

Schnittstellenspezifikation Zahlungsmaske yellowpay

anwenden

Koordinaten der Finanzinstitute

Für Interessenten E-Payment/yellowpay

Beratung und Verkauf Geschäftskunden
Telefon +41 (0)848 848 848 (Normaltarif)

Für bestehende E-Payment-/yellowpay-Merchants

Die Schweizerische Post
PostFinance
Kundendienst yellowpay
3002 Bern
Telefon +41 (0)31 338 24 23
E-Mail merchanthelp@postfinance.ch

Inhaltsverzeichnis

1. Zahlungsmaskenaufruf	4
1.1 Aufruf der Zahlungsmaske mit https POST	4
1.2 Zeichensatz	4
1.3 Standardparameter für alle Zahlungsarten	5
1.4 Shopperangaben für alle Zahlungsarten	7
1.5 Parameter für die Zahlungsart PostFinance-E-Rechnung	8
1.6 Dynamische Zahlungsartenauswahl	9
1.7 Parametervalidierung	10
1.8 Refresh der Merchant-Webseite nach Aufruf der Zahlungsmaske	10
2. Zahlungsmaskenrücksprung	11
2.1 Rücksprung-URL «Abbrechen»	11
2.2 Rücksprung-URL «Erfolgreich»	11
2.3 Rücksprung-URL «Fehlgeschlagen»	11
2.4 txtShopPara	11
2.5 Bekannte Probleme	12
3. Autorisierungsquittung	13
3.1 Autorisierungsquittung per http oder https	13
3.2 Autorisierungsquittung per E-Mail	14
4. Meldungen Zahlungsmaske yellowpay	16
4.1 Validierung der Parameter beim Zahlungsmaskenaufruf	16
4.2 Validierung der Eingaben des Shoppers	17
4.3 Autorisierungsmeldungen	17
5. Unterstützte Browser und Betriebssysteme	18

1. Zahlungsmaskenaufruf

1.1 Aufruf der Zahlungsmaske mit https POST

Die Zahlungsmaske yellowpay wird immer über ein separates Browserfenster angezeigt. Um dieses zu öffnen, sendet die Shopseite per https POST Parameter an eine PostFinance-URL. Die Antwortseite von PostFinance ist für das Öffnen der Zahlungsmaske als Fenster oder Popup verantwortlich. https POST wird benutzt, da im Gegensatz zu https GET keine Längenbeschränkung besteht und zudem die Gefahr von fehlerhaften Aufrufen durch unerlaubte Zeichen reduziert wird. Erfolgt der Aufruf mit GET, kann PostFinance das korrekte Funktionieren des Zahlungsmaskenaufrufs nicht garantieren.

Beim Verwenden der Zahlungsmaske werden einerseits die beim Aufruf übergebenen Parameter berücksichtigt, andererseits die im Shopprofil hinterlegten Felder wie Shopname, Rücksprung-URLs usw. In den folgenden Kapiteln wird beschrieben, welche obligatorischen Parameter vom Shop an die Zahlungsmaske yellowpay per https POST übergeben werden müssen und welche optionalen Parameter der Shop zusätzlich übergeben kann.

1.2 Zeichensatz

Damit Sonderzeichen korrekt übergeben werden, muss das verwendete HTML-Formular mit dem **Zeichensatz ISO-8859-1** kodiert sein. Die HTML-Seite sollte deshalb den folgenden Tag enthalten:

```
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
```

Parameter, für die in den folgenden Kapiteln keine restriktivere Validierung angegeben ist, werden beim Aufruf der Zahlungsmaske auf nichtkonforme Zeichen geprüft. Zeichen, die nicht diesem Zeichensatz entsprechen, werden von yellowpay zurückgewiesen, und dem Shopper wird eine entsprechende Fehlermeldung angezeigt (siehe Kapitel 4).

Wenn der Sourcecode das Charset=ISO-8859-1 oder Windows-1252, enthält, wird die Seite automatisch im korrekten Format gespeichert. Wenn der Sourcecode kein Charset enthält, muss die Seite zwingend im ANSI-Format gespeichert werden.

