Programmiergrundlagen

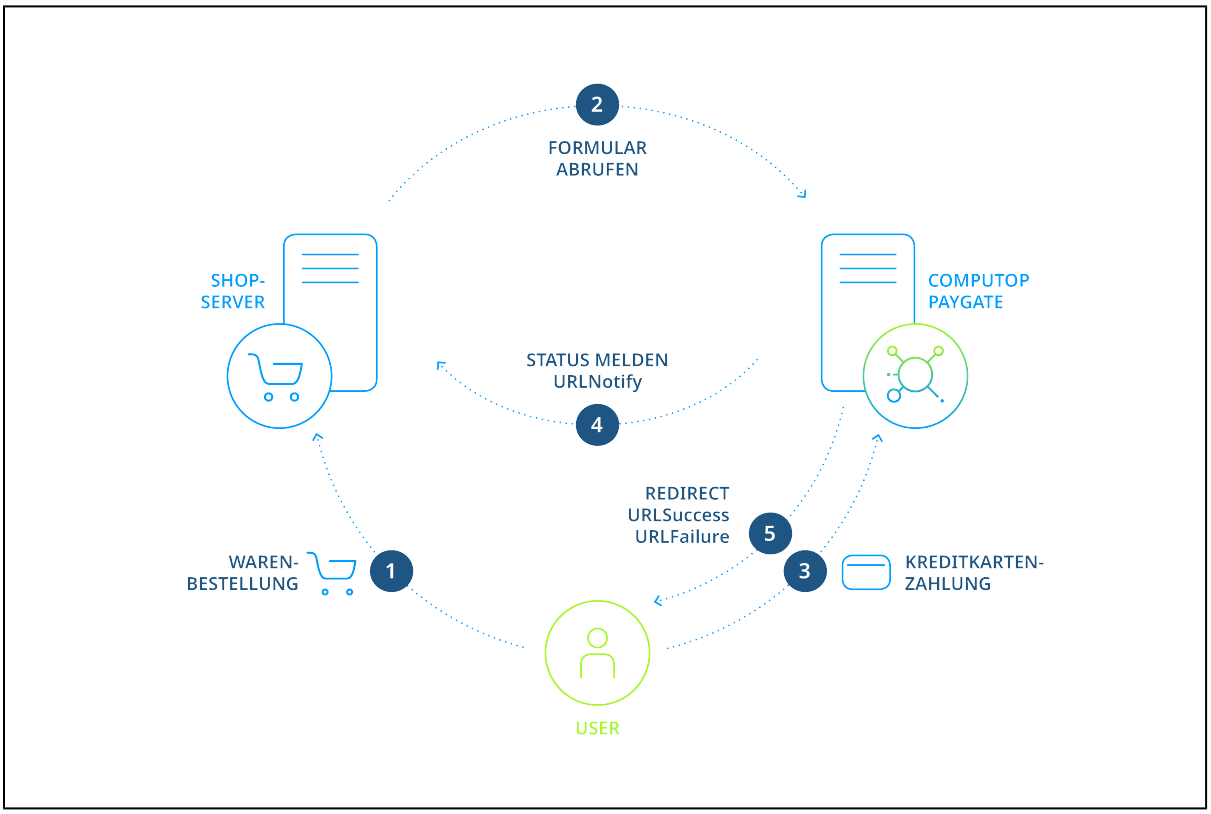
Programmierung

Varianten der Händler-Schnittstelle

Das Paygate erlaubt drei Formen der Online-Kommunikation mit Händler-Systemen: Zum einen stellt das 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 Paygate-Server im Hintergrund abwickeln.

