*TransID*MerchantID*Status*Code`

Der Parameter MAC wird nur an [URLSuccess](#) oder [URLFailure](#) sowie für [URLNotify](#) zurückgegeben.

Ihre Integration muss prüfen, ob die erhaltene Antwort authentisch ist.

Folgende Tabelle beschreibt, wie Sie die Hash-Werte erzeugen, um die erhaltene Antwort vom Computop Paygate zu validieren:

Schritt	Aufgabe
1	Melden Sie sich bitte beim <a href="#">Computop Helpdesk</a> an, der Ihnen das Hash-Kennwort mitteilt.



2

Der HMAC-Wert wird mit Hilfe des Kennworts und mehrerer Parameterwerte berechnet. Zur Berechnung werden die Parameter PayID, TransID, MerchantID, Status und Code verwendet und mit Sternchen getrennt:

PayID\*TransID\*MerchantID\*Status\*Code

Key	Wert	Anmerkungen
PayID	Referenzierte PayID	Zurückgegebene PayID von Computop Paygate
TransID	Ihre Transaktions-ID zur Referenzierung / Identifikation Ihrer Anfrage	Ihre eigene Referenz zur Identifikation jeder Anfrage / jedes Zahlungsvorgangs.
MerchantID	Ihre von Computop vergebene MerchantID	Ihre MerchantID zur Identifikation dieser Anfrage. Bitte verwenden Sie den Wert des Parameters MID aus der Benachrichtigungsanfrage von Computop Paygate.
Status	Status in der Antwort	Status der Antwort, z.B. AUTHORIZED, FAILED, OK, ...
Code	Code in der Antwort	Code der Antwort, z.B. 00000000, 22720040, ...
YourHmacPassword	Ihr von Computop zugeteiltes HMAC-Kennwort	Ihr zu einer bestimmten MID zugeordnetes HMAC-Kennwort; falls Sie mehrere MIDs haben, haben Sie auch verschiedene HMAC-Kennwörter.

Beispiele zur MAC-Berechnung	Formel	Ergebnis
Autorisierte Zahlung	HmacSHA256( "7bbb448155234d8cbee323778952ce28*TID-12033175321270170232*YourMerchantID*AUTHORIZED*0000000", "mySecret" )	F1DE7608013C1E3FD3CC9964A049E26703137C0A6F29448545C700B4695EABE5
Gescheiterte Zahlung	HmacSHA256( "7bbb448155234d8cbee323778952ce28*TID-12033175321270170232*YourMerchantID*FAILED*22720040", "mySecret" )	1D9A8AAA306316359B8192070237670950DB77073F9F34ED7EB483D9B59DE1DD

3

Verwenden Sie den HMAC SHA-256-Algorithmus, den fast alle Programmiersprachen unterstützen, um den Hash-Wert mit dem Kennwort und den Parameterwerten zu berechnen.

4

Überprüfen Sie

- den erhaltenen HMAC-Wert aus der Antwort vom Computop Paygate
- dessen Übereinstimmung mit dem selbst berechneten MAC-Wert

um sicherzustellen, dass die erhaltene Nachricht authentisch ist.



#### Ihre Implementierung prüfen

Eine einfache Anwendung zur Überprüfung der Umsetzung Ihrer HMAC-Berechnung finden Sie hier: <https://computop.com/paygate-test>

Mit der Anwendung können Sie mit unserer Paygate API spielen – verwenden Sie einfach Ihre MerchantID und Ihr Blowfish-Kennwort, die Sie bereits erhalten haben.

Der Parameter MAC wird nur an die URLSuccess oder URLFailure und für Notifys zurückgegeben.



**Wichtig:** Der Shop muss überprüfen, ob eine Benachrichtigungsanfrage wirklich von Computop Paygate stammt. Dazu muss aus den übermittelten Werten für PayID, TransID, MerchantID, Status und Code mit Ihrem HMAC-Passwort ein HMAC-Wert errechnet und dieser mit dem MAC-Wert der Anfrage verglichen werden. Sind die Werte nicht identisch, so darf die Benachrichtigungsanfrage nicht verarbeitet werden.

**Wichtig:** Zur Berechnung wird dieses Mal die von Computop Paygate in der Benachrichtigungsanfrage übermittelte MID verwendet.