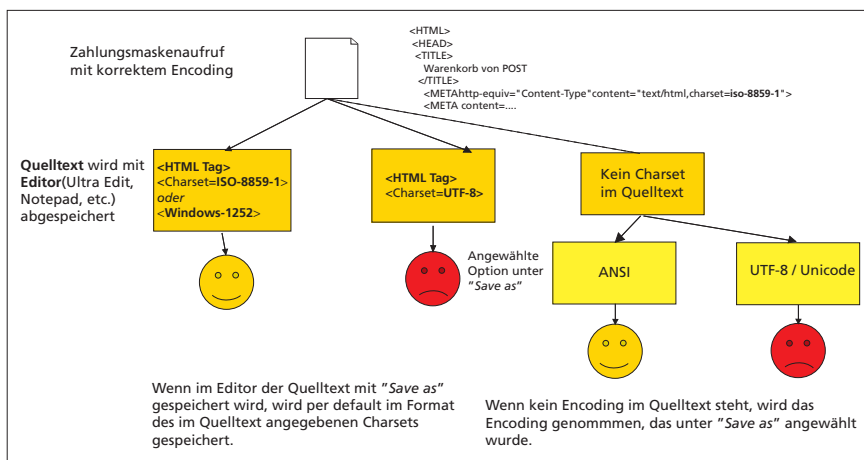


Abbildung 1: Kodierung des Zeichensatzes

1.3 Standardparameter für alle Zahlungsarten

Bezeichnung	Feldlänge, Validierung	fak./obl. ¹	Bemerkungen	Beispiel
MasterShopID (txtShopId)	1-30 Zeichen case-insensitive	obl.	Gemäss Anmeldebestätigung	shop1000_yp
Shop-Parameter (txtShopPara)	0-255 Zeichen URL encodiert	fak.	Dieser Parameter wird bei allen Rücksprüngen der Rücksprung-URL angehängt (siehe Kapitel 2.4). Bei der Parameterrückgabe mittels http(s) werden die Key/Value Pairs einzeln zurückgegeben (siehe Kapitel 3.1).	SessionID=12&type=business
Sprache Zahlungsmaske (txtLangVersion)	Zeichennumerischer Sprachcode: 2055, 4108, 2064, 2057	obl.	Deutsch = 2055 Französisch = 4108 Italienisch = 2064 Englisch = 2057	2055
Preistotal des Warenkorbs (txtOrderTotal)	Stellen vor dem Punkt: 0-9 Zahlen Trennzeichen: . Stellen nach dem Punkt: 1-2 Zahlen Keine vorangehenden Leerschläge	obl.	Der Wert wird gemäss folgender Regular Expression validiert: [0-9]{0,9}\.[0-9]{1,2}	100.20
Währung (txtArtCurrency)	3 Zeichen ISO-4217-Währungscode (CHF, EUR, USD)	obl.	Für die Zahlungsarten MasterCard und Visa können auch Zahlungen in USD und EUR ausgeführt werden, sofern entsprechende Verträge vom Kreditkarteninstitut ausgestellt wurden und PostFinance diese Währungen freigeschaltet hat.	CHF
Hash-Wert (txtHash)	32 Zeichen; Zeichen 0-9 und a-f (case-sensitive)	fak. ²	Details siehe unten im Anschluss an diese Tabelle.	96c9a5b399e95a898684d1 baaf9ab3d6
OrderIDShop (txtOrderIDShop)	1-18 Zeichen	fak.	Zur freien Verfügung des Online-Shops. Bei gewissen Kreditkarteninstituten wird dieser Feldinhalt bei der Vergütungsanzeige als Referenznummer (Retrieval-Nummer) verwendet. Die OrderID sollte eindeutig pro Zahlung/Bestellung sein.	order_2738

¹ fak. = fakultativ, obl. = obligatorisch

² Wird voraussichtlich im Jahr 2009 obligatorisch

Bezeichnung	Feldlänge, Validierung	fak./obl. ¹	Bemerkungen	Beispiel						
Zahlungsverarbeitung (deliveryPaymentType)	immediate oder deferred, case-sensitive	fak.	Bei leerem Feldinhalt wird der Defaultwert deferred eingesetzt (Ausnahme siehe Kapitel 1.5).	immediate						
Popup/Fenster Aufruf (txtUsePopup, txtUseWindow)	true oder false, case-sensitive	fak.	Um die Zahlungsmaske als Fenster zu öffnen, muss txtUsePopup=false und txtUseWindow=true übergeben werden. Ohne Angabe wird die Zahlungsmaske als Popup angezeigt.	true						
Aufrufziel (txtDestination)	pfpopup, pfwindow, case-sensitive	fak.	Parameter zur Steuerung der Zahlungsmaskenanzeige (Popup, Fenster). Dieser ersetzt die beiden Parameter txtUsePopup und txtUseWindow. txtDestination ist nur aktiv, wenn weder txtUsePopup noch txtUseWindow übergeben wurden.	pfpopup						
			<table border="1"> <thead> <tr> <th>Wert</th> <th>Beschreibung</th> </tr> </thead> <tbody> <tr> <td>pfpopup (Standard)</td> <td>Zahlungsmaske wird als Popup geöffnet (analog txtUsePopup=true)</td> </tr> <tr> <td>pfwindow</td> <td>Zahlungsmaske wird als Popup geöffnet, bei welchem man die Grösse ändern kann (analog txtUseWindow=true)</td> </tr> </tbody> </table>	Wert	Beschreibung	pfpopup (Standard)	Zahlungsmaske wird als Popup geöffnet (analog txtUsePopup=true)	pfwindow	Zahlungsmaske wird als Popup geöffnet, bei welchem man die Grösse ändern kann (analog txtUseWindow=true)	
Wert	Beschreibung									
pfpopup (Standard)	Zahlungsmaske wird als Popup geöffnet (analog txtUsePopup=true)									
pfwindow	Zahlungsmaske wird als Popup geöffnet, bei welchem man die Grösse ändern kann (analog txtUseWindow=true)									
Aufruf mit history.back() (txtHistoryBack)	true oder false, case-sensitive	fak.	Wird dieser Parameter auf false gesetzt, dann erfolgt beim Zahlungsmaskenaufruf kein history.back(). Defaultwert ist: true	false						

Um zu verhindern, dass Dritte den Aufruf der Zahlungsmaske manipulieren können, verwendet PostFinance einen Sicherheitsparameter, der als «elektronische Unterschrift des Zahlungsmaskeninhalts» bezeichnet werden kann. Die Berechnung des Hash-Werts (case-sensitive) ist nur durch Merchants mit Payment Service Provider PostFinance vorzunehmen.