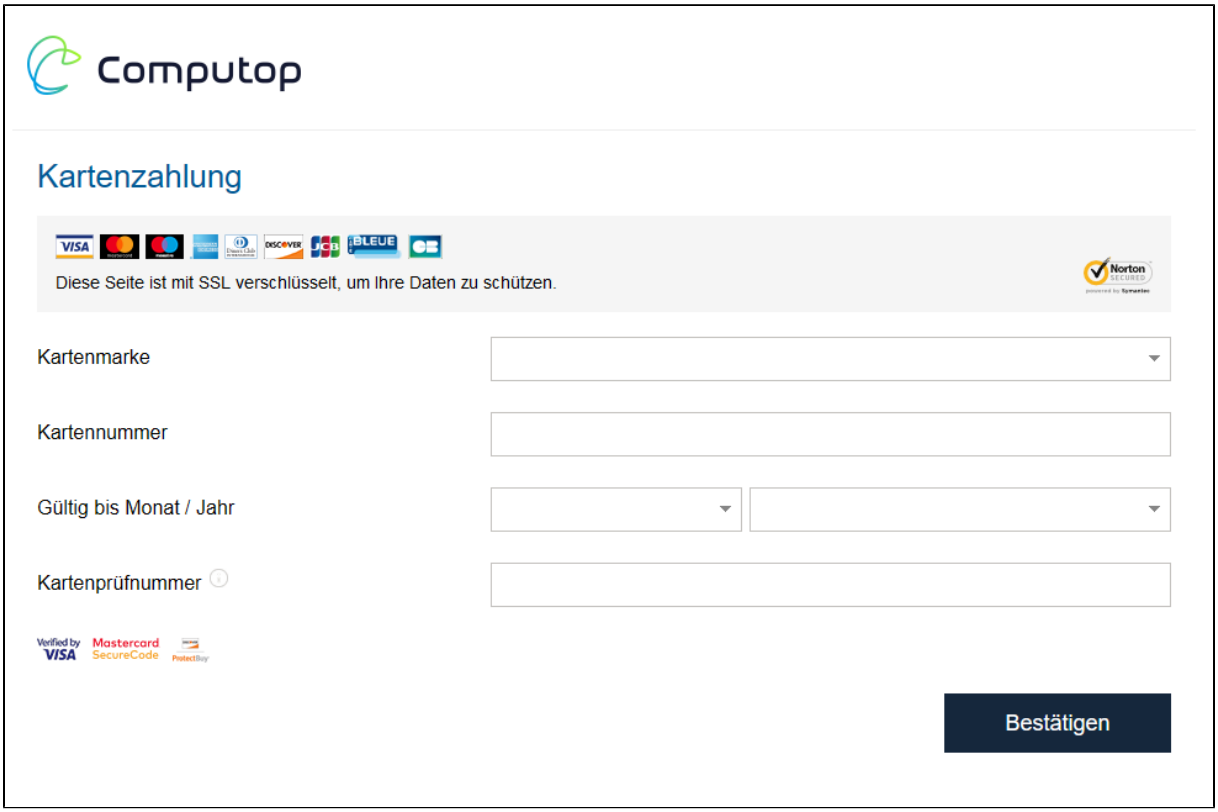
Paygate-Formulare

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 Paygate zu verbinden. Der Kunde gibt dann seine Zahlungsdaten im HTML-Formular des Paygate ein, das ein SSL-Zertifikat von Computop verwendet. Das Paygate führt die Zahlung aus und informiert den Shop über den Transaktionsstatus (URLNotify, URLSuccess, URLFailure). Formulare verursachen den geringsten Programmieraufwand.



Ablauf einer Zahlung mit Paygate HTML-Formularen

Ein Vorteil ist, dass Kreditkartendaten und Kontoverbindungen nur auf dem 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.

