Internet Payment Gateway

Integrationsleitfaden

Connect

Version 4

amys IT-Solutions GmbH
www.amys-it.com
info@amys-it.com

Internet Payment Gateway

INTEGRATIONSLEITFADEN

Connect

Version 4

Inhalt

Unterstützung bei Fragen

Für das Internet Payment Gateway sind verschiedene Handbücher erhältlich. Der vorliegende Integrationsleitfaden Connect ist für die technische Integration besonders nützlich. Daneben finden Sie im Benutzerhandbuch Virtual Terminal wichtige Hinweise zur Hinterlegung der Internetadressen Ihres Bestellformulars und Ihrer Antwortseiten, die dem Händler nach der Zahlungstransaktion angezeigt werden sollen. Zusätzlich finden Sie dort Hinweise zur individuellen Anpassung der Zahlseiten, dem Abrufen von Berichten und Grafiken zu Ihren Zahlungsvorgängen sowie zur Transaktionsverarbeitung durch manuelle Eingabe der Daten.

Wenn Sie in der verfügbaren Dokumentation keine Antwort auf Ihre Fragen finden, hilft Ihnen gerne unser Support Team weiter:

E-Mail: support@amys-it.com

Telefon +49 69 34874 025 0

1 Einführung

Mit Connect bietet sich eine einfache Methode, einen Online-Shop mit dem leistungsstarken Internet Payment Gateway zu verbinden.

Connect erledigt dabei Ihre gesamte Interaktion mit Kreditkartenprozessoren und Kreditinstituten.

Das vorliegende Dokument beschreibt, wie Sie Ihre Website mit Connect verbinden um möglichst schnell damit beginnen zu können, Zahlungen über Ihren Webshop zu akzeptieren.

2 Optionen für den Zahlungsvorgang

2.1 Gehostete oder eigene Eingabeformulare

Connect stellt Ihnen grundsätzlich zwei Möglichkeiten der Integration in Ihre Website zur Wahl:

- Bei der einfachsten Lösung nutzen Sie für den Zahlungsvorgang vorgefertigte Formularseiten, die wir auf unserem Server für Sie bereitstellen. In diesem Fall wird der Kunde für den Zahlungsvorgang an weitergeleitet, erfasst und übermittelt die Daten auf einer SSL-gesicherten Seite und wir leiten ihn im Anschluss zu einer von Ihnen definierten Seite Ihres Shops zurück. Daneben informieren wir Sie bzw. Ihr Shopsystem über das Ergebnis des Zahlungsvorgangs.
- Wenn Sie möchten, dass der Kunde zur Zahlung Ihre Shopumgebung nicht verlässt, können Sie eigene Formularseiten erstellen, die Sie komplett individuell im Design Ihres Shops gestalten können. Obwohl das Formular zur Dateneingabe dann von Ihnen bereitgestellt wird, können die sensiblen Kartendaten direkt vom Karteninhaber an das Gateway übermittelt werden, sodass Sie diese nicht bei sich speichern müssen und Sicherheitsrisiken vermeiden können. Damit der Kunde schon bei der Anzeige Ihres Eingabeformulars eine verschlüsselte Verbindung angezeigt bekommt, muss Ihre Website in diesem Fall eine sichere SSL-Verbindung über einen HTTPS-Server zur Verfügung stellen.

Bitte beachten Sie **unbedingt** die Richtlinien zur PCI-Zertifizierung für Ihre Entscheidung der verwendeten Methode. Fragen Sie dazu bitte Ihren Acquirer.

Daneben stehen drei verschiedene Modi zur Auswahl, die den Umfang der Daten festlegen, die über das Gateway erfasst werden sollen. Somit können Sie entsprechend Ihrer individuellen Geschäftsprozesse auswählen, ob nur Zahldaten oder auch Rechnungs- und Lieferadresse zu einem Bestellvorgang übermittelt werden sollen.

Je nach Komplexität Ihrer Geschäftsprozesse kann auch eine zusätzliche Integration der API (siehe dazu Integrationsleitfaden API) sinnvoll sein.

2.2 PayOnly Modus

Im PayOnly Modus sammelt das Internet Payment Gateway einen Mindestbestand an Informationen für die Transaktion (z. B. Kontonummer und Bankleitzahl für Lastschrift-Transaktionen). Bei Nutzung der von gehosteten Zahlseite bekommt der Karteninhaber nur eine Seite gezeigt, auf der die Angaben für die Zahlung eingetragen werden können.

2.3 PayPlus Modus

Im PayPlus Modus sammelt das Gateway zusätzlich zu den unter PayOnly genannten Angaben einen kompletten Bestand an Rechnungsinformationen. Bei Nutzung der gehosteten Eingabeformulare bekommt der Karteninhaber zwei Seiten angezeigt, eine für die Rechnungsangaben und eine für die Zahlungsinformationen.

2.4 FullPay Modus

Wenn Connect sämtliche verfügbaren Informationen (Angaben zu Rechnungsadresse, Lieferadresse und Zahlungsweise) sammeln soll, empfehlen wir die Nutzung des FullPay Modus. FullPay erlaubt Ihnen, den Gesamtbetrag der Bestellung an Connect zu senden. Das System übernimmt dann die Sammlung aller weiteren notwendigen Angaben. Dies ist die einfachste Methode, Ihren Webshop in Connect zu integrieren. Optional können Sie auch hier Ihre eigenen Formulare für die Eingabe der Daten verwenden.

3 Die ersten Schritte

Dieser Abschnitt enthält ein einfaches Beispiel, wie Sie Ihre Website im FullPay Modus in das Internet Payment Gateway integrieren. Sie finden Beispiele für die Nutzung von ASP und PHP. Dieser Abschnitt geht davon aus, dass der Entwickler grundlegende Kenntnisse von der gewählten Skriptsprache besitzt.

3.1 Checkliste

Folgendes benötigen Sie für die Integration mit dem Gateway:

- **storename**
  Die ID Ihres Shops, die Sie von amys-IT erhalten haben.
  Zum Beispiel: 10123456789

- **Shared Secret** (gemeinsamer Schlüssel)
  Der gemeinsam verwendete (symmetrische) Schlüssel, den Sie von amys-IT erhalten haben.
  Er wird zur Erzeugung des Hash-Wertes (siehe unten) benötigt.

3.2 Hash Berechnung

Zur Absicherung der Transaktion und des Transaktionsergebnises wird ein Hash-Wert berechnet. Der Hashwert setzt sich aus verschiedenen Parametern zusammen. Die Parameter zuerst als String verketten. Hierbei ist zu beachten, dass auch der Betrag hier als String verarbeitet wird. Dieser String wird anschließend stellenweise in den entsprechenden Hexadezimalwert gewandelt und dann mit dem SHA-1 in den Hash gewandelt.

Beispiel siehe Anhang I:

3.3 Hinweise zur Implementierung der Schnittstelle Connect

Bitte beachten Sie, dass die Daten per POST direkt vom Kundenbrowser an die Schnittstelle übergeben werden und nicht Technologien wie z.B. AJAX verwendet werden. Somit gewährleisten Sie, dass die Schnittstelle, insbesondere bei 3D Secure und Giropay, korrekt arbeitet. Das Zahlungsergebnis sollte immer aus den POST-Parametern ausgewertet werden.

3.4 ASP-Beispiel

Das folgende Beispiel für ASP zeigt eine einfache Seite, die im FullPay Modus mit dem Internet Payment Gateway kommuniziert. Sobald der Karteninhaber auf ‘Submit’ (Absenden) klickt, wird er auf die gesicherten Seiten von weitergeleitet, wo er seine Rechnungs-, Liefer- und Zahlungsangaben machen kann. Nach Abschluss der Zahlung gelangt der Anwender wieder zurück zum Shop. Der Ort der Seite, auf die der Kunde zurückgeleitet wird ist konfigurierbar.

```
<!-- #include file="ipg-util.asp"-->

<html>
  <head><title>IPG Connect Sample for ASP</title></head>
  <body>
  <p><h1>Order Form</h1></p>

  <form method="post" action="
https://test.ipg-online.com/connect/gateway/processing ">
```

```
        <input type="hidden" name="txntype" value="sale">
        <input type="hidden" name="timezone" value="CET"/>
        <input type="hidden" name="txndatetime" value="<% getDateTime()
%>"/>
        <input type="hidden" name="hash" value="<% call createHash(
"13.00","978" ) %>"/>
        <input type="hidden" name="storename" value="12066666666" />
        <input type="hidden" name="mode" value="fullpay"/>
        <input type="text" name="chargetotal" value="13.00" />
        <input type="hidden" name="currency" value="978"/>
        <input type="submit" value="Submit">
  </form>
  </body>
</html>
```

Der in Anhang I aufgelistete Code ipg-util.asp enthält den Code zur Erzeugung eines SHA1 Hash. Die Bereitstellung eines Hash wie im Beispiel stellt sicher, dass Sie als Händler der einzige sind, der Transaktionen für diesen Shop einreichen darf.

Bitte beachten Sie, dass die POST URL nur für den Test der Integration verwendet wird. Wenn Sie bereit für die Umstellung auf Produktivbetrieb sind, wenden Sie sich bitte an unser Support-Team, um die URL für den Produktivbetrieb zu erhalten.

Beachten Sie, dass der in Anhang I aufgeführte Code ipg-util.asp eine serverseitige JavaScript-Datei zur Erstellung des SHA1 Hash verwendet. Diese Datei kann auf Anfrage bereitgestellt werden. Wir empfehlen aus Sicherheitsgründen jedoch, den Hash-Wert auf Ihrem Server zu erzeugen.

3.5 PHP-Beispiel

Das folgende Beispiel für PHP zeigt eine einfache Seite, die im FullPay Modus mit dem Internet Payment Gateway kommuniziert. Sobald der Karteninhaber auf ‘Submit’ (Absenden) klickt, wird er auf die gesicherten Seiten von weitergeleitet, wo er seine Liefer-, Rechnungs- und Zahlungsangaben machen kann. Nach Abschluss der Zahlung gelangt der Anwender wieder zurück zur Belegseite des Händlers. Der Ort der Belegseite ist konfigurierbar.

```
<? include("ipg-util.php"); ?>

<html>
<head><title>IPG Connect Sample for PHP</title></head>
  <body>
  <p><h1>Order Form</h1>

<form method="post"
action="https://test.ipg-online.com/connect/gateway/processing">
  <input type="hidden" name="txntype" value="sale">
  <input type="hidden" name="timezone" value="CET"/>
  <input type="hidden" name="txndatetime" value="<?php echo
getDateTime() ?>"/>
  <input type="hidden" name="hash" value="<?php echo createHash(
"13.00","978" ) ?>"/>
  <input type="hidden" name="storename" value="12066666666"/>
<input type="hidden" name="mode" value="fullpay"/>
<input type="text" name="chargetotal" value="13.00"/>
<input type="hidden" name="currency" value="978"/>

  <input type="submit" value="Submit">
```

```
  </form>
  </body>
</html>
```

Bitte beachten Sie, dass die POST URL nur für den Test der Integration verwendet wird. Wenn Sie bereit für die Umstellung auf Produktivbetrieb sind, wenden Sie sich bitte an das unser Support-Team, um die URL für den Produktivbetrieb zu erhalten.

Der in Anhang II aufgelistete Code ipg-util.php enthält den Code zur Erzeugung eines SHA1 Hash. Die Bereitstellung eines Hash wie im Beispiel stellt sicher, dass Sie als Händler der einzige sind, der Transaktionen für diesen Shop einreichen darf.

3.6 Beträge für Testtransaktionen

Auf dem Testsystem werden bei Kreditkartentransaktionen die Nachkommastellen des Zahlbetrages (chargetotal) als Fehlercode interpretiert. Sie können dadurch im Testsystem steuern, ob Sie als Zahlungsergebnis „Genehmigt“ oder „Abgelehnt“ als Antwort bekommen. Glatte Beträge (z.B. 5,00 oder 13,00) führen zu einer erfolgreichen Transaktion. Mit abweichenden Nachkommastellen im Betrag wird eine Ablehnung vom Autorisierungssystem simluliert (z.B 5,96 = Fehler 96 ; 13,05 = Fehler 05).

Verwenden Sie daher für Testtransaktionen am besten glatte Beträge, z. B. 13,00 EUR wie in den obigen Beispielen.

4 Pflichtfelder

Je nach Transaktionstyp müssen die folgenden Felder in dem an das Gateway eingereichten Formular enthalten sein (X=Pflichtfeld):

Feldname	**Beschreibung, mögliche Werte und Formatangaben**	**„Sale“ Transaktion**	**Vorautorisierung ***	**Buchung einer Vorautorsierung ***	**Storno**
txntype	'sale', 'preauth', 'postauth' oder 'void' (Der Transaktionstyp – bitte beachten Sie hierzu die Erläuterungen im Benutzerhandbuch Virtual Terminal) *Die Möglichkeit ‚void‘ zu senden ist eingeschränkt. Bitte wenden Sie sich an das Support.Team, wenn Sie diese Option nutzen wollen.*	X (sale)	X (preauth)	X (postauth)	X (void)
timezone	GMT, CET oder EET (Die Zeitzone der Transaktion)	X	X	X	X
txndatetime	YYYY:MM:DD-hh:mm:ss (Der genaue Zeitpunkt der Transaktion)	X	X	X	X
hash	Dies ist ein SHA1 Hash der folgenden Felder: storename + txndatetime + chargetotal + currency + sharedsecret. Beachten Sie, dass der Hash in genau dieser Reihenfolge zusammengestellt wird. Weiter unten finden Sie ein Beispiel für die Generierung eines SHA1 Hash.	X	X	X	X
storename	Ihre Shop-ID, wie von amys-IT mitgeteilt.	X	X	X	X
mode	‘fullpay’, ‘payonly’ oder ‘payplus’ (Der gewünschte Modus für diese Transaktion)	X	X		
chargetotal	Der Gesamtbetrag der Transaktion. Als Dezimal-	X	X	X	X

	Trennzeichen muss ein Komma oder Punkt verwendet werden (z. B. 12,34 für 12 Euro und 34 Cent). Tausender-Trennzeichen (z. B. 1.000 EUR) sind nicht zugelassen.				
currency	Die Währung der Transaktion als dreistelliger numerischer ISO 4217 Wert (siehe Beispiele unten).	X	X	X	
oid	Bestellnummer (Order ID) des Vorgangs zu dem eine Buchung der Vorautorisierung oder ein Storno erfolgen soll			X	X
tdate	Genaue Kennzeichnung der Transaktion eines Vorgangs, die storniert werden soll. Diesen Wert erhalten Sie als Antwortparameter 'tdate' zur entsprechende Transaktion				X

- * Die Transaktionsart „Vorautorisierung" funktioniert ausschließlich mit den Bezahlarten „Kreditkarten", „PayPal" und „Click&Buy".

Beispiele ISO 4217 Währungscodes

Währung	Währungs-kennzeichen	Numerischer ISO 4217 Wert
Euro	EUR	978
Britische Pfund	GBP	826
Chinesischer Renimbi	CNY	156
US Dollar	USD	840
Ungarischer Forint	HUF	348
Schweizer Franken	CHF	756
Bahrein Dollar	BHD	048
Tschechische Kronen	CZK	203
Dänische Kronen	DKK	208
Hong Kong Dollar	HKD	344
Polnische Zloty	PLN	985
Rumänischer Neuer Leu	RON	946

Saudi Rihal	SAR	682
Singapore Dollar	SGD	702
Süd Afrikanischer Rand	ZAR	710
Süd Koreanischer Won	KRW	410
Indischer Rupee	INR	356
Israelischer Neuer Shekel	ISL	376
Japanischer Yen	JPY	392
Kuwaiti Dinar	KWS	414
Litauischer LItas	LTL	440
Mexikanischer Peso	MXN	484
Neuseländischer Dollar	NZD	554
Südafrikanische Rand	ZAR	710
Schwedische Kronen	SEK	752
Türkischer Lira	TRY	949
UAE Dirham	AED	784
Kanadische Dollar	CAD	124
Kroatische Kuna	HRK	191

5 Optionale Formularfelder

Die in diesem Abschnitt beschriebenen Felder sind für eine Transaktion optional.

- Mobile Mode

  Benutzen Ihre Kunden für den Einkauf in Ihrem Online Shop mobile Endgeräte, können den „Mobile Mode“ mit dem Parameterwert „true“ aktivieren. Diese Ergänzung führt dazu, dass diese Kunden zum Checkout Prozess geführt werden, der speziell nach den Bedürfnissen mobiler Geräte gestaltet ist.

- **paymentMethod**
  Erfolgt die Auswahl der Zahlungsweise (z. B. MasterCard, Visa oder Lastschrift) bereits in Ihrem Shop bzw. möchten Sie die Zahlart vorgeben, übergeben Sie bei Zahlungstransaktionen (sale, preauth) zusätzlich den Parameter *paymentMethod*. Die dafür gültigen Werte sind

Zahlungsmethode	Value
MasterCard	**M**
Visa (Credit/Debit/Electron/Delta)	**V**
American Express	**A**
Diners	**C**
JCB	**J**
Direct Debit Germany	**debitDE**

giropay	**giropay**
Laser	**L**
Maestro	**MA**
Maestro UK/Solo	**maestroUK**
PayPal	**paypal**
ClickandBuy	**clickAndBuy**
DirektÜberweisung / Direkt.Ident	**direkt**

Wird dieser Parameter nicht angegeben, bekommt der Kunden eine Auswahl aller für Ihren Shop freigeschalteten Zahlungsweisen angezeigt und wählt dort selbst die gewünschte Zahlungsart..

- **oid** (max. 100 Zeichen)

  Dieses Feld ermöglicht Ihnen, eine eindeutige Kennung für eine Bestellung zu Vergeben. Mit der Erweiterungsfunktion „Debit Text“ kann diese Angabe bei Lastschrifttransaktionen an die Bank des Kunden weitergeleitet werden, sodass sie auf dem Kontoauszug Ihres Kunden ausgewiesen werden kann. Die ersten 30 Zeichen der Bestellnummer werden bei Kreditkartenzahlungen mit an Ihren Acquirer übertragen und können eventuell mit auf der Händlerabrechnung ausgewiesen werden. Wenn Sie selbst keine Bestellnummer vergeben möchten, generiert das System automatisch eine für Sie.

- **customerid** (max. 32 Zeichen)

  Dieses Feld ermöglicht Ihnen einen beliebigen Wert, z. B. eine Kennung für den Kunden zu übergeben. Mit der Erweiterungsfunktion „Debit Text“ kann diese Angabe bei Lastschrittransaktionen an die Bank des Kunden weitergeleitet werden, sodass sie auf dem Kontoauszug Ihres Kunden ausgewiesen werden kann. Die ersten 30 Zeichen der Kundennummer werden bei Kreditkartenzahlungen mit an Ihren Acquirer und die Bank des Karteninhabers übertragen und können eventuell mit auf der Händlerabrechnung, bzw. Karteninhaberabrechnung ausgewiesen werden.

- **invoicenumber** (max. 48 Zeichen)

  Dieses Feld ermöglicht Ihnen einen beliebigen Wert, z. B. eine Rechnungsnummer oder Warengruppe zu übergeben.

- **mandateReference**

  In diesem Feld wird bei Lastschrift die Mandatsreferenz übermittelt.

- **refer** (max. 2000 Zeichen)
  Dieses Feld gibt an, wer dem Kunden Ihren Shop empfohlen hat.

- **comments** (max. 2000 Zeichen)
  Hier tragen Sie mögliche Anmerkungen zur Transaktion ein.

- **responseSuccessURL**
  Die URL, zu der Sie den Kunden nach erfolgreicher Transaktion leiten möchten (die "Dankeschön"-Seite in Ihrem Shop). Dies wird zwingend benötigt, wenn Sie im Virtual Terminal keine URL in den Einstellungen für die Connect Schnittstelle hinterlegt haben. Der Wert übersteuert, wenn er bei Transaktionen an die Schnittstelle übergeben wird, einen eventuell im Virtual Terminal hinterlegten Wert für die "Dankeschön"-Seite.

- **responseFailURL**
  Die URL, zu der Sie den Kunden nach abgelehnter oder gescheiterter Transaktion leiten möchten (die "Tut-uns-leid"-Seite in Ihrem Shop). Dies wird zwingend benötigt, wenn Sie im Virtual Terminal keine URL in den Einstellungen für die Connect Schnittstelle hinterlegt haben. Der Wert übersteuert, wenn er bei Transaktionen an die Schnittstelle übergeben wird, einen eventuell im Virtual Terminal hinterlegten Wert für die " Fehlerseite".

- **transactionNotificationURL**
  Die URL, an die das Transaktionsergebnis direkt mitgeteilt werden soll (siehe auchTransaktionsergebnis)

- **hashExtended**

  Der erweiterte Hash ist ein optionales Sicherheitsfeature, welches erlaubt alle Parameter der Anfrage zu integrieren.

- **trxOrigin**

  Dieser Wert erlaubt Ihnen das sichere und gehostete Zahlungsformular in Ihre Anwendung für Mail and Telephone (MOTO) Order Zahlungen zu integrieren. Mögliche Werte sind „MOTO“ für den MOTO Channel und „ECI“ für die Nutzung in ecommerce Umgebungen, in denen Ihr Kunden seine Zahlungsdetails eigenständig eingibt.

- **language**
  Mit der Angabe einer Sprache für die Zahlseite können Sie ausländischen Kunden die Zahlseite in deren Sprache anzeigen. Die für Ihren Shop hinterlegte Standardsprache wird dabei überschrieben. Aktuell sind folgende Sprachen wählbar:

Sprache	language
Deutsch	de_DE
Englisch (USA)	en_US
Englisch (Großbritannien)	en_GB
Finnisch	fi_FI
Französisch	fr_FR
Italienisch	it_IT

6 Verwendung eigener Eingabeformulare

Entscheiden Sie sich eigene Eingabeformulare bereitszustellen, d. h. nicht auf die gehosteten Formulare zurück zu greifen, sind zusätzlich zu den oben genannten Pflichtfeldern die in den folgenden Abschnitten (je nach gewähltem Modus) aufgeführten Felder in das Formular aufzunehmen.

Darüber hinaus sollten Sie vor Ausführung der Transaktion prüfen, ob Ihr Kunde in seinem Browser JavaScript aktiviert hat und ggf. darauf hinweisen, dass JavaScript für den Zahlungsvorgang aktiviert sein muss.

Die Verwendung des mode „payonly“ empfielt sich, wenn Sie Adressdaten die im Shop bereits erfasst wurden, an die Schnittstelle übergeben wollen um diese in den Zahlungsdetails darzustellen. Die zusätzlichen b- und s-Parameter werden in diesem Modus immer mit verarbeitet.

6.1 PayOnly Modus

Nach der Auswahl der Zahlungsart durch den Kunden, stellen Sie ihm eine zur Zahlart passende HTML-Seite mit einem Formular zur Eingabe der Bezahlinformationen sowie versteckten Parametern mit den weiteren Transaktionsinformationen bereit.

Neben den oben gelisteten Pflichtfeldern (ggf. als versteckte Parameter) muss Ihr Zahlungsformular folgende Felder enthalten:

Feldname	**Beschreibung, mögliche Werte und Formatangaben**	**Kreditkartenzahlung** (+ Visa Debit/Electron/Delta)	**Lastschrift (Direct Debit)**	**Maestro**	**giropay**	**PayPal, ClickandB**GB Direktüberweisung	**Maestro UK/Solo**
cardnumber	Für die Kartennummer des Kunden (12 bis 24 Zeichen)	X		X			X
expmonth	Für den Ablaufmonat der Karte (zweistellig)	X		X			X
expyear	Für das Ablaufjahr der Karte (vierstellig)	X		X			X
cvm	Für die Kartenprüfnummer, die meist auf der Rückseite der Karte angegeben ist (3- bis 4-stellig)	X					(X)
iban	Für die IBAN des Kunden (22 stellig)		X				
bic	Für die BIC des Kunden (8 oder 11 stellig)				X		

6.2 PayPlus Modus

Bei Nutzung des PayPlus Modus ist es möglich, zusätzlich Lieferangaben an das Zahlungsgateway zu übermitteln. Der folgenden Tabelle können Sie das Format dieser zusätzlichen Felder entnehmen:

Feldname	Mögliche Werte	Beschreibung
bcompany	maximal 96 Alphanumerische Zeichen, Leerstellen und Gedankenstriche	Firma des Kunden
bname	maximal 96 Alphanumerische Zeichen, Leerstellen und Gedankenstriche	Name des Kunden
baddr1	Maximal 30 Zeichen, einschließlich Leerstellen	Zeile 1 Rechnungsadresse des Kunden
baddr2	maximal 30 Zeichen, einschließlich Leerstellen	Zeile 2 Rechnungsadresse des Kunden
bcity	maximal 30 Zeichen, einschließlich Leerstellen	Stadt Rechnungsadresse
bstate	maximal 30 Zeichen, einschließlich Leerstellen	Bundesland oder US-Bundesstaat
bcountry	2 Buchstaben Länderkennung (Großbuchstaben!)	Länderkennung Lieferadresse
bzip	maximal 24 Zeichen, Internationaler Postcode	Postleitzahl
phone	maximal 20 Zeichen	Telefonnummer des Kunden
fax	maximal 20 Zeichen	Faxnummer des Kunden
email	maximal 45 Zeichen	E-Mail-Adresse des Kunden

6.3 FullPay Modus

Bei Nutzung des FullPay Modus ist es möglich, zusätzlich Lieferangaben an das Zahlungsgateway zu übermitteln. Der folgenden Tabelle können Sie das Format der Rechnungsfelder entnehmen:

Feldname	Mögliche Werte	Beschreibung
sname	maximal 96 Alphanumerische Zeichen, Leerstellen und	Name Lieferadresse

	Gedankenstriche	
saddr1	maximal 30 Zeichen, einschließlich Leerstellen	Zeile 1 Lieferadresse
saddr2	maximal 30 Zeichen, einschließlich Leerstellen	Zeile 2 Lieferadresse
scity	maximal 30 Zeichen, einschließlich Leerstellen	Stadt Lieferadresse
sstate	maximal 30 Zeichen, einschließlich Leerstellen	Bundesland oder US-Bundesstaat
scountry	2 Buchstaben Länderkennung (Großbuchstaben!)	Länderkennung Lieferadresse
szip	maximal 24 Zeichen, Internationaler Postcode	Postleitzahl

6.4 Plausibiltätsprüfungen

Vor der Autorisierungsanfrage für eine Transaktion führt das Internet Payment Gateway einige Plausibilitätsprüfungen durch:

- Das Verfalldatum von Karten muss in der Zukunft liegen
- Die Kartenprüfnummer muss drei- oder vierstellig numerisch sein
- Der Aufbau einer Kartennummer muss korrekt sein (LUHN Check)
- Eine IBAN darf nicht länger als 22 Stellen sein
- Eine BIC muss acht- oder elfstellig sein

Sollten die angegebenen Daten nicht plausibel sein, wird dem Kunden eine entsprechende Fehlerseite angezeigt.

Um bei Verwendung eigener Zahlformulare diese Fehlerseite zu vermeiden, können Sie mit der Transaktion den zusätzlichen Parameter

full_bypass=true

übergeben. In diesem Fall erhalten Sie das Ergebnis der Plausibilitätsprüfung im Transaktionsergebnis zurück und können basierend darauf eine eigene Fehlerseite anzeigen.

7 Zusätzliche eigene Felder

Wenn gewünscht, können Sie weitere eigene Felder an das Gateway senden. Die eigenen Felder werden gemeinsam mit allen übrigen Feldern an die Antwort-URL zurückgeliefert.

Sie können im Virtual Terminal bis zu fünfzehn eigene Felder in Ihrer Shopkonfiguration dokumentieren. Diese Felder lassen sich dazu verwenden, zusätzliche Kundendaten zu sammeln, die für Sie speziell von Belang sind. Sie können damit z. B. demografische Kundendaten erheben und in der eigenen Datenbank für die weitere Analyse speichern.

8 3D Secure

Die Connect Schnittstelle bietet die technische Voraussetzung um Zahlungen über die Sicherheitssysteme Verified by Visa und MasterCard SecureCode zu authentifizieren. Wenn Ihr Kreditkarten-Akzeptanzvertrag diese Verfahren einschließt und Ihre Vertragsnummer für diesen Service aktiviert wurde, muss Ihre Zahlseite dafür nicht gesondert erweitert werden.

Grundsätzlich kann es bei 3D Secure vorkommen, dass eine Authentifizierung des Karteninhabers aus technischen Gründen nicht durchgeführt werden kann. Wenn die notwendigen Systeme zur Authentifizierung vorübergehend nicht verfügbar sind, wird die Zahlung in der Regel als „normale“ Zahlung (GICC ECI 7) durchgeführt. **Eine Übertragung der Haftung für einen eventuellen Zahlungsausfall („Chargeback“) auf den Kartenherausgeber ist in diesem Fall nicht gewährleistet.** Wenn Sie wünschen, dass solche Transaktionen nicht zur Autorisierung eingereicht werden, kann unser technisches Support-Team diese für Ihren Shop sperren. Da dies zu Umsatzverlusten führen kann, empfehlen wir diese Einstellung im Zweifel mit Ihrer Kreditkartengesellschaft (Acquirer) zu besprechen.

Wenn Sie aus bestimmten Gründen einzelne Transaktionen ohne die Verwendung von 3D Secure durchführen möchten, können Sie dies über den zusätzlichen Parameter *authenticateTransaction* mit den Werten "true" oder "false" steuern.

Beispiel für eine Transaktion ohne 3D Secure:

```
<input type="hidden" name="authenticateTransaction" value="false"/>
```

Bitte beachten Sie, dass es im technischen Ablauf von 3D Secure Transaktionen einige Unterschiede zu Transaktionen ohne 3D Secure gibt. Sollten Sie bereits eine Shopanbindung haben und nachträglich 3D Secure aktivieren wollen, empfehlen wir zuvor einige Testtransaktionen auf unserem Testsystem durchzuführen.

Kreditkartentransaktionen unter Verwendung von 3D Secure zeigen den Status an z.B, während der Käufer sich erstmalig für das Verfahren anmeldet: „?:waiting 3dsecure“. Bei Ablaufen der Session wird dem Käufer diese Meldung angezeigt “N:-5103:Cardholder did not return from ACS”. Die Transaktion muss dann wiederholt werden.

9 Erweiterungsfunktion Data Storage

Mit der Erweiterungsfunktion Data Storage können Sie Kreditkartendaten und Bankverbindungen Ihrer Kunden in einer verschlüsselten Datenbank hinterlegen, um auf diese für spätere Zahlungen zurückgreifen zu können.

Wenn Sie diese Funktion beauftragt haben, bietet Ihnen Connect die folgenden Funktionen:

- **Speicherung oder Aktualisierung der Zahlungsinformationen bei einer Transaktion**

  Übermitteln Sie bei einer Zahlungstransaktion zusätzlich den Parameter ***hosteddataid (max. 128 Zeichen)*** mit einer eindeutigen Kennung für die zu hinterlegenden Zahlungsinformationen. Je nach Zahlart werden bei einer erfolgreichern Zahlungstransaktion unter dieser Kennung Kartennummer und Verfalldatum bzw. Kontonummer und Bankleitzahl hinterlegt. Ist die ‚hosteddataid' bereits vorhanden, werden die gespeicherten Informationen überschrieben.

- **Zahlungstransaktionen mit hinterlegten Daten**

  Wurden zu einem Kunden Zahlungsinformationen hinterlegt, können Sie unter Angaben der ‚hosteddataid' Zahlungstransaktionen durchführen ohne dass eine erneute Angabe von Kartennummer und Verfalldatum bzw. Kontonummer und Bankleitzahl notwendig sind.

  Bitte beachten Sie, dass die Kartenprüfnummer (meistens auf der Rückseite der Kreditkarte) nicht gespeichert werden darf und daher bei Kreditkartenzahlungen zusätzlich vom Kunden angegeben werden muss. Bei Verwendung der gehosteten Eingabeformulare von werden dem Kunden dazu die letzten vier Stellen der hinterlegten Kreditkartennummer, das Verfalldatum der Karte sowie ein Eingabefeld für die Kartenprüfnummer angezeigt.

  Bei der Verwendung mehrerer Store IDs ist es möglich, hinterlegte Datensätze einer Store ID auch für andere Store IDs zu verwenden, sodass ggf. mehrere Ihrer Vertriebskanäle auf einen gemeinsamen Datenbestand zurückgreifen können. Übergeben Sie dazu mit dem zusätzlichen Parameter ‚hosteddatastoreid' die Store ID, die bei der Speicherung der Kartendaten verwendet wurde.

- **Sperrung der Verwendung von gleichen Zahlungsinformationen für mehrere Datensätze**

  Zur Vermeidung, dass Kunden sich bei Ihnen mehrmals mit denselben Zahlungsinformationen registrieren können, besteht die Möglichkeit, bei der Speicherung den zusätzlichen Parameter ***declineHostedDataDuplicates*** zu übermitteln. Gültige Werte für diesen Parameter sind 'true' und 'false'. Wird der Wert 'true' übergeben und die übermittelten Zahlungsinformationen liegen bereits unter einer anderen 'hosteddataid' vor, wird der Vorgang abgelehnt.

Weitere Möglichkeiten der Erweiterungsfunktion Data Storage finden Sie im Integrationsleitfaden API.

10 Solvency Informationen von Bürgel Wirtschaftsinformationen GmbH & Co. KG

Das IPG hat die Schnittstelle zur Bürgel Wirtschaftschaftsinformationen GmbH und Co. KG, einem führenden Anbieter von Business Informationen, integriert.

Die Integration ermöglicht es Ihnen, die Zahlart zu selektieren, die Sie einem Einkäufer in Ihrem Online-Shop auf Grundlage des erhaltenen Zahlungsausfallrisikos anbieten möchten. Für weitere Details zu den möglichen Einstellungen schauen Sie bitte in das Handbuch zum Virtuellen Terminal.

Wenn Sie einen Vertrag mit Bürgel Wirtschaftsinformationen GmbH & Co. KG haben, und Sie „Solvency Management „ für das IPG bestellt haben, benutzen Sie bitte die folgenden Parameter für Ihre Transaktionsanfragen:

Feldname	**Beschreibung**	**Verpflichtend**
valueaddedservices	buergel	Bitte nutzen Sie diesen Paramter für alle Transaktionen, für die Sie einen Solvency Check durchführen lassen möchten.
bfirstname, blastname, bname	Customer name	Ja, bfirstname UND blastname ODER bname
baddr1	Customer address	Ja, FORMAT Strasse UND Hausnummer
bzip	Customer ZIP or Postal Code	Ja
bcity	Customer city	Ja
bcountry	Customer country	Ja, im ISO Format z.B: DE
bbirthday	Customer birthday	Kein Pflichtfeld. Format: DD.MM.YYYY

Sollte eine der Pflichtangaben fehlen, wird der Solvency Check abgelehnt.

11 Wiederkehrende Zahlungen

Connect ermöglicht Ihnen die Einrichtung regelmäßiger Abbuchungen auf Basis von Kreditkarten, Lastschrift- und PayPal –Zahlungen-. Um diese Funktion zu nutzen, müssen folgende zusätzliche Parameter bei der initialen Zahlungstransaktion übergeben werden:

Feldname	**Mögliche Werte**	**Beschreibung**
recurringInstallmentCount	Nummer zwischen 1 und 999	Anzahl der Abbuchungen, die insgesamt vorgenommen werden sollen (inklusive der Ersttransaktion)

recurringInstallmentPeriod	day week month year	Zeitraum für die Definition der Abbuchungshäufigkeit (z. B. jede zweite Woche – ‚week')
recurringInstallmentFrequency	Nummer zwischen 1 und 99	Häufigkeit der Abbuchnungen (z. B. alle ‚2' Wochen)
recurringComments	Maximal 100 Zeichen, einschließlich Leerstellen	Beliebiger Kommentar zur Abbuchung

Bitte berücksichtigen Sie, dass als Startdatum der Abbuchung systemseitig automatisch der jeweils aktuelle Tag verwendet wird.

Die über Connect eingerichteten wiederkehrenden Zahlungen können mit Hilfe des Virtual Terminal oder der API bei Bedarf nachträglich geändert oder gelöscht werden.

12 Transaktionsergebnis

Nach der Verarbeitung einer Transaktion werden die Transaktionsdaten als versteckte Felder an die von Ihnen definierte responseSuccessURL oder responseFailURL geschickt:

Feldname	**Beschreibung**
approval_code	Genehmigungscode der Transaktion Das erste Zeichen kennzeichnet das Transaktionsergebnis: ‚Y' – Transaktion erfolgreich ‚N' – Transaktion nicht erfolgreich "?" – Transaktion wurde erfolgreich initialisiert, und noch nicht finalisiert. Transaktion wird zum späteren Zeitpunkt aktualisiert.
oid	Bestellnummer (Order ID)
refnumber	Referenznummer
status	Transaktionsstatus
txndate_processed	Zeitpunkt der Transaktionsverarbeitung
tdate	Transaktionskennung mit der die Transaktion ggf. später storniert werden kann
fail_reason	Grund für ein etwaiges Scheitern der Transaktion

response_hash	Hash-Wert zur Absicherung der Kommunikation (siehe Hinweise unten)
processor_response_code	Der Antwortcode der Transaktionsverarbeitung Bitte beachten Sie, dass diese Antwortcodes je nach Zahlungsart und entsprechendem Hintergrundsystem unterschiedlich sein können. Während bei Kreditkartenzahlungen z. B. der Antwortcode ‚00' auf eine erfolgreiche Genehmigung hinweist, ist der vom Betreibersystem übermittelte Antwortcode für erfolgreiche giropay-Transaktionen ‚4000'.
fail_rc	Internes Verarbeitungsmerkmal bei fehlgeschlagenen Transaktionen
terminal_id	Die Terminal ID, die für die Transaktion verwendet wurde
ccbin	6-stellige Kennung der kartenherausgebenden Bank
cccountry	3-stelliger ISO Code für das Land des Karteninhabers (z.B. USA, DEU, ITA, etc.) "N/A", sofern das Land nicht ermittelt werden kann oder keine Kreditkarte genutzt wird.
ccbrand	Brand of the credit or debit card: MC VISA AMEX DINERS/DISCOVER JCB UNIONPAY MAESTRO LASER "N/A" wenn keine Kreditkarte

Bei 3D Secure Transaktionen zusätzlich:

response_code_3dsecure	Der Antwortcode der 3D Secure Authentifizierung: **1** – Erfolgreiche Authentifizierung (GICC ECI 11/10) **2** – Erfolgreiche Authentifizierung ohne AVV (GICC ECI 11/10) **3** – Authentifizierung nicht erfolgreich / falsches Passwort (Transaktion abgelehnt) **4** – Authentifizierungsversuch (GICC ECI 13/12) **5** – Authentifizierung nicht möglich / Directory Server

	antwortet nicht (GICC ECI 7) **6** – Authentifizierung nicht möglich / Access Control Server antwortet nicht (GICC ECI 7) **7** – Karte nicht für 3D Secure freigeschaltet (GICC ECI 13/12) **8** – Ungültige 3D Secure Werte erhalten (in den meisten Fällen vom Access Control Server der kartenherausgebenden Bank) Bitte beachten Sie die Hinweise zur Sperrung von GICC ECI 7 Transaktionen im Kapitel 3D Secure.

Bei eigener Fehlerseite für die Plausibiltätsprüfung (full_bypass = true) zusätzlich:

fail_reason_details	Komma-separierte Liste fehlender bzw. unplausibler Angaben
invalid_cardholder_data	**true** – bei negativem Ergebnis der Plausibiltätsprüfung **false** – wenn das Ergebnis der Plausibiltätsprüfung positiv war, die Transaktion aber aus anderen Gründen gescheitert ist

Zusätzlich werden an die spezifische URL Ihre selbst definierten Felder und die Felder mit Liefer- und Rechungsdaten gesendet.

Der Parameter *response_hash* ermöglicht Ihnen zu überprüfen, ob das empfangene Transaktionsergebnis auch tatsächlich vom Internet Payment Gateway stammt und kann Sie somit vor betrügerischen Manipulationen schützen.

Erzeugen Sie dazu einen SHA 1 Hash aus dem Parameter-String

```
sharedsecret + approval_code + chargetotal + currency + txndatetime + storename
```

Bei der Hash-Berechnung ist der Parameter chargetotal in Formtierung Sprachabhängig. Bitte verwenden Sie für die HASH-Berechnung, die Formatierung, wie sie in der Antwort zurück kommt.

Zusätzlich besteht die Möglichkeit, dass die oben genannten Ergebnisparameter an eine von Ihnen bestimmte URL gesendet werden.. Um diese Funktion zu nutzen, übergeben Sie bei der Transaktion Ihre entsprechende URL im zusätzlichen Parameter

transactionNotificationURL

Bitte beachten Sie, dabei folgende Punkte:

- Es findet hierbei kein „SSL-Handshake“ oder eine Verifizierung von SSL Zertifikaten statt
- Ihre angebene URL muss für Port 80 (http) oder Port 443 (https) freigeschaltet sein. Andere Ports werden nicht unterstützt.
- Der dazugehörige Hash-Wert (SHA1 Algorithmus) zur Absicherung der Kommunikation ‘notification_hash’ wird aus folgendem Parameter-String erzeugt:

- `chargetotal + sharedsecret + currency + txndatetime + storename + approval_code`

13 Anhang I – Anleitung zur Generierung eines SHA Hashes

1. Hängen Sie folgende Informationen aneinander: storename, txndatetime, chargetotal, Währung und sharedsecret
2. Wandeln Sie jeden Buchstaben in seine ascii hexadezimal Zahl um.
3. Übergeben Sie das Egrebnis an den SHA1 Algorithmus
4. Übergeben Sie das Ergebnis an das Internet Payment Gateway

Beispiel:

- storename = 98765432101
- txndatetime = 2013:07:16-09:57:08
- chargetotal = 1.00
- currency = 826
- sharedsecret = TopSecret

Schritt1: Ergebnis : 9876543210 12013:07:16-09:57:08 1.00 826 TopSecret

Schritt2: Ergebnis:
393837363534333231303132303133 3a30373a31362d30393a35373a3038312e3030383236546f70536563726574#

Schritt3: Ergebnis_

SHA1(393837363534333231303132303133 3a30373a31362d30393a35373a3038312e3030383236546f70536563726574)

Schritt 4 Ergebnis:

83ba1beaf113a45a2557fcaffcf87ec35e6b9aae

<input type="hidden" name="hash" value="83ba1beaf113a45a2557fcaffcf87ec35e6b9aae"/>

14 Appendix II – ipg-util.asp

```
<Script LANGUAGE=JScript RUNAT=Server src="sha1.js">
</SCRIPT>
```

```
<Script LANGUAGE=JScript RUNAT=Server>
	var today = new Date();
	var formattedDate = today.formatDate("Y:m:d-H:i:s");

	/*
		Function that calculates the hash of the following parameters:
		 - storename
		 - Date/Time(see $dateTime above)
		 - chargetotal
		 - shared secret
		 - currency (numeric ISO value)
	*/
	function createHash(chargetotal, currency) {
		// Please change the storename to your individual storename
		var storename = "12066666666;
		// NOTE: Please DO NOT hardcode the secret in that script. For
example read it from a database.
		var sharedSecret = "ganzGeheim";

		var stringToHash = storename + formattedDate + chargetotal +
currency + sharedSecret;

		var ascii = getHexFromChars(stringToHash);

		var hash = calcSHA1(ascii);

		Response.Write(hash);
	}
	function getHexFromChars(value) {
		var char_str = value;
		var hex_str = "";
		var i, n;
		for(i=0; i < char_str.length; i++) {
			n = charToByte(char_str.charAt(i));
			if(n != 0) {
				hex_str += byteToHex(n);
			}
		}
		return hex_str.toLowerCase();
	}
```

```
	function getDateTime() {
		Response.Write(formattedDate);
	}
</SCRIPT>
```

15 Anhang III - ipg-util.php

```
<?php
	$dateTime = date("Y:m:d-H:i:s");

	function getDateTime() {
		global $dateTime;
		return $dateTime;
	}

	function createHash($chargetotal, $currency) {
		$storename = "12066666666";
$sharedSecret = "ganzGeheim";

		$stringToHash = $storename . getDateTime() . $chargetotal .
$currency . $sharedSecret;

		$ascii = bin2hex($stringToHash);

		return sha1($ascii);
	}

?>
```

16 Appendix IV – PayPal transaction type mapping and address handling

Transaction types

Connect Transaction Type (txntype)	PayPal operation
sale	SetExpressCheckoutPayment (sets *PaymentAction* to *Authorization* in *SetExpressCheckout* and *DoExpressCheckoutPayment* requests)
preauth	GetExpressCheckoutDetails
sale – with additional parameters for installing a Recurring Payment	DoExpressCheckoutPayment*
postauth	DoCapture (,DoReauthorization)
void	DoVoid

Adressverarbeitung

Wenn Sie einen kompletten Satz von Addressdaten innerhalb einer Connect Anfrage durchführen werden diese Anfragewerte an PayPal weitergeleitet,

Wenn Sie fehlerhafte Adressdaten für die Connect Anfrage nutzen, werden keine Adressdaten an Paypal weiter geleitet.

Bitte beachten Sie, dass die Weiterleitung der Versandadresse an PayPal eine notwendige Voraussetzung für PayPals Händlerschutz ist.