**Wichtig:** Kennwörter dürfen **niemals** per E-Mail versendet werden, weil in diesem Fall **sofort** die Sicherheit verschlüsselter Anfragen /Antworten nicht mehr gewährleistet ist. Falls versehentlich Kennwörter per E-Mail versendet wurden, müssen neue Kennwörter auf Kosten des Händlers oder bei der nächsten Standardfreigabe hinterlegt werden. Computop **weist ausdrücklich auf das Risiko** der weiteren Verwendung **solcher kompromittierter MIDs hin**. Falls ein Händler eine solche kompromittierte MID dennoch weiter verwendet, trägt er selbst das Haftungsrisiko für mögliche Verluste durch die kompromittierten Kennwörter.

## Benachrichtigung des Shops

Nach Durchführung der Zahlung informiert das Paygate den Shop über das Ergebnis der Zahlung. Dazu ruft das Paygate die **URLNotify** per HTTP POST auf. Das ist eine völlig separate Anfrage, die mit der ursprünglichen Verbindung zwischen Shop, Kunde und Paygate nichts zu tun hat. Die Parameter werden im HTTP Body als Parameterzeichenkette Blowfish-verschlüsselt übergeben. Der Content-type lautet **application/x-www-form-urlencoded; charset=iso-8859-1**. Damit können die Werte über die bekannten Techniken für HTML-Formularauswertung eingesetzt werden.

**Hinweis:** Bitte beachten Sie, dass der Notify-Aufruf aus Sicherheitsgründen nur über Port 443 (TLS) erlaubt ist.

Sofern die **URLNotify** des Shops nicht erreichbar ist (z.B. HTTP-Status 500/404), wird die Benachrichtigung 8-mal wiederholt. In diesem Fall erfolgt die Weiterleitung des Kunden zum Shop vor dem **URLNotify**-Aufruf. Deshalb sollte der Shop die beiden Status-Rückmeldungen von **URLNotify** und Weiterleitung (**URLSuccess**, **URLFailure**) auswerten und abgleichen.

Wiederholung	Wartezeit	Zeit nach 1. Notify
0	sofort	0
1	0:01 h	0:01 h
2	0:08 h	0:09 h
3	0:27 h	0:36 h
4	1:04 h	1:40 h
5	2:05 h	3:45 h
6	3:36 h	7:21 h
7	5:43 h	13:04 h
8	8:32 h	21:36 h

Zeitpunkte der Wiederholung des Notify jeweils berechnet nach dem ersten gescheiterten Versuch

**Hinweis:** Die Parameterübergabe erfolgt **URL-encoded** in Schlüssel-Werte-Paaren (Schlüssel1=Wert1&Schlüssel2=Wert2). Beachten Sie bitte, dass jederzeit neue Parameter unangekündigt hinzukommen können. Verwenden Sie daher bitte den Parameter-Namen für die Auswertung und **nicht** die Reihenfolge, weil diese sich jederzeit ändern kann! Die Groß-/Kleinschreibung der Parameter sollte nicht beachtet werden, da sich diese ebenfalls ändern kann. Empfehlenswert ist es zum Beispiel, alle Parameter per Funktion „to lower“ umzuwandeln und einheitlich mit Kleinschreibweise weiterzuarbeiten.

Weitere Informationen finden Sie hier:

[www.w3.org/MarkUp/html-spec/html-spec\\_8.html#SEC8.2.1](http://www.w3.org/MarkUp/html-spec/html-spec_8.html#SEC8.2.1)

## Weiterleitung des Kunden zum Shop

Nachdem die Zahlung erfolgt ist, wird der Kunde per HTTP GET wieder zum Shop weitergeleitet. Dabei liefert das Paygate ein HTTP Status 302 (object moved) zurück und hängt das Zahlungsergebnis als Blowfish-verschlüsselte Parameter an die **URLSuccess** oder **URLFailure**. Im Gegensatz zum Zahlungsauftrag enthält das Zahlungsergebnis keine MerchantID. Die Parameter Len und Data haben dieselbe Funktion.

## Richtig testen

Bis Sie die Programmierung des Zahlungsverkehrs abgeschlossen haben, befindet sich Ihre Paygate-Kasse im Testmodus: Kreditkartenzahlungen werden autorisiert aber es fließt kein Geld, weil das Paygate keine Buchung ausführt.

**Hinweis:** Bitte nutzen Sie auch im Testmodus nur kleine Beträge zwischen 0,11 und 2 Euro, denn die Kreditkartenautorisierungen sind auch im Test echt und reduzieren das Limit Ihrer Kreditkarte. Wenn Sie größere Beträge nutzen und das Kartenlimit erreichen, wird sonst Ihre Kreditkarte temporär nicht mehr funktionieren.