PostFinance überprüft die Gültigkeit dieses Hash-Parameters auf Eindeutigkeit und erkennt potenzielle Manipulationen der Zahlungsparameter oder des Hash-Parameters durch Unbefugte.

Ferner kann der Shop dank dem Parameter txtHashBack verifizieren, ob die Autorisierungsquittung (siehe Kapitel 3) von PostFinance stammt. Besitzt der Shop einen aktivierten Hash-Check, wird automatisch mit der Autorisierungsquittung auch der Parameter txtHashBack mit einem neuen Algorithmus als Inhalt retourniert.

Details betreffend Generierung der Parameter txtHash und txtHashBack werden dem Merchant im geschützten Bereich des Merchant-GUI yellowpay, im Menü Services\Download\Dokumente kommuniziert.

Merchants mit externem Payment Service Provider wenden sich diesbezüglich an ihren Payment Service Provider.

¹ fak. = fakultativ, obl. = obligatorisch

1.4 Shopperangaben für alle Zahlungsarten

Diese Parameter sind fakultativ (mit Ausnahme der in Kapitel 1.5 erwähnten Parameter). Sie werden dem Shopper nicht angezeigt, dem Merchant aber in der Autorisierungsquittung retourniert und im Merchant-GUI yellowpay abgebildet bzw. über die EPASS für Merchant-Schnittstelle retourniert.

Bezeichnung	Feldlänge, Validierung	fak./obl. ³	Bemerkungen	Beispiel
Shopper Anrede (txtBTitle)	0-30 Zeichen	fak.		Frau
Shopper Name (txtBLastName)	0-40 Zeichen	fak.	Obligatorisch für Zahlungsart PostFinance-E-Rechnung!	Bernasconi
Shopper Vorname (txtBFirstName)	0-40 Zeichen	fak.		Maria
Shopper Adresse 1 (txtBAddr1)	0-40 Zeichen	fak.	Obligatorisch für Zahlungsart PostFinance-E-Rechnung!	Bahnhofstrasse 1
Shopper PLZ (txtBZipCode)	0-10 Zeichen	fak.	Obligatorisch für Zahlungsart PostFinance-E-Rechnung!	3000
Shopper Ort (txtBCity)	0-40 Zeichen	fak.	Obligatorisch für Zahlungsart PostFinance-E-Rechnung!	Bern
Shopper Land (txtBCountry)	2 Zeichen ISO-3166-Ländercode Grossbuchstaben	fak.	Wird dieser Parameter übergeben, dann wird geprüft, ob es sich dabei um einen gültigen ISO-3166-Ländercode handelt.	CH
Shopper Telefon (txtBTel)	0-40 Zeichen	fak.		031 / 111 11 11
Shopper Fax (txtBFax)	0-40 Zeichen	fak.		031 / 111 11 12
Shopper Mail (txtBEmail)	0-40 Zeichen	fak.		Abc123@mail.ch

³ fak. = fakultativ, obl. = obligatorisch

1.5 Parameter für die Zahlungsart PostFinance-E-Rechnung

Sofern die Zahlungsart PostFinance-E-Rechnung vom Merchant angeboten wird, kommen unten stehende Zusatzparameter zum Einsatz. Zahlungen mit PostFinance-E-Rechnung sind im Merchant-GUI yellowpay nicht nachbearbeitbar und werden deshalb immer mit dem `deliveryPaymentType` «immediate» autorisiert, unabhängig davon ob das Feld `deliveryPaymentType` mit Wert «deferred» übergeben wurde.

Bezeichnung	Feldlänge, Validierung	fak./obl. ⁴	Bemerkungen	Beispiel
ESR-Teilnehmernummer (txtESR_Member)	6- bis 11-stellig inkl. Trennstriche	obl.		01-999999-1
Referenznummer (txtESR_Ref)	16 oder 27 Ziffern mit Modulo 10 Rekursiv Prüfziffer (letzte Ziffer)	fak.	Sofern beim Zahlungsmaskenaufruf keine Referenznummer mitgegeben wird, vergibt PostFinance für die Rechnungserstellung eine selbst generierte Referenznummer.	1234567890123456
Shopper Name (txtBLastName)	1-40 Zeichen	obl.		Bernasconi
Shopper Adresse 1 (txtBAddr1)	1-40 Zeichen	obl.		Bahnhofstrasse 1
Shopper PLZ (txtBZipCode)	1-10 Zeichen	obl.		3000
Shopper Ort (txtBCity)	1-40 Zeichen	obl.		Bern

Die Parameter `txtBLastName`, `txtBAddr1`, `txtBZipCode`, `txtBCity` sind nur bei der Zahlungsart PostFinance-E-Rechnung obligatorisch (sonst fakultativ). Jeder Merchant, der diese Zahlungsart aktiviert hat, muss diese Parameter übergeben, auch wenn der Shopper in der Zahlungsartenauswahl eine andere Zahlungsart auswählt (wird während des Öffnens der Zahlungsmaske geprüft). Ausnahme: Wird die Zahlungsart dynamisch gewählt (siehe Kapitel 1.6) und handelt es sich dabei um eine andere Zahlungsart als PostFinance-E-Rechnung, dann müssen diese Parameter nicht übergeben werden.

⁴fak. = fakultativ, obl. = obligatorisch

1.6 Dynamische Zahlungsauswahl

Der Merchant hat die Möglichkeit, direkt eine bestimmte Zahlungsart aufzurufen, ohne vorher die Zahlungsauswahl durch yellowpay einblenden zu lassen. Hierzu übergibt der Merchant den Wert «true» im Feld «txtUseDynPM» sowie die entsprechende Zahlungsart mit dem Wert «true». Da die Parameter txtPM_<Zahlungsart>_Status den Defaultwert «false» haben, müssen nur die Zahlungsarten übergeben werden, die in der Zahlungsmaske einblendet werden sollen.

Bezeichnung	Feldlänge, Validierung	fak./obl. ⁵	Bemerkungen	Beispiel
txtUseDynPM	true oder false, case-sensitive	fak.	Aktiviert die Möglichkeit, direkt die Zahlungsmaske einer bestimmten Zahlungsart aufzurufen	true
txtPM_PostFinanceCard_Status	true oder false, case-sensitive	fak.	Aktiviert Zahlungsart PostFinance Card	true
txtPM_yellownet_Status	true oder false, case-sensitive	fak.	Aktiviert Zahlungsart PostFinance-E-Finance	false
txtPM_Master_Status	true oder false, case-sensitive	fak.	Aktiviert Zahlungsart Mastercard	true
txtPM_Visa_Status	true oder false, case-sensitive	fak.	Aktiviert Zahlungsart Visa	false
txtPM_Amex_Status	true oder false, case-sensitive	fak.	Aktiviert Zahlungsart American Express	false
txtPM_Diners_Status	true oder false, case-sensitive	fak.	Aktiviert Zahlungsart Diners Club	true
txtPM_yellowbill_Status	true oder false, case-sensitive	fak.	Aktiviert Zahlungsart PostFinance-E-Rechnung	true

yellowpay berechnet die Schnittmenge der über diese Parameter ausgewählten Zahlungsarten und der im Shopprofil (Stammdaten) aufgeschalteten Zahlungsarten.

Ist die Schnittmenge leer, wird dem Shopper in der Zahlungsmaske eine Fehlermeldung angezeigt (siehe Kapitel 4).

Besteht die Schnittmenge aus genau einer Zahlungsart, wird die Zahlungsauswahl übersprungen und direkt die zahlungsartenspezifische Eingabemaske angezeigt.

Besteht die Schnittmenge aus mehr als einer Zahlungsart, wird die Zahlungsauswahl angezeigt.

⁵ fak. = fakultativ, obl. = obligatorisch

1.7 Parametervalidierung

Die Validierung des Zahlungsmaskenaufrufs geschieht in der folgenden Reihenfolge:

- Alle vom Merchant übergebenen Parameter entsprechen den Anforderungen gemäss Kapitel 1.1 bis 1.6.
- txtShopID ist der Schlüssel, um die Stammdaten des entsprechenden Merchants zu finden. Wird kein passender Eintrag gefunden hat dies die Anzeige einer Fehlermeldung in der Zahlungsmaske zur Folge.
- Shopstatus: Je nach Fortschritt im Aufschaltprozess des Shops sind produktive Zahlungen erlaubt oder nicht. Das gleiche gilt für das Kundentestsystem, jedoch werden über dieses System die Autorisierungen lediglich simuliert.
- Browser- und Betriebssystemcheck.
- Referrercheck: Um die Berechtigung des Zahlungsmaskenaufrufs zu verifizieren wird die Referrer-URL überprüft (Adresse/URL von der die Zahlungsmaske aufgerufen wird). Grundsätzlich können beliebig viele Referrer-URLs in den Shopstammdaten erfasst werden. Es wird geprüft, ob der beim Aufruf vom Browser automatisch übergebene Referrer mit einem in den Stammdaten hinterlegten Referrer übereinstimmt. Übereinstimmung heisst, dass der übergebene Referrer gleich beginnen muss wie ein beliebiger für den Shop hinterlegter Referrer.

Beispiel

- Stammdaten: <http://www.shop.ch> und <http://shop.ch>
- übergebener Referrer: <http://shop.ch/basket> → **OK**
- übergebener Referrer: <http://www.shop.ch/basket> → **NOK** (wegen https)

1.8 Refresh der Merchant-Webseite nach Aufruf der Zahlungsmaske


Hat der Merchant PostFinance als Payment Service Provider gewählt, dann führt die Zahlungsmaske nach dem Öffnen ein JavaScript `history.back()` aus, um auf die aufrufende Shopseite zurückzukehren.

