

GestPay

Specifiche tecniche sicurezza con crittografia

Sommario

Informazioni documento	3
Informazioni versione	4
1 Introduzione	5
2 Architettura del sistema	6
3 Descrizione fasi del processo	8
3.1 Fase I: crittografia dati transazione	8
3.2 Fase II: chiamata pagina di pagamento	8
3.3 Fase III: comunicazione esito transazione	10
3.3.1 Risposta all'esercente	10
3.3.2 Risposta all'acquirente	10
3.4 Fase IV: decrittografia esito transazione	10
4 Autenticazione	12
5 Struttura dati transazione di pagamento	13
5.1 Dati transazione da inviare a GestPay	13
Dati transazione ricevuti da GestPay	15
6 Profilo esercente	17
6.1 Configurazione autenticazione	17
6.2 Configurazione url di risposta ed e-mail	18
6.3 Configurazione Campi & Parametri	19
7 Descrizione oggetto GestPayCrypt	20
8 Webservice	23
Istruzioni per l'utilizzo del modulo di crittografia con interfaccia WEB SERVICE ...	23
Elenco chiamate disponibili del webservice WSCryptDecrypt.	25
9 Requisiti software	27
9.1 Requisiti browser dell'acquirente	27
9.2 Requisiti server esercente	27
9.2.1 Installazione GestPayCrypt.class (Java)	27
9.2.2 Installazione GestPayCrypt.dll (COM)	28
10 Transazioni d'esempio	30
10.1 Transazione numero 1	30
10.2 Transazione numero 2	33
11 Esempi di implementazione	36
12 Tabella errori	39
13 Tabella codici divisa	43
14 Tabella codici lingua	44
15 Tabella codici Verified by Visa	45
16 Ordini di pagamento in ambiente di Test	46
17 Links	46

Informazioni documento

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

Informazioni versione

Versione	Descrizione	Data	Autore
1.0.0	Versione iniziale	15/03/2001	Sellanet
1.0.1	Gestione attributo TransactionResult	20/03/2001	Sellanet
1.0.2	Correzione elenco capitolo 2 Modifica url GestPay	22/03/2001	Sellanet
1.1.0	Revisione completa del documento	28/03/2001	Sellanet
1.1.1	Aggiornamento requisiti browser	09/04/2001	Sellanet
1.1.2	Aggiornamento requisiti Server	22/11/2001	Sellanet
1.1.3	Aggiornamento requisiti campi custom	04/03/2002	Sellanet
1.1.4	Aggiornamento Codici Errore	15/03/2002	Sellanet
1.1.5	Aggiornamento Codici Lingua	30/05/2002	Sellanet
1.1.6	Aggiornamento requisiti campi custom e parametri gestpay	20/08/2002	Sellanet
1.1.7	Aggiornamento codici valuta	27/01/2003	Sellanet
2.0.0	3D Secure	28/01/2003	Sellanet
2.0.1	Errata Corrige	20/04/2005	Easy Nolo S.p.A.
2.0.2	Introduzione del dominio specifico per i 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.
2.1	Specifiche WebService Crittografia	12/1/2010	EasyNolo S.p.a.
2.1.2	Correzione nome parametri WebService	9/7/2010	EasyNolo 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.

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 permettere a GestPay di processare in modo corretto le transazioni

Nel capitolo **Descrizione oggetto GestPayCrypt** verrà approfondito l'utilizzo del componente che si occupa di gestire la comunicazione server to server durante le fasi che prevedono questo tipo di comunicazione tra il server che ospita il negozio virtuale e GestPay.

Nel capitolo **WebService** verrà approfondito l'utilizzo del webservice che si occupa di gestire le fasi di crittografia e decrittografia in sostituzione dell'oggetto GestpayCrypt descritto sopra tra il server che ospita il negozio virtuale e GestPay.

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.

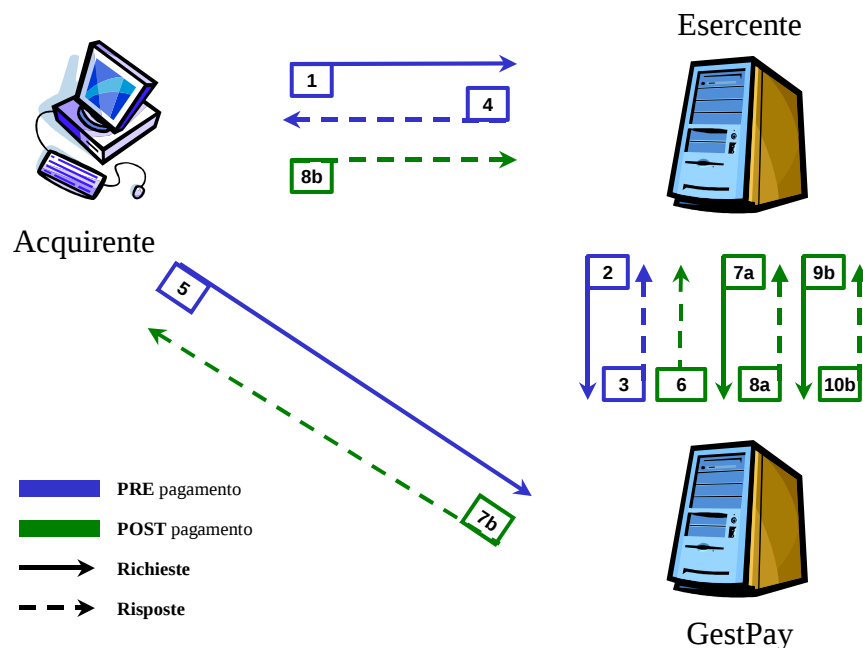
2 Architettura del sistema

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.