Bei erfolgreichen Zahlungen liefert das Paygate im Parameter **Code** den Wert Null zurück. Falls eine Zahlung scheitert, ist der Parameter **Code** größer Null, und das kann viele Gründe haben: Ein falsches Ablaufdatum, ein überschrittenes Kartenlimit oder auch eine gesperrte Karte sind nur einige Beispiele. Eine vollständige Liste der Fehlercodes finden Sie als Excel-Datei in der Fehlercode-Liste.

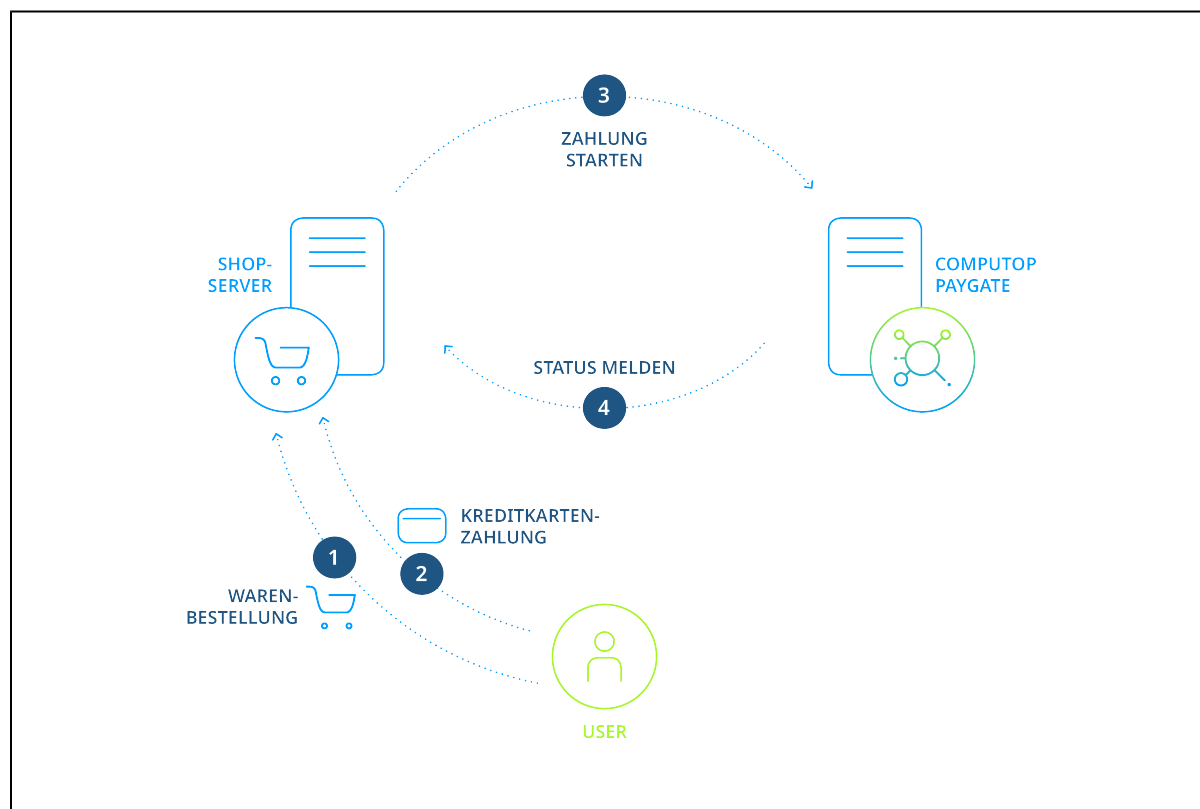
Wenn Sie die verschiedenen Fehlerfälle testen wollen, erlaubt das Paygate eine Simulation der gewünschten Fehlercodes. Um einen Fehler zu simulieren, übergeben Sie im Parameter **OrderDesc** das Schlüsselwort **Test** und den vierstelligen Detail-Fehlercode, also zum Beispiel "Test:0110", um eine abgelaufene Kreditkarte zu simulieren. Das Paygate wird dann den vierstelligen Detail-Fehlercode mit den jeweiligen Antwort-Parametern zurückgeben.

