GestPay

Security with Cryptography

Technical Specifications

Summary

Document Information

Project Name:	GestPay
Tiltle	Security with Cryptography
Creation Date	09/01/2004 13.33.00
Lingua	English
Società	EasyNolo

Versione	Descrizione	Data	Autore
1.0.0	Starting Version	15/03/2001	Sellanet
1.0.1	TransactionResult Attribute Management	20/03/2001	Sellanet
1.0.2	Chapter 2 Modification url GestPay List Correction	22/03/2001	Sellanet
1.1.0	Document Complete Revision	28/03/2001	Sellanet
1.1.1	Browser Requirements Update	09/04/2001	Sellanet
1.1.2	Server Requirements Update	05/12/2001	Sellanet
1.1.3	Custom Fields Requirements Update	20/08/2002	Sellanet
1.1.4	Error Codes Update	20/08/2002	Sellanet
1.1.5	Language Codes Update	20/08/2002	Sellanet
1.1.6	Custom Fields & Parameters Requirements Update	20/08/2002	Sellanet
1.1.7	Currency Codes Update	27/01/2003	Sellanet
1.1.8	Domain for test codes	13/06/2007	Easy Nolo S.p.A.
1.0.9	New response parameter 3DLevel	15/07/2009	Easy Nolo S.p.A.

1 Introduction

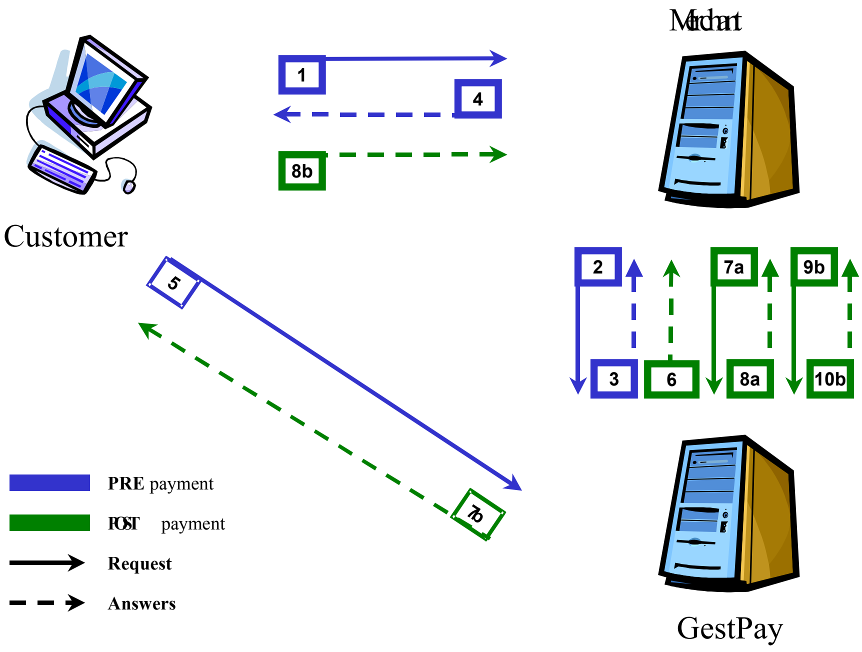
This document has the intent of showing the architectural and functional aspects of GestPay platform giving the necessary indications to the interfacing.
The chapter **System Architecture** describes the system components and the modalities of interaction between the different components and who is involved (merchant, buyer and GestPay).
The chapter **Process Phases Description** will take in exam all the phases that make up the payment process underlining the information that must be passed to GestPay and the information that will be returned.
In the chapter **Authentication** it is described how GestPay recognizes the merchant server that makes calls to the system.
The chapter **Payment Transaction Data Structure** describes the information that identifies a payment transaction and the result that GestPay returns after the processing.
In the chapter **Merchant Profile** it is described how to configure the merchant profile that allows GestPay to process transactions correctly.
The chapter **GestPayCrypt Object Description** will examine the use of the component that attends to run the server-to-server communication during the phases that provide this kind of communication between the server that receives the virtual shop as guest and GestPay.
The chapter **Software Qualifications** underlines the minimum qualifications required for the software installation necessary to the interfacing with GestPay.
The chapter **Transactions of Example** describes some typical transactions underlining the information exchanged and the interaction modalities between the components.
There are, indeed, some tables that allow codifying some information sent or received by GestPay.

2 System Architecture

In the system architecture you can identify 3 components:

- Buyer client
- Merchant Server
- GestPay Server

Communication among the different components takes place on the Internet using http or https protocol (GestPay server has a 128 bit Verisign digital certificate).
The payment process is divided in communication steps in which the components interact exchanging the information needed to the transaction performance.



Architecture Scheme

1. The buyer selects the items to buy and decides to go on with the payment.
2. Merchant server contacts via the Internet GestPay server to cipher payment transaction data.
3. GestPay makes merchant server authentication and transaction data validation controls returning, in positive case, encrypted parameters string that represents the payment transaction that must be processed.
4. The encrypted parameters string is communicated to the browser of the client that is addressed to GestPay server to complete the payment process.
5. Merchant's browser calls backs the payment page passing the encrypted parameters string and the code assigned to the merchant (Shop Login). They are made data security controls of the transaction that, if exceeded, allow the visualisation of the payment page and the insert of the data needed to complete the transaction. The following steps describe the modality with which is communicated the transaction result both to the merchant and to the buyer.

6. GestPay communicates to merchant's server an encrypted parameter string that returns the transaction result.

7a. Merchant's server contacts via the Internet GestPay server to decrypt the encrypted data string. that returns the transaction result.

8a. GestPay decrypts the string and gives back decoded the parameters that return the transaction result.

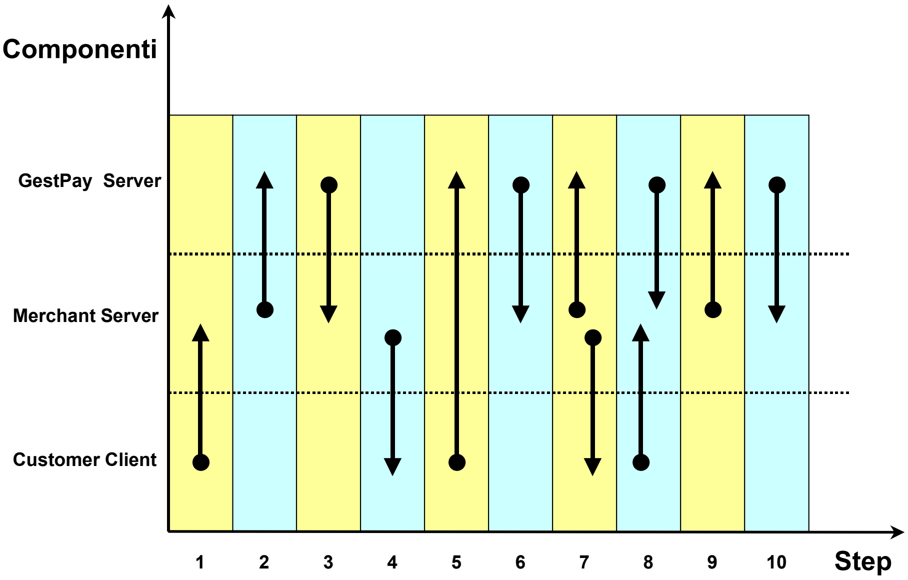
7b. GestPay communicates the encrypted parameters string that brings the transaction result to the browser of the client that is addressed to merchant's server.

