Servizio POS Virtuale "Virtual Pay"

Integrazione con il Sito del Merchant

Autore	Phoenix Informatica Bancaria spa
Ultima Revisione:	giugno 2013

Interfaccia con il sistema di pagamento

Dati da inviare al Sistema di Pagamento

La tabella 1 indica i parametri da passare al Sistema di Pagamento attraverso un **POST HTTP** (l'operazione di GET HTTP viene rifiutata dal sistema di pagamento).

Nome	Obbligatorio	Descrizione
MERCHANT_ID	S	Identificatore Merchant (char 20)
ORDER_ID	S	Identificativo dell'ordine (char 20)
IMPORTO	S	Importo dell'ordine
DIVISA	S	Valuta codice ISO International Standard 4217 (EUR=Euro) (char 3)
ABI	S	Abi della Banca: nell'ottica di un Server di Pagamento che funge da centro multiservizi specifica a quale Banca deve essere indirizzata la transazione. (char 5)
SEPARATORI	N	Due separatori: il primo separa gli n articoli scelti, il secondo separa i dati relativi ad un articolo. Il campo è facoltativo: per default i separatori utilizzati sono ';' e '^'
ITEMS	S	Elenco degli articoli del carrello della spesa riempito dal Buyer: <codice articolo (char 32)>**^**<descrizione articolo (char 120)>**^**<quantità (int 4)>**^**<importo>**^**<divisa (char 3)>**;**
EMAIL	N	Indirizzo di e-mail del cliente; se il campo non è presente verrà richiesto all'utente insieme ai dati della carta di credito
LINGUA	N	Lingua nella quale devono essere mostrati i messaggi di integrazione con l'utente finale. Il campo è facoltativo; di default la lingua è quella ITALIANA ("**ita**"). In alternativa può essere specificato INGLESE (valorizzare con "**ing**"), oppure TEDESCO ("**ted**"), FRANCESE ("**fra**") e SPAGNOLO ("**spa**")
URLOK	S	URL completa verso la quale redirigere il browser del cliente a pagamento avvenuto (deve comprendere tutti gli eventuali parametri da passare) (char 1024)
URLKO	S	URL completa verso la quale eseguire una redirect per rimandare l'utente al negozio virtuale se esso decide di interrompere l'operazione di pagamento prima del suo completamento (deve comprendere tutti gli eventuali parametri da passare). (char 1024)
URLACK	N	URL del Merchant system verso la quale effettuare la GET di notifica di pagamento andato a buon fine.
URLNACK	N	URL del Merchant system verso la quale effettuare la GET di notifica di pagamento NON andato a buon fine per mancata autorizzazione.
MAC	S	Message Authentication Code che il Merchant può utilizzare per certificare l'integrità dei dati ordine che invia al Server di Pagamento. Da riportare sempre in **UPPERCASE**!

Tabella 1

L'interfacciamento tra il sito del Merchant ed il Server di Pagamento avviene quindi mediante la predisposizione di un FORM HTML sul sito del Merchant che effettua un POST ad un URL del server secondo le specifiche fornite in tabella 1. L'URL a cui effettuare il post viene fornito da Phoenix in fase di attivazione del servizio.

Il POST determina il passaggio al Server di Pagamento dei dati di compentenza del Merchant necessari alla procedura di pagamento (id del merchant, id ordine, importo, articoli, ed altre opzioni).

Note:

- Se uno dei parametri indicati come obbligatori non viene passato, il software interrompe l'esecuzione e visualizza all'utente una pagina di errore generico.
- Il codice che identifica ogni ordine (specificato nel parametro ORDER_ID) **deve essere univoco**, e non potrà più essere riproposto al server di Pagamento, indipendentemente dall'esito del POST.
- Il codice che identifica ogni articolo (specificato nel parametro ITEMS) deve essere univoco all'interno di uno stesso ordine.
- Gli ITEMS contengono in sequenza i seguenti valori: codice articolo, descrizione articolo, quantità, importo, divisa importo (esempio: "`art1^Descrizione articolo^3^123,45^EUR;`").
- Il **parametro MAC** (chiave di controllo a firma digitale, descritta più avanti) viene richiesto obbligatoriamente e non è possibile disabilitarlo.
- Il parametro ITEMS, **obbligatorio,** deve essere sempre valorizzato.
- Per gli importi in EURO devono essere **sempre** passate due cifre decimali separate da virgola (es. 1674,00 ; 1674,78 ; 0,99 ; 0,09 ; 2,00).
- Il parametro ISSUER consente al Merchant di specificare quali carte di credito accettare per una certa transazione, se non viene passato l'acquirente può scegliere tra tutte le carte alle quali il Merchant è convenzionato. I valori accettati sono: 01 - 02 - 06 – 07 e devono essere separati dal carattere ',' (es. 02,07,06).
- Il parametro LINGUA: se specificato nei parametri postati vengono ammessi solo i valori indicati nella tabella precedente ("ita", "ing", "ted", "fra" e "spa"); se il dato non viene specificato il sistema di pagamento assegna di default la lingua italiana.

Controllo di integrità dei dati scambiati tra il Merchant ed il Server di Pagamento

Esiste la possibilità che un acquirente malintenzionato modifichi i dati relativi all'ordine prima che questi vengano inviati al Server di Pagamento (ad

esempio editando manualmente la pagina del sito Merchant che è incaricata di eseguire il POST di tali dati).
Il Server di Pagamento consente al Merchant di riconoscere questo evento e di prevenirlo.

Con l'obbligatorietà del parametro MAC (firma di integrità), il servizio prevede che il Merchant invii, assieme ai dati ordine, una firma (che chiameremo MAC) che consenta al gateway di pagamento di verificarne l'integrità dei dati ricevuti.
Questo approccio (di tipo *"preventivo"*) aumenta la complessità dell'interfacciamento con il Server di Pagamento, ma consente al gateway di pagamento di riconoscere i tentativi di frode scaricando il Merchant di tale responsabilità ed è quindi consigliato.
Anche in questo caso è comunque consigliabile che il Merchant System verifichi la congruenza tra i dati in suo possesso e quelli restituiti dal gateway di pagamento (compreso il MAC che li accompagna) così come è buona norma "congelare il carrello" (cioè rendere non più modificabile l'elenco degli articoli che costituiscono un certo ordine) prima di cedere il controllo al sistema di pagamento.

Il parametro MAC dovrà essere così formato:

MAC = MD5(MID + OID + IMP + DIV + ABI + ITEMS + KEY)

Dove:

- MID è l'identificativo del merchant (Merchant ID) comunicato in fase di attivazione del servizio
- IMP è l'importo (formattato come nei dati in POST)
- DIV è la divisa (EUR)
- ABI è l'ABI della banca (comunicato in fase di attivazione)
- ITEMS è la stringa passata nel campo ITEMS (obbligatorio se si usa il MAC)
- KEY è una chiave segreta conosciuta solo dal Merchant e dal Server di Pagamento (comunicata al Merchant in fase di attivazione del servizio)

Alla stringa ottenuta concatenando i parametri di cui sopra, nell'ordine indicato, va applicato l'algoritmo di hash MD5 [1] che produce una stringa binaria che va convertita in notazione esadecimali (32 caratteri). Sono disponibili implementazioni standard dell'algoritmo per tutti i maggiori linguaggi di programmazione in ambiente web.

[1] Per la definizione dell'algoritmo MD5 si può far riferimento a:
R. L. Rivest, *"The MD5 Message Digest Algorithm"* RFC 1321, Apr. 1992

La stringa così ottenuta va passata nel post HTTP nel campo MAC, mettendola in UPPERCASE.

Esempio:

```
MID = 123456700001
OID = ORD00023
IMP = 0,01
DIV = EUR
ABI = 03599
ITEMS = cod1^aaa^1^0,01^EUR;
KEY = AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

La stringa ottenuta dalla concatenazione è:

```
1234567000010RD000230,01EUR03599cod1^aaa^1^0,01^EUR;AAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAA
```

Su questa si applica l'hash MD5; il risultato ottenuto va codificato come stringa esadecimale (uppercase) per cui si ottiene:

```
5906F278259CE31549793EE38CB497C6
```

che sarà il valore inviato nel POST mediante il campo MAC.

Dati restituiti dal Server di Pagamento

In funzione dell'esito della transazione il Server di Pagamento visualizza una pagina di riepilogo in cui è presente un pulsante che dirige il browser verso l'indirizzo specificato dal Merchant nel parametro **URLOK** (se la transazione è andata a buon fine) o **URLKO** (se la transazione non è andata a buon fine). Lo scopo di questi URL è quindi quello di riportare la navigazione dell'acquirente al sito del merchant una volta effettuato il pagamento.
L'utente non necessariamente utilizzerà questi pulsanti, quindi sono previsti degli URL (facoltativi) che il sistema del merchant può utilizzare per effettuare un allineamento dei propri archivi in seguito alla transazione di pagamento:
- l'indirizzo **URLACK** viene sempre invocato (GET HTTP) automaticamente dal server in seguito all'esito positivo del pagamento.
- l'indirizzo **URLNACK** viene sempre invocato (GET HTTP) automaticamente dal server in seguito all'esito negativo del pagamento (mancata autorizzazione.

Rimane inoltre l'eventualità che l'acquirente, una volta passato al sistema di pagamento, decida di non completarlo.

A tutti gli URL sopra descritti il server di pagamento aggiunge i dati necessari ad identificare la transazione di pagamento:

- **TRANSACTION_ID** identificativo univoco della transazione
- **MERCHANT_ID** identificativo del Merchant.
- **ORDER_ID** identificativo dell'ordine.
- **COD_AUT** codice di autorizzazione restituito dall'ente autorizzante.
- **IMPORTO** importo dell'ordine.
- **DIVISA** divisa.
- **MAC** codice di controllo dell'integrità (descritto successivamente).

Esempio:
Supponiamo che il Merchant passi al sistema il seguente parametro:
`URLACK = http://www.merchant.com/ordini/end.asp`
se la transazione termina correttamente, la risposta del server di pagamento sarà una GET HTTP al seguente URL:

```
http://www.merchant.com/ordini/end.asp?TRANSACTION_ID=471C3702DAEA11D3AD0200
6097C97962&COD_AUT=17&MERCHANT_ID=00001&ORDER_ID=ORD949932127628
&IMPORTO=250&DIVISA=EUR&MAC=3A4F701594CCB265512492E74AB90171
```

Per consentire ai Merchant di verificare l'integrità dei dati relativi all'esito di una operazione di pagamento, si fa ricorso ad un MAC (Message Authentication Code) basato su una chiave segreta comunicata al Merchant all'atto della sottoscrizione del servizio, in modo analogo alla modalità prevista per il passaggio dei dati in POST dal sito del Merchant al server di

Pagamento.

Il calcolo del MAC avviene secondo la seguente specifica:

MAC = MD5(TRANSACTION_ID + MERCHANT_ID + ORDER_ID + COD_AUT + IMPORTO + DIVISA + KEY)

ovvero il MAC è ottenuto applicando l’algoritmo MD5 alla concatenazione delle stringhe rappresentati: identificativo transazione, identificativo Merchant, identificativo ordine, codice autorizzazione, importo ordine, codice divisa e chiave segreta del Merchant. La stringa ottenuta è sempre riportata in UPPERCASE.

Per verificare il MAC in fase di ritorno dal gateway di pagamento (richiamo degli URLOK, URLKO, URLACK, URLNACK) il sito del Merchant deve concatenare i dati ricevuti come esito (TRANSACTION_ID, MERCHANT_ID, ORDER_ID, COD_AUT, IMPORTO e DIVISA), aggiungervi la propria chiave segreta (KEY), applicare alla stringa così ottenuta l’algoritmo MD5 e confrontare il risultato con il MAC ricevuto dal server di pagamento.
Se il risultato non coincide con il campo inviato nell’URL, il Merchant dovrà considerare non attendibili i dati ricevuti.

Mail di notifica

Al termine di ogni operazione di pagamento, e indipendentemente dal suo esito, il sistema invia al Merchant e al Buyer una mail di riepilogo della transazione con i dati riassuntivi della stessa e l’esito (pagamento andato a buon fine oppure no).
Il testo delle email di notifica è personalizzabile dall’esercente, per le istruzioni dettagliate fare riferimento al Manuale Operativo Esercente fornito al merchant in fase di attivazione del servizio.

Multilingua

Il sistema di pagamento prevede la possibilità di utilizzare testi in diverse lingue: attualmente italiano, inglese, francese, tedesco e spagnolo.
L’impostazione della lingua al momento del pagamento viene comunicata dinamicamente dal sito dell’esercente.
La scelta della lingua (qualora prevista) da parte del titolare carta viene effettuata sul sito dell’esercente.
Da questa scelta dipende anche la lingua con cui vengono effettuate le successive comunicazioni via posta elettronica.

Personalizzazione delle pagine Web

Al Merchant è data la facoltà di personalizzare le pagine gestite dal sistema (pagina di inserimento dei dati carta e di esito della transazione) attraverso l'uso di un foglio di stile (Cascading Style Sheet) che consente la definizione di sfondo, colore e fonts di ogni oggetto della pagina.
Può inoltre inserire in tali pagine il suo logo (sotto forma di immagine in formato GIF).

La modifica dei files necessari alla personalizzazione viene effettuata dall'esercente attraverso l'apposita console web di gestione. Per le istruzioni dettagliate fare riferimento al Manuale Operativo Esercente fornito al merchant in fase di attivazione del servizio.