## Testfälle mit Timeout

Eine Kreditkartenzahlung ist normalerweise innerhalb von ein bis zwei Sekunden abgeschlossen. In seltenen Fällen kommt es aber vor, dass Zahlungen aufgrund langer Verarbeitungszeiten im Banknetzwerk abgebrochen werden. Das Paygate bricht Kreditkartenzahlungen nach 90 Sekunden ab. Wenn Sie kürzere Timeouts wünschen, kann unser [Computop Helpdesk](#) den Abbruch für Sie individuell beispielsweise nach 45 Sekunden konfigurieren.

## Zahlungen per Server-zu-Server-Verbindung

Bei Zahlungen über die Server-zu-Server-Kommunikation sind Zahlungsdaten wie Kreditkartennummern und Bankverbindungen beim Händler schon vorhanden. Shop oder Warenwirtschaftssystem bauen eine TLS-Socket-Verbindung zum Paygate-Server auf, um eine Zahlungstransaktion durchzuführen.



Ablauf einer Server-zu-Server-Zahlung

**Hinweis:** Bei der Zahlungsabwicklung über eine Server-zu-Server-Verbindung müssen Sie die Kommunikation mit dem Paygate selbst steuern. Das kann in Einzelfällen kompliziert sein.

**Hinweis:** Bitte stellen Sie sicher, dass Sie auf eine Zahlung (PayID) nicht mehrere Aufrufe/Request zeitgleich senden, da dies zu Fehlern in der Transaktionsverarbeitung führen kann. Stellen Sie sicher, dass zwischen zwei Aufrufen auf eine Zahlung/PayID mehrere Sekunden liegen.

## Ablauf einer Server-zu-Server-Zahlung

Der Aufruf einer Zahlung beginnt mit der korrekten Zusammenstellung der Parameter, die aus einem Schlüssel und einem Wert bestehen und durch ein Gleichheitszeichen (=) getrennt sind. Es handelt sich hier um sogenannte Name-Value-Paare (NVP):

MerchantID=IhreHaendlerID

Alle Parameter werden in einer Zeichenkette aneinandergereiht und durch das Zeichen & getrennt:

Amount=100&Currency=EUR&TransID=12345

**Hinweis:** Da die Zeichen "=" und "&" als Trennzeichen verwendet werden, können diese Zeichen nicht als Wert übergeben werden. Alle Werte, die Sie ohne BlowFish-Verschlüsselung übergeben, müssen URL-Encoded sein. Von dieser Regel gibt es nur eine Ausnahme: Bei Kreditkarten, die für Verified/SecureCode/SafeKey/JSecure/ProtectBuy registriert sind, wird z.B. die ACSURL uncodiert übergeben.

Eine korrekte Parameter-Zeichenkette für das Paygate enthält grundsätzlich drei Parameter: **MerchantID**, **Len** und **Data**. Die Parameter **MerchantID** und **Len** sind unverschlüsselt. Nur der Parameter Data wird Blowfish-verschlüsselt:

MerchantID=IhreHaendlerID&Len=67&Data=0A67FE96a65d384350F50FF1

Der Parameter **Data** enthält die sensiblen Zahlungsdaten wie Betrag und Währung. Die verschlüsselten Bytes sind Hex-codiert und auf zwei Zeichen von links mit einer Null aufgefüllt. Die Verschlüsselung erfolgt über Blowfish ECB und steht Ihnen als Source-Code und Komponente zur Verfügung.

Für die Entschlüsselung ist der Parameter **Len** sehr wichtig, der die Länge der **unverschlüsselten(!)** Zeichenkette im Parameter **Data** enthält. Da bei der Verschlüsselung mit Blowfish die zu verschlüsselnde Datenmenge auf ein Vielfaches von 8 vergrößert wird, muss bei der Entschlüsselung die korrekte Länge der Zeichenkette bekannt sein. Andernfalls tauchen am Ende der Zeichenkette zufällige Zeichen auf.

Die folgenden Listings zeigen die Entwicklung eines Zahlungsaufrufs. Das erste Listing ist die unverschlüsselte Parameterzeichenkette:

MerchantID=IhreHaendlerID&TransID=100000001&Amount=11&Currency=EUR&OrderDesc=Mein  
Einkauf&CCNr=1111333355557777&CCVC=123&CCExpiry=202012&CCBrand=VISA

**Hinweis:** Bitte beachten Sie, dass jedem Parameter ein Wert zugewiesen wird. Leere Parameter dürfen nicht übergeben werden, da andernfalls die Zahlung scheitern kann.

Diese Zeichenkette wird mit Blowfish verschlüsselt:

MerchantID=IhreHaendlerID&Len=140&Data=D622C5FE7414F73539A1852C2CE7AA0BE904A7E2339DCF9363DA6ACDBE5EF98E169FC3092  
B1602564DBF2C3C75173A62C484962A247B8A91EA7A544ADCF2A037135421FD0CE092C174A7D1D63517BD45099AC2B682F5E3CD2C942  
A6F0E741A833C

Um Zahlungen über eine Server-zu-Server-Verbindung auszuführen, öffnen Sie eine TLS-Socket-Verbindung zum Paygate und übergeben die erzeugte Zeichenkette an die folgende URL:

<https://www.computop-paygate.com/direct.aspx>

Sobald die TLS-Socket-Verbindung steht, wird ein normaler HTTP POST der Version 1.1 ausgeführt. Dabei müssen folgende Felder im HTTP-Header angegeben werden:

Feld	Wert
Host	<a href="https://www.computop-paygate.com/">https://www.computop-paygate.com/</a>
Connection	Close
Content-type	application/x-www-form-urlencoded
Content-length	Länge der Zeichenkette, die HTTP-Body übergeben wird
Charset	UTF-8

Pflichtangaben im HTTP-Header

Der HTTP-Body enthält die Parameterzeichenkette. Beachten Sie, dass die Werte URL-encoded übergeben werden müssen. Das folgende Listing ist ein Beispiel für eine Kreditkartenzahlung:

POST /direct.aspx HTTP/1.1

Host: <https://www.computop-paygate.com/>

Connection: Close

Content-type: application/x-www-form-urlencoded

Content-Length: 287

MerchantID=IhreHaendlerID&Len=162&Data=E98D40FFFD622C5FE7414F73539A1852C2CE7C8B09D3E876F52CBECF59EC63E9B8AA0130FA92F65964E3EEE74DF217E27FA2E194B9968DE9ABAE3B1F44B5485EFE3EF2597C7395BADBAD4340CDFD000DD57129EEFAA0BE904A7E2339DCF9363DA6ACDBE5EF98E169FC3092B1602564DBF2C3C75173A62C484962A247B8A91EA7A5

**Hinweis:** Bitte beachten Sie, dass die maximale Länge einer Zahlungsanfrage auf 5120 Zeichen begrenzt ist. Wenn Sie längere Zeichenketten benötigen, melden Sie sich bitte beim [Computop Helpdesk](#).

Die Antwort des Paygate zeigt das folgende Listing. Das Paygate schreibt die Daten Blowfish-verschlüsselt in den Socket:

HTTP/1.0 200 OK

Connection: Close

Content-type: text/plain

Content-Length: 228

Len=125&Data=ECF59EC63E9BEE74DF217E27FA2E194B92597C7395BADBAD4340CDFD000DD57129EEFAA0BE904A7E233ACDBE5EF98E1692B1602564DBF2C3C75173A62C484962A247B8A91EA7A544

Die entschlüsselte Antwort des Paygate im **Data**-Parameter sieht dann in etwa so aus:

PayID=a234b678e01f34567090e23d567890ce&XID=50f35e768edf34c4e090e23d567890ce&TransID=100000001&Status=AUTHORIZED&Description=AUTHORIZED&Code=00000000

Es handelt sich um eine synchrone Kommunikation, so dass die Socket-Verbindung offen bleibt, bis das Paygate die Antwort geliefert hat. Wenn eine Anfrage nicht innerhalb von 120 Sekunden beantwortet werden kann, liefert das Paygate eine Timeout-Fehlermeldung.

**Hinweis:** Die Parameterübergabe erfolgt **URL-encoded** in Schlüssel-Werte-Paaren (Schlüssel1=Wert1&Schlüssel2=Wert2). Beachten Sie bitte, dass jederzeit neue Parameter unangekündigt hinzukommen können. Verwenden Sie daher bitte den Parameter-Namen für die Auswertung und nicht die Reihenfolge, weil diese sich jederzeit ändern kann! Die Groß-/Kleinschreibung der Parameter sollte nicht beachtet werden, da sich die-se ebenfalls ändern kann. Weitere Informationen finden Sie hier:

[www.w3.org/MarkUp/html-spec/html-spec\\_8.html#SEC8.2.1](http://www.w3.org/MarkUp/html-spec/html-spec_8.html#SEC8.2.1)