8b. Buyer's browser calls backs the response page created by the merchant passing the encrypted parameters string.

9b. Merchant's server contacts via the Internet GestPay server to decrypt the encrypted data string that returns the transaction result.

10b. GestPay decrypts the string and gives back decoded the parameters that return the transaction result allowing the merchant to give the buyer the needed references to finish the purchase process.

The following scheme analyses the payment process underlining the chronological order in which the communication steps take place. Notice that in some cases (steps 7 and 8) contemporary communications are established among the components you have to consider when they implement the procedures that will have to manage the information exchanged among the steps.



3 Process Phases Description

A payment transaction is made up of 4 basic phases in which there are one or more communication steps. In each phase, information necessary to the transaction elaboration is exchanged among the various components.

3.1 Phase I: Transaction Data Cryptography

Information necessary to the payment is previously communicated to GestPay to be encrypted. To guarantee an optimum security level, no sensible information are communicated uncoded to the buyer's server.
In this phase, the merchant's server asks the cryptography service to GestPay obtaining the encrypted string that represents the transaction to process. Data that identify a transaction and their use will be described in chapter 4.
Communication server to server is managed by GestPayCrypt object released by EasyNolo and that must be previously installed on merchant's server. The virtual shop pages that are concerned with managing the information necessary to the payment will call the object back.
If the merchant's authentication controls and the transaction data validation are exceeded, GestPay will return the encrypted data string to the merchant's server that will be sent to the buyer's server to continue the payment process. Otherwise, a specific error code that will allow identifying the found out anomaly will be returned.

3.2 Phase II: Payment Page Call

Got the encrypted data string (as indicated in the paragraph above), the buyer's browser will be addressed to the payment page on GestPay server at the address:

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

for test codes

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

Call to page will be made passing two parameters:
a. Code that identifies merchant (Shop Login)
b. Encrypted data string that identifies transaction
The payment page will acquire parameters and will make identity controls (parameter a must be referable to a recognized merchant) and of transaction data security (parameter b must correspond it the encrypted data string communicated by the merchant in previous phase).
If controls are exceeded, the payment page will be visualized to buyer that will have to insert data necessary to complete the payment process.

If controls are not exceeded, the payment page is not visualized and you go to the following phase for the communication of the negative transaction result.

3.3 Phase III: Transaction Result Communication

GestPay communicates transaction result both to merchant and to buyer.

3.3.1 Response to Merchant

Notification is forwarded with a call server- to- server to the page opportunely prepared on merchant's server (notification page URL is one of the information that make up merchant's profile configurable thorough GestPay Backoffice environment). Call syntax is the following:

*http://<url server to server>?**a**=<ShopLogin>**&b**=<encrypted string>*

The call to the page will be made passing two parameters:

a. Code which identifies merchant (Shop Login)
b. Encrypted data string which brings back transaction result

If there are communications errors, GestPay will make more forwarding attempts for two days after the transaction.
Merchant will also receive a transaction result notification e-mail to the address configured in his profile.
Processed transaction, moreover, can be visualized entering GestPay Backoffice environment in the Active Report section.

3.3.2 Response to Buyer

GestPay, visualizing the «virtual ticket» immediately, notifies transaction result that reports data essential to the transaction.
GestPay will address buyer's browser to merchant's server to finish buying process. Merchant will have to prepare two Url (and configure them in merchant's profile) that will be called back in case of negative and positive answer and will allow merchant to manage the communication with the buyer keeping the editorial style that characterizes the virtual shop. Call syntax is the following:

*http://<url merchant>?**a**=<ShopLogin>**&b**=<encrypted string>*

If there is an anomaly in the server to server communication described above, GestPay will visualize a warning message to the buyer notifying that there could be problems addressing him to merchant's server to finish the buying process. In this situation, buyer has received a notification by GestPay about the transaction result and will be invited, if there are anomalies, to contact merchant using other channels (i.e. e-mail) to finish the buying process.
The buyer will also receive a transaction result notification e-mail to the address eventually indicated in the payment page.

3.4 Phase IV: Decryptography Transaction Result

GestPay notifies transaction result through an encrypted string (parameter b of the call to the url preset by merchant). The string is forwarded to the merchant a first time during the server to server communication and allows, once it's decoded, updating the state of the transaction registered in the merchant's informative system. The same string is also transported by buyer's browser to the merchant's server and allows, once it's decoded, to finish the payment process.

Web pages preset by the merchant for the transaction result reception (both in case of server to server communication and through the buyer's browser) will have to call back GestPay server to request the decryptography service and obtain uncoded the information that represent the result of the elaborated transaction.

Server to server communication is managed by the object GestPayCrypt released by EasyNolo and that must be preventively installed on the merchant's server.

4 Authentication

Servers to server calls are managed by a component released by EasyNolo. Server authentication of the merchant who asks the cryptography or decryptography services is made verifying:

- **Shop Login validity**: ShopLogin parameter must correspond to a code registered in GestPay customers' details.
- **IP address server**: calling server IP address must correspond to one of the IP addresses configured in the merchant's profile.
- **Shop Login status**: merchant's state must be active (merchant's state is managed by GestPay administrator and not directly by the merchant).

If the authentication controls are not exceeded, it will be given back a specific error that will allow identifying the anomaly found in the authentication process.

5 Payment Transaction Data Structure

A transaction is characterized by a series of information that must be communicated to GestPay to make the payment process and by information given back to the system as transaction result.
Merchant can define, configuring opportunely the profile through back office environment with which modality and which information send or receive from GestPay.

5.1 Transaction Data to Send to GestPay

Some of the information to communicate to GestPay are obligatory to do the payment process whereas others can be left out without compromise transaction elaboration. Merchant, by GestPay back office environment, can define which information are obligatory and which instead are facultative.
Some information essential by the payment process point of view, are setup as obligatory by GestPay and you can't modify this attribute.
The following table gives the information that must be communicated to GestPay to make a transaction:

Name	Format	Type	O/F	Description
ShopLogin	VarChar (30)	P	O	ShopLogin
Currency	Num (3)	P	O	Code that identifies the currency in which is denominated transaction amount (see **Currency Codes** table)
Amount	Num (9)	P	O	Transaction amount. Do not insert separator of thousands. Decimals (max 2 numbers) are optional and separator is the full mark (see examples).
ShopTransactionID	VarChar (50)	P	O	Identifier attributed to merchant's transaction
CardNumber	VarChar (20)	I/P	O	Credit card number
ExpMonth	Char (2)	I/P	O	Credit card expiry month
ExpYear	Char (2)	I/P	O	Credit card expiry year
BuyerName	VarChar (50)	I/P	F	Buyer's name and surname
BuyerEmail	VarChar (50)	I/P	F	Buyer's e-mail address
Language	Num (2)	P	F	Code that identifies the language used in the communication with the

				buyer (see **Language Code** table)
CustomInfo[1]	VarChar (1000)	P	F	String that has the specific information as configured in the merchant's profile

[1] Each field can be maximum 300 characters

The **Name** column reports the attribute identifier with which a specific information is communicated to the object GestPayCrypt that attends to the server to server communication for the cryptography services.

The **Format** column underlines if the information value is numeric or alphanumeric. If it is alphanumeric, it's given in brackets the maximum accepted characters number.

The **Type** column specifies if the information must be communicated to the component (passed as **P**arameter) or if it can be insert by buyer (passed as **I**nput) in the payment page.

The **O/F** column specifies if the information is **O**bligatory (in case of omission you can process the transaction) or **F**acultative.

However, the minimum information set, that allows elaboration of phase I, is made up of:

- Currency
- Amount
- Shop TransactionID

These information, in fact, are defined as obligatory and must be communicated to GestPay using the GestPayCrypt component.

During phase I, GestPay makes validation controls on the information that constitute the payment transaction verifying coherence with the merchant's profile setup. In case of anomalies, transaction is left returning a specific error. This approach allows identifying immediately possible anomalies connected to the transaction, preventing that the buyer is addressed to the payment page with an encrypted data string that corresponds to a not valid transaction.

The CustomInfo attribute contains specific information that the merchant wants to communicate or receive from GestPay. Definition of which information are inserted in the CustomInfo attribute is realised in back office environment in the Fields and Parameters section.

The inserted information will follow this formalism:

datum1=value1*P1*datum2=value2*P1* … *P1*datumn=valuen

Separator among logically different information is the reserved data sequence ***P1***, datum value must not contain reserverd characters

Reserved Characters					
&	**(space)**	**§**	**(**	**)**	*****
<	**>**	**,**	**;**	**:**	***P1***
/	**[**	**]**	**?**	**=**	

5.2 Transaction Data Received by GestPay

GestPay communicates the payment transaction result to the merchant by an encrypted data string that contains a series of information returned.
Using GestPayCrypt object, merchant will obtain uncoded the information that report the transaction result and he will be able to update his own informative system allowing buyer to finish the buying process.
The following table reports the information that are returned by GestPay as transaction result.

Name	Format	Type	O/F	Description
ShopLogin	VarChar (30)	P	O	ShopLogin
Currency	Num (3)	P	O	Code that identifies the currency in which is denominated transaction amount (see **Currency Codes** table)
Amount	Num (9)	P	O	Transaction amount. Do not insert separator of thousands. Decimals (max 2 numbers) are optional and separator is the full mark (see examples).
ShopTransactionID	VarChar (50)	P	O	Identifier attributed to merchant's transaction
BuyerName	VarChar (50)	I/P	F	Buyer's name and surname
BuyerEmail	VarChar (50)	I/P	F	Buyer's e-mail address
TransactionResult	Char (2)	P	O	Transaction result
AuthorizationCode	VarChar (6)	P	O	Transaction authorizations code
BankTransactionID	Num (9)	P	O	Identifier attributed to the transaction by GestPay
ErrorCode	Num (9)	P	O	Error code
ErrorDescription	VarChar (255)	P	O	Error description
AlertCode	Num (9)	P	F	Alert code
AlertDescription	VarChar (255)	P	F	Alert description in language
3DLevel	VarChar (255)	P	F	Visa VBV / Mastercard Securecode authentication level
CustomInfo(1)	VarChar (1000)	P	F	String that has the specific information as configured in the merchant's profile

[1] Each field can be maximum 300 characters.

The minimum information set that report transaction result (defined obligatory) is made up of:

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

Other information are defined facultative and will be returned according to the merchant’s profile settings made by GestPay back office.

You can interpret a transaction result verifying TransactionResult field value.

The possible values are:

TransactionResult	Description
OK	Positive transaction result
KO	Negative transaction result
XX	Suspended transaction result (only in Money Transfer case)

6 Merchant's Profile

Every merchant can configure the profile entering the GestPay back office environment achievable at the address:

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

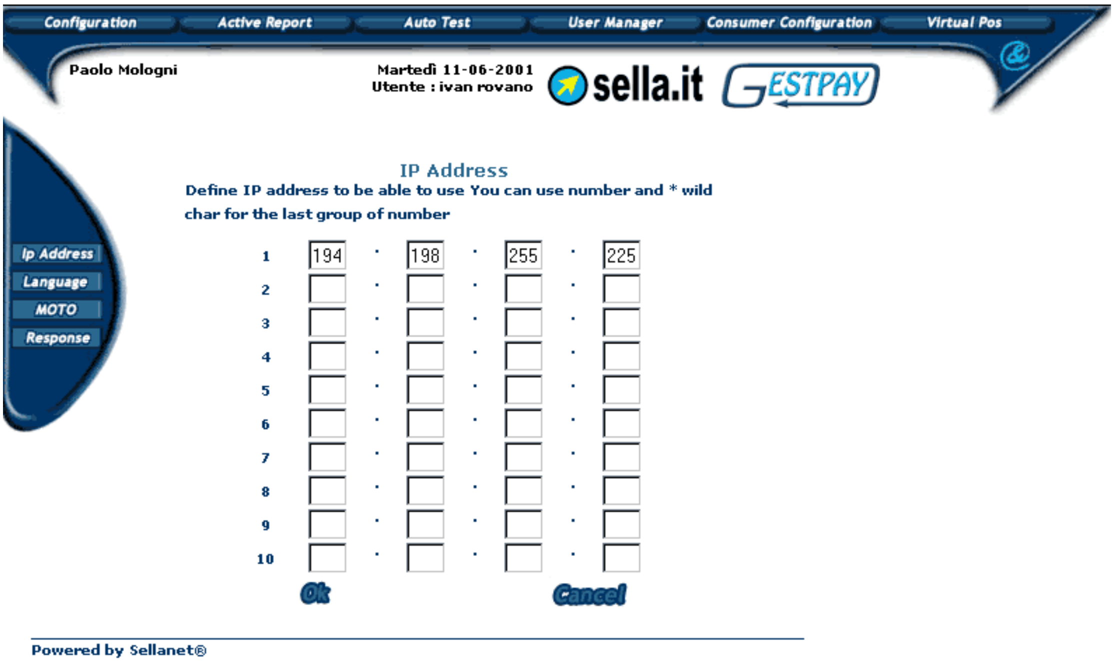
for test codes

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

Other settings concern with modality and information that must be sent or that will be returned by GestPay.

6.1 Authentication Configuration

GestPay identifies the merchant, who requires ciphering service using GestPayCrypt component, comparing calling server IP address to the IP addresses configured in the profile associated to the Shop Login used for the call. If the calling server is not recognised, transaction process ends and a specific error is returned.
Merchant can insert, in the **Configuration – Environment – IP Addresses** section of the back office environment, until a maximum of 10 IP addresses (if calls to GestPay come from a server farm).



Paolo Mologni

Martedì 11-06-2001
Utente : ivan rovano

IP Address

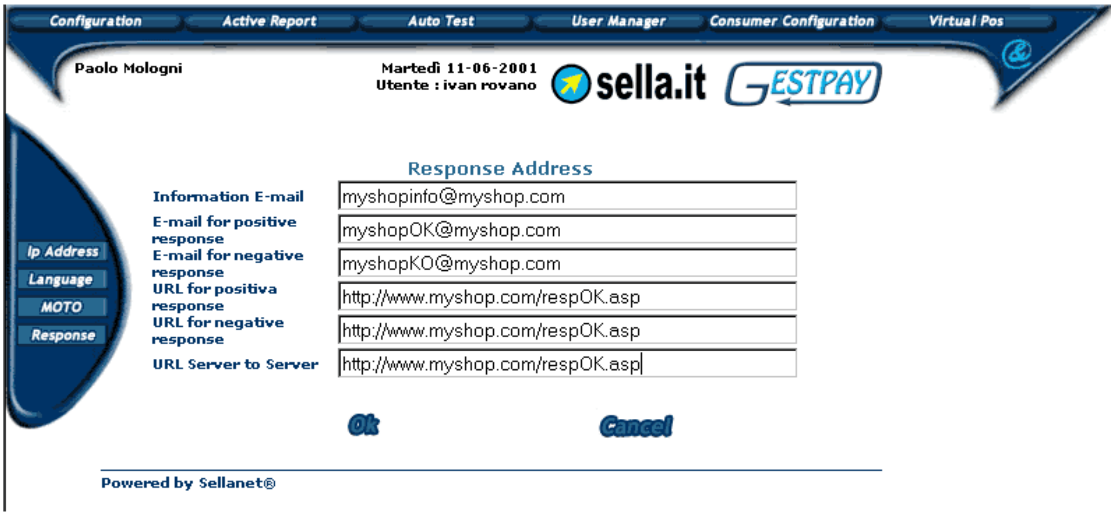
Define IP address to be able to use You can use number and * wild char for the last group of number

1	194	198	255	225
2				
3				
4				
5				
6				
7				
8				
9				
10				

Powered by Sellanet®

6.2 Answer url Configuration and e-mail

GestPay notifies the transaction result with a server to server call to the page opportunely prepared by merchant and addressing buyer's browser to the pages prepared by merchant (different pages in case of positive or negative result).
In the **Configuration – Environment – Responses** section in the back office environment, you can specify the URLs used by the system to notify the transaction result.
In this section you can also specify the addresses that will be used for the notifications made via e-mail.



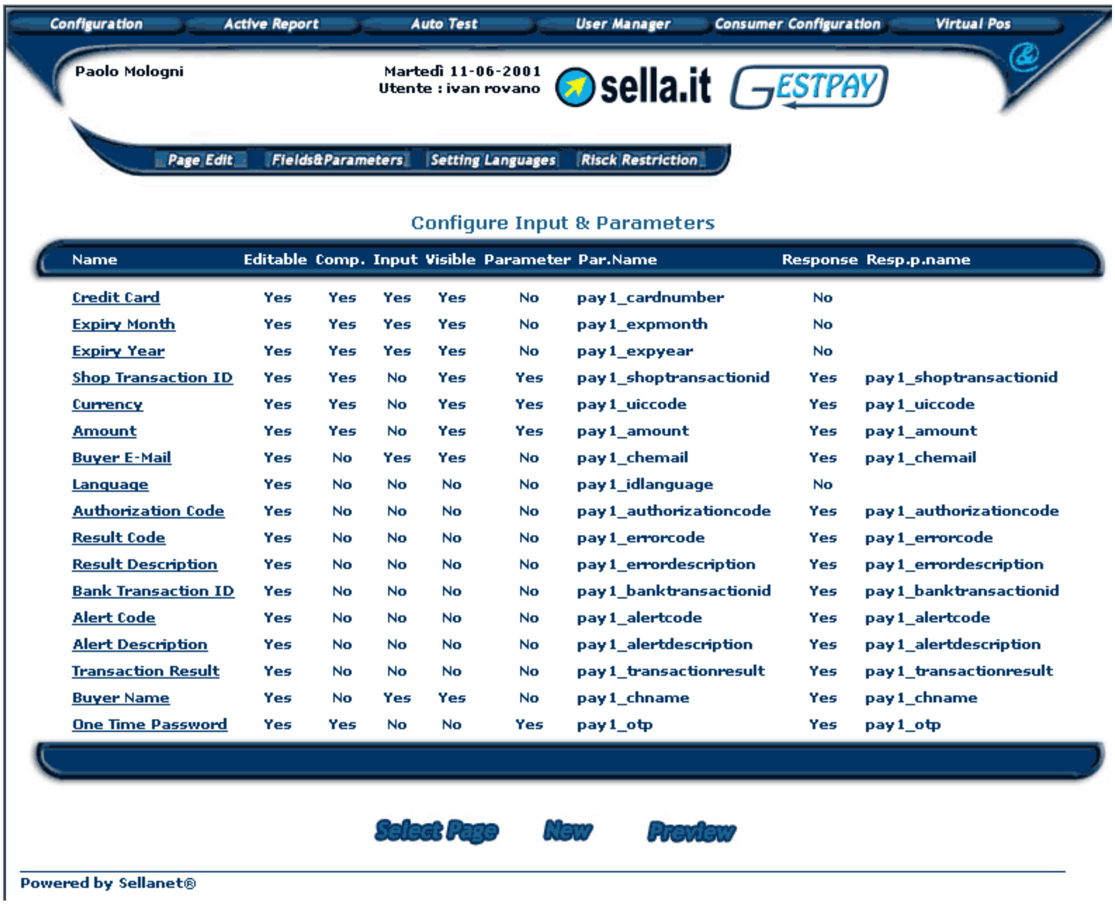
Response Address

Information E-mail	myshopinfo@myshop.com
E-mail for positive response	myshopOK@myshop.com
E-mail for negative response	myshopKO@myshop.com
URL for positiva response	http://www.myshop.com/respOK.asp
URL for negative response	http://www.myshop.com/respOK.asp
URL Server to Server	http://www.myshop.com/respOK.asp

6.3 Fields & Parameters Configuration

Merchant can define the transaction structure (specifying which information, beside those that are obligatory, will have to be sent to GestPay) configuring in back office environment which are the information to sent in phase I and which ones must be returned when the transaction result is communicated.

This system allows the merchant to customize transaction structure with proprietary information that will be stored in GestPay archives and will allow identifying each transaction using customized search keys. Moreover, customized information can be returned with the transaction result communication allowing the merchant's informative system to manage opportunely these information.



Paolo Mologni

Martedì 11-06-2001
Utente : ivan rovano

Configure Input & Parameters

Name	Editable	Comp.	Input	Visible	Parameter	Par.Name	Response	Resp.p.name
Credit Card	Yes	Yes	Yes	Yes	No	pay1_cardnumber	No	
Expiry Month	Yes	Yes	Yes	Yes	No	pay1_expmonth	No	
Expiry Year	Yes	Yes	Yes	Yes	No	pay1_expyear	No	
Shop Transaction ID	Yes	Yes	No	Yes	Yes	pay1_shoptransactionid	Yes	pay1_shoptransactionid
Currency	Yes	Yes	No	Yes	Yes	pay1_uiccode	Yes	pay1_uiccode
Amount	Yes	Yes	No	Yes	Yes	pay1_amount	Yes	pay1_amount
Buyer E-Mail	Yes	No	Yes	Yes	No	pay1_chemail	Yes	pay1_chemail
Language	Yes	No	No	No	No	pay1_idlanguage	No	
Authorization Code	Yes	No	No	No	No	pay1_authorizationcode	Yes	pay1_authorizationcode
Result Code	Yes	No	No	No	No	pay1_errorcode	Yes	pay1_errorcode
Result Description	Yes	No	No	No	No	pay1_errordescription	Yes	pay1_errordescription
Bank Transaction ID	Yes	No	No	No	No	pay1_banktransactionid	Yes	pay1_banktransactionid
Alert Code	Yes	No	No	No	No	pay1_alertcode	Yes	pay1_alertcode
Alert Description	Yes	No	No	No	No	pay1_alertdescription	Yes	pay1_alertdescription
Transaction Result	Yes	No	No	No	No	pay1_transactionresult	Yes	pay1_transactionresult
Buyer Name	Yes	No	Yes	Yes	No	pay1_chname	Yes	pay1_chname
One Time Password	Yes	Yes	No	No	Yes	pay1_otp	Yes	pay1_otp

Powered by Sellanet®

7 GestPayCrypt Object Description

Server to server communication between GestPay and the merchant will be automatically managed by GestPayCrypt component released by EasyNolo. This component is a java library that will be called back by the web pages preset by the merchant to manage the transaction data ciphering and the deciphering of the result communicated by GestPay.
GestPayCrypt library is available *open source* on EasyNolo site.
Table 1 reports the attributes and the methods returned available by java library.
Merchant will implement, in the virtual shop pages that deal with managing the payment, a call to the GestPayCrypt component that will deal with managing requests to GestPay cryptography service.
Class attributes will be filled in with data that identify the transaction.
To require the ciphering service you will have to call again the Encrypt method.
If the ciphering operation has ended up correctly (ErrorCode attribute value= 0), encrypted data string returned by GestPay will be available reading the EncryptedString attribute value. Otherwise, ErrorCode and ErrorDescription attributes values will allow identifying the reasons that have prevent the ciphering operation.
To require the deciphering service, you will have to call again the Decrypt method, after you have filled in Shop Login and EncryptedString attributes with values communicated by GestPay in phase III.
Information that report the transaction result will be available reading java library attributes that correspond to the information that concern with the transaction result.

Here GestPayCrypt java library attributes and methods are described:

GestPayCrypt Class	
Attributes	
ShopLogin	Shop Login that identifies merchant
Currency	Code that identifies the currency in which is denominated the amount
Amount	Transaction amount
ShopTransactionID	Identifier attributed to merchant's transaction
CardNumber	Credit card number
ExpMonth	Credit card expiry month
ExpYear	Credit card expiry year
BuyerName	Buyer's name and surname
BuyerEmail	Buyer's e-mail address
Language	Language code used for the communication with the buyer
CustomInfo	String that has the specific merchant's information
TransactionResult	Transaction result
AuthorizationCode	Transaction authorizations code
BankTransactionID	Identifier attributed to the transaction by GestPay
ErrorCode	Error code
ErrorDescription	Error description
AlertCode	Alert code
AlertDescription	Alert description
EncryptedString	Encrypted string
3DLevel	Visa VBV / Mastercard Securecode autentication level
Methods	
SetShopLogin (val)	Used to fill in ShopLogin attribute
SetCurrency (val)	Used to fill in Currency attribute
SetAmount (val)	Used to fill in Amount attribute
SetShopTransactionID (val)	Used to fill in ShopTransactionID attribute
SetCardNumber (val)	Used to fill in CardNumber attribute
SetExpMonth (val)	Used to fill in ExpMonth attribute
SetExpYear (val)	Used to fill in ExpYear attribute
SetBuyerName (val)	Used to fill in BuyerName attribute
SetBuyerEmail (val)	Used to fill in BuyerEmail attribute
SetLanguage (val)	Used to fill in Language attribute
SetCustomInfo (val)	Used to fill in CustomInfo attribute
SetEcryptedString (val)	Used to fill in EncryptedString attribute
GetShopLogin	Used to read ShopLogin attribute
GetCurrency	Used to read Currency attribute
GetAmount	Used to read Amount attribute
GetShopTransactionID	Used to read ShopTransactionID attribute
GetCardNumber	Used to read CardNumber attribute
GetExpMonth	Used to read ExpMonth attribute
GetExpYear	Used to read ExpYear attribute
GetBuyerName	Used to read BuyerName attribute
GetBuyerEmail	Used to read BuyerEmail attribute
GetLanguage	Used to read Language attribute
GetCustomInfo	Used to read CustomInfo attribute
GetTransactionResult	Used to read TransactionResult attribute
GetAuthorizationCode	Used to read AuthorizationCode attribute

GetBankTransactionID	Used to read BankTransactionID attribute
GetErrorCode	Used to read ErrorCode attribute
GetErrorDescription	Used to read ErrorDescription attribute
GetAlertCode	Used to read AlertCode attribute
GetAlertDescription	Used to read AlertDescription attribute
GetEncryptedString	Used to read EncryptedString attribute
Get	Used to read 3DLevel attribute
Decrypt	Used to require ciphering service
Encrypt	Used to require deciphering service

Attributes and methods GestPayCrypt class

8 Software Qualifications

Software qualifications required by GestPay concern with the buyer's browser and server that hosts the virtual shop.

8.1 Buyer's Browser Qualifications

Domain https://ecomm.sella.it/gestpay/ is associated a 128 bit Verisign digital certificate. Browsers will have to be consistent to this cryptography level. Minimum required versions are Internet Explorer 4.0 and Netscape 4.76.
Client's browser must be setup to accept cookies and javascript.

8.2 Merchant's Server Qualifications

GestPayCrypt java library (GestPayCrypt. class) will have to be copied in web server directory that contains java libraries.
For example, in a system with architecture based on Windows NT and Internet Information Server it will have to be installed in directory:

...\java\TrustLib

On the web server that hosts web pages that call back GestPayCrypt library, Java Virtual Machine (from 1.1.3 version on) must be installed.
In order to check the communications verify that the web server be able to connect to the following address:
For Http connection
http://ecomms2s.sella.it/testhttp/test.asp

for test codes
http://testecomm.sella.it/testhttp/test.asp

For Https connection
https://ecomms2s.sella.it/testhttps/test.asp

for test codes
https://testecomm.sella.it/testhttps/test.asp

9 Transactions of Example.

In this chapter, there are examples of interfacing to GestPay considered very significant.
Ex.: ShopLogin is 9000001
Merchant’s profile is the following:

Merchant’s Profile	
IP Address	171.85.234.97
Server to server Communication Url	http://www.myshop.com/s2s.asp
Positive responses Url	http://www.myshop.com/respOK.asp
Negative responses Url	http://www.myshop.com/respKO.asp
E-mail to send OK result	result_OK@myshop.com
E-mail to send KO result	result_KO@myshop.com
E-mail to send information	info@myshop.com

9.1 Transaction # 1

Merchant decides to communicate to GestPay only the indispensable information to allow the buyer to make the payment. Payment page will have to be visualized by the buyer who will insert in protected modality (SSL 128 bit) sensible data necessary to complete payment.
Transaction to process has the following characteristics:

Merchant’s Transaction	
Shop Transaction ID	34az85ord19
Transaction Amount	1828.45
Currency Transaction	euro
Language	English

Suppose that transaction will end up positively (payment will be made) reporting the following result:

Result	
Authorization code	54e813
Bank transaction ID	216

In the following pages, every single phase that make up the payment process will be described, underlining information exchanged between GestPay and merchant’s server.

Phase I

Merchant's server communicates to GestPay, increasing GestPayCrypt attributes, information that characterizes transaction:

GestPayCrypt	
ShopLogin	9000001
Currency	242
Amount	1828.45
ShopTransactionID	34az85ord19
Language	2

GestPay makes authentication controls of the calling server and of information validation that characterizes transaction. If controls are exceeded, it will return to GestPay an encrypted string:

Encrypted Data String	
ShopLogin	9000001
EncryptString	2C53F1B5..................

Phase II

Buyer's server will be addressed to GestPay server to complete the payment process. Call to the payment page will be made passing two parameters that correspond to Shop login and to the encrypted data string received in the previous phase by GestPay:

Payment page Url
Https://ecomm.sella.it/gestpay/pagam.asp?a=9000001&b=2C53F1B5....................

GestPay will make verification controls on Shop login (parameter a) and security controls on the encrypted data string (parameter b). If controls are exceeded, the buyer that will be able to insert data necessary to complete payment will visualize payment page. Otherwise, an error will be communicated.

Phase III

After you have processed transaction, GestPay communicates transaction result (encrypted data string) to merchant.

Server to server communication
Http://www.myshop.com/s2s.asp?a=9000001&b=4D341A8B..............

After that server to server communication has end up positively, GestPay will address buyer’s browser on merchant’s server (in this case of positive response Url). Otherwise, buyer will be communicated that it is not possible to be addressed on merchant’s server to finish the buying process.

Buyer’s Redirect Client
Http://www.myshop.com/respOK.asp?a=90000011&b=4D341A8B.............

Transaction result is also notified to merchant via e-mail

Send E-mail
Result_OK@myshop.com

Phase IV

GestPay communicates to merchant the transaction result, sending an encrypted data string. Merchant will have to, using GestPayCrypt object, require string ciphering to interpret correctly the transaction result and update information on his own informative system allowing the buyer to finish the buying process.
Merchant’s server communicates to GestPay, through GestPayCrypt, the encrypted data string that reports the transaction result.

Encrypted Data String	
ShopLogin	9000001
EncryptedString	4D341A8B.............

GestPay makes calling server authentication and encrypted data string controls. If controls are exceeded, it returns to GestPayCrypt uncoded information allowing merchant to interpret correctly the transaction result:

GestPay Result	
ShopLogin	9000001
Currency	242
Amount	1828.45
ShopTransactionID	34az85ord19
TransactionResult	OK
AuthorizationCode	54e813
BankTransactionID	216
ErrorCode	0
ErrorDescription	Transaction Executed

9.2 Transaction #2

Merchant decides to acquire on his own site all the information necessary to make a payment (information that buyer in the previous case would have typed on the payment page visualized by GestPay).
Indispensable pre-requisite to acquire directly buyer's **sensible data is to have a safe server (a site protected by a digital certificate).**

Transaction to process has the following characteristics:

Transaction	
Shop Transaction ID	Or784sR71
Amount	450600
Currency	Lire
Credit Card Number	4321432143214321
Expiry Month	12
Expiry Year	01
Buyer's Name and Surname	Paolo Rossi
Buyer's E-mail Address	paolo.rossi@isp.it

In this case, suppose that transaction will not end up positively (payment will not be made because credit card is not existing). Result communicated by GestPay is the following:

Result	
Bank transaction ID	3861
Error Code	1024
Error Description	Not recognized card

In the following pages, every single phase that make up the payment process will be described, underlining information exchanged between GestPay and merchant's server.

Phase I

Merchant's server communicates to GestPay, increasing GestPayCrypt attributes, information that characterizes transaction:

GestPayCrypt	
ShopLogin	9000001
Currency	242
Amount	1828.45
ShopTransactionID	34az85ord19
Language	2

GestPay makes authentication controls of the calling server and of information validation that characterizes transaction. If controls are exceeded, it will return to GestPay an encrypted string:

Encrypted Data String	
ShopLogin	9000001
EncryptString	2C53F1B5..................

Phase II

Buyer's server will be addressed to GestPay server to complete the payment process. Call to the payment page will be made passing two parameters that correspond to Shop login and to the encrypted data string received in the previous phase by GestPay:

Payment page Url
Https://ecomm.sella.it/gestpay/pagam.asp?a=9000001&b=F374A15C....................

GestPay will make verification controls on Shop login (parameter a) and security controls on the encrypted data string (parameter b). If controls are exceeded, payment page will not be visualized to buyer (data necessary to complete transaction are already available) but you go on directly to transaction elaboration without visualising nothing to buyer. Otherwise, an error will be communicated.

Phase III

After you have processed transaction, GestPay communicates transaction result (encrypted data string) to merchant.

Server to server communication
Http://www.myshop.com/s2s.asp?a=9000001&b=6C12459A............

After that server to server communication has end up positively, GestPay will address buyer's browser on merchant's server (in this case of positive response Url). Otherwise, buyer will be communicated that it is not possible to be addressed on merchant's server to finish the buying process.

Buyer's Redirect Client
Http://www.myshop.com/respOK.asp?a=90000011&b=6C12459A............

Transaction result is also notified to merchant via e-mail

Send E-mail
result_KO@myshop.com
paolo.rossi@isp.it

Phase IV

GestPay communicates to merchant the transaction result, sending an encrypted data string. Merchant will have to, using GestPayCrypt object, require string ciphering to interpret correctly the transaction result and update information on his own informative system allowing the buyer to finish the buying process.
Merchant's server communicates to GestPay, through GestPayCrypt, the encrypted data string that reports the transaction result.

Encrypted Data String	
ShopLogin	9000001

GestPay makes calling server authentication and encrypted data string controls. If controls are exceeded, it returns an uncoded data string that reports the transaction result:

GestPay Result	
ShopLogin	9000001
Currency	18
Amount	450600
ShopTransactionID	Or784sR71
TransactionResult	KO
AuthorizationCode	<null>
BankTransactionID	3861
ErrorCode	1024
ErrorDescription	Not recognized card

9.3 Transaction #3

Merchant decides to communicate to GestPay, not only information indispensable to allow buyer to make the payment, but also his name, surname and e-mail address (these information will be proposed as default in the payment page in order to avoid that buyer has to insert them a second time).
Other customized information will be sent by merchant (client code attributed to buyer and a technical information). Payment page will have to be visualized to buyer that will insert sensible data necessary to complete the payment in protected modality (SSL 128 bit). In the payment page, moreover, one of the customized information will have to be visualized (client code).
Transaction to process has the following characteristics:

Transaction	
Shop Transaction ID	34az85ord19
Transaction Amount	1245.6
Currency Transaction	Euro
Language	Spanish

Buyer’s Name and Surname	Mario Bianchi
Buyer’s E-mail Address	mario.bianchi@isp.it
Customized info 1	BV_CODCLIENTE=12
Customized info 2	BV_SESSIONID=398

Suppose that transaction will end up positively (payment will be made) reporting the following result:

Result	
Authorization code	9823y5
Bank transaction ID	860

In the following pages, every single phase that make up the payment process will be described, underlining information exchanged between GestPay and merchant’s server.

Phase I

Merchant’s server communicates to GestPay, increasing GestPayCrypt attributes, information that characterizes transaction:

GestPayCrypt	
ShopLogin	9000001
Currency	242
Amount	1828.45
ShopTransactionID	34az85ord19
Language	2
BuyerName	Mario Bianchi
BuyerEmail	mario.bianchi@isp.it
CustomInfo	BV_CODCLIENTE=12*P1*SESSIONID=398

GestPay makes authentication controls of the calling server and of information validation that characterizes transaction. If controls are exceeded, it will return to GestPay an encrypted string:

Encrypted Data String	
ShopLogin	9000001
EncryptString	30715CA8………………..

Phase II

Buyer’s server will be addressed to GestPay server to complete the payment process. Call to the payment page will be made passing two parameters that correspond to

Shop login and to the encrypted data string received in the previous phase by GestPay:

Payment page Url
Https://ecomm.sella.it/gestpay/pagam.asp?a=9000001&b=30715CA8....................

GestPay will make verification controls on Shop login (parameter a) and security controls on the encrypted data string (parameter b). If controls are exceeded, the buyer that will be able to insert data necessary to complete payment will visualize payment page. Otherwise, an error will be communicated.

Phase III

After you have processed transaction, GestPay communicates transaction result (encrypted data string) to merchant.

Server to server communication
Http://www.myshop.com/s2s.asp?a=9000001&b=F45E129A..............

After that server to server communication has end up positively, GestPay will address buyer's browser on merchant's server (in this case of positive response Url). Otherwise, buyer will be communicated that it is not possible to be addressed on merchant's server to finish the buying process.

Buyer's Redirect Client
Http://www.myshop.com/respOK.asp?a=90000011&b= F45E129A.............

Transaction result is also notified to merchant and buyer via e-mail

Send E-mail
result_OK@myshop.com
mario.bianchi@isp.it

Phase IV

GestPay communicates to merchant the transaction result, sending an encrypted data string. Merchant will have to, using GestPayCrypt object, require string ciphering to interpret correctly the transaction result and update information on his own informative system allowing the buyer to finish the buying process.
Merchant's server communicates to GestPay, through GestPayCrypt, the encrypted data string that reports the transaction result.

Encrypted Data String	
ShopLogin	9000001
EncryptedString	6C12459A............

GestPay makes calling server authentication and encrypted data string controls. If controls are exceeded, it returns an uncoded data string that reports the transaction result:

GestPay Result	
ShopLogin	9000001
Currency	242
Amount	1245.6
ShopTransactionID	34az85ord19
TransactionResult	OK
AuthorizationCode	9823y5
BankTransactionID	860
CustomInfo	BV_CODCLIENTE=12*P1*SESSIONID=398
ErrorCode	0
ErrorDescription	Transaction Executed

10 Examples of Implementation

In this chapter it is described an example of interfacing to GestPay realized using ASP language.
On http://service.easynolo.it/download.asp you can download functioning scripts realized using some of the most widely distributed development languages (ASP, JSO, PHP…).

ASP Example

PAGE CONNECTED TO PAYMENT PAGE
(PAYMENT REQUEST)

```
<%
‘START CRYPTOGRAPHY SCRIPT
‘DO NOT MODIFY THIS PART
Set objCrypt = GetObject("java:GestPayCrypt")
if Err.number <> 0 then
Response.Write Err.number & Err.description
end if
‘MODIFY THIS PART (VALORIZATION TRANSACTION ATTRIBUTES)
‘Insert instead of messages in square brackets []
‘data needed to make transaction.
‘Lines containing data checked as NOT OBLIGATORY
‘ must be deleted if not used.
‘OBLIGATORY FIELDS
myshoplogin= “[SHOP LOGIN]” ‘Ex. 9000001
mycurrency=[CODICE DIVISA] ‘Ex. 242 for euro or 18 for lira
myamount=[AMOUNT WITHOUT SEPARATOR OF THOUSANDS WITH SEPARATOR FOR
DECIMALS Ex. 1256.28] ‘Ex. 1256.28
myshoptransactionID=“[TRANSACTION IDENTIFIER]”
‘Ex. “34az85ord19”
myerrpage=”[CONNECTION ERROR COMMUNICATION URL]”
‘Es. “http://www.myshop.com/errorconnection.html”
‘FIELDS NOT OBLIGATORY (DELETE NOT INTERESTED LINES)
mybuyername=”[BUYER’S NAME AND SURNAME]”‘Ex. “Mario Bianchi”
mybuyeremail=”[BUYER’S EMAIL]”‘Es. “Mario.bianchi@isp.it”
mylanguage=[LANGUAGE CODE TO USE IN COMMUNICATION]
‘Ex. 3 for Spanish
mycustominfo=”[PERSONAL PARAMETERS ]”
‘Es. “BV_CODCLIENTE=12*P1*BV_SESSIONID=398”
‘DO NOT MODIFY THIS PART
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
else
Response.Redirect myerrorpage
end if
‘END CRYPTOGRAPHY SCRIPT.
```

```
‘IF EVERYTHING IS OK, YOU HAVE TWO VARIABLES A AND B TO USE FOR THE
PARAMETERS
PASSAGE TO BANCA SELLA
‘FORM HTML EXAMPLE
%>
<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>
```