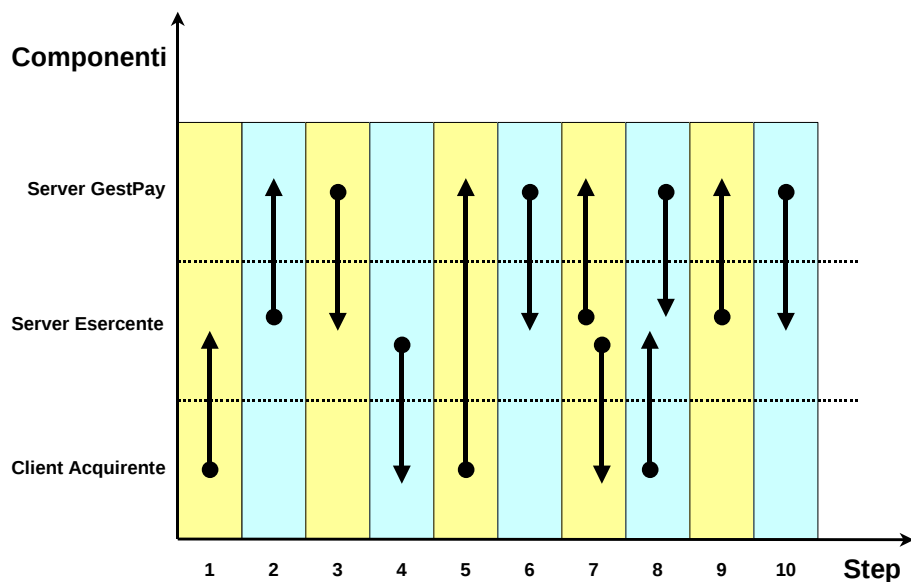
Schema architettura

- 1 L'acquirente seleziona i prodotti da acquistare e decide di procedere con il pagamento.
- 2 Il server dell'esercente contatta via internet il server di GestPay per cifrare i dati della transazione di pagamento.
- 3 GestPay effettua i controlli di autenticazione del server dell'esercente e di validazione dei dati della transazione restituendo, in caso positivo, una stringa parametri cifrata che rappresenta la transazione di pagamento che dovrà essere processata.
- 4 La stringa parametri cifrata viene comunicata al browser del cliente che viene indirizzato sul server di GestPay per completare il processo di pagamento.
- 5 Il browser dell'acquirente richiama la pagina di pagamento passando la stringa parametri cifrata ed il codice attribuito all'esercente (Shop login). Vengono effettuati i controlli 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.

- 6 GestPay comunica al server dell' esercente una stringa parametri cifrata che riporta l'esito della transazione.
- 7a Il server dell' esercente contatta via internet il server di GestPay per decifrare la stringa dati cifrata che riporta l'esito della transazione.
- 8a GestPay decifra la stringa e restituisce in chiaro i parametri che riportano l'esito della transazione.
- 7b GestPay comunica la stringa parametri cifrata che riporta l'esito della transazione al browser del cliente che viene indirizzato sul server dell' esercente.
- 8b Il browser dell' acquirente richiama la pagina di risposta realizzata dall' esercente passando la stringa parametri cifrata.
- 9b Il server dell' esercente contatta via internet il server di GestPay per decifrare la stringa dati cifrata che riporta l'esito della transazione.
- 10b GestPay decifra la stringa e restituisce in chiaro i dati che riportano l'esito della transazione permettendo all' esercente di fornire all' acquirente le indicazioni necessarie a concludere il processo di acquisto.

Lo schema seguente analizza il processo di pagamento evidenziando l'ordine cronologico i cui avvengono gli step di comunicazione. E' da notare che in alcuni casi (step 7 e 8) si instaurano comunicazioni contemporanee tra le componenti di cui si deve tener conto quando si implementano le procedure che dovranno gestire le informazioni scambiate nei vari step.



3 Descrizione fasi del processo

Una transazione di pagamento può essere scomposta in 4 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: crittografia dati transazione

Le informazioni necessarie al pagamento vengono preventivamente comunicate a GestPay per essere cifrate. Per garantire un livello di sicurezza ottimale, nessuna informazione sensibile viene comunicata in chiaro al browser dell'acquirente.

In questa fase il server dell'esercente richiede il servizio di crittografia a GestPay ottenendo la stringa cifrata che rappresenta la transazione da processare. I dati che identificano una transazione ed il loro utilizzo verrà descritto nel capitolo 4.

La crittografia può essere gestita in due modi :

Utilizzo oggetto GestPayCrypt

La comunicazione server to server viene gestita dall'oggetto GestPayCrypt rilasciato da EasyNolo e che deve essere preventivamente installato sul server dell'esercente. L'oggetto sarà richiamato dalle pagine del negozio virtuale che si occupano di gestire le informazioni necessarie al pagamento.

Utilizzo Webservice WSCryptDecrypt

L'utilizzo del webservice non richiede nessuna installazione sul server ma la semplice chiamata al webservice su protocollo https. La risposta è in formato XML.

Se i controlli di autenticazione dell'esercente e validazione dei dati della transazione i vengono superati, GestPay restituirà al server dell'esercente la stringa dati cifrata che sarà inviata al browser dell'acquirente per continuare il processo di pagamento. In caso contrario verrà restituito un codice d'errore specifico che permetterà di identificare l'anomalia riscontrata.

3.2 Fase II: chiamata pagina di pagamento

Ottenuta la stringa dati cifrata (come descritto al paragrafo precedente), il browser dell'acquirente, verrà indirizzato alla pagina di pagamento presente sul server GestPay all'indirizzo:

<https://ecommm.sella.it/gestpay/pagam.asp?a=<ShopLogin>&b=<stringa cifrata>>

per i codici di test:

<https://testecommm.sella.it/gestpay/pagam.asp?a=<ShopLogin>&b=<stringa cifrata>>

La chiamata alla pagina verrà effettuata passando due parametri:

- a** codice che identifica l'esercente (Shop login)
- b** stringa dati cifrata 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 di integrità dei

dati della transazione (il parametro b deve corrispondere alla stringa dati cifrata comunicata all'esercente nella fase precedente).

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.

3.3 Fase III: comunicazione esito transazione

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

3.3.1 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 cifrata>

La chiamata alla pagina verrà effettuata passando due parametri:

- a** codice che identifica l'esercente (Shop login)
- 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.

3.3.2 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 cifrata>

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.

3.4 Fase IV: decrittografia esito transazione

GestPay notifica l'esito della transazione mediante una stringa cifrata (parametro b della chiamata all'url predisposta dall'esercente). La stringa viene inoltrata

all' esercente una prima volta durante la comunicazione server to server e permette, una volta decifrata, di aggiornare lo stato della transazione registrata nel sistema informativo dell' esercente. La stessa stringa viene inoltre trasportata dal browser dell' acquirente al server dell' esercente e permette, una volta decifrata, di concludere il processo d' acquisto.

Le pagine web predisposte dall' esercente per la ricezione dell' esito della transazione (sia nel caso di comunicazione server to server sia tramite il browser dell' acquirente) dovranno richiamare il server di GestPay per richiedere il servizio di decrittografia ed ottenere in chiaro le informazioni che rappresentano l' esito della transazione elaborata.

La richiesta di decrittografia della stringa ricevuta puo' essere eseguita tramite:

Oggetto GestPayCrypt

La comunicazione server to server viene gestita dall' oggetto GestPayCrypt rilasciato da EasyNolo e che deve essere preventivamente installato sul server dell' esercente.

WebService WSCryptDecrypt

L' utilizzo del webservice non richiede nessuna installazione sul server

La comunicazione avviene tramite la chiamata al webservice su protocollo https e la risposta è in formato XML

4 Autenticazione

Le chiamate server to server vengono gestite da un componente rilasciato da EasyNolo.

L'autenticazione del server dell'esercente che richiede i servizi di crittografia o decrittografia viene effettuata verificando:

- ◆ **Validità Shop login:** il parametro ShopLogin deve corrispondere ad un codice censito nell'anagrafica di GestPay
- ◆ **Indirizzo IP server:** l'indirizzo IP del server chiamante deve corrispondere ad uno degli indirizzi IP configurati nel profilo esercente
- ◆ **Stato Shop login:** 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.

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
ShopLogin	VarChar (30)	P	O	Shop login
Currency	Num (3)	P	O	Codice che identifica la divisa in cui è denominato l'importo della transazione (vedi tabella Codici divisa)
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)
ShopTransactionID	VarChar (50)	P	O	Identificativo attribuito alla transazione dall'esercente.
CardNumber	VarChar (20)	I/P	O	Numero carta di credito
ExpMonth	Char (2)	I/P	O	Mese di scadenza carta di credito (01, 02...12)
ExpYear	Char (2)	I/P	O	Anno di scadenza carta di credito (01, 02...99)
BuyerName	VarChar (50)	I/P	F	Nome e cognome dell'acquirente
BuyerEmail	VarChar (50)	I/P	F	Indirizzo e-mail dell'acquirente
Language	Num (2)	P	F	Codice che identifica la lingua utilizzata nella comunicazione con l'acquirente (vedi tabella Codici lingua).
CustomInfo ⁽¹⁾	VarChar (1000)	P	F	Stringa che contiene informazioni specifiche come configurato nel profilo dell'esercente

¹ Ogni singolo campo può essere al massimo lungo 300 caratteri

La colonna **Nome** riporta l'identificativo dell'attributo con il quale una specifica informazione viene comunicata all'oggetto GestPayCrypt che si occupa della comunicazione server to server per i servizi di crittografia.

La colonna **Formato** evidenzia se il valore dell'informazione è di tipo numerico o alfanumerico. Nel caso alfanumerico viene riportato tra parentesi il numero di caratteri massimo accettato.

La colonna **Tipo** specifica se l'informazione deve essere comunicata al componente (passata come **Parametro**) oppure se può essere inserita dall'acquirente (passata come **Input**) nella pagina di pagamento.

La colonna **O/F** specifica se l'informazione è **Obbligatoria** (in caso di omissione non è possibile elaborare la transazione) o **Facoltativa**.

In ogni caso, il set minimo di informazioni che consente l'elaborazione della fase I è composto da:

- ◆ Currency
- ◆ Amount
- ◆ ShopTransactionID

Tali informazioni, infatti, sono definite come obbligatorie e devono essere comunicate a GestPay utilizzando il componente GestPayCrypt.

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. Quest'approccio permette di identificare immediatamente eventuali anomalie legate alla transazione impedendo che l'acquirente sia indirizzato alla pagina di pagamento con una stringa di dati cifrata che corrisponde ad una transazione non valida.

L'attributo CustomInfo contiene informazioni specifiche che l'esercente intende comunicare o ricevere da GestPay. La definizione di quali informazioni sono inserite nell'attributo CustomInfo è realizzata nell'ambiente di back office nella sezione campi & Parametri.

Le informazioni inserite dovranno seguire il seguente formalismo:

dato1=valore1*P1*dato2=valore2*P1*...*P1*daton=valoren

Il separatore tra informazioni logicamente differenti è la sequenza di caratteri riservata ***P1***

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

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

Dati transazione ricevuti da GestPay

L'esito della transazione di pagamento viene comunicato all'esercente tramite una stringa dati cifrata che contiene una serie di informazioni restituite da GestPay.

Utilizzando l'oggetto GestPayCrypt, l'esercente otterrà in chiaro le informazioni che riportano l'esito della transazione e potrà aggiornare il proprio sistema informativo permettendo all'acquirente di concludere il processo d'acquisto.

La tabella seguente riporta le informazioni che vengono restituite da GestPay come esito della transazione.

Nome	Formato	Tipo	O/F	Descrizione
ShopLogin	VarChar (30)	P	O	Shop login
Currency	Num (3)	P	O	Codice che identifica la divisa in cui è denominato l'importo della transazione (vedi tabella Codici divisa)
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)
ShopTransactionID	VarChar (50)	P	O	Identificativo attribuito alla transazione dall'esercente.
BuyerName	VarChar (50)	P	F	Nome e cognome dell'acquirente
BuyerEmail	VarChar (50)	P	F	Indirizzo e-mail dell'acquirente
TransactionResult	Char (2)	P	O	Esito transazione
AuthorizationCode	VarChar (6)	P	O	Codice di autorizzazione della transazione
BankTransactionID	Num (9)	P	O	Identificativo attribuito alla transazione da GestPay
Country	VarChar (30)	P	F	Nazionalità istituto che ha emesso la carta di credito utilizzata per la transazione
VbV	VarChar (50)	P	F	Flag per transazioni Verified by Visa (vedi tabella Codici VbV)
ErrorCode	Num (9)	P	O	Codice d'errore
ErrorDescription	VarChar (255)	P	O	Descrizione dell'errore
AlertCode	Num (9)	P	F	Codice alert
AlertDescription	VarChar (255)	P	F	Descrizione alert in lingua
3DLevel	VarChar(255)	P	F	Livello di autenticazione in caso di transazione Visa VbV / Mastercard Secudecode. La stringa potrà assumere valore FULL o HALF
CustomInfo ⁽¹⁾	VarChar (1000)	P	F	Stringa che contiene informazioni specifiche come configurato nel profilo dell'esercente

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:

- ◆ Currency
- ◆ Amount
- ◆ ShopTransactionID
- ◆ TransactionResult
- ◆ AuthorizationCode
- ◆ ErrorCode
- ◆ ErrorDescription

◆ 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 campo TransactionResult.

I valori possibili sono:

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://ecommm.sella.it/gestpay/login.asp>

per i codici di test

<https://testecommm.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 autenticazione

GestPay identifica l'esercente, che richiede il servizio di cifratura utilizzando il componente GestPayCrypt, confrontando l'indirizzo IP del server chiamante con gli indirizzi IP configurati nel profilo associato allo Shop login utilizzato per la chiamata. Se il server chiamante non viene riconosciuto, l'elaborazione della transazione termina e viene restituito un errore specifico.

L'esercente può inserire, nella sezione **Configurazione - Indirizzi IP** dell'ambiente di back office, fino ad un massimo di 10 indirizzi IP (nel caso le chiamate a GestPay provengano da una server farm).

The screenshot shows the 'Indirizzi IP' configuration page in the GestPay back office. The page has a blue header with navigation tabs: Configurazione, Active Report, Auto Test, Gestione Utenti, Configurazione Cliente, and Pos Virtuale. Below the header, it displays 'shop 2 di test con edizione advanced', the date 'Martedì 3/31/01', the user 'Utente : ivan rovano', and logos for 'sella.it' and 'GESTPAY'. The main section is titled 'Indirizzi IP' and contains the instruction: 'Inserimento indirizzi IP da verificare E' possibile utilizzare numeri e il carattere * per l'ultimo gruppo di numeri'. There is a table with 10 rows for entering IP addresses, each with four input fields separated by dots. The first row is pre-filled with '171', '85', '234', and '97'. To the left of the table is a sidebar with buttons for 'Indirizzi IP', 'Lingua', 'MOTO', and 'Risposte'. At the bottom of the table are 'Ok' and 'Annulla' buttons. The footer of the page says 'Powered by Sellanet'.

	1	2	3	4
1	171	85	234	97
2				
3				
4				
5				
6				
7				
8				
9				
10				

Configurazione – Indirizzi IP

6.2 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.

Indirizzi Risposte	
E-mail informazioni	info@mionegozio.com
E-mail per risposta positiva	esito_OK@mionegozio.com
E-mail per risposta negativa	esito_KO@mionegozio.com
URL per risposta positiva	http://www.mionegozio.com/rispOK.asp
URL per risposta negativa	http://www.mionegozio.com/rispKO.asp
URL Server to Server	http://www.mionegozio.com/s2s.asp

Ok Annulla

Powered by Sellanet®

Configurazione – Risposte

6.3 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.

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
Active Report
Auto Test
Gestione Utenti
Configurazione Cliente
Pos Virtuale

shop 2 di test con edizione advanced
Martedì 3/31/01
Utente : ivan rovano
sella.it
GESTPAY

Modifica Pagina
Campi&Parametri
Selezione Lingua
Limitazione Rischio

Configura Campi e Parametri

Nome	Modificabile	Obbl.	Input	Visibile	Parametro	Nome Par.	Risposta	Nome p.Risp.
<u>Credit Card</u>	Si	No	Si	Si	No	pay1_cardnumber	No	
<u>Expiry Month</u>	Si	Si	Si	Si	No	pay1_expmonth	No	
<u>Expiry Year</u>	Si	Si	Si	Si	No	pay1_expyear	No	
<u>Shop Transaction ID</u>	Si	Si	No	Si	Si	pay1_shoptransactionid	Si	pay1_shoptransactionid
<u>Currency</u>	Si	Si	No	Si	Si	pay1_uiccode	Si	pay1_uiccode
<u>Amount</u>	Si	Si	No	Si	Si	pay1_amount	Si	pay1_amount
<u>Buyer E-Mail</u>	Si	No	Si	Si	No	pay1_chemail	Si	pay1_chemail
<u>Language</u>	Si	No	No	No	Si	pay1_idlanguage	No	
<u>Authorization Code</u>	Si	No	No	No	No	pay1_authorizationcode	Si	pay1_authorizationcode
<u>Result Code</u>	Si	No	No	No	No	pay1_errorcode	Si	pay1_errorcode
<u>Result Description</u>	Si	No	No	No	No	pay1_errordescription	Si	pay1_errordescription
<u>Bank Transaction ID</u>	Si	No	No	No	No	pay1_banktransactionid	Si	pay1_banktransactionid
<u>Alert Code</u>	Si	No	No	No	No	pay1_alertcode	Si	pay1_alertcode
<u>Alert Description</u>	Si	No	No	No	No	pay1_alertdescription	Si	pay1_alertdescription
<u>Transaction Result</u>	Si	No	No	No	No	pay1_transactionresult	Si	pay1_transactionresult

Soluzione Pagina
Nuovo
Anteprima

Powered by Sellanet®

Configurazione profilo esercente – Campi & Parametri

7 Descrizione oggetto GestPayCrypt

La comunicazione server to server tra GestPay e l'esercente verrà automaticamente gestita dal componente GestPayCrypt rilasciato da EasyNolo. Tale componente è una libreria java che dovrà essere richiamata dalle pagine web predisposte dall'esercente per gestire la cifratura dei dati della transazione e la decifratura dell'esito comunicato da GestPay.

La libreria GestPayCrypt è disponibile *open source* sul sito EasyNolo.

La tabella 1 riporta gli attributi ed i metodi resi disponibili dalla libreria java.

L'esercente dovrà implementare, nella pagine del negozio virtuale che si occupano di gestire il pagamento, una chiamata al componente GestPayCrypt che si occuperà di gestire le richieste al servizio di crittografia di GestPay.

Gli attributi della classe saranno valorizzati con i dati che identificano la transazione.

Per richiedere il servizio di cifratura si dovrà richiamare il metodo Encrypt.

Se l'operazione di cifratura si è conclusa correttamente (valore dell'attributo ErrorCode = 0) la stringa dati cifrata restituita da GestPay sarà disponibile leggendo il valore dell'attributo EncryptedString. In caso contrario i valori degli attributi ErrorCode ed ErrorDescription permetteranno di identificare le cause che hanno impedito l'operazione di cifratura.