Je nach Browsereinstellungen und Meta-Parametern der Shopseite (Expires, Pragma, cache-control) wird die Seite neu geladen oder vom Browser aus dem Cache geladen.

Wird die Seite neu geladen, muss der Merchant sicherstellen, dass der Reload korrekt funktioniert, was insbesondere bei durch http POST geladenen Seiten nicht immer selbstverständlich ist.

Der Merchant kann den `history.back()` mit dem optionalen Parameter `txtHistoryBack` verhindern, allerdings bleibt die Shopseite dann bis zum Aufruf der Rücksprung-URL leer.

2. Zahlungsmaskenrücksprung

Schliesst der Shopper die Zahlungsmaske, werden je nach Autorisierungsstatus verschiedene Rücksprung-URLs angesteuert. Geschlossen wird die Zahlungsmaske vom Shopper durch Anklicken des entsprechenden Buttons in der Zahlungsmaske (z.B. «Weiter» nach erfolgreicher Autorisierung, «Abbruch» in der Zahlungsartenauswahl usw.) oder indem das Zahlungsmaskenfenster geschlossen wird (z.B.  bzw. ALT + F4 auf Windows-Systemen).

2.1 Rücksprung-URL «Abbrechen»

Diese Rücksprung-URL wird angesteuert, wenn die Zahlungsmaske geschlossen wird, ohne dass eine Autorisierung stattgefunden hat.

2.2 Rücksprung-URL «Erfolgreich»

Diese Rücksprung-URL wird angesteuert, wenn die Zahlungsmaske geschlossen wird und eine erfolgreiche Autorisierung stattgefunden hat.

Der Rücksprung nach einer erfolgreichen Autorisierung darf vom Merchant **nicht** als Auslöser für den shopseitigen Bestellabschluss verwendet werden. Damit der Merchant sicher sein kann, dass die Autorisierung erfolgreich war, muss die Autorisierungsquittung verwendet werden (siehe Kapitel 3). Eine Autorisierung kann erfolgreich sein, ohne dass die entsprechende Rücksprung-URL aufgerufen wird, z.B. wenn der Shopper die Zahlungsmaske nicht schliesst oder wenn Probleme beim Aufruf der Rücksprung-URLs auftreten (siehe Kapitel 2.5).

2.3 Rücksprung-URL «Fehlgeschlagen»

Diese Rücksprung-URL wird angesteuert, wenn die Zahlungsmaske geschlossen wird und eine nichterfolgreiche Autorisierung stattgefunden hat.

2.4 txtShopPara

Der Parameter txtShopPara wird bei allen Rücksprüngen (siehe Kapitel 2) der entsprechenden Rücksprung-URL angehängt.

Enthält die in den Stammdaten hinterlegte Rücksprung-URL schon einen Query String, dann wird dieser mit txtShopPara verknüpft. Der Query String wird seitens PostFinance nicht weiterverarbeitet, insbesondere wird keine URL-Kodierung vorgenommen, d.h. die Verantwortung, aber auch die Kontrolle für die korrekte Kodierung innerhalb des Parameters txtShopPara liegt beim Merchant (Details siehe RFC 3986).

Beispiel 1

Rücksprung-URL (Stammdaten): <https://server.domain.ch/app?key1=value1>

txtShopPara (dynamisch übergeben): «key2=value2&key3=value3»

Resultierende Rücksprung-URL:

<https://server.domain.ch/app?key1=value1&key2=value2&key3=value3>

Beispiel 2

Rücksprung-URL (Stammdaten):

<https://pwd@server.domain.ch:88/app?key1=val1&key2=val2#Ref>

txtShopPara (dynamisch übergeben): «key3=öäè&key4=.,;?&»

Resultierende Rücksprung-URL:

<https://pwd@server.domain.ch:88/app?key1=val1&key2=val2#Ref&key3=öäè&key4=.,;?&>

2.5 Bekannte Probleme

- Aus Sicherheitsgründen kann der Browser das Aufrufen der Rücksprung-URLs verweigern.
- Bei technischen Problemen, bezogen auf die Internet Service Provider des Clients oder des Shops, ist ein Rücksprung ebenfalls nicht möglich.

3. Autorisierungsquittung

Kann eine Zahlung erfolgreich autorisiert werden, schickt PostFinance dem Merchant Parameter an die primäre Zieladresse für den Empfang der Autorisierungsquittung (URL oder E-Mail), abhängig von den hinterlegten Shopstammdaten. Dies geschieht in Form einer Server-zu-Server-Kommunikation, welche für den Shopper unsichtbar ist. Die Zahlungsdaten können so direkt im Online-Shop des Merchants weiterverarbeitet werden. Nicht erfolgreiche Autorisierungen haben nie eine Autorisierungsquittung zur Folge.