PAGE FOR MANAGING PAYMENT RESPONSE

```
<%
‘START CRYPTOGRAPHY SCRIPT
‘DO NOT MODIFY THIS PART
‘INPUT PARAMETERS ARE READ AND PARAMETER B IS DECRYPTED
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
‘HERE THERE IS A LIST OF I VARIABLES FILLED IN WITH DATA RECEIVED BY
GestPay.
‘USE THEM FOR INTEGRATION WITH YOUR OWN SYSTEM
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.GetBankTransactionID)
myalertcode=trim(objdeCrypt.GetAlertCode)
myalertdescription=trim(objdeCrypt.GetAlertDescription)
mycustominfo=trim(objdeCrypt.GetCustomInfo)
‘END DECRYPTOGRAPHY SCRIPT
%>
```

11 Table of Errors

Code	Description
0	*Transaction correctly processed*
57	*Blocked credit card*
58	*Confirmed amount exceeds authorized amount*
63	*Demand for settlement of one nonexistent transaction*
64	*Expired preauthorization*
65	*Wrong currency*
66	*Preauthorization already notified*
74	*Authorization denied*
97	*Authorization denied*
100	*Transaction interrupted by bank authorizative system*
150	*Wrong merchant configuration in bank authorizative system*
208	*Wrong expiry date*
212	*Bank authorizative system not available*
251	*Insufficient credit*
401	*Call credit card company*
402	*System error*
403	*Merchant not recognized*
404	*Collect card*
405	*Authorization refused by credit card companies*
406	*Bank authorizative system not available*
409	*Richiesta in corso*
412	*Operation not allowed*
413	*Importo non valido*
414	*Card not recognized*
416	*Pin errato*
417	*Authorization denied*
418	*Network not available*
419	*Wrong transaction date*
420	*Wrong card date*
430	*Invalid format*
433	*Card expired*
436	*Card not qualified*
438	*PIN attempts exhausted*
439	*Carta inesistente*
451	*Amount not available*
454	*Card expired*
461	*Too big amount*
462	*Blocked credit card*
468	*Bank authorizative system not available*
475	*PIN attempts exhausted*
490	*Not permitted transaction*
810	*Bank authorizative system not available*
811	*Wrong merchant configuration in bank authorizative system*
901	*Authorization denied*

902	*Authorization denied*
903	*Authorization denied*
904	*Authorization denied*
905	*Authorization denied*
906	*Authorization denied*
907	*Authorization denied*
908	*Authorization denied*
910	*Authorization denied*
911	*Authorization denied*
913	*Authorization denied*
914	*Authorization denied*
915	*Authorization denied*
916	*Authorization denied*
917	*Authorization denied*
918	*Authorization denied*
919	*Authorization denied*
920	*Authorization denied*
950	*Not qualified credit card*
951	*Wrong merchant configuration in bank authorizative system*
998	*Credit card with wrong check-digit*
999	*Operation not performed*
1100	*Empty parameter string*
1101	*Invalid format of parameter string*
1102	*No parameter name precedes = symbol*
1103	*Parameter string ending with a separator*
1104	*Invalid parameter name*
1105	*Invalid parameter value*
1106	*Repeated parameter name*
1107	*Unexpected parameter name. Please double check "Fields and Parameters" configuration in Back Office.*
1108	*Compulsory parameter not set*
1109	*Missing parameter*
1110	*Missing PAY1_UICCODE parameter*
1111	*Invalid currency code*
1112	*Missing PAY1_AMOUNT parameter*
1113	*Not numeric amount*
1114	*Amount with a wrong number of decimal digits*
1115	*Missing PAY1_SHOPTRANSACTIONID parameter*
1116	*Too long PAY1_SHOPTRANSACTIONID parameter*
1117	*Invalid language identifier*
1118	*Not numeric characters in credit card number*
1119	*Credit card number with wrong length*
1120	*Credit card with wrong check-digit*
1121	*Credit card belongs to a Company not enabled*
1122	*Expiry year without expiry month*
1123	*Expiry month without expiry year*
1124	*Invalid expiry month*

1125	*Invalid expiry year*
1126	*Expired expiry date*
1127	*Invalid cardholder email address*
1128	*Too long parameter string*
1129	*Too long parameter value*
1130	*Not accepted call: missing parameter A*
1131	*Not accepted call: Shop not recognized*
1132	*Not accepted call: shop is not in active state*
1133	*Not accepted call: missing parameter B*
1134	*Not accepted call: empty parameter B*
1135	*Not accepted call: other parameters beside A and B are present*
1136	*Not accepted call: transaction did not begin with a call to server-server cryptography system*
1137	*Not accepted call: transaction already processed before*
1138	*Not accepted call: card number or expiry date are missing*
1139	*Not accepted call: missing published payment page*
1140	*Transaction cancelled by buyer*
1141	*Not accepted call: input parameter string not acceptable*
1142	*Not accepted call: invalid IP Address*
1143	*Transaction abandoned by buyer*
1144	*Compulsory field not set*
1145	*Invalid OTP*
1146	*Too small amount*
1147	*Too big amount*
1148	*Invalid cardholder name*
1150	*IPIN must be set*
1151	*Parameters error*
1999	*Technical error in connection with Credit Card Company network*
2000	*Transaction exceeds maximum operations number in time period*
2001	*Transaction exceeds maximum number of operations performed by the same buyer in time period*
2002	*Transaction exceeds maximum amount in time period*
2003	*Transaction exceeds maximum amount payable by same buyer in time period*
2004	*Transaction contains a field value that had been declared not acceptable*
2005	*Buyer abandoned the transaction because it was double*
2006	*Wrong line length*
2007	*Wrong value in SHOPTRANSACTIONID field*
2008	*Wrong value in CURRENCY field*
2009	*Wrong value in AMOUNT field*
2010	*Wrong value in AUTHORIZATION DATE field*
2011	*Transaction not found*
2012	*Transaction ambiguous*
2013	*Text file contains more rows related to the same transaction*
2014	*You requested a refund operation with an amount exceeding transaction balance*

2015	*Wrong value in BANKTRANSACTIONID field*
2016	*Fields BANKTRANSACTIONID and SHOPTRANSACTIONID are empty*
2017	*Transacion can not be deleted*
2018	*Transacion can not be refunded*
2019	*Transacion can not be settled*
2020	*Transacion can not be renounced*
7401	*Authorization refused by credit card companies*
7402	*Card not qualified*
7403	*Card not recognized*
7404	*Card expired*
7405	*Call credit card company*
7406	*Wrong card date*
7407	*Wrong transaction date*
7408	*System error*
7409	*Merchant not recognized*
7410	*Invalid format*
7411	*Amount not available*
7412	*Not settled*
7413	*Operation not allowed*
7414	*Network not available*
7415	*Collect card*
7416	*PIN attempts exhausted*
7417	*Blocked terminal*
7418	*Forcedly Closed terminal*
7419	*Not permitted transaction*
7420	*Not authorized transaction*
7421	*Servizio sospeso il 01/01/2002.*
9997	*Phase with error*
9998	*Phase correctly ended*
9999	*System Error*

12 Currency codes table

Currency code is managed by GestPay through currency attribute

Code UIC	Description
18	Italian lira
242	Euro
1	Dollar
2	Pound

13 Language codes table

Code	Description
1	Italian
2	English
3	Spanish
4	French
5	German