Pay4one Gateway Dokumentation

V.1.4 06.11.2020

payment solution by amys IT

Inhaltsverzeichnis

Einführung:

Die AMYS IT-Solutions GmbH bietet Ihnen mit der pay4one Connect Schnittstelle die Möglichkeit zur einfachen Einbindung unterschiedlicher Bezahlarten in Ihr Projekt.

Die pay4one Connect Schnittstelle übernimmt für Sie die komplette Interaktion mit Kreditkartenprozessoren, Kreditistituten und weiteren Payment Service Providern.

Die vorliegende Dokumentation erklärt Schritt für Schritt wie Sie Ihr Projekt, z.B. Ihren Onlineshop mit der pay4one Connect Schnittstelle verbinden und somit schnellstmöglich beginnen können Zahlungen zu akzeptieren.

Optionen für den Bezahlvorgang

Für den einfachen, sicheren Transfer der sensiblen Bezahldaten bietet die Schnittstelle, eine Formular an, auf welches Ihr Projekt beim Abschluss der Bestellung weiterleitet. Sie können bei der Integration bestimmen ob dem Kunden direkt das zur gewählten Bezahlart bestimmte Formular angezeigt wird, oder Sie überlassen der Schnittstelle die Anzeige aller möglichen Zahlungsarten und der Kunde wählt dort die für Ihn passende Zahlart aus.

PayOnlyModus

Hier werden nur die für die Zahlung notwendigen Daten von Ihrem Shop übertragen, die Zahlungsdaten werden auf der PaymentPage eingesammelt und die Transaktion durchgeführt.

PayPlus Modus

Hier besteht die Möglichkeit zusätzliche Kundendaten an die Schnittstelle zu liefern (z.B. Name,Lieferadresse usw.) diese Daten stehen Ihnen dann im pay4one Backend zur Verfügung.

FullPay Modus

Als Erweiterung können hier sämtliche im Shop verfügbaren Daten übertragen werden, diese stehen Ihnen dann im pay4one Backend zur Verfügung.

Bitte beachten Sie das bei den Modi PayPlus und FullPay evtl. zusätzliche Vereinbarungen zwischen Ihnen, Ihren Kunden und AMYS IT-Solutions notwendig sind um die Verarbeitung DSGVO konform abzuwicklen.

Erste Schritte

In diesem Abschnitt stellt ein einfaches Beispiel die Integration der Schnittstelle vor.
Dieser Abschnitt setzt Grundkenntnisse der Skriptsprache PHP vorraus.

Vorbereitung

Bitte stellen Sie sicher das Ihnen die folgenden Zugangsdaten vorliegen:

Stornename : diesen erhalten Sie von AMYS-IT

SharedSecret: dieses erhalten Sie ebenfalls von AMYS-IT

Sollten Ihnen noch keine Zugangsdaten vorliegen kontaktieren Sie unseren Support unter support@amys-it.com für die Zusendung von Testzugangsdaten oder unser Sales Teram sales@amys-it.com für ein Angebot für einen Akzeptanzvertrag.

Hash Berechnung

Zur Absicherung und Authentifizierung der Transaktion muss ein Hash-Wert berechnet werden.

Der Hash-Wert setzt sich aus unterschiedlichen Parametern zusammen. Diese Parameter werden zuerst als String verkettet, dann in Hexadezimalwerte umgewandelt und anschließend mit SHA256 gehasht.

Ein Beispiel finden Sie im Anhang.

Hinweise zur Impementierung der Schnittstelle

Die Daten werden per HTTP POST REQUEST an das Gateway übertragen, bitte beachten Sie das hierzu keine Technologien wie z.B. AJAX verwendet werden dürfen. Somit ist gewährleistet, dass die Schnittstelle, speziell bei 3D-Secure Transaktionen oder Giropay fehlerfrei arbeitet. DasErgebnis der Transaktion sollte immer aus den zurückgelieferten POST-Parametern ausgewertet werden.

PHP Beispiel

```php
<?php include("utility.php");?>
<html>
  <head><title>pay4one Gateway Connect Integration Sample</title></head>
    <body>
      <h1>pay4one Gateway Connect Integration Sample</h1>
      <form method="post" action="https://test.p4gw.com/payment">
        <input type="text" name="txntype" value="sale">
        <input type="text" name="timezone" value="Europe/Berlin"/>
        <input type="text" name="txndatetime" value="<?php echo $txndatetime ?>"/>
        <input type="text" name="hash_algorithm" value="SHA256"/>
        <input type="text" name="hash" value="<?php echo createHash("STORENAME", $txndatetime,
"8.00", "EUR", $sharedSecret); ?>"/>
        <input type="text" name="storename" value="STORENAME"/>
        <input type="text" name="mode" value="payonly"/>
        <input type="text" name="chargetotal" value="8.00"/>
        <input type="text" name="currency" value="EUR"/>
        <input type="text" name="oid" value="Test001"/>
        <input type="text" name="paymentMethod" value="V"/>
        <input type="text" name="responseSuccessURL" value="https://yourserver.com/success"/>
        <input type="text" name="responseFailURL" value="https://yourserver.com/failure"/>
        <input type="text" name="authenticateTransaction" value="true"/>
        <input type="text" name="language" value="de_DE"/>
        <input type="submit" value="Submit">
      </form>
    </body>
</html>
```

Das Beispiel stellt nur die notwendigen Informationen zur Integration dar, bitte beachten Sie bei Ihrer Entwicklung die aktuellen Sicherheitsstandards.

Bitte beachten Sie das die POST_URL nur für den Test der Integration genutzt werden kann.
Wenn Sie bereit für den Produktivbetrieb sind kontaktieren Sie den Support support@amys-it.com um die Live Zugangsdaten zu erhalten

Im Anhang finden Sie den Beispielcode für die refferenzierte util.php bitte beachten Sie auch hier das die Integration nach den aktuellen Sicherheitsstandards erfolgen muss.

Beträge für Testtransaktionen

Auf dem Testsystem werden bei Kreditkartentransaktionen die Nachkommastellen als Fehlercode interpretiert. Dadurch ist es möglich zu steuern ob eine Transaktion erfolgreich oder abgelehnt als Ergebnis haben soll.

Glatte Beträge (zb. 2,00 oder 7,00) führen zu einer erfolgreichen Transaktion. Mit abweichenden Nachkommastellen kann ein Fehler simuliert werden (z.B. 2,05 gibt den Fehler 05 zurück)

Verwenden Sie daher bitte zum testen glatte Beträge (z.B. 2,00) wie im Beispiel.

Pflichtfelder

Je nach Transaktionstyp müssen die folgenden Felder in Ihrer Übergabe enthalten sein.

Feldname	Beschreibung	„Sale“ Transaktion	Vorautorisierung	Buchung einer Vorautorisierung	Storno
txntype	'sale', 'preauth', 'postauth' oder 'void' (Der Transaktionstyp) Die Möglichkeit ‚void‘ zu senden ist eingeschränkt. Bitte wenden Sie sich an das Support-Team, wenn Sie diese Option nutzen wollen.	x	x	x	x
timezone	(Die Zeitzone der Transaktion) z.B. Africa/Johannesburg America/New_York America/Sao_Paulo Asia/Calcutta Australia/Sydney Europe/Berlin Europe/London	x	x	x	x
txndatetime	YYYY:MM:DD-hh:mm:ss (Der exakte Zeitpunkt der Transaktion)	x	x	x	x
hash_algorithm	aktuell SHA256	x	x	x	x
hash	Der verkettete kodierte SHA256 Hash	x	x	x	x
storename	Der Storenamen den Sie von AMYS IT-Solutionserhalten haben	x	x	x	x
mode	"fullpay', ‘payonly’ oder ‘payplus’	x	x		
chargetotal	Der Gesamtbetrag der Transaktion. Als Dezimal-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.	x	x	x	x
currency	Die Währung der Transaktion als dreistelliger numerischer ISO 4217 Wert	x	x	x	
oid	Bestellnummer (Order ID) des Vorgangs zu dem eine Buchung	x	x	x	x

	der Vorautorisierung oder ein Storno erfolgen soll.				
tdate	Genaue Kennzeichnung der Transaktion eines Vorgangs, die storniert werden soll. Diesen Wert erhalten Sie als Antwortparameter 'tdate' zur entsprechende Transaktion				x

Hinweis : Die Transaktionsarten „preauth“ und „postauth“ funktionieren ausschließlich mit den Bezahlarten „Kreditkarten“, „PayPal“ und „Klarna“.

Währung Währungskennzeichen

Beispiele ISO 4217 Währungscodes

Währung	Kennzeichen	ISO 2417
Australian Dollar	AUD	036
Brazilian Real	BRL	986
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 Krone	CZK	203
Dänische Krone	DKK	208
Hong Kong Dollar	HKK	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	ZAR	410
Indischer Rupee	INR	356
Israelischer Neuer Schekel	ISL	376
Japanischer Yen	JPY	392
Kuwaiti Dinar	KWS	414

Litauischer Lltas	LTL	440
Mexikanischer Peso	MXN	484
Neuseländischer Dollar	NZD	554
Schwedische Krone	SEK	752
Türkischer Lira	TRY	949
UAE Dirham	AED	784
Kanadische Dollar	CAD	124
Kroatische Kuna	HRK	191

Payment Method

Zahlart	Kürzel
MasterCard	M
Visa	V
American Express	A
Diners	C
JCB	J
CUP	CUP
DirectDebit Germany	debitDE
giropay	giropay
Maestro	MA
MaestroUK/Solo	maestroUK
PayPal	paypal
SOFORT	sofort
DirektÜberweisung	direkt
ideal	ideal

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

oid

(max. 78 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. Von der oid können maximal 78 Zeichen im Verwendungszweck für SEPA Lastschriften an die Bank übertragen werden. Die ersten 30 Zeichen der Bestellnummer werden bei Kreditkartenzahlungen mit an Ihren Acquirer übertragen und können eventuell mit auf der Händlerabrechnung ausgewiesen werden. Bei allen SEPA Zahlungsverfahren (Direct Debit, Giropay, Direkt Überweisung, Sofortüberweisung) dürfen nur Zeichen verwendet werden, die im SEPA-Verfahren erlaubt sind.

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 Lastschrifttransaktionen an die Bank des Kunden weitergeleitet werden, sodass sie auf dem Kontoauszug Ihres Kunden ausgewiesen werden kann. Die customerid wird im Verwendungszweck der oid angehängt und an die Bank übertragen. 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.

MandateType

Dieses Feld erlaubt Ihnen Einzel- und Folgelastschriften auszulösen: ´single´ für Einzellastschriften und ´recurringCollection´ für wiederkehrende bzw. Folgelastschriften. Wurden für eine IBAN einmal Mandatsdaten für eine wiederkehrende Zahlung übermittelt, werden alle weiteren Transaktionen mit dieser IBAN zurzeit ebenfalls als wiederkehrende Transaktion geflaggt. Einmalige (‚Single‘) Mandate sind für diese IBAN nicht mehr möglich. Bei SEPA Direct Debit Zahlungen als ‚recurringCollection‘ ist die Angabe der ‚mandateReference‘ verpflichtend.

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 auch Transaktionsergebnis). Unterstützt werden die Ports 80 und 443.

TrxOrigin

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

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:

de_DE
en_US

Verwendung eigener Eingabeformulare

Entscheiden Sie sich eigene Eingabeformulare bereitzustellen, d. h. nicht auf die von AMYS IT 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. AMYS IT empfiehlt die Verwendung des Modes „payonly“ 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.

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.

Feldname	Beschreibung	Kreditkarte	SEPA Lastschrift	Maestro	giropay	PayPal, SOFORT, Direktüberweisung	MaestroUK / Solo
cardnumber	Kartennummer	x		x			x
expmonth	Ablaufdatum Monat (MM)	x		x			x
expyear	Ablaufdatum Jahr (YYYY)	x		x			x
cvm	Kartenprüfnummer	x		x			x
iban	IBAN des Kunden (22 St.)		x				
bic	BIC (8 oder 11 Stellen)		x		x		

Plausibilitätsprüfungen

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 von TeleCash angezeigt. Um bei Verwendung eigener Zahlformulare diese Fehlerseite von TeleCash 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.

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.

3D Secure

TeleCash bietet Ihnen mit der Connect Schnittstelle die technische Voraussetzung um Zahlungen über die Sicherheitssysteme Verified by Visa, MasterCard SecureCode und American Express Safekey 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 (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.

Anhang – Anleitung zur Generierung eines SHA-256 Hashes

Hängen Sie folgende Informationen aneinander: storename, txndatetime, chargetotal, Währung und sharedsecret Wandeln Sie jeden Buchstaben in seine ascii hexadezimal Zahl um. Übergeben Sie das Egrebnis an den SHA-256 Algorithmus Übergeben Sie das Ergebnis an das Internet Payment Gateway

Beispiel:

```
storename    :  123456
txndatetime  :  2020:04:21-06:48:21
chargetotal  :  14.00
currency     :  978
sharedSecret :  secret

Wird verkettet zu:
1234562020:04:21-06:48:2114.00978secret

in Hexadezimal   :
313233343536323032303a30343a32312d30363a34383a323131342e3030393738736563726574

und gehasht      :
bd98c5bd69adb5b0f1ed501ae4b27730e2408cd556298458dcca9d5685b37ecf
```

Anhang – utility.php

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

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

function createHash($chargetotal, $currency) {
  $storename = "STORENAME";
  $sharedSecret = "SHAREDSECRET";
        // $sharedSecret = "HT6VHh7EVTf91jsfQPOE";
  $stringToHash = $storename . getDateTime() . $chargetotal .
  $currency . $sharedSecret;
  $ascii = bin2hex($stringToHash);
  return hash('sha256', $ascii);
}
?>
```

Informationen

Dieses Handbuch wurde mit größter Sorgfalt erstellt und wird regelmäßig aktualisiert.
Wenn Ihnen ein Fehler in der Dokumentation auffallen sollte senden Sie uns bitte eine Mail an support@amys-it.com wir werden dies dann umgehend prüfen.

Bitte beachten Sie das die im Handbuch vorhandenen Quelltexte nur funktionale Beispiele darstellen. Entwickeln Sie Ihre Integration in Ihren Systemen immer gemäß der aktuellen Sicherheitsrichtlinien.
Speichern Sie z.B. keine Passwörter im Klartext.

Die beschriebene Schnittstelle verarbeitet die sensiblen Bezahldaten in einem geschützten Bereich auf unseren Servern, Sie benötigen also keine Aufwändige Vollzertifizierung gemäß des PCI-DSS (PaymentSecurityStandard). Je nach Anforderungen des Kreditkartenacquirers kann jedoch eine Selbstauskunft tgemäß der PCI-DSS Richtlinien notwendig sein, da Sie, bei korrekter Integration, keine sensiblen Zahlungsdaten verarbeiten ist dieser vereinfachte Fragebogen leicht zu beantworten.

Für Fragen zur Integration in Ihrer Anwendung stehen wir Ihnen gerne zur Verfügung.