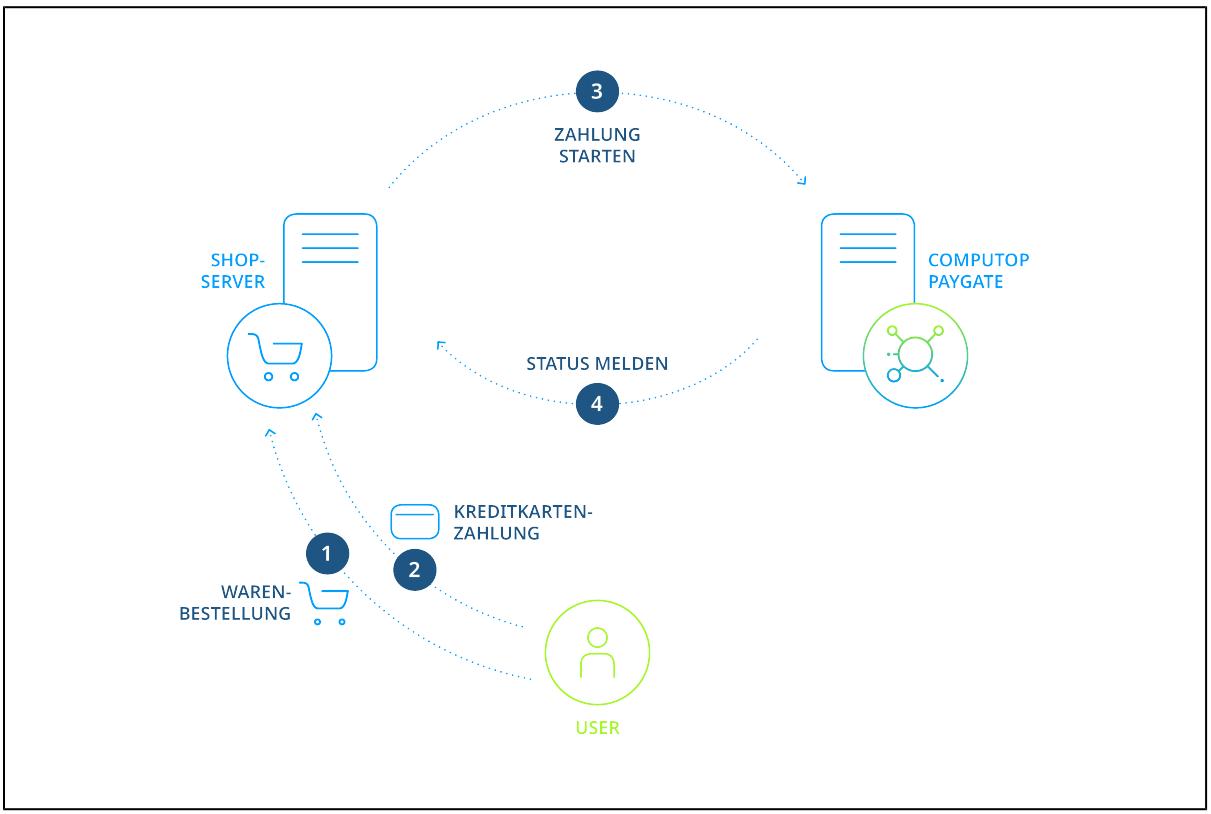


Standard-Paygate-Formular für Kreditkartenzahlungen

Die Formulare des 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

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 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 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 Schnittelle 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).

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 Bit TLS-Verschlüsselung (HTTPS). Um eine Transaktion auszuführen, wird je nach Zahlungsmethode eine bestimmte Internet-Seite aufgerufen.

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 Paygate 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**.

