GestPay
Specifiche tecniche sicurezza con OTP

Sommario

Informazioni documento

Nome progetto	GestPay
Titolo documento	GestPay - Specifiche tecniche sicurezza con OTP
Data creazione	Marco Loro
Lingua	Italiano
Società	EasyNolo

Informazioni versione

Versione	Descrizione	Data	Autore
1.0.0	Versione iniziale	25/03/2001	Sellanet
1.0.1	Aggiornamento requisiti browser	09/04/2001	Sellanet
1.0.2	Correzione esempio chiamata pagina di pagamento	08/02/2002	Sellanet
1.0.3	Aggiornamento requisiti campi custom	04/03/2002	Sellanet
1.0.4	Aggiornamento Codici Errore	15/03/2002	Sellanet
1.0.5	Aggiornamento Codici Lingua	30/05/2002	Sellanet
1.0.6	Aggiornamento requisiti campi custom e parametri gestpay	20/08/2002	Sellanet
1.0.7	Aggiornamento codici valuta	27/01/2003	Sellanet
2.0.0	3D Secure	28/0172003	Sellanet
2.0.1	Errata Corrige	20/04/05	Easy Nolo S.p.A.
2.0.2	Introduzione dominio per codici di test	13/06/2007	Easy Nolo S.p.A.
2.0.3	Introduzione nuovo parametro in risposta 3DLevel	15/07/2009	Easy Nolo S.p.A.

1 Introduzione

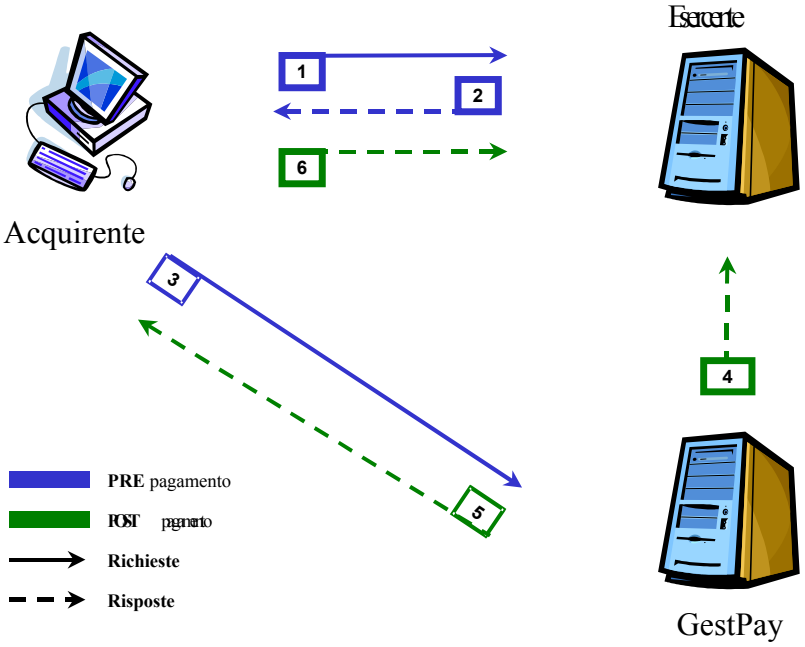
Questo documento ha lo scopo di illustrare gli aspetti funzionali e di architettura della piattaforma GestPay fornendo le indicazioni necessarie all'interfacciamento.
Nel capitolo **Architettura del sistema** si descriveranno le componenti del sistema e le modalità di interazione tra i vari componenti e gli attori coinvolti (esercente, acquirente e GestPay).
Nel capitolo **Descrizione fasi del processo** verranno prese in esame le singole fasi che compongono il processo di pagamento evidenziando le informazioni che devono essere passate a GestPay e le informazioni che verranno restituite.
Nel capitolo **Autenticazione** viene descritto come GestPay riconosce il server dell'esercente che effettua le chiamate al sistema e la logica di utilizzo delle OTP.
Nel capitolo **Struttura dati transazione di pagamento** vengono descritte le informazioni che identificano una transazione di pagamento e l'esito che GestPay restituisce dopo l'elaborazione.
Nel capitolo **Profilo esercente** viene descritto come configurare il profilo esercente per permetter a GestPay di processare in modo corretto le transazioni
Nel capitolo **Requisiti software** verranno evidenziati i requisiti minimi richiesti per l'installazione del software necessario all'interfacciamento con GestPay.
Nel capitolo **Transazioni d'esempio** vengono descritte alcune transazioni tipiche ponendo in evidenza le informazioni scambiate e le modalità di interazione tra le componenti.
Sono presenti, inoltre, alcune tabelle che permettono di codificare alcune informazioni inviate o ricevute da GestPay.

2 Architettura del sistema

Nell'architettura del sistema si possono identificare 3 componenti:

- Client dell'acquirente
- Server dell'esercente
- Server di GestPay

La comunicazione tra i vari componenti avviene via internet utilizzando il protocollo http o https (il server GestPay dispone di un certificato digitale Verisign a 128 bit).
Il processo di pagamento è suddiviso in step di comunicazione durante i quali i componenti interagiscono scambiandosi una serie di informazioni necessarie all'esecuzione della transazione.



Schema architettura

1 L'acquirente seleziona i prodotti da acquistare e decide di procedere con il pagamento.

2 Il server dell'esercente invia la stringa parametri al browser dell'acquirente con tutte le informazioni necessarie al processo di pagamento

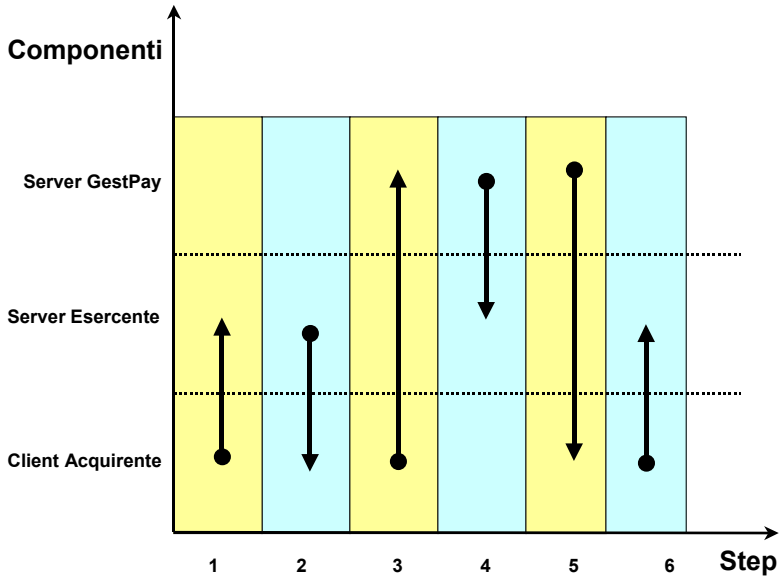
3 Il browser dell'acquirente richiama la pagina di pagamento sul server GestPay passando la stringa parametri. Vengono effettuati i controlli di autenticazione e di integrità dei dati della transazione che, se superati, permettono la visualizzazione della pagina di pagamento e l'inserimento dei dati necessari a completare la transazione. I passi successivi descrivono la modalità con cui viene comunicato l'esito della transazione sia all'esercente che all'acquirente.

4 GestPay comunica al server dell'esercente una stringa parametri che riporta l'esito della transazione.

5 GestPay comunica la stringa parametri che riporta l'esito della transazione al browser del cliente che viene indirizzato sul server dell'esercente.

6 Il browser dell'acquirente richiama la pagina di risposta realizzata dall'esercente passando la stringa parametri

Lo schema seguente analizza il processo di pagamento evidenziando l'ordine cronologico i cui avvengono gli step di comunicazione.



Step di comunicazione

3 Descrizione fasi del processo

Una transazione di pagamento può essere scomposta in 2 fasi fondamentali durante le quali vengono eseguiti uno o più step di comunicazione. In ogni fase vengono scambiate tra le varie componenti le informazioni necessarie all'elaborazione della transazione.

3.1 Fase I: chiamata pagina di pagamento

Il browser dell'acquirente viene indirizzato alla pagina di pagamento presente sul server GestPay all'indirizzo:

*https://ecomm.sella.it/gestpay/pagam.asp?**a**=<ShopLogin>&**b**=<stringa parametri>*

per codici di test

*https://testecomm.sella.it/gestpay/pagam.asp?**a**=<ShopLogin>&**b**=<stringa parametri>*

La chiamata alla pagina verrà effettuata passando due parametri:

a codice che identifica l'esercente (ShopLogin)
b stringa dati che identifica la transazione

La pagina di pagamento acquisirà i parametri ed effettuerà i controlli di identità (il parametro a deve essere riconducibile ad un esercente riconosciuto e la OTP utilizzata deve essere riconosciuta) e di coerenza dei dati della transazione (il parametro b deve contenere una serie di informazioni che permettono di elaborare una transazione di pagamento).
Se i controlli vengono superati, la pagina di pagamento verrà visualizzata all'acquirente che dovrà inserire i dati necessari a completare il processo di pagamento.
Se i controlli non vengono superati, la pagina di pagamento non viene visualizzata e si passa direttamente alla fase successiva per la comunicazione dell'esito negativo della transazione.

3.2 Fase II: comunicazione esito transazione

L'esito della transazione viene comunicato da GestPay sia all'esercente che all'acquirente.

3.2.1 Risposta all'esercente

La notifica, viene inoltrata con una chiamata server to server alla pagina opportunamente predisposta sul server dell'esercente (l'url della pagina di notifica è una delle informazioni che compongono il profilo dell'esercente configurabile tramite l'ambiente di back office di GestPay). La sintassi della chiamata è la seguente:

*http://<url server to server>?**a**=<ShopLogin>&**b**=<stringa parametri>*

La chiamata alla pagina verrà effettuata passando due parametri:

a codice che identifica l'esercente (ShopLogin)

b stringa dati cifrata che riporta l'esito della transazione

La pagina residente nel server dell'esercente dovrà necessariamente avere nel sorgente i tag html <HTML></HTML>.

Nell'eventualità di errori di comunicazione, GestPay effettua più tentativi di inoltro per un periodo di due giorni successivi alla transazione.

L'esercente riceverà anche un'email di notifica esito transazione all'indirizzo configurato nel suo profilo.

Le transazioni processate, inoltre, sono visualizzabili accedendo all'ambiente di back office di GestPay nella sezione Active Report.

3.2.2 Risposta all'acquirente

L'esito della transazione viene immediatamente notificato da GestPay visualizzando lo **"scontrino virtuale"** che riporta i dati essenziali della transazione.

GestPay indirizzerà il browser dell'acquirente sul server dell'esercente per concludere il processo d'acquisto. L'esercente dovrà predisporre due url (e configurarle nel profilo esercente) che saranno richiamate nel caso di risposta positiva e negativa e permetteranno all'esercente di gestire la comunicazione con l'acquirente mantenendo lo stile editoriale che caratterizza il negozio virtuale. La sintassi della chiamata è la seguente:

*http://<url esercente>?**a**=<ShopLogin>&**b**=<stringa parametri>*

Nel caso si sia manifestata un'anomalia nella comunicazione server to server descritta al paragrafo precedente, GestPay visualizzerà un messaggio di avviso all'acquirente segnalando che potrebbero esserci problemi nell'indirizzarlo sul server dell'esercente per completare il processo d'acquisto. In questa situazione, l'acquirente ha comunque ricevuto una notifica da GestPay sull'esito della transazione e sarà invitato, nel caso di anomalie, a contattare l'esercente utilizzando altri canali (ad esempio l'email) per concludere il processo d'acquisto.

L'acquirente riceverà anche un'email di notifica esito transazione all'indirizzo eventualmente indicato nella pagina di pagamento.

4 Autenticazione

GestPay utilizza OTP (One Time Password) per autenticare le chiamate alla pagina di pagamento e per permettere all'esercente di riconoscere il sistema GestPay durante la fase di comunicazione dell'esito della transazione. Le OTP saranno gestite tramite il parametro **PAY1_OTP**.
L'autenticazione dell'esercente, a favore del quale verrà elaborata la transazione di pagamento, viene effettuata verificando:

- **Validità ShopLogin**: il parametro ShopLogin deve corrispondere ad un codice censito nell'anagrafica di GestPay
- **Esistenza OTP**: l'OTP inviata a GestPay deve essere presente nel file di password associato allo ShopLogin
- **Stato ShopLogin**: lo stato dell'esercente deve essere attivo (lo stato dell'esercente è gestito dall'amministratore di GestPay e non direttamente dall'esercente)

Se i controlli di autenticazione non vengono superati verrà restituito un errore specifico che permetterà di identificare l'anomalia riscontrata nel processo di autenticazione.

La logica di sicurezza connessa all'uso delle OTP prevede che ogni password non debba essere utilizzata una seconda volta per effettuare le chiamate alla pagina di pagamento o per verificare le risposte provenienti da GestPay. La password deve essere cancellata dal file dal quale è stata prelevata.
I file di password consegnati all'esercente, in fase di attivazione, sono due:

- <*ShopLogin*>.**ric:** contiene le password che dovranno essere utilizzate per le chiamate alla pagina di pagamento.
- <*ShopLogin*>.**ris:** contiene le password che dovranno essere utilizzate per verificare le risposte comunicate dalla banca all'esercente.

Copie di questi file sono presenti sul server GestPay e sono utilizzate, rispettivamente, per la verifica delle OTP al momento della chiamata e per la comunicazione dell'esito della transazione.
Nella chiamata alla pagina di pagamento (fase I), l'esercente dovrà utilizzare una OTP prelevata dal file <*ShopLogin*>.**ric** e cancellare tale password dal file. GestPay verifica che l'OTP inviata sia presente nel file associato allo ShopLogin.
In caso positivo, la chiamata viene autenticata ed il processo di pagamento può continuare.
In caso negativo, la pagina di pagamento non viene visualizzata all'acquirente e GestPay restituisce un esito negativo all'esercente. In questa situazione, GestPay non utilizza una OTP prelevata dal file **.ris** associato all'esercente (per non disallineare i file di OTP) per cui il parametro PAY1_OTP sarà vuoto.
La chiamata a GestPay non deve essere effettuata utilizzando la pagina residente nella cache del browser del cliente per evitare che venga riutilizzata una password già cancellata e quindi la chiamata sia rifiutata.