Die Autorisierungsquittung erfolgt asynchron zum eigentlichen Zahlungsprozess und wird unmittelbar nach erfolgreicher Autorisierung ausgelöst, unabhängig davon, ob der Shopper die Zahlungsmaske schliesst oder nicht. Bei erfolgloser Zustellung wiederholt yellowpay die Zustellung der Autorisierungsquittung drei weitere Male in einem Intervall von einer Minute. Nach vier erfolglosen Zustellversuchen wird die Autorisierungsquittung an die sekundäre Zieladresse (E-Mail oder URL) geschickt.

Damit der Merchant sicher sein kann, dass die Autorisierung erfolgreich war, muss die Autorisierungsquittung und nicht der Aufruf der Rücksprung-URLs vom Merchant als Auslöser für den shopseitigen Bestellabschluss verwendet werden. Eine Autorisierung kann erfolgreich sein, ohne dass die entsprechende Rücksprung-URL aufgerufen wird, z.B. wenn der Shopper die Zahlungsmaske nicht schliesst oder wenn Probleme beim Aufruf der Rücksprung-URLs auftreten (siehe Kapitel 2.5).

Ferner kann der Merchant dank dem Parameter txtHashBack verifizieren, ob die Autorisierungsquittung von PostFinance stammt. Besitzt der Shop einen aktivierten Hash-Check, wird automatisch mit der Autorisierungsquittung auch der Parameter txtHashBack mit einem neuen Algorithmus als Inhalt retourniert.

3.1 Autorisierungsquittung per http oder https

Wird in den Stammdaten als primäre bzw. sekundäre Zieladresse für den Empfang der Autorisierungsquittung eine URL hinterlegt, werden die Rückgabeparameter per http oder https POST geschickt. Die Zustellung der Autorisierungsquittung ist aus Sicht von yellowpay erfolgreich, wenn der Server des Shops einen gültigen http-Status zurückgibt. Im Moment wird weder der Inhalt der Antwort noch die Bedeutung des http-Status-Codes ausgewertet, d.h. ein http/1.1 404 Not Found wird ebenso als erfolgreiche Zustellung interpretiert wie ein http/1.1 200 OK.

PostFinance behält sich allerdings vor, in Zukunft die erfolgreiche Zustellung der Autorisierungsquittung von einem http/1.1 200 OK abhängig zu machen, und empfiehlt deshalb, Autorisierungsquittungen immer mit einem http/1.1 200 OK und einer leeren Antwortseite an PostFinance zu beantworten (keine HTML-Tags).

Die Autorisierungsquittung enthält:

- Alle vom Merchant übergebenen Parameter ausser deliveryPaymentType (deferred/immediate), welcher nur im Zahlungsdetail des Merchant-GUI yellowpay sichtbar ist
- txtTransactionID (PaymentID, von PostFinance generiert)
- txtEp2TrxID (TransactionID, ep2-Transaktionsreferenz bei Zahlungsart PostFinance Card von PostFinance generiert; die ersten 8 alphanumerischen Stellen repräsentieren die ep2-TerminalID, die folgenden 8 numerischen Stellen entsprechen der ep2-Transaktions-Laufnummer)
- txtPayMet (vom Shopper gewählte Zahlungsart, von PostFinance generiert)

- txtESR_Member, wenn die Zahlungsart PostFinance-E-Rechnung gewählt wurde
- txtESR_Ref, wenn die Zahlungsart PostFinance-E-Rechnung gewählt wurde
- txtHashBack⁶

Der beim Zahlungsmaskenaufruf übergebene, optionale Parameter txtShopPara wird im http oder https POST nicht als einzelner Parameter zurückgegeben, sondern in einzelne Key/Value Pairs aufgespalten.

Aus «key1=value1&key2=value2» wird im http oder https POST:

key1=value1

key2=value2

Beispiel (HTTP Body)

Message Content:

```
SESSIONID = 123           ← wurde aus txtShopPara extrahiert
txtArtCurrency = CHF
txtBAddr1 = Bahnhofstrasse 1
txtBCity = Bern
txtBCountry = CH
txtBFirstName = Peter
txtBLastName = Muster
txtBTitle = Herr
txtBZipCode = 3030
txtHistoryBack = true
txtLangVersion = 2055
txtOrderIDShop = yp_47
txtOrderTotal = 0.10
txtPayMet = PostFinance Card
txtShopId = planet1001_yp
txtTransactionID = 104950
txtEp2TrxID = 3016567800000001
txtUseWindow = false
```

Abbildung 2: Beispiel einer Autorisierungsquittung an URL

3.2 Autorisierungsquittung per E-Mail

Wird in den Stammdaten als primäre bzw. sekundäre Zieladresse für den Empfang der Autorisierungsquittung eine E-Mail Adresse hinterlegt, werden die Rückgabeparameter per SMTP geschickt.

Die Zustellung der Autorisierungsquittung ist für yellowpay erfolgreich, wenn der SMTP-Gateway den SMTP-Request quittiert hat. Existiert eine E-Mail-Adresse nicht, dann wird dies in der Regel von der PostFinance-Applikation nicht erkannt und dementsprechend als erfolgreiche Zustellung interpretiert. Dies lässt sich nicht vermeiden, da bei SMTP der Sender keine direkte Antwort des Zielsystems (E-Mail-Empfänger) erhält, sondern nur von vermittelnden Systemen.