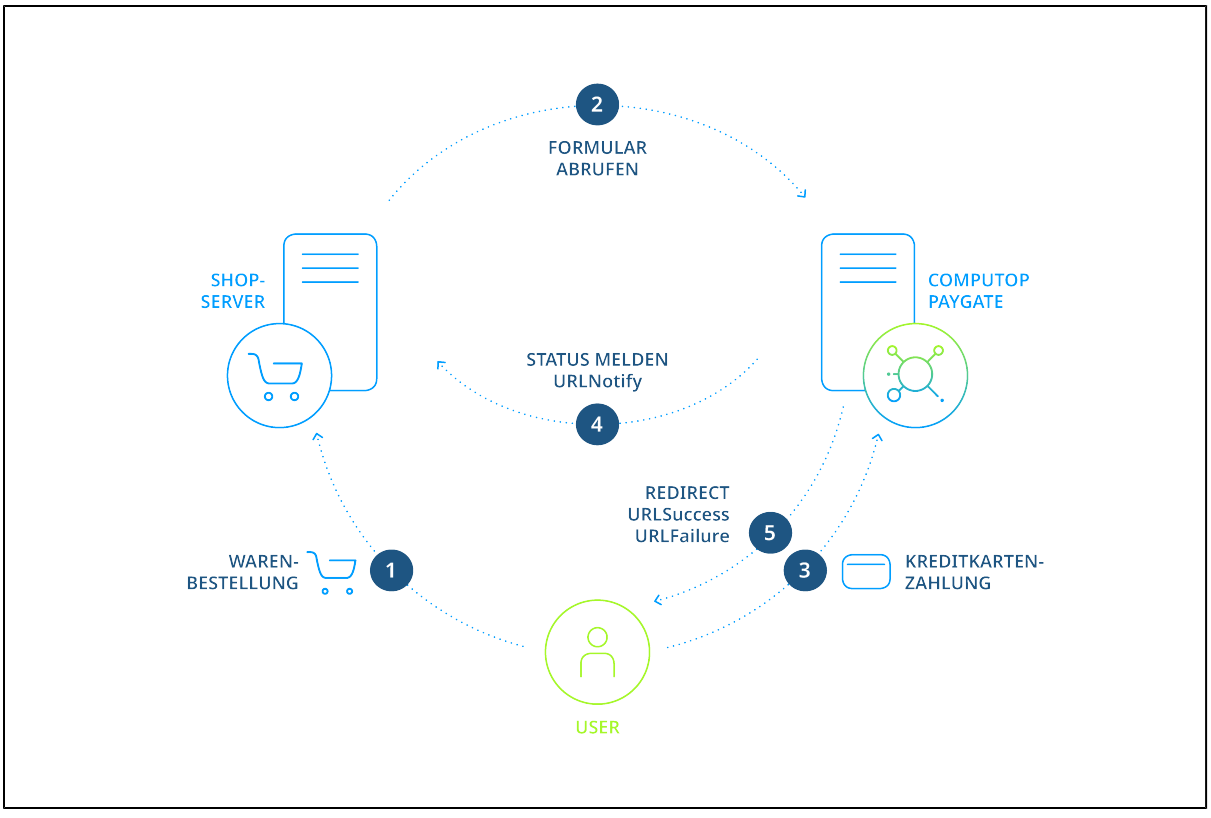
2 Der Shop generiert eine Zeichenkette (String) mit Händlernummer, Betrag und Warenkorb: "HAENDLER=IhreHaendlerID&BETRAG=49&WARENKORB=Blumen"

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 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.

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 Support.

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=IhreHaendlerID&Len=162&Data=E98D40FFFD622C5FE7414F73539A1852C2CE7C8B09D34DF217E27FA2E194B9968DE9ABAE3B
1F44B5485EFE3EF2597C7395BADBAD4340CDFD000DD57129EEFAA0BE904A7E2339DCF9363DA6ACDBE5EF98E169FC3092B160252A0371
35421FD0CE092C174A7D1D63517BD45099AC2B682F5E3CD2C942A6F0E741A833C0&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="IhreHaendlerID">

    <INPUT type="hidden" name="Len"       value="162">

    <INPUT type="hidden" name="Data"      value="
E98D40FFFD622C5FE7414F73539A1852C2CE7C8B09D34DF217E27FA2E194B9968DE9ABAE3B1F44B5485EFE3EF2597C7395BADBAD4340
CDFD000DD57129EEFAA0BE904A7E2339DCF9363DA6ACDBE5EF98E169FC3092B160252A037135421FD0CE092C174A7D1D63517BD45099
AC2B682F5E3CD2C942A6F0E741A833C0">