Nella comunicazione dell'esito della transazione (fase II), GestPay utilizza una OTP prelevata dal file <*ShopLogin*>.**ris**. La stessa OTP viene utilizzata sia nella risposta server to server che nella risposta inviata utilizzando il browser dell'acquirente. L'esercente dovrà controllare che la password inviata da GestPay sia presente nel file

<*ShopLogin*>.**ris** in suo possesso e, in caso negativo, non considerare attendibile l'esito inviato (GestPay non è stato autenticato da una OTP corretta).
Se l'OTP inviata è corretta, l'esercente dovrà cancellarla dal file <*ShopLogin*>.**ris** solo quando riceverà l'esito dal browser del cliente.
Le password contenute nei file sono in formato testo e sono composte da 32 caratteri alfanumerici. L'ordine in cui sono inserite non ha alcuna importanza ma, ai fini del processo di autenticazione, è sufficiente che la OTP sia presente nel file.

4.1 Generazione Set di OTP

Per generare un nuovo set di OTP è sufficiente effettuare le seguenti operazioni:

Accedere all'ambiente di Back Office

https://ecomm.sella.it/gestpay/

per codici di test

https://testecomm.sella.it/gestpay/

Una volta entrati nel Back Office,è necessario seguire il seguente percorso di menu :
Configurazione cliente > OTP
Si aprira' una nuova pagina da cui sara' possibile generare nuovi file di OTP in tre semplici passi:

1. Cliccare sul pulsante "RICHIESTA": verra' visualizzato un menu' a tendina dove impostare il numero di OTP desiderato (da un minimo di 10 ad un massimo di 15.000) e cliccare poi su "OK". Il sistema procedera' dunque a generare le OTP comunicando via e-mail, all'indirizzo specificato nella sezione configurazione/risposte/e-mail informazioni, che le OTP richieste sono state generate correttamente e quindi scaricabili
.
2. Cliccare sul pulsante "DOWNLOAD": verra' effettuato lo scaricamento dei file contenenti le OTP e sara' visualizzata una pagina che indichera' la data dell'operazione e il numero di OTP richieste. Le OTP appena generate dovranno essere aggiunte a quelle gia' in Suo possesso non ancora utilizzate, ma potranno essere utilizzate per la chiamata alla pagina di pagamento soltanto dopo la loro attivazione.

3. Cliccare sul pulsante "ATTIVAZIONE": verranno attivate le OTP generate e sara' visualizzata una pagina che indichera' la data dell'operazione e il numero di OTP attivate. Da questo momento le OTP saranno attive e dunque riconosciute da Gestpay al momento della chiamata alla pagina di pagamento.

5 Struttura dati transazione di pagamento

Una transazione è caratterizzata da una serie di informazioni che devono essere comunicate a GestPay per effettuare il processo di pagamento e da informazioni restituite dal sistema come esito della transazione.
L'esercente può definire, configurando opportunamente il profilo tramite l'ambiente di back office, con quale modalità e quali informazioni inviare o ricevere da GestPay.

5.1 Dati transazione da inviare a GestPay

Alcune delle informazioni da comunicare a GestPay sono obbligatorie per eseguire il processo di pagamento mentre altre possono essere omesse senza pregiudicare l'elaborazione della transazione. L'esercente, tramite l'ambiente di back office di GestPay, può definire quali informazioni sono obbligatorie e quali invece sono facoltative.
Alcune informazioni, essenziali dal punto di vista del processo di pagamento, sono impostate come obbligatorie da GestPay e non è possibile modificare quest'attributo.
La tabella seguente riporta le informazioni che devono essere comunicate a GestPay per effettuare una transazione.

Nome	Formato	Tipo	O/F	Descrizione
CustomInfo [(1)]	VarChar (1000)	P	F	Stringa che contiene informazioni specifiche come configurato nel profilo dell'esercente
PAY1_AMOUNT	Num (9)	P	O	Importo della transazione. Il separatore delle migliaia non deve essere inserito. I decimali (max 2 cifre) sono opzionali ed il separatore è il punto. (vedi esempi)
PAY1_CARDNUMBER	VarChar (20)	I/P	O	Numero carta di credito
PAY1_CHEMAIL	VarChar (50)	I/P	F	Indirizzo e-mail dell'acquirente
PAY1_CHNAME	VarChar (50)	I/P	F	Nome e cognome dell'acquirente
PAY1_EXPMONTH	Char (2)	I/P	O	Mese di scadenza carta di credito (01, 02...12)
PAY1_EXPYEAR	Char (2)	I/P	O	Anno di scadenza carta di credito (01, 02...99)
PAY1_IDLANGUAGE	Num (2)	P	F	Codice che identifica la lingua utilizzata nella comunicazione con l'acquirente (vedi tabella **Codici lingua**).
PAY1_OTP	Char (32)	P	O	OTP ric
PAY1_SHOPTRANSACTIONID	VarChar (50)	P	O	Identificativo attribuito alla transazione dall'esercente.
PAY1_UICCODE	Num (3)	P	O	Codice che identifica la divisa in cui è denominato l'importo della transazione (vedi tabella **Codici divisa**)
ShopLogin	VarChar (30)	P	O	ShopLogin

[1] Ogni singolo campo può essere al massimo lungo 300 caratteri

La colonna **Nome** riporta l'identificativo con il quale una specifica informazione viene comunicata a GestPay. I nomi dei parametri devono essere considerati delle sequenze di caratteri riservate a GestPay.
La colonna **Formato** evidenzia se il valore dell'informazione è di tipo numerico o alfanumerico.
La colonna **Tipo** specifica se l'informazione deve essere comunicata nella chiamata alla pagina di pagamento (passata come **P**arametro) oppure se può essere inserita dall'acquirente (passata come **I**nput) nella pagina di pagamento.
La colonna **O/F** specifica se l'informazione è **O**bbligatoria (in caso di omissione non è possibile elaborare la transazione) o **F**acoltativa.
In ogni caso, il set minimo di informazioni che permette la visualizzazione della pagina di pagamento è composto da:

- Divisa (PAY1_UICCODE)
- Importo (PAY1_AMOUNT)
- ShopTransactionID (PAY1_SHOPTRANSACTIONID)
- One Time Password (PAY1_OTP)

Tali informazioni, infatti, sono definite come obbligatorie e devono essere comunicate a GestPay come parametri nella chiamata alla pagina di pagamento.
Il separatore tra informazioni logicamente differenti è la sequenza di caratteri riservata ***P1***
Durante la fase I, GestPay effettua dei controlli di validazione sulle informazioni che costituiscono la transazione di pagamento verificando la coerenza con le impostazioni del profilo esercente. In caso di anomalie, la transazione viene abbandonata restituendo un errore specifico.