Per richiedere il servizio di decifratura si dovrà richiamare il metodo Decrypt dopo aver valorizzato gli attributi Shop login e EncryptedString con i valori comunicati da GestPay nella fase III

Le informazioni che riportano l'esito della transazione saranno disponibili leggendo gli attributi della libreria java che corrispondono alle informazioni che riguardano l'esito della transazione.

Di seguito vengono descritti gli attributi ed i metodi della libreria GestPayCrypt.

Classe: GestPayCrypt	
Attributi	
AlertCode	Codice alert
AlertDescription	Descrizione alert
Amount	Importo della transazione
AuthorizationCode	Codice di autorizzazione della transazione
BankTransactionID	Identificativo attribuito alla transazione da GestPay
BuyerEmail	Indirizzo e-mail dell'acquirente
BuyerName	Nome e cognome dell'acquirente
CardNumber	Numero carta di credito
Country	Nazionalità istituto che ha emesso la carta di credito
Currency	Codice che identifica la divisa in cui è denominato l'importo
CustomInfo	Stringa che contiene informazioni specifiche dell'esercente
CVV	Stringa contenente il valore del codice Cvv2 / Cvc2 / 4dbc della carta di credito.
EncryptedString	Stringa cifrata
Encryption	Flag per attivare la crittografia locale
ErrorCode	Codice d'errore
ErrorDescription	Descrizione dell'errore
ExpMonth	Mese di scadenza carta di credito
ExpYear	Anno di scadenza carta di credito
Language	Codice della lingua per la comunicazione con l'acquirente
MIN	Non utilizzato
PasswordEncrypt	Password per crittografia locale
ShopLogin	Shop login che identifica l'esercente
ShopTransactionID	Identificativo attribuito alla transazione dall'esercente
TransactionResult	Esito transazione
VBV	Flag per transazioni Verified by Visa
VBVrisp	Non utilizzato
3DLevel	Livello di autenticazione per transazioni Visa VBV / Mastercard Secudecode
Metodi SET	
SetAmount (val)	Utilizzato per valorizzare l'attributo Amount
SetBuyerEmail (val)	Utilizzato per valorizzare l'attributo BuyerEmail
SetBuyerName (val)	Utilizzato per valorizzare l'attributo BuyerName
SetCardNumber (val)	Utilizzato per valorizzare l'attributo CardNumber
SetCurrency (val)	Utilizzato per valorizzare l'attributo Currency
SetCustomInfo (val)	Utilizzato per valorizzare l'attributo CustomInfo
SetCVV	Utilizzato per valorizzare l'attributo Cvv
SetExpMonth (val)	Utilizzato per valorizzare l'attributo ExpMonth
SetExpYear (val)	Utilizzato per valorizzare l'attributo ExpYear
SetEncryptedString (val)	Utilizzato per valorizzare l'attributo EncryptedString
SetEncryption	Utilizzato per valorizzare l'attributo Encryption a TRUE
SetLanguage (val)	Utilizzato per valorizzare l'attributo Language
SetMIN	Non utilizzato
SetPasswordEncrypt	Utilizzato per valorizzare l'attributo PasswordEncrypt
SetShopLogin (val)	Utilizzato per valorizzare l'attributo ShopLogin
SetShopTransactionID (val)	Utilizzato per valorizzare l'attributo ShopTransactionID
SetWithoutEncryption	Utilizzato per valorizzare l'attributo Encryption a FALSE

Metodi GET

Decrypt	Utilizzato per richiedere il servizio di cifratura
Encrypt	Utilizzato per richiedere il servizio di decifratura
GetAlertCode	Utilizzato per leggere l'attributo AlertCode
GetAlertDescription	Utilizzato per leggere l'attributo AlertDescription
GetAmount	Utilizzato per leggere l'attributo Amount
GetAuthorizationCode	Utilizzato per leggere l'attributo AuthorizationCode
GetBankTransactionID	Utilizzato per leggere l'attributo BankTransactionID
GetBuyerEmail	Utilizzato per leggere l'attributo BuyerEmail
GetBuyerName	Utilizzato per leggere l'attributo BuyerName
GetCountry	Non utilizzato
GetCurrency	Utilizzato per leggere l'attributo Currency
GetCustomInfo	Utilizzato per leggere l'attributo CustomInfo
GetEncryptedString	Utilizzato per leggere l'attributo EncryptedString
GetErrorCode	Utilizzato per leggere l'attributo ErrorCode
GetErrorDescription	Utilizzato per leggere l'attributo ErrorDescription
GetShopLogin	Utilizzato per leggere l'attributo ShopLogin
GetShopTransactionID	Utilizzato per leggere l'attributo ShopTransactionID
GetTransactionResult	Utilizzato per leggere l'attributo TransactionResult
GetVBV	Utilizzato per leggere l'attributo VbV
GetVBVrisp	Non utilizzato
Get3DLevel	Utilizzato per leggere l'attributo 3DLevel

8 WebService

Istruzioni per l'utilizzo del modulo di crittografia con interfaccia WEB SERVICE

Il presente documento contiene le istruzioni necessarie per l'utilizzo del webservice **WSCryptDecrypt**.

Tale componente è una libreria che dovrà essere richiamata dalle pagine web predisposte dall'esercente per gestire la cifratura dei dati della transazione e la decifratura dell'esito comunicato da GestPay.

Il web service WSCryptDecrypt è disponibile sui server di produzione e di test e non necessita di alcuna installazione sul server dell'esercente.

L'esercente dovrà implementare, nella pagine del negozio virtuale che si occupano di gestire il pagamento, una chiamata al webservice che si occuperà di gestire le richieste al servizio di crittografia di GestPay.

Per richiedere il servizio di cifratura si dovrà richiamare il metodo **Encrypt**.

Esempio di risposta XML positiva restituita dal webservice

```
<?xml version="1.0" encoding="utf-8" ?>
<GestPayCryptDecrypt>
  <TransactionType>ENCRYPT</TransactionType>
  <TransactionResult>OK</TransactionResult>
  <CryptDecryptString>CF66F38B4EC881....</CryptDecryptstring>
  <ErrorCode>0</ErrorCode>
  <ErrorDescription />
</GestPayCryptDecrypt>
```

Se l'operazione di crittografia si è conclusa correttamente (valore TransactionResult = OK) la stringa dati cifrata restituita da GestPay sarà disponibile leggendo il valore dell'attributo CryptDecryptString.

In caso contrario i valori degli attributi ErrorCode ed ErrorDescription permetteranno di identificare le cause che hanno impedito l'operazione di cifratura.

Per richiedere il servizio di decrittografia si dovrà richiamare il metodo **Decrypt** passando gli attributi Shoplogin e EncryptedString con i valori comunicati da GestPay nella fase III.

Le informazioni che riportano l'esito della transazione saranno disponibili leggendo il file XML di risposta che corrispondono alle informazioni che riguardano l'esito della transazione.

Il webService dovrà essere richiamato dall'applicativo predisposto dall'esercente per gestire l'invio dei dati della transazione e la lettura dell'esito comunicato da GestPay in formato XML.

Indirizzo del servizio al seguente URL:

<https://ecomms2s.sella.it/gestpay/gestpayws/WSCryptDecrypt.asmx>

per codici di test

<https://testecomm.sella.it/gestpay/gestpayws/WSCryptDecrypt.asmx>

Generazione Classe Proxy per utilizzare le funzionalità del WebService da diversi linguaggi

La classe proxy nel linguaggio preferito puo' essere creata automaticamente tramite l'utilizzo in questo caso dal programma wsdl.exe (in questo caso fornito da Microsoft) semplicemente specificando il file di contratto relativo al WebService in questo caso:

Indirizzo descrizione del servizio al seguente URL

Per i codici di produzione

<https://ecomms2s.sella.it/gestpay/gestpayws/WSCryptDecrypt.asmx?WSDL>

per codici di test

<https://testecomm.sella.it/gestpay/gestpayws/WSCryptDecrypt.asmx?WSDL>

ad esempio

wsdl /language:VB /out: wss2sProxyClass.vb

<https://testecomm.sella.it/gestpay/gestpayws/WSCryptDecrypt.asmx?WSDL>

verrà generato il file .vb con la gestione della classe proxy relativa al WebService che andrà semplicemente importato nel progetto ed utilizzato

Con visual Studio .net è possibile aggiungere le reference del web service per avere automaticamente a disposizione nel progetto le classi del web service referenziato vedi "Add Web Reference" .

Per gli altri linguaggi verificare le normali operazioni di interfacciamento verso i webservice.

Elenco chiamate disponibili del webservice WSCryptDecrypt.

Di seguito è riportato l'elenco completo dei metodi dell'oggetto WSCryptDecrypt

Metodi WEBSERVICE

Nome metodo	Descrizione
Encrypt	Crittografia
Decrypt	Decrittografia

Le varie chiamate ai metodi sono gestite come chiamate a funzione al Webservice e non con il passaggio di una stringa XML.

I valori della varie chiamate devono essere passati come parametri

Parametri Input metodo Encrypt

Nome metodo	Descrizione
shopLogin	Utilizzato per valorizzare l'attributo ShopLogin
uicCode	Assegna il codice divisa
amount	Assegna importo transazione
shopTransactionId (val)	Assegna il codice attribuito dall' esercente alla transazione
cardNumber (val)	Assegna il numero di carta
expiryMonth (val)	Assegna il mese di scadenza della carta
expiryYear (val)	Assegna l'anno di scadenza della carta
buyerName (val)	Assegna il nome del compratore
buyerEmail	Assegna l'indirizzo e-mail del compratore
languageId (val)	Assegna la lingua per le mail al compratore
cvv (val)	Assegna il codice di sicurezza stampato sulla carta
customInfo (val)	Assegna una stringa contenente eventuali parametri personalizzati

Parametri Input metodo Decrypt

Nome metodo	Descrizione
shopLogin	Utilizzato per valorizzare l'attributo ShopLogin
CryptedString	Stringa da decriptare ricevuta da GestPay

Il file XML e' descritto e può essere validato tramite il relativo file GestPayCryptDecrypt.xsd che qui andiamo a descrivere nel dettaglio

Valori XML restituiti	
Nome metodo	Descrizione
TransactionType	Tipo di richiesta eseguita può assumere i seguenti valori: ENCRYPT (E) DECRYPT (D)
TransactionResult (E,D)	Restituisce l'esito della transazione con valori OK e KO
CryptDecryptString (E)	Restituisce la stringa cryptata
ShopTransactionID (D)	Restituisce il codice attribuito dall'esercente alla transazione
BankTransactionID (D)	Restituisce il codice attribuito dalla banca alla transazione
AuthorizationCode (D)	Restituisce il codice di autorizzazione
Currency (D)	Restituisce il codice della divisa
Amount (D)	Restituisce l'importo della transazione
Country (D)	Restituisce nazionalità istituto emittente la carta di credito
CustomInfo (D)	Restituisce gli eventuali parametri aggiuntivi
BuyerType (D)	Restituisce l'indirizzo nome e e-mail del compratore divisi come segue
	BuyerEmail Restituisce l'indirizzo e-mail del compratore
	BuyerName Restituisce il nome del compratore
ErrorCode (E,D)	Restituisce un codice relativo all'esito della transazione
ErrorDescription (E,D)	Restituisce la descrizione associata al valore di ErrorCode
AlertCode (D)	Restituisce il codice di violazione dei criteri di risk management
AlertDescription (D)	Restituisce la descrizione associata al valore di AlertCode

9 Requisiti software

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

9.1 Requisiti browser dell'acquirente

Al dominio <https://ecommm.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 ed abilitato all'esecuzione di script in linguaggio Javascript.

9.2 Requisiti server esercente

Verificare con l'amministratore del server che la macchina possa raggiungere:
in caso di utilizzo della tipologia di comunicazione http (porta 80) l'indirizzo

<http://ecommm.sella.it/testhttp/test.asp>

per codici di test

<http://testecommm.sella.it/testhttp/test.asp>

in caso di utilizzo della tipologia di comunicazione https (porta 443) l'indirizzo

<https://ecommm.sella.it/testhttps/test.asp>.

per codici di test

<https://testecommm.sella.it/testhttps/test.asp>

9.2.1 Installazione GestPayCrypt.class (Java)

La libreria java GestPayCrypt (GestPaycrypt.class) dovrà essere copiata nella directory del web server che contiene le librerie java.

Ad esempio in un sistema con architettura basata su Windows NT e Internet Information Sever dovrà essere installata nella directory:

.....\java\TrustLib

Sul web server che ospita le pagine web che richiamano la libreria GestPayCrypt dovrà essere installata la Java Virtual Machine (dalla versione 1.1.3 in poi).