    <INPUT type="hidden" name="Background"

value="https://www.meinshop.de/grafik/hintergrundbild.jpg">

    <INPUT type="submit" name="Zahlen"    value="Zahlen">

</FORM>
```

Hash MAC-Authentisierung

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

Hintergrund: Anders als das HMAC-Verfahren hat jede Verschlüsselungsmethode den Nachteil, dass es eine passende Entschlüsselungsmethode gibt. Wer den richtigen Schlüssel besitzt oder die Verschlüsselung knackt, kann die Daten lesen und manipulieren. Eine Verschlüsselungsmethode ist daher nie zu 100% sicher. Beim Hash-Verfahren ist eine Entschlüsselung hingegen nicht möglich, so dass ein Hash-Wert die Authentizität der Nachricht zweifelsfrei bestätigen kann.

Um die Authentizität Ihrer Zahlungen zu überprüfen, nutzt das Computop Paygate einen Hash Message Authentication Code (HMAC). Dafür wird der Algorithmus MACSHA-256 mit einer 32stelligen Schlüssellänge (256 Bit) verwendet. Durch das zusätzliche Passwort ist das HMAC-Verfahren besonders sicher.

Die folgende Tabelle beschreibt, wie Sie die Hash-Werte für Ihre Zahlung generieren können:

Schritt	Aufgabe
1	Bitte melden Sie sich im Computop Support, der Ihnen das Hash-Passwort mitteilt.
2	Die Berechnung des HMAC-Wertes erfolgt mit Hilfe des Passworts und mehreren Parameter-Werten. Für die Berechnung werden die Parameter PayID, TransID, MerchantID, Amount und Currency verwendet und mit Sternchen getrennt: PayID*TransID*MerchantID*Amount*Currency Hinweis: Falls eine Transaktion nicht alle diese Parameter unterstützt, können Sie den fehlenden Wert einfach weglassen. Zum Beispiel gibt es bei der ersten Transaktion noch keine PayID, so dass sie diese nicht übergeben müssen. Bei Folgetransaktionen ist die PayID Bestandteil der Hash-Berechnung: Beispiel 1 ohne PayID (z.B. bei Autorisierung): *B456Ref890*IhreHändlerID*9900*EUR Beispiel 2 mit PayID (z.B. bei Buchung): 1237890*B456Ref890*IhreHändlerID*9900*EUR Beispiel 3 ohne TransID: 1237890**IhreHändlerID*9900*EUR
3	Verwenden Sie den MAC SHA-256-Algorithmus, den fast alle Programmiersprachen unterstützen, um den Hash-Wert mit Passwort und die Parameterwerte zu berechnen.

4	Nutzen Sie den Parameter MAC, um den hexcodierten Hash-Wert bei jeder Transaktion im verschlüsselten Data-Feld an das Paygate zu übergeben.

Hinweis: Beachten Sie, dass der Parameter MAC für alle Folgetransaktionen (z.B. Buchung, Gutschrift) Pflicht ist, wenn er bei der ersten Transaktion (z.B. Autorisierung) übergeben wurde.