CustomInfo sono informazioni personalizzate che l'esercente intende comunicare o ricevere da GestPay. La definizione di quali informazioni e con che nomi sono identificate è realizzata nell'ambiente di back office nella sezione Campi & Parametri.
Le informazioni (inserite nel parametro b della chiamata alla pagina di pagamento) dovranno seguire il seguente formalismo:

dato*1*=valore*1P1**dato2*=valore*2**P1*…*P1*dato*n*=valore*n***

Il separatore tra informazioni è la sequenza di caratteri riservata ***P1*** (come per le informazioni riconosciute da GestPay).

Altri caratteri da non utilizzare all'interno dei valori dei parametri codificati da GestPay e nelle informazioni personalizzate sono :

&	**(spazio)**	**§**	**(**	**)**	*****
<	**>**	**,**	**;**	**:**	***P1***
/	**[**	**]**	**?**	**=**	**--**
/*	**%**	**//**			

5.2 Dati transazione ricevuti da GestPay

L'esito della transazione di pagamento viene comunicato all'esercente tramite una stringa dati che contiene una serie di informazioni restituite da GestPay.
La tabella seguente riporta le informazioni che vengono restituite da GestPay come esito della transazione.

Nome	Formato	Tipo	O/F	Descrizione
CustomInfo [1]	VarChar (1000)	P	F	Stringa che contiene informazioni specifiche come configurato nel profilo dell'esercente
PAY1_ALERTCODE	Num (9)	P	F	Codice alert
PAY1_ALERTDESCRIPTION	VarChar (255)	P	F	Descrizione alert in lingua
PAY1_AMOUNT	Num (9)	P	O	Importo della transazione. Il separatore delle migliaia non è inserito. I decimali (max 2 cifre) sono opzionali ed il separatore è il punto. (vedi esempi)
PAY1_AUTHORIZATIONCODE	VarChar (6)	P	O	Codice di autorizzazione della transazione
PAY1_BANKTRANSACTIONID	Num (9)	P	O	Identificativo attribuito alla transazione da GestPay
PAY1_COUNTRY	VarChar (30)	P	F	Nazionalità istituto che ha emesso la carta di credito utilizzata per la transazione
PAY1_CHEMAIL	VarChar (50)	P	F	Indirizzo e-mail dell'acquirente
PAY1_CHNAME	VarChar (20)	P	F	Nome e cognome dell'acquirente
PAY1_ERRORCODE	Num (9)	P	O	Codice d'errore
PAY1_ERRORDESCRIPTION	VarChar (255)	P	O	Descrizione dell'errore
PAY1_OTP	Char (32)	P	O	OTP ris
PAY1_SHOPTRANSACTIONID	VarChar (50)	P	O	Identificativo attribuito alla transazione dall'esercente.
PAY1_TRANSACTIONRESULT	Char (2)	P	O	Esito transazione
PAY1_UICCODE	Num (3)	P	O	Codice che identifica la divisa in cui è denominato l'importo della transazione (vedi tabella **Codici divisa**)
PAY1_VBV	VarChar (50)	P	F	Flag per transazioni Verified by Visa (vedi tabella **Codici VbV**)
ShopLogin	VarChar (30)	P	O	ShopLogin
PAY1_3DLevel	VarChar(255)	P	F	Livello di autenticazione in caso di transazione Visa VBV / Mastercard Secudecode. La stringa potrà assumere valore FULL o HALF

[1] Ogni singolo campo può essere al massimo lungo 300 caratteri

Il set minimo di informazioni che riportano l'esito della transazione (definite obbligatorie) è composto da:

- Divisa (PAY1_UICCODE)
- Importo (PAY1_AMOUNT)
- Shop Transaction ID (PAY1_SHOPTRANSACTIONID)
- One Time Password (PAY1_OTP)
- Esito transazione (PAY1_TRANSACTIONRESULT)
- Codice d'autorizzazione (PAY1_AUTHORIZATIONCODE)
- Codice d'errore (PAY1_ERRORCODE)
- Descrizione errore (PAY1_ERRORDESCRIPTION)
- Bank Transaction ID (PAY1_BANKTRANSACTIONID)

Altre informazioni sono definite facoltative e verranno restituite in funzione delle impostazioni del profilo esercente effettuate tramite il back office di GestPay.
E' possibile interpretare l'esito di una transazione verificando il valore del parametro PAY1_TRANSACTIONRESULT.
I valori possibili sono:

PAY1_TRANSACTIONRESULT	Descrizione
OK	Esito transazione positivo
KO	Esito transazione negativo
XX	Esito transazione sospeso (solo in caso di pagamento con bonifico)

6 Profilo esercente

Ogni esercente ha la possibilità di configurare il profilo accedendo all'ambiente di back office di GestPay raggiungibile all'indirizzo

https://ecomm.sella.it/gestpay/login.asp

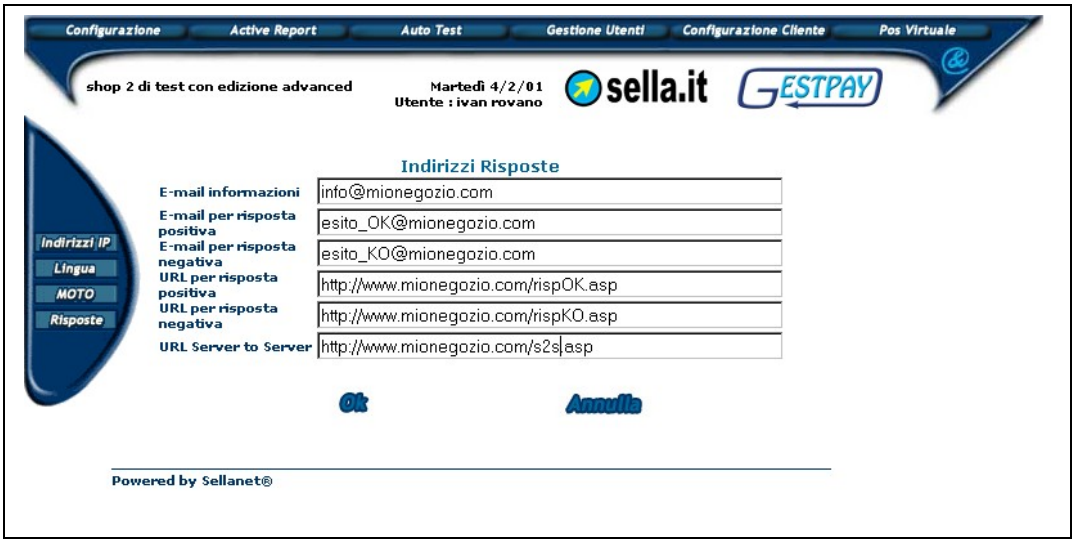
per codici di test

https://testecomm.sella.it/gestpay/login.asp

Alcune impostazioni riguardano la modalità e le informazioni che devono essere inviate o che saranno restituite da GestPay.