9.2.2 Installazione GestPayCrypt.dll (COM)

L'oggetto COM può essere installato solo su ambienti Windows (NT 4.0 o superiore; MTS; Installazione IE 4.x o superiore con **Microsoft VM Java**), salvato in qualunque punto del disco e successivamente registrato con una delle seguenti operazioni:

Windows NT - 2000

- da Prompt dei comandi utilizzando il comando:

REGSVR32 path (es. c:\winnt\system32\GestPayCrypt.dll)

Nota.

Per le versioni Windows Server 2003 e Windows Xp questo metodo di registrazione è sconsigliato

- Attraverso Com+ (per Windows 2000 o superiori) o MTS (per NT 4.0)

Percorso:

Pannello di Sinistra

consolerooot /Microsoft transaction server/Computer/MyComputer (o altro nome della macchina)/ Packages Installed

Tasto destro > Creare un nuovo pacchetto (attenzione a non utilizzare Interactive User, ma assegnare un account con diritti sul sistema per il pacchetto)

Aprire il pacchetto/Components

Tasto destro > New Component > Install new component >Add

Selezionare la Dll

OK

Nota.

Per approfondimenti è possibile consultare il sito Microsoft all'indirizzo:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/cos sdk/html/pgcreatingapplications_06ib.asp

Windows 2003

Seguire il manuale disponibile all'indirizzo:

http://service.easynolo.it/download/Tutorial_Installazione_oggetti.zip

10 Transazioni d'esempio

In questo capitolo verranno descritti alcuni esempi di interfacciamento a GestPay considerati particolarmente significativi.

Lo Shop login d'esempio è 9000001.

Il profilo esercente è il seguente:

Profilo esercente	
Indirizzo IP	171.85.234.97
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

10.1 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	18.45
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

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 server dell'esercente comunica a GestPay, valorizzando gli attributi di GestPayCrypt, le informazioni che caratterizzano la transazione:

GestPayCrypt	
ShopLogin	9000001
Currency	242
Amount	18.45
ShopTransactionID	34az85ord19
Language	2

GestPay, effettua i controlli di autenticazione del server chiamante e di validazione delle informazioni che caratterizzano la transazione. Se i controlli vengono superati, restituirà a GestPayCrypt una stringa dati cifrata:

Stringa dati cifrata	
ShopLogin	9000001
EncryptString	2C53F1B5.....

Fase II

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 Shop login e alla stringa dati cifrata ricevuta nella fase precedente da GestPay:

Url pagina di pagamento
https://ecomm.sella.it/gestpay/pagam.asp?a=9000001&b=2C53F1B5.....

GestPay effettuerà controlli di verifica sullo Shop login (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 III

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=4D341A8B.....

Dopo che la comunicazione server to server si è conclusa positivamente, GestPay indirizzerà il browser dell'acquirente sul server dell'esercente (in questo caso all'url di risposta positiva).

In caso contrario verrà comunicato all'acquirente che non è possibile indirizzarlo sul server dell'esercente per concludere il processo d'acquisto.

Redirect client acquirente

<http://www.mionegozio.com/rispOK.asp?a=9000001&b=4D341A8B.....>

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

Invio e-mail

esito_OK@mionegozio.com

Fase IV

GestPay comunica all'esercente l'esito della transazione inviando una stringa dati cifrata. L'esercente dovrà, utilizzando l'oggetto GestPayCrypt, richiedere la decifratura della stringa per poter interpretare correttamente l'esito della transazione ed aggiornare le informazioni sul proprio sistema informativo permettendo all'acquirente di concludere il processo d'acquisto.

Il server dell'esercente comunica a GestPay, attraverso GestPayCrypt, la stringa dati cifrata che riporta l'esito della transazione:

Stringa dati cifrata

ShopLogin	9000001
EncryptedString	4D341A8B.....

GestPay, effettua i controlli di autenticazione del server chiamante e di integrità della stringa dati cifrata. Se i controlli vengono superati, restituisce a GestPayCrypt le informazioni in chiaro permettendo all'esercente di interpretare in modo corretto l'esito della transazione:

Esito GestPay

ShopLogin	9000001
Currency	242
Amount	18.45
ShopTransactionID	34az85ord19
TransactionResult	OK
AuthorizationCode	54e813
BankTransactionID	216
ErrorCode	0
ErrorDescription	Transazione eseguita

10.2 Transazione numero 2

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	15.6
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

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 server dell' esercente comunica a GestPay, valorizzando gli attributi di GestPayCrypt, le informazioni che caratterizzano la transazione:

GestPayCrypt	
ShopLogin	9000001
Currency	242
Amount	15.6
ShopTransactionID	34az85ord19
Language	3
BuyerName	Mario Bianchi
BuyerEmail	mario.bianchi@isp.it
CustomInfo	BV_CODCLIENTE=12*P1*B*BV_SESSIONID=398

GestPay, effettua i controlli di autenticazione del server chiamante e di validazione delle informazioni che caratterizzano la transazione. Se i controlli vengono superati, restituirà a GestPayCrypt una stringa dati cifrata:

Stringa dati cifrata	
ShopLogin	9000001
EncryptString	30715CA8.....

Fase II

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 Shop login e alla stringa dati cifrata ricevuta nella fase precedente da GestPay:

Url pagina di pagamento
https://ecommm.sella.it/gestpay/pagam.asp?a=9000001&b=30715CA8.....

GestPay effettuerà controlli di verifica sullo Shop login (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 III

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=F45E129A.....

Dopo che la comunicazione server to server si è conclusa positivamente, GestPay indirizzerà il browser dell'acquirente sul server dell'esercente (in questo caso all'url di risposta negativa).

In caso contrario verrà comunicato all'acquirente che non è possibile indirizzarlo sul server dell'esercente per concludere il processo d'acquisto.

Redirect client acquirente
http://www.mionegozio.com/rispOK.asp?a=9000001&b=F45E129A.....

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

Fase IV

GestPay comunica all'esercente l'esito della transazione inviando una stringa dati cifrata. L'esercente dovrà, utilizzando l'oggetto GestPayCrypt, richiedere la decifratura della stringa per poter interpretare correttamente l'esito della transazione ed aggiornare le informazioni sul proprio sistema informativo permettendo all'acquirente di concludere il processo d'acquisto.

Il server dell'esercente comunica a GestPay, attraverso GestPayCrypt, la stringa dati cifrata che riporta l'esito della transazione:

Stringa dati cifrata	
ShopLogin	9000001
EncryptedString	6C12459A.....

GestPay, effettua i controlli di autenticazione del server chiamante e di integrità della stringa dati cifrata. Se i controlli vengono superati, restituisce una stringa dati in chiaro che riporta l'esito della transazione:

Esito GestPay	
ShopLogin	9000001
Currency	242
Amount	15.6
ShopTransactionID	34az85ord19
TransactionResult	OK
AuthorizationCode	9823y5
BankTransactionID	860
CustomInfo	BV_CODCLIENTE=12*P1*BV_SESSIONID=398
ErrorCode	0
ErrorDescription	Transazione eseguita

11 Esempi di implementazione

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

Sul sito www.easynolo.it sarà possibile scaricare gli script funzionanti realizzati utilizzando alcuni dei linguaggi di sviluppo più diffusi (ASP, JSP, PHP...)

Esempio in ASP

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

```
<%
' INIZIO SCRIPT DI CRITTOGRAFIA

'PARTE DA NON MODIFICARE

    Set objCrypt = GetObject("java:GestPayCrypt")

    if Err.number <> 0 then
        Response.Write Err.number & Err.description
    end if

'PARTE DA MODIFICARE (VALORIZZAZIONE ATTRIBUTI TRANSAZIONE)

'Inserire al posto delle scritte con parentesi quadre [] I dati
'necessari per effettuare la transazione.
'Le righe contenenti i dati contrassegnati come NON OBBLIGATORI
'devono essere eliminate se non utilizzate

'CAMPI OBBLIGATORI

    myshoplogin= "[SHOP LOGIN]" 'Es. 90000001
    mycurrency=[CODICE DIVISA] 'Es. 242 per euro o 18 lira
    myamount=[IMPORTO SENZA SEPARATORI DI MIGLIAIA
    CON SEPARATORE PUNTO PER DECIMALI] 'Es. 1256.28
    myshoptransactionID="[IDENTIFICATIVO TRANSAZIONE]"
    'Es. "34az85ord19"

'CAMPI NON OBBLIGATORI (CANCELLARE LE RIGHE NON INTERESSATE)

    mybuyername="[NOME E COGNOME ACQUIRENTE]" 'Es. "Mario Bianchi"
    mybuyeremail="[EMAIL ACQUIRENTE]" 'Es. "Mario.bianchi@isp.it"
    mylanguage=[CODICE LINGUA DA UTILIZZARE NELLA COMUNICAZIONE]
    'Es. 3 per spagnolo
    mycustominfo="[PARAMETRI PERSONALIZZATI]"
    'Es. "BV_CODCLIENTE=12*P1*BV_SESSIONID=398"
```

'PARTE DA NON MODIFICARE

```
objCrypt.SetShopLogin(myshoplogin)
objCrypt.SetCurrency(mycurrency)
objCrypt.SetAmount(myamount)
objCrypt.SetShopTransactionID(myshoptransactionID)
objCrypt.SetBuyerName(mybuyername)
objCrypt.SetBuyerEmail(mybuyeremail)
objCrypt.SetLanguage(mylanguage)
objCrypt.SetCustomInfo(mycustominfo)
```

```
call objCrypt.Encrypt
```

```
if objCrypt.GetErrorCode = 0 then
    b = objCrypt.GetEncryptedString
    a = objCrypt.GetShopLogin
end if
```

'FINE SCRIPT PER CRITTOGRAFIA.

'SE TUTTO OK SI HANNO 2 VARIABILI A E B DA UTILIZZARE PER IL
'PASSAGGIO DEI PARAMETRI A BANCA SELLA

'ESEMPIO CON FORM HTML

%>

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

PAGINA PER LA GESTIONE DELLA RISPOSTA DI PAGAMENTO

```
<%
'INIZIO SCRIPT PER DECRITTOGRAFIA
'DA NON MODIFICARE

'VENGONO LETTI I PARAMETRI IN INPUT E VIENE DECRIPTATO IL
'PARAMETRO B

parametro_a = trim(request("a"))
parametro_b = trim(request("b"))

Set objdeCrypt = GetObject("java:GestPayCrypt")

if Err.number <> 0 then
    Response.Write Err.number & Err.description
end if

objdeCrypt.SetShopLogin(parametro_a)
objdeCrypt.SetEncryptedString(parametro_b)

call objdeCrypt.Decrypt

'DI SEGUITO SI HANNO UNA SERIE DI VARIABILI VALORIZZATE CON I
'DATI RICEVUTI DA GESTPAY DA UTILIZZARE PER L'INTEGRAZIONE CON
'IL PROPRIO SISTEMA

myshoplogin=trim(objdeCrypt.GetShopLogin)
mycurrency=objdeCrypt.GetCurrency
myamount=objdeCrypt.GetAmount
myshoptransactionID=trim(objdeCrypt.GetShopTransactionID)
mybuyername=trim(objdeCrypt.GetBuyerName)
mybuyeremail=trim(objdeCrypt.GetBuyerEmail)
mytransactionresult=trim(objdeCrypt.GetTransactionResult)
myauthorizationcode=trim(objdeCrypt.GetAuthorizationCode)
myerrorcode=trim(objdeCrypt.GetErrorcode)
myerrordescription=trim(objdeCrypt.GetErrorDescription)
myerrorbanktransactionid=trim(objdeCrypt.GetBankTransacti
onID)
myalertcode=trim(objdeCrypt.GetAlertCode)
myalertdescription=trim(objdeCrypt.GetAlertDescription)
mycustominfo=trim(objdeCrypt.GetCustomInfo)

'FINE SCRIPT DI DECRITTOGRAFIA
%>
```

12 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

Note.

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](#)

13 Tabella codici divisa

Il codice divisa viene gestito da GestPay tramite l'attributo Currency

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

14 Tabella codici lingua

Il codice lingua viene gestito da GestPay tramite l'attributo Language.

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

15 Tabella codici Verified by Visa

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

Codice	Descrizione
OK	Transazione certificata VbV
KO	Transazione non certificata VbV

16 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.

17 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://ecommm.sella.it/gestpay/backoffice/LoginGestPay.asp>)

Ambiente di **Back Office** per esercenti di **test**

(<https://testecommm.sella.it/gestpay/backoffice/loginigestpay.asp>)