Wichtig: Transaktionen mit falschen oder fehlenden HMAC-Werten lehnt das Paygate frühzeitig ohne weitere Bearbeitung ab, weil dies ein Hinweis auf Hacker-Angriffe ist. Transaktionen, die das Paygate mit den Fehlercodes 20100044 oder 20120044 ablehnt, erscheinen deshalb nicht in Computop Analytics.

Listing mit HMAC-Beispielen

Request ohne PayID:

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

Zeichenfolge für MAC-Generierung:

*100000001*Test*11*EUR

Request mit MAC:

MerchantID=IhreHaendlerID&TransID=100000001&Amount=11&Currency=EUR&URLSuccess=https://www.shop.de/ok.html&URLFailure=https://www.shop.de/failed.html&OrderDesc=Mein Einkauf&MAC=A0E3A8BB9473CF4D3F91181E0859650A9AF3F4AD0AE1E839AC7B750247A2E947

Request ohne TransID:

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

Zeichenfolge für MAC-Generierung:

8ee4e922c39446ac9ee66095a4a4b475**Test*100*USD

Request mit MAC:

MerchantID=IhreHaendlerID&PayID=8ee4e922c39446ac9ee66095a4a4b475&Amount=100&Currency=USD&MAC=F1EB4A8BB9473CF4D3F91181F0859659A9AF3F4AD0AE1E839AC7B750247A2D636

Listing: Beispiele für Hash Message Authentication Codes (HMAC)

Der Shop muss verifizieren, dass ein Notifikationsrequest wirklich von Computop kommt. Sonst kann ein Angreifer eine Transaktion initialisieren und dann diese Notifikation fälschen. Ein Shop-Betreiber wird nicht bei jeder Transaktion manuell prüfen, ob eine entsprechende Transaktion tatsächlich durchgeführt wurde. Daher muss das Modul dies automatisch erledigen.

Zurzeit wird der Notifikationsrequest nur verschlüsselt. Allerdings garantiert die Verschlüsselung nicht die Authentizität einer Nachricht. Es ist lediglich sichergestellt, dass eine Nachricht nicht mitgehört werden kann. Daher ist diese Sicherheitsmaßnahme nicht ausreichend. Deshalb wird der Antwortparameter MAC verwendet, der über denselben Algorithmus gebildet wird wie beim Eingangs-MAC. Lediglich die Datenparameter unterscheiden sich. Folgendes Daten-Muster gilt hier für die Hash-Generierung: PayID*TransID*MerchantID*Status*Code

Der Parameter MAC wird nur an die Success- oder Failure-URL und bei Notifys zurückgegeben.

Wichtig: Passwörter dürfen **niemals** via E-Mail versandt werden, da dann **sofort** die Sicherheit der verschlüsselten Requests/Responses nicht mehr gegeben ist. Sollten versehentlich Passwörter via E-Mail versandt worden sein, müssen neue Passwörter kostenpflichtig im Einzelprozess oder im nächsten Standard-Release hinterlegt werden. Computop **weist ausdrücklich auf das Risiko** hin, **derart kompromittierte MIDs** fortzuführen. Sollte der Händler dennoch eine kompromittierte MID fortführen, hat er das Haftungsrisiko für eventuelle Schäden aufgrund der aktuell kompromittierten Passwörter selbst zu tragen.

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

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.

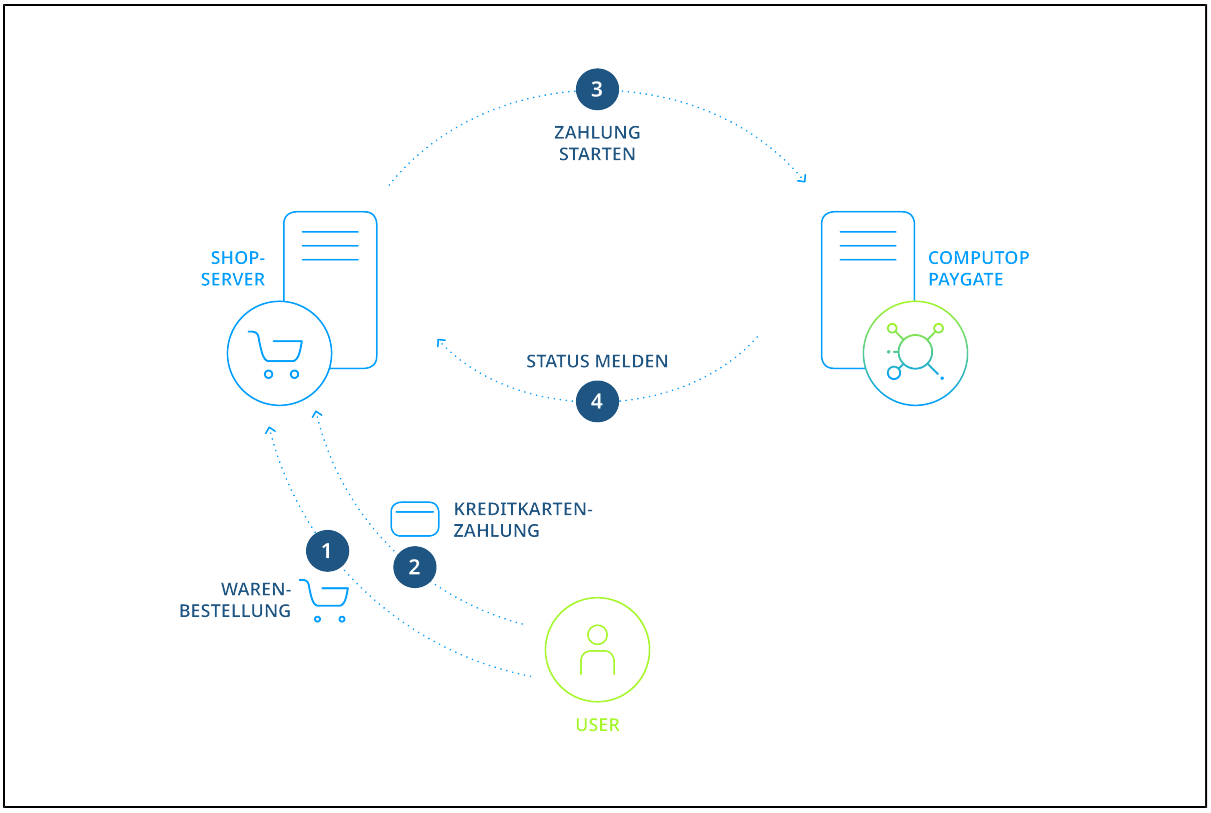
Wenn Sie die verschiedenen Fehlerfälle testen wollen, erlaubt das Paygate eine Simulation der gewünschten Fehlercodes. Um einen Fehler zu simulieren, übergeben Sie im Parameter **OrderDesc** das Schlüsselwort **Test** und den vierstelligen Detail-Fehlercode, also zum Beispiel "Test:0110", um eine abgelaufene 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 Support 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 eines 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&CCCVC=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=D622C5FE7414F73539A1852C2CE7AA0BE904A7E2339DCF9363DA6ACDBE5EF98E169FC3092B
1602564DBF2C3C75173A62C484962A247B8A91EA7A544ADCF2A037135421FD0CE092C174A7D1D63517BD45099AC2B682F5E3CD2C942A6
F0E741A833C
```

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	www.computop-paygate.com
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: www.computop-paygate.com

Connection: Close

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

Content-Length: 287


MerchantID=IhreHaendlerID&Len=162&Data=E98D40FFFD622C5FE7414F73539A1852C2CE7C8B09D3E876F52CBECF59EC63E9B8AA0130FA
92F65964E3EEE74DF217E27FA2E194B9968DE9ABAE3B1F44B5485EFE3EF2597C7395BADBAD4340CDFD000DD57129EEFAA0BE904A7E23
39DCF9363DA6ACDBE5EF98E169FC3092B1602564DBF2C3C75173A62C484962A247B8A91EA7A5
```

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 Support.

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=ECF59EC63E9BEE74DF217E27FA2E194B92597C7395BADBAD4340CDFD000DD57129EEFAA0BE904A7E233ACDBE5EF98E1
692B1602564DBF2C3C75173A62C484962A247B8A91EA7A544
```

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

```
PayID=a234b678e01f34567090e23d567890ce&XID=50f35e768edf34c4e090e23d567890ce&TransID=100000001&Status=AUTHORIZED&Descript
ion=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