

# **GestPay**

## **Security Technical Specifications**

### **With OTP**

Document Information.....	3
Version Information.....	4
1 Introduction.....	5
2 System Architecture.....	6
Architecture Scheme.....	6
3 Process Phases Description.....	8
3.1 Phase I: Payment Page Call.....	8
3.2 Phase II: Transaction Result Communication.....	8
3.2.1 Response to Merchant.....	8
3.3.2 Response to Buyer.....	9
4 Authentication.....	10
5 Payment Transaction Data Structure.....	12
5.1 Transaction Data to Send to GestPay.....	12
5.2 Transaction Data Received by GestPay.....	14
6 Merchant's Profile.....	16
6.1 Answer url Configuration and e-mail.....	16
6.2 Fields & Parameters Configuration.....	16
7 Software Qualifications.....	18
7.1 Buyer's Browser Qualifications.....	18
7.2 Merchant's Server Qualifications.....	18
8 Transactions of Example.....	19
8.1 Transaction # 1.....	19
Payment page Url.....	20
8.2 Transaction #2.....	21
8.3 Transaction #3.....	22
9 Examples of Implementation.....	25
10 Table of Errors.....	26
11 Currency codes table.....	29
12 Language codes table.....	29

## Document Information

Project Name	GestPay
Document Title	GestPay – Security Technical Specifications with OTP
Creation Date	DD/01/YYYY 12:05:00
Language	English
Società	EasyNolo

## Version Information

Version	Description	Date	Author
1.0.0	Starting Version	03/15/2001	Sellanet
1.0.1	Browser Requirements Update	04/09/2001	Sellanet
1.0.2	Example errata corrige	08/02/2002	Sellanet
1.0.3	Custom Fields Requirements Update	20/08/2002	Sellanet
1.0.4	Error Codes Update	20/08/2002	Sellanet
1.0.5	Language Codes Update	20/08/2002	Sellanet
1.0.6	Custom Fields & Parameters Requirements Update	20/08/2002	Sellanet
1.0.7	Currency Codes Updated	27/01/2003	Sellanet
1.0.8	Domain for test codes	13/06/2007	Easy Nolo S.p.A.
1.0.9	Errata corrige, Update parameters list, Update Pay1_VBV possible values	28/01/2009	Easy Nolo S.p.A.
1.1.0	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 **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.

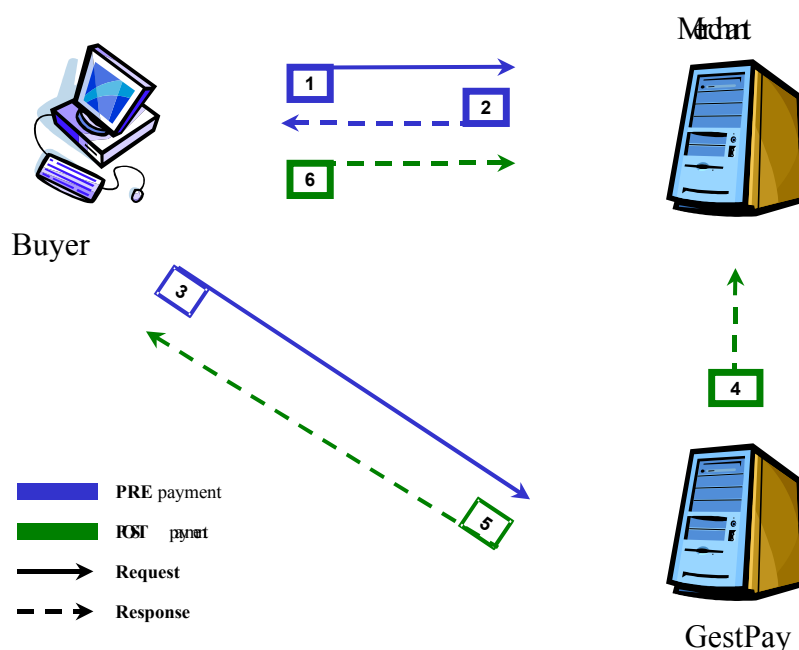
## 2 System Architecture

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).