6.1 Configurazione url di risposta ed e-mail

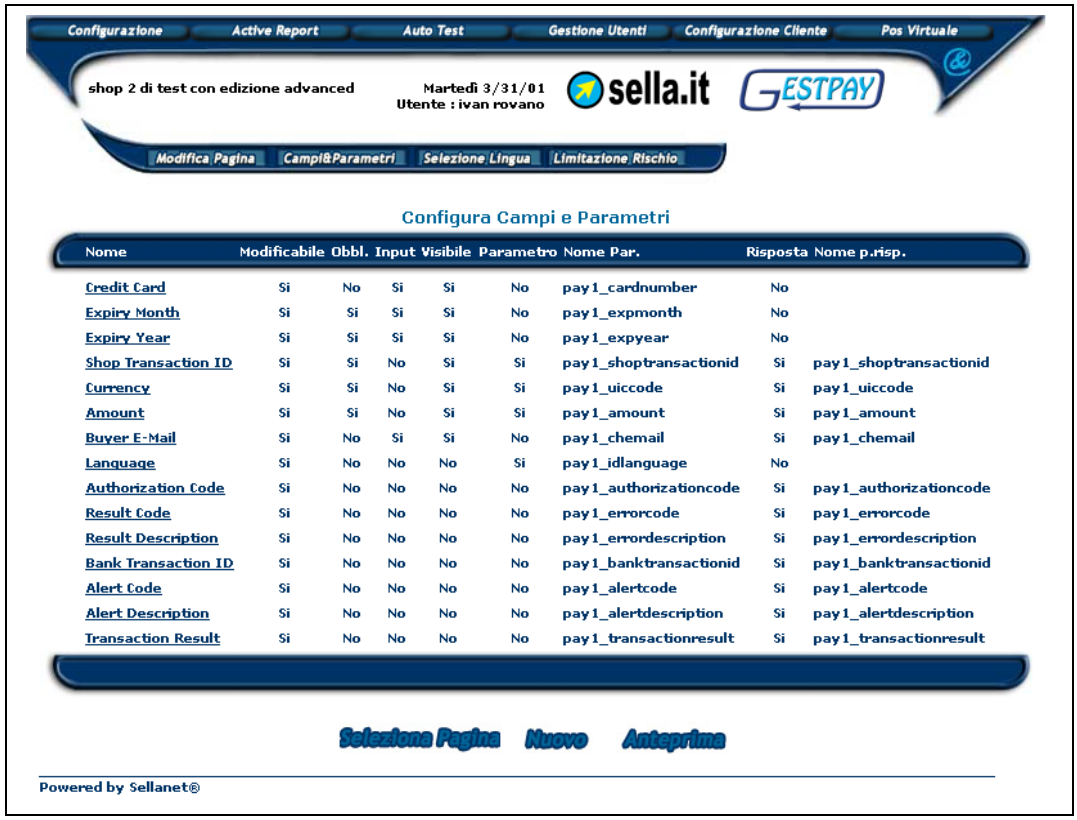
GestPay notifica l'esito della transazione con una chiamata server to server alla pagina opportunamente predisposta dall'esercente e indirizzando il browser dell'acquirente alle pagine predisposte dall'esercente (pagine differenti nel caso di esito positivo o negativo).
Nella sezione **Configurazione – Risposte** dell'ambiente di back office è possibile specificare le url utilizzate dal sistema per notificare l'esito della transazione.
In questa sezione è inoltre possibile specificare gli indirizzi che saranno utilizzati per le notifiche effettuate via e-mail.



Configurazione – Risposte

6.2 Configurazione Campi & Parametri

L'esercente può definire la struttura della transazione (specificando quali informazioni, oltre a quelle obbligatorie, dovranno essere inviate a GestPay) configurando nell'ambiente di back office quali informazioni inviare nella fase I e quali debbano essere restituite al momento della comunicazione dell'esito della transazione (fase II).
Questo sistema permette all'esercente di personalizzare la struttura della transazione con informazioni proprietarie che saranno memorizzate negli archivi di GestPay e permetteranno di identificare la singola transazione utilizzando chiavi di ricerca personalizzate. Inoltre le informazioni personalizzate potranno essere restituite con la comunicazione dell'esito della transazione permettendo al sistema informativo dell'esercente di gestire in modo opportuno queste informazioni.



Configurazione profilo esercente – Campi & Parametri

7 Requisiti software

I requisiti software richiesti da GestPay riguardano il browser dell'acquirente ed il server che ospita il negozio virtuale.

7.1 Requisiti browser dell'acquirente

Al dominio https://ecomm.sella.it/gestpay/ è associato un certificato digitale Verisign a 128 bit. I browser dovranno essere compatibili con questo livello di crittografia.
Le versioni minime consigliate sono Internet Explorer 4.0 e Netscape 4.76
Il browser del cliente deve essere impostato per accettare i cookie.

7.2 Requisiti server esercente

Il server che ospita il negozio virtuale non deve non deve possedere particolari requisiti.
Solo se l'esercente decide di inoltrare direttamente a GestPay il numero di carta di credito dell'acquirente, dovrà realizzare un sito protetto da certificato digitale (i dati sensibili dell'acquirente devono essere protetti quando comunicati via internet). Questa situazione è tipica di esercenti che possiedono anagrafiche clienti comprensive del numero di carta di credito o che decidono di acquisirlo direttamente sul proprio sito.

8 Transazioni d'esempio

In questo capitolo verranno descritti alcuni esempi di interfacciamento a GestPay considerati particolarmente significativi.
Lo ShopLogin d'esempio è 9000001.
Il profilo esercente è il seguente:

Profilo esercente	
Url comunicazione server to server	http://www.mionegozio.com/s2s.asp
Url per risposte positive	http://www.mionegozio.com/rispOK.asp
Url per risposte negative	http://www.mionegozio.com/rispKO.asp
E-mail per invio esito OK	esito_OK@mionegozio.com
E-mail per invio esito KO	esito_KO@mionegozio.com
E-mail per invio informazioni	info@mionegozio.com

8.1 Transazione numero 1

L'esercente decide di comunicare a GestPay solo le informazioni indispensabili per permettere all'acquirente di effettuare il pagamento. La pagina di pagamento dovrà essere visualizzata all'acquirente che inserirà in modalità protetta (SSL 128 bit) i dati sensibili necessari a completare il pagamento.
La transazione da processare ha le seguenti caratteristiche:

Transazione esercente	
Shop Transaction ID	34az85ord19
Importo transazione	15.25
OTP ric	34gJkui8326Fbs08uwe6387hlmKasfr8
Divisa transazione	euro

Si suppone che la transazione si concluderà positivamente (il pagamento verrà effettuato) riportando l'esito seguente:

Esito	
Codice di autorizzazione	54e813
Bank transaction ID	216
OTP ris	Osyu2AsbKs3vO7EVXt56cthauuy2IEiO

Nelle pagine seguenti saranno descritte le singole fasi che compongono il processo di pagamento evidenziando le informazioni scambiate tra GestPay e il server dell'esercente.

Fase I

Il browser dell'acquirente verrà indirizzato sul server di GestPay per completare il processo di pagamento. La chiamata alla pagina di pagamento dovrà essere effettuata passando due parametri che corrispondono allo ShopLogin e alla stringa dati composta dai parametri della transazione:

Chiamata pagina di pagamento

https://ecomm.sella.it/gestpay/pagam.asp?
a=9000001&b=**PAY1_UICCODE**=242***P1***PAY1_AMOUNT**=15.25***P1***PAY1_SHOPTRANSACTIONID**=34az85ord19***P1***PAY1_OTP**=34gJkui8326Fbs08uwe6387hlmKasfr8

GestPay effettuerà controlli di verifica sullo ShopLogin (parametro a) e di integrità sulla stringa dati (parametro b). Se i controlli vengono superati, la pagina di pagamento sarà visualizzata all'acquirente che potrà inserire i dati necessari a completare il pagamento. In caso contrario verrà comunicato un errore.

Fase II

Dopo aver elaborato la transazione, GestPay comunica l'esito della transazione all'esercente.

Comunicazione server to server

http://www.mionegozio.com/s2s.asp?
a=9000001&b=**PAY1_UICCODE**=242***P1***PAY1_AMOUNT**=15.25***P1***PAY1_SHOPTRANSACTIONID**=34az85ord19***P1***PAY1_OTP**=Osyu2AsbKs3vO7EVXt56cthauuy2lEiO***P1***PAY1_TRANSACTIONRESULT**=OK***P1***PAY1_AUTHORIZATIONCODE**=54e813***P1***PAY1_BANKTRANSACTIONID**=216***P1***PAY1_ERRORCODE**=0***P1***PAY1_ERRORDESCRIPTION**=Transazione%20eseguita

GestPay indirizzerà il browser dell'acquirente sul server dell'esercente (in questo caso all'url di risposta positiva) comunicando la stessa stringa esito.

Redirect client acquirente

http://www.mionegozio.com/rispOK.asp?
a=9000001&b=**PAY1_UICCODE**=242***P1***PAY1_AMOUNT**=15.25***P1***PAY1_SHOPTRANSACTIONID**=34az85ord19***P1***PAY1_OTP**=
Osyu2AsbKs3vO7EVXt56cthauuy2lEiO***P1***PAY1_TRANSACTIONRESULT**=OK***P1***PAY1_AUTHORIZATIONCODE**=54e813***P1***PAY1_BANKTRANSACTIONID**=216***P1***PAY1_ERRORCODE**=0***P1***PAY1_ERRORDESCRIPTION**=Transazione
%20eseguita

L'esito della transazione viene inoltre notificato all'esercente via e-mail

Invio e-mail

esito_OK@mionegozio.com

8.2 Transazione numero 2

L'esercente decide di acquisire sul proprio sito tutte le informazioni necessarie ad effettuare un pagamento (anche le informazioni che l'acquirente nel caso precedente avrebbe digitato sulla pagina di pagamento visualizzata da GestPay).
Un prerequisito indispensabile per poter acquisire direttamente i dati sensibili dell'acquirente è quello di avere un server sicuro (un sito protetto da un certificato digitale).

La transazione da processare ha le seguenti caratteristiche:

Transazione	
Shop Transaction ID	Or784sR71
Importo transazione	10.25
OTP ric	34gJkui8326Fbs08uwe6387hlmKasfr8
Divisa transazione	lire
Numero carta di credito	4321432143214321
Mese di scadenza	12
Anno di scadenza	01
Nome e cognome acquirente	Paolo Rossi
Indirizzo e-mail acquirente	paolo.rossi@isp.it

In questo caso si suppone che la transazione non si concluderà positivamente (il pagamento non verrà effettuato poiché la carta risulta inesistente). L'esito comunicato da GestPay è il seguente:

Esito	
Bank transaction ID	3861
OTP ris	9ljds548yyH23d7thGs43ug122y6w6ur
Codice d'errore	1024
Descrizione errore	Carta non riconosciuta

Nelle pagine seguenti saranno descritte le singole fasi che compongono il processo di pagamento evidenziando le informazioni scambiate tra GestPay e il server dell'esercente.

Fase I

Il browser dell'acquirente verrà indirizzato sul server di GestPay per completare il processo di pagamento. La chiamata alla pagina di pagamento dovrà essere effettuata passando due parametri che corrispondono allo ShopLogin e alla stringa dati composta dai parametri della transazione:

Chiamata pagina di pagamento

```
https://ecomm.sella.it/gestpay/pagam.asp?
a=9000001&b=PAY1_UICCODE=242*P1*PAY1_AMOUNT=10.25*P1*PAY1_SHOPT
RANSACTIONID=Or784sR71*P1*PAY1_OTP=34gJkui8326Fbs08uwe6387hlmKasfr
8*P1*PAY1_CARDNUMBER=4321432143214321*P1*PAY1_EXPMONTH=12*P1*P
AY1_EXPYEAR=01*P1*PAY1_CHNAME=Paolo
%20Rossi*P1*PAY1_CHEMAIL=paolo.rossi@isp.it
```

GestPay effettuerà controlli di verifica sullo ShopLogin (parametro a) e di integrità sulla stringa dati (parametro b). Se i controlli vengono superati, la pagina di pagamento non sarà visualizzata all'acquirente (i dati necessari per completare la transazione sono già disponibili) ma si procede direttamente all'elaborazione della transazione senza visualizzare nulla all'acquirente. In caso contrario verrà comunicato un errore.

Fase II

Dopo aver elaborato la transazione, GestPay comunica l'esito della transazione all'esercente.

Comunicazione server to server

http://www.mionegozio.com/s2s.asp?
a=9000001&b=**PAY1_UICCODE**=242***P1***PAY1_AMOUNT**=10.25***P1***PAY1_SHOPTRANSACTIONID**=Or784sR71***P1***PAY1_OTP**=9ljds548yyH23d7thGs43ug122y6w6ur***P1***PAY1_TRANSACTIONRESULT**=KO***P1***PAY1_AUTHORIZATIONCODE**=***P1***PAY1_BANKTRANSACTIONID**=3861***P1***PAY1_ERRORCODE**=1024***P1***PAY1_ERRORDESCRIPTION**=Carta%20non%20riconosciuta

GestPay indirizzerà il browser dell'acquirente sul server dell'esercente (in questo caso all'url di risposta negativa) comunicando la stessa stringa esito.

Redirect client acquirente

http://www.mionegozio.com/ rispKO.asp?
a=9000001&b=**PAY1_UICCODE**=242***P1***PAY1_AMOUNT**=10.25***P1***PAY1_SHOPTRANSACTIONID**=Or784sR71***P1***PAY1_OTP**=9ljds548yyH23d7thGs43ug122y6w6ur***P1***PAY1_TRANSACTIONRESULT**=KO***P1***PAY1_AUTHORIZATIONCODE**=***P1***PAY1_BANKTRANSACTIONID**=3861***P1***PAY1_ERRORCODE**=1024***P1***PAY1_ERRORDESCRIPTION**= Carta%20non%20riconosciuta

L'esito della transazione viene inoltre notificato via e-mail all'esercente e all'acquirente

Invio e-mail

esito_KO@mionegozio.com
paolo.rossi@isp.it

8.3 Transazione numero 3

L'esercente decide di comunicare a GestPay, oltre alle informazioni indispensabili per permettere all'acquirente di effettuare il pagamento, anche il nome, il cognome e l'indirizzo e-mail (queste informazioni saranno proposte come default nella pagina di pagamento per evitare che l'acquirente le debba inserire una seconda volta).
Altre informazioni personalizzate saranno inviate dall'esercente (il codice cliente attribuito all'acquirente e un'informazione tecnica). La pagina di pagamento dovrà essere visualizzata all'acquirente che inserirà in modalità protetta (SSL 128 bit) i dati sensibili necessari a completare il pagamento. Nella pagina di pagamento, inoltre, dovrà essere visualizzata una delle informazioni personalizzate (il codice cliente).
La transazione da processare ha le seguenti caratteristiche:

Transazione	
Shop Transaction ID	34az85ord19
Importo transazione	25.78
OTP ric	34gJkui8326Fbs08uwe6387hlmKasfr8
Divisa transazione	euro
Lingua comunicazione	spagnolo
Nome e cognome acquirente	Mario Bianchi
Indirizzo e-mail acquirente	mario.bianchi@isp.it
Info personalizzata 1	BV_CODCLIENTE=12
Info personalizzata 2	BV_SESSIONID=398

In questo caso si suppone che la transazione si concluderà positivamente (il pagamento verrà effettuato) riportando l'esito seguente:

Esito	
Codice di autorizzazione	9823y5
Bank transaction ID	860
OTP ris	9ljds548yyH23d7thGs43ug122y6w6ur

Nelle pagine seguenti saranno descritte le singole fasi che compongono il processo di pagamento evidenziando le informazioni scambiate tra GestPay e il server dell'esercente.

Fase I

Il browser dell'acquirente verrà indirizzato sul server di GestPay per completare il processo di pagamento. La chiamata alla pagina di pagamento dovrà essere effettuata passando due parametri che corrispondono allo ShopLogin e alla stringa dati cifrata ricevuta nella fase precedente da GestPay:

Chiamata pagina di pagamento
https://ecomm.sella.it/gestpay/pagam.asp? a=9000001&b=**PAY1_UICCODE**=242***P1***PAY1_AMOUNT**=25.78***P1***PAY1_SHOPTRANSACTIONID**=34az85ord19***P1***PAY1_OTP**=34gJkui8326Fbs08uwe6387hlmKasfr8***P1***PAY1_IDLANGUAGE**=3***P1***PAY1_CHNAME**=Mario%20Bianchi***P1***PAY1_CHEMAIL**=mario.bianchi@isp.it***P1***BV_CODCLIENTE**=12***P1***BV_SESSIONID**=398

GestPay effettuerà controlli di verifica sullo ShopLogin (parametro a) e di integrità sulla stringa dati cifrata (parametro b). Se i controlli vengono superati, la pagina di pagamento sarà visualizzata all'acquirente che potrà inserire i dati necessari a completare il pagamento. In caso contrario verrà comunicato un errore.

Fase II

Dopo aver elaborato la transazione, GestPay comunica l'esito della transazione (una stringa dati cifrata) all'esercente.

Comunicazione server to server
http://www.mionegozio.com/s2s.asp? **a**=9000001&**b**=**PAY1_UICCODE**=242***P1***PAY1_AMOUNT**=25.78***P1***PAY1_SHOPTRANSACTIONID**=34az85ord19***P1***PAY1_OTP**=9ljds548yyH23d7thGs43ug122y6w6ur***P1***PAY1_TRANSACTIONRESULT**=OK***P1***PAY1_AUTHORIZATIONCODE**=9823y5***P1***PAY1_BANKTRANSACTIONID**=860***P1***PAY1_ERRORCODE**=0***P1***PAY1_ERRORDESCRIPTION**=Transazione %20eseguita***P1***BV_CODCLIENTE**=12***P1***BV_SESSIONID**=398

GestPay indirizzerà il browser dell'acquirente sul server dell'esercente (in questo caso all'url di risposta positiva) comunicando la stessa stringa esito.

Redirect client acquirente
http://www.mionegozio.com/ rispOK.asp? **a**=9000001&**b**=**PAY1_UICCODE**=242***P1***PAY1_AMOUNT**=25.78***P1***PAY1_SHOPTRANSACTIONID**=34az85ord19***P1***PAY1_OTP**=9ljds548yyH23d7thGs43ug122y6w6ur***P1***PAY1_TRANSACTIONRESULT**=OK***P1***PAY1_AUTHORIZATIONCODE**=9823y5***P1***PAY1_BANKTRANSACTIONID**=860***P1***PAY1_ERRORCODE**=0***P1***PAY1_ERRORDESCRIPTION**=Transazione %20eseguita***P1***BV_CODCLIENTE**=12***P1***BV_SESSIONID**=398

L'esito della transazione viene inoltre notificato via e-mail all'esercente e all'acquirente

Invio e-mail
esito_OK@mionegozio.com
mario.bianchi@isp.it

9 Esempi di implementazione

In questo capitolo verrà descritto un esempio di interfacciamento a GestPay realizzato utilizzando il linguaggio HTML.

Esempio in HTML

PAGINA PER LA CONNESSIONE ALLA PAGINA DI PAGAMENTO (RICHIESTA DI PAGAMENTO)

```
<form action="https://ecomm.sella.it/gestpay/pagam.asp">
<input type="hidden" name="a" value="9000001">
<input type="hidden" name="b" value="PAY1_AMOUNT=15.25...">
</form>
```

10 Tabella errori

Codice	Descrizione
0	Transazione correttamente effettuata
57	Carta bloccata
58	Importo conferma superiore ad importo autorizzato
63	Richiesta di movimentare una autorizzazione inesistente
64	Preautorizzazione scaduta
65	Divisa non corretta
66	Preautorizzazione già notificata
74	Autorizzazione negata
97	Autorizzazione negata
100	Transazione interrotta dal sistema autorizzativo della banca
150	Configurazione esercente errata in sistema autorizzativo banca
208	Data carta errata
212	Sistema autorizzativo banca non disponibile
251	Disponibilità carta non sufficiente
810	Sistema autorizzativo banca non disponibile
811	Configurazione esercente errata in sistema autorizzativo banca
901	Autorizzazione negata
902	Autorizzazione negata
903	Autorizzazione negata
904	Autorizzazione negata
905	Autorizzazione negata
906	Autorizzazione negata
907	Autorizzazione negata
908	Autorizzazione negata
910	Autorizzazione negata
911	Autorizzazione negata
913	Autorizzazione negata
914	Autorizzazione negata
915	Autorizzazione negata
916	Autorizzazione negata
917	Autorizzazione negata
918	Autorizzazione negata
919	Autorizzazione negata
920	Autorizzazione negata
950	Carta non abilitata
951	Configurazione esercente errata in sistema autorizzativo banca
998	Carta di credito con Check-digit errato
999	Operazione non effettuata
1100	Stringa di parametri vuota
1101	Formato non valido della stringa di parametri
1102	Simbolo = non preceduto da nome parametro
1103	La stringa di parametri termina con un separatore
1104	Nome parametro non valido

Codice	Descrizione
1105	Valore parametro non valido
1106	Nome parametro ripetuto
1107	Nome parametro non previsto. Verificare la configurazione "Campi e Parametri" nel Back Office.
1108	Parametro obbligatorio non valorizzato
1109	Parametro mancante
1110	Parametro PAY1_UICCODE non presente
1111	Codice divisa non valido
1112	Parametro PAY1_AMOUNT non presente
1113	Importo non numerico
1114	Importo con numero di decimali errato
1115	Parametro PAY1_SHOPTRANSACTIONID non presente
1116	Parametro PAY1_SHOPTRANSACTIONID troppo lungo
1117	Identificativo lingua non valido
1118	Il numero di carta contiene caratteri non numerici
1119	Lunghezza errata del numero di carta di credito
1120	Carta di credito con Check-digit errato
1121	Carta di credito di una compagnia non abilitata
1122	Anno di scadenza senza mese di scadenza
1123	Mese di scadenza senza anno di scadenza
1124	Mese di scadenza non valido
1125	Anno di scadenza non valido
1126	Data scadenza superata
1127	Indirizzo email compratore non valido
1128	Stringa di parametri troppo lunga
1129	Il valore assegnato al parametro è troppo lungo
1130	Chiamata non accettata: parametro A mancante
1131	Chiamata non accettata: negozio non riconosciuto
1132	Chiamata non accettata: il negozio non è attivo
1133	Chiamata non accettata, manca il parametro B
1134	Chiamata non accettata: parametro B vuoto
1135	Chiamata non accettata: presenti altri parametri oltre ad A e B
1136	Chiamata non accettata: la transazione non è iniziata con una chiamata al sistema di crittografia server-server
1137	Chiamata non accettata: la transazione è già stata processata precedentemente
1138	Chiamata non accettata: numero carta o scadenza carta mancanti
1139	Chiamata non accettata: il negozio non ha una pagina di pagamento pubblica
1140	Transazione abbandonata dal cliente
1141	Chiamata non accettata: stringa di parametri non accettabile
1142	Chiamata non accettata: indirizzo IP non valido
1143	Transazione abbandonata dal compratore
1144	Campo obbligatorio non valorizzato
1145	OTP invalida
1146	Importo troppo basso

Codice	Descrizione
1147	Importo troppo alto
1148	Nome del compratore non valido
1150	Valorizzare IPIN
1151	Parametri errati
1999	Errore tecnico nel colloquio con i circuiti internazionali
2000	La transazione eccede il numero massimo di operazioni nell'intervallo di tempo
2001	La transazione eccede il numero Massimo di operazioni effettuate dallo stesso utente nell'intervallo di tempo
2002	La transazione eccede l'importo massimo nell'intervallo di tempo
2003	La transazione eccede l'importo massimo pagabile dallo stesso utente nell'intervallo di tempo
2004	La transazione contiene un valore dichiarato come non accettabile
2005	La transazione è stata abbandonata in quanto duplicato di una effettuata precedentemente
2006	Lunghezza linea errata
2007	Campo SHOPTRANSACTIONID non correttamente valorizzato
2008	Campo DIVISA non correttamente valorizzato
2009	Campo IMPORTO non correttamente valorizzato
2010	Campo DATA AUTORIZZAZIONE non correttamente valorizzato
2011	Transazione non esistente
2012	Transazione non univoca
2013	Il file contiene più di una riga relativa alla stessa transazione
2014	Avete richiesto uno storno per un importo eccedente la disponibilità residua della transazione
2015	Campo BANKTRANSACTIONID non correttamente valorizzato
2016	Campi BANKTRANSACTIONID e SHOPTRANSACTIONID non valorizzati
2017	Transazione non cancellabile
2018	Transazione non stornabile
2019	Transazione non movimentabile
2020	Transazione non annullabile
7401	Autorizzazione negata dai circuiti
7402	Carta non abilitata
7403	Carta non riconosciuta
7404	Carta scaduta
7405	Chiamare Ente
7406	Data carta errata
7407	Data transazione errata
7408	Errore di sistema
7409	Esercente non riconosciuto
7410	Formato invalido
7411	Importo non disponibile
7412	Non movimentata
7413	Operazione non permessa
7414	Rete non disponibile

Codice	Descrizione
7415	Ritirare carta
7416	Tentativi PIN esauriti
7417	Terminale bloccato
7418	Terminale chiuso forzatamente
7419	Transazione non permessa
7420	Transazione non autorizzata
7421	Servizio sospeso il 01/01/2002.
9997	Fase con errori
9998	Fase correttamente eseguita
9999	Errore di Sistema

Nota.
I codici di errore restituiti da GestPay sono in continuo aggiornamento.
In caso non troviate il codice di errore che la procedura Vi ha restituito Vi preghiamo di consultare la voce “Codici Errore” presente nella sezione “Help OnLine” dell’ambiente di Back Office

11 Tabella codici divisa

Il codice divisa viene gestito da GestPay tramite il parametro PAY1_UICCODE

Codice UIC	Descrizione
18	Lira italiana
242	Euro
1	Dollari
2	Sterline
71	Yen Giapponese
103	Dollaro Hong Kong
234	Real

12 Tabella codici lingua

Il codice lingua viene gestito da GestPay tramite il parametro PAY1_IDLANGUAGE.

Codice	Descrizione
1	Italiano
2	Inglese
3	Spagnolo
4	Francese
5	Tedesco

13 Tabella codici Verified by Visa

Il codice VbV viene gestito da GestPay tramite l'attributo PAY1_VBV.

Codice	Descrizione
OK	Transazione certificata VbV
KO	Transazione non certificata VbV

14 Ordini di pagamento in ambiente di Test

Vi ricordiamo che per simulare l'autorizzazione di un ordine di pagamento in ambiente di test è necessario utilizzare una carta di credito in corso di validità.
Gli importi relativi agli ordini di pagamento autorizzati verranno prenotati nel plafond della carta utilizzata e non verranno mai addebitati, consigliamo pertanto di effettuare ordini di pagamento di importi esigui in modo da non decrementare completamente il plafond della carta utilizzata per i test.

15 Links

Codici di Test (http://service.easynolo.it/download.asp)
Supporto Tecnico (http://www.easynolo.it/ecommerce/assistenza/richiedi_assistenza.jsp?p=com_42)
F.A.Q. (http://www.easynolo.it/ecommerce/assistenza/faq_ecommerce.jsp?p=com_55)
Forum (http://service.easynolo.it/forum.asp)
E-Commerce su Sella.it (https://www.sella.it/gbs/shop/ecommerce/gestpay/index.jsp)
Ambiente di **Back Office** per esercenti **effettivi**
(https://ecomm.sella.it/gestpay/backoffice/LoginGestPay.asp)
Ambiente di **Back Office** per esercenti di **test**
(https://testecomm.sella.it/gestpay/backoffice/logingestpay.asp)