Im Gegensatz zum http oder https POST wird txtShopPara bei der E-Mail-Autorisierungsquittung als einzelner Wert zurückgegeben und nicht in separate Key/Value Pairs aufgespalten.

Folgende obligatorische Parameter werden immer mit Feldnamen und Feldinhalt retourniert:

- txtTransactionID (PaymentID, von PostFinance generiert)
- txtEp2TrxID (TransactionID, ep2-Transaktionsreferenz bei Zahlungsart PostFinance Card von PostFinance generiert; die ersten 8 alpha-numerischen Stellen repräsentieren die ep2-TerminalID, die folgenden 8 numerischen Stellen entsprechen der ep2-Transaktions-Laufnummer)

⁶ Nur bei Shops mit aktiviertem Sicherheitsparameter yellowpay

- txtPayMet (vom Shopper gewählte Zahlungsart, von PostFinance generiert)
- txtArtCurrency (Währung)
- txtOrderTotal (Total)
- txtHashBack⁷

Folgende optionale Parameter werden immer mit Feldnamen und Feldinhalt retourniert, unabhängig davon, ob sie übergeben wurden. Hat keine Übergabe stattgefunden, ist der Feldinhalt leer:

- ESR Member (txtESR_Member)
- ESR Referenznummer (txtESR_Ref)
- OrderID (txtOrderIDShop)
- Hash (txtHash)
- txtShopPara (Shoppparameter)

Bei den hier aufgeführten, optionalen Parametern wird nur der Feldinhalt und nicht der Feldname zurückgeschickt:

- txtBTitle (Shopper Anrede)
- txtBLastName, txtBFirstName (Shopper Name, Shopper Vorname)
- txtBAddr1 (Shopper Adresse 1)
- txtBZipCode (Shopper PLZ)
- txtBCountry, txtBZipCode, txtBCity (Shopper Land, Shopper PLZ, Shopper Ort)
- txtBTel (Shopper Telefon)
- txtBFax (Shopper Fax)
- txtBEmail (Shopper Mail)

Der Parameter deliveryPaymentType (deferred/immediate) ist nur im Zahlungsdetail des Merchant-GUI yellowpay sichtbar und wird nicht mit der Autorisierungsquittung an den Shop übermittelt.

Die Betreff-Zeile (Subject) enthält den Wert: <txtShopId>:<PaymentID>.

Beispiel

From: yellowpay@postfinance.ch

To: muster@shop.ch

Subject: planet: 104952

```
TransactionsID: 104952
ep2TransactionID: 3016567800000003
Shoppparameter:
SESSIONID=123
```

```
Kunde:
Herr
Muster Peter
Bahnhofstrasse 1
CH-3030 Bern
031 333 33 33
031 333 33 33
mail@mail.ch
```

```
Zahlungsart: PostFinance Card
ESR Member:
ESR Referenznummer:
Order-ID: yp_47
Währung: CHF
Total: 0.10
Hash:
```

Abbildung 3: Beispiel einer Autorisierungsquittung an E-Mail-Adresse

⁷ Nur bei Shops mit aktiviertem Sicherheitsparameter yellowpay

4. Meldungen Zahlungsmaske yellowpay

Die Zahlungsmaske yellowpay enthält drei unterschiedliche Typen von Meldungen, welche dem Shopper angezeigt werden:

- Validierung der Parameter beim Zahlungsmaskenaufruf
- Validierung der Eingaben des Shoppers
- Autorisierungsmeldungen

Für die Implementation der Zahlungsmaske sind nur Meldungen des Typs «Validierung der Parameter beim Zahlungsmaskenaufruf» relevant. Alle anderen Meldungen dienen dem Shopper lediglich zur Information während des Zahlungsvorgangs.

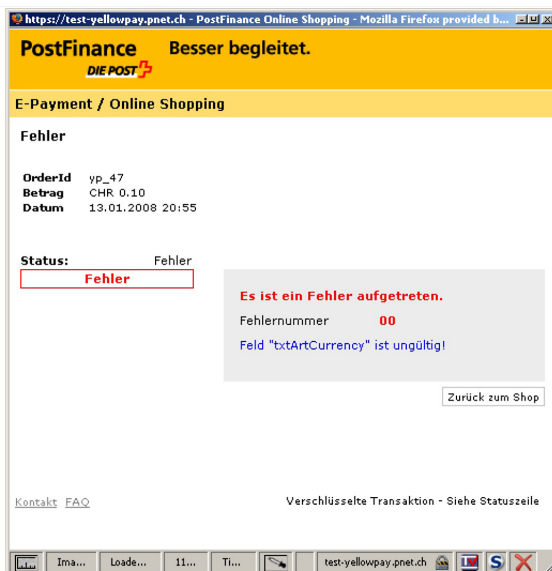
4.1 Validierung der Parameter beim Zahlungsmaskenaufruf

Wenn ein oder mehrere Parameter beim Zahlungsmaskenaufruf nicht korrekt übergeben wurden, wird dem Shopper die entsprechende Fehlermeldung angezeigt.

In den meisten Fällen kann für den Shop keine Zahlung durchgeführt werden, weil die Implementation des Merchants fehlerhaft ist.

Um diesen Problemen vorzubeugen, empfiehlt PostFinance unbedingt, den Zahlungsmaskenaufruf auf unserem Kundentest-System vor der produktiven Inbetriebnahme zu testen.

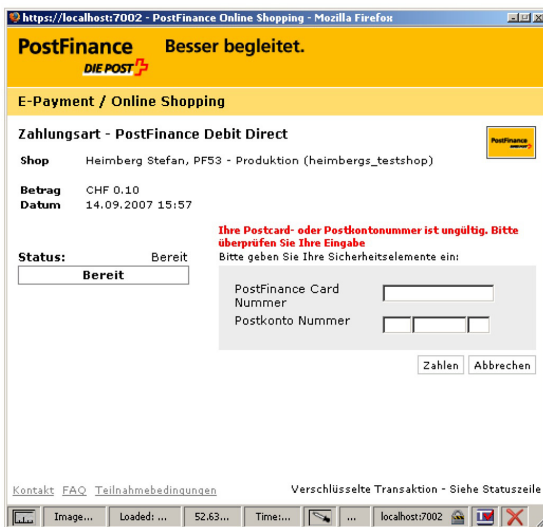
Beispiel



4.2 Validierung der Eingaben des Shoppers

Diese Fehlermeldungen werden angezeigt, wenn der Shopper fehlerhafte Eingaben gemacht hat. In unserem Beispiel hat der Kunde für die Zahlungsart PostFinance Card eine ungültige/fehlerhafte Postcard-/Postkontonummer eingegeben.

Beispiel



4.3 Autorisierungsmeldungen

Bei Fehlern während der Autorisierung wird folgende Meldung ausgegeben: «Es ist ein Fehler aufgetreten», Fehlernummer nnn. Diese Meldung dient zur Information des Shoppers. Der Kundendienst Shopperhelp von PostFinance kann bei Angabe der Fehlernummer die Fehlerursache finden und das Problem lösen.

Beispiel



5. Unterstützte Browser und Betriebssysteme

Die Zahlungsmaske yellowpay wurde auf folgenden Betriebssystemen und Browsern auf einwandfreie Darstellung und Funktion getestet:

https://paymentserver2k.post.ch/epa/epa_config_de.htm

Alle anderen Systemkonfigurationen werden zwar auf die Zahlungsmaske yellowpay zugelassen, aber nicht von PostFinance getestet und unterstützt. Der Browser des Shoppers muss JavaScript aktiviert haben und fähig sein, SSLv3 mit mindestens 128 Bit zu verschlüsseln.

Auf dem Browser aktivierte Popup-Blocker oder andere Software wie z.B. Security Suites mit ähnlichen Mechanismen (z.B. Altavista Bar, Google Toolbar oder Content-Filter) können die Anzeige der yellowpay-Zahlungsmasken unterdrücken. Über das Einblenden einer Zwischenseite können allerdings fast alle Popup-Blocker übersteuert werden.

Die Zahlungsmaske yellowpay verwendet keine Cookies.

Verwendet der Shopper eine von yellowpay nicht unterstützte Systemkonfiguration, wird er darauf mit folgender Meldung hingewiesen:

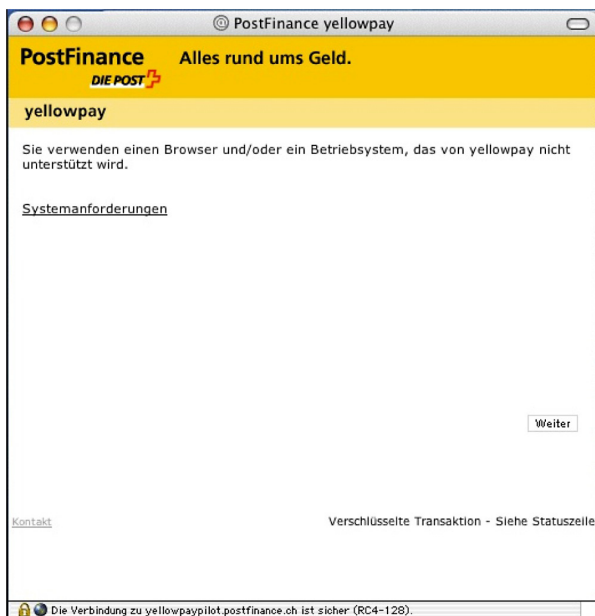


Abbildung 4: Meldung bei nicht unterstützter Betriebssystem- und/oder Browserkonfiguration

Momentan werden allerdings nur Browser und Betriebssysteme gesperrt, die nachweislich nicht mit der Zahlungsmaske funktionieren. Mit Ausnahme von IE 5.x auf Mac OS werden zurzeit alle auf dem Markt erhältlichen Browser und Betriebssysteme zugelassen.