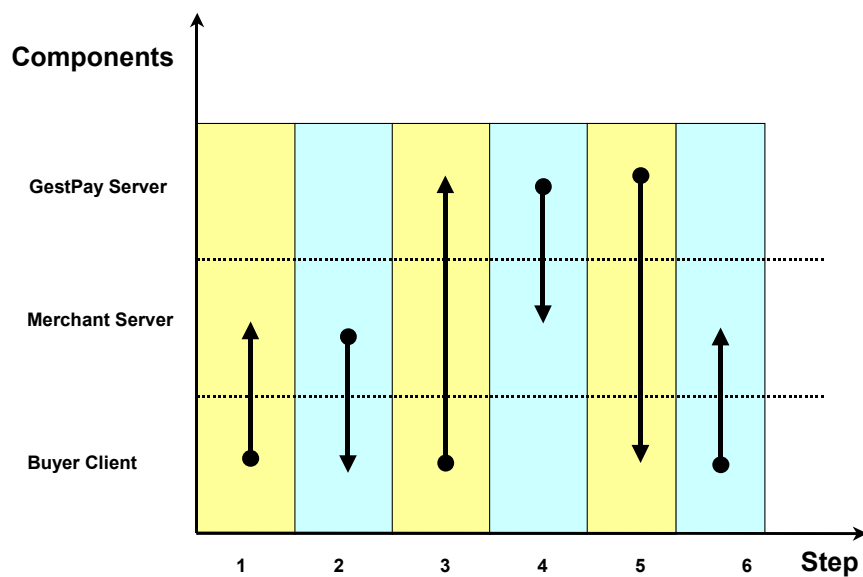
The payment process is divided in communication steps in which the components interact exchanging the information needed to the transaction performance.



### Architecture Scheme

1. The buyer selects the items to buy and decides to go on with the payment.
2. Merchant server send the parameters string to the buyer browser with all the the information need to perform the payment.
3. The buyer browser call the payment page on GestPay server sending the parameters string. GestPay do an authentication and integrity check to the string, if all the data sent where ok the buyer will be able to view the payment page to fill all the forms needed to complete the purchase. The following steps describe the way the response will be transfer to the merchant and to the buyer.
4. GestPay send the response in a parameters string to the buyer browser that will be redirect to the merchant server.
5. The buyer browser call the merchant response page sending the parameters string.
6. GestPay communicates to the merchant server to server page the parameter string that returns the transaction result.

The following scheme analyses the payment process underlining the chronological order in which the communication steps take place.



### 3 Process Phases Description

A payment transaction is made up of 2 basic phases in which there are one or more communication steps. In each phase, information necessary to the transaction elaboration is exchanged among the Gestpay server and Merchant Server through browser

#### 3.1 Phase I: Payment Page Call

The buyer's browser will be directed to the payment page on GestPay server at the address:

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

for test codes

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

Call to page will be made passing two parameters:

- a. Code that identifies merchant (Shop Login)
- b. 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 contain some informations that will enable to process the payment transaction).

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.

#### 3.2 Phase II: Transaction Result Communication

GestPay communicates transaction result both to merchant and to buyer.

##### 3.2.1 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=<parameters string>>

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



- a. Code which identifies merchant (Shop Login)
- b. Data string that contains the transaction result

The page on merchant server must have html tag <HTML></HTML> on source.

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 on GestPay Backoffice area in the Active Report section.

### 3.3.2 Response to Buyer

GestPay notifies immediately the transaction result by the visualization of «virtual ticket» that reports essential transaction data.

GestPay will direct buyer's browser to merchant's server to finish buying process. Merchant will have to prepare two Urls (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=<parameters 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.

## 4 Authentication

GestPay use OTP (One Time Password) to authenticate call to payment page and allows the merchant to recognize GestPay system when he receives the answer with the transaction response. The OTP are managed by the PAY1\_OTP parameter. Gestpay verify:

- **Shop Login validity:** ShopLogin parameter must correspond to a code registered in GestPay customers' details.
- **OTP Existence:** the otp send to Gestpay must be contains on otp.ric file associated to ShopLogin
- **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.

Security logic connected to OTP use provides that every password cannot be used a second time to make the payment page call and to verify responses coming from GestPay. Password must be deleted from the file where it has been withdrawn.

Password files delivered to merchant, in activation phase, are:

- **<ShopLogin>.ric:** contains passwords that must be used for the payment page calls.
- **<ShopLogin>.ris:** contains passwords that must be used to verify responses communicated by the bank to the merchant.

These files copies are on GestPay server and are used, respectively, for OTP verification when calling and for transaction result communication.

In the payment page call (phase I), merchant will have to use an OTP withdrawn from <ShopLogin>.ric file and delete that password from file. GestPay verify that the sent OTP is in the file associated to ShopLogin.

When positive, call is authenticated and payment process can go on.

When negative, payment page is not visualized to buyer and GestPay returns a negative result to merchant. In this situation, GestPay doesn't use an OTP withdrawn by .ris file associated to merchant (to not disalign OTP files) so that parameter c will be not communicated.

Call to GestPay must not be made using the resident page in the client's browser cache to avoid that a deleted password is reused and the call refused.

In the transaction result communication (phase II), GestPay uses an OTP taken from <ShopLogin>.ris file. Merchant must control that password sent by GestPay is in the <ShopLogin>.ris file he owns and, when negative, doesn't consider reliable the sent result (GestPay is not authenticated by a correct OTP).

If the sent OTP is not correct, merchant will have to delete it from <ShopLogin>.ris file.

Passwords contained in files are in text format and are made up of 32 alphanumerical characters. Their order is not important but, for the authentication process, is enough that OTP is in file.

## 4.1 OTP Set Generation

In order to create a new otp set is necessary to enter into back office area at this following addresses:

<https://ecommm.sella.it/gestpay/>

for test codes

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

and reach into Consumer Configuration/OTP section keeping this following steps:

1. Click on the button REQUEST: a pull-down menu will appear where to set the desired OPT number (from min. 10 up to max. 10000); then click on OK. The system will generate the OTP and send via e-mail at the address given in Configuration/ Response/ Information email, the message that the OTP requested have been correctly created, and can be downloaded. We remind you that the maximum waiting time to generate new passwords is about 2 hours.

2. Click on DOWNLOAD: the OTP files will be downloaded and a page with date of operation and number of the OTP requested will appear. The OTP just created will have to be added to the OTP you already have and not still used.

The use of the OTP is possible only after they have been activated.

3. Click on SWITCH ON: the OTP created will be activated and a page with the date of the operation and the number of activated OTP will appear. From this point on the OTP are active and recognised by GestPay when calling the payment page.

## 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
PAY1_UICCODE	Num (3)	P	O	Code that identifies the currency in which is denominated transaction amount (see <b>Currency Codes</b> table)
PAY1_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).
PAY1_SHOPTRANSACTIONID	VarChar (50)	P	O	Identifier attributed to merchant's transaction
PAY1_OTP	Char (32)	P	O	OTP ric
PAY1_CARDNUMBER	VarChar (20)	I/P	O	Credit card number
PAY1_EXPMONTH	Char (2)	I/P	O	Credit card expiry month
PAY1_EXPYEAR	Char (2)	I/P	O	Credit card expiry year
PAY1_CHNAME	VarChar (50)	I/P	F	Buyer's name and

				surname
PAY1_CHEMAIL	VarChar (50)	I/P	F	Buyer's e-mail address
PAY1_IDLANGUAGE	Num (2)	P	F	Code that identifies the language used in the communication with the buyer (see <b>Language Code</b> table)
PAY1_CVV	Num (4)	I/P	F	Card Verification Value
PAY1_3DLEVEL	VarChar (255)	P	F	Visa VBV / Mastercard Securecode authentication level
CustomInfo <sup>(1)</sup>	VarChar (1000)	P	F	String that has the specific information as configured in the merchant's profile

<sup>1</sup> 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 Parameter) or if it can be insert by the buyer (passed as Input) in the payment page.

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

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

- Currency (PAY1\_UICCODE)
- Amount (PAY1\_AMOUNT)
- Shop TransactionID (PAY1\_SHOPTRANSACTIONID)
- One Time Password (PAT1\_OTP)

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 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 reserved characters

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

## 5.2 Transaction Data Received by GestPay

GestPay communicates the payment transaction result to the merchant by a string that contains a series of information returned.

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
PAY1_UICCODE	Num (3)	P	O	Code that identifies the currency in which is denominated transaction amount (see <b>Currency Codes</b> table)
PAY1_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).
PAY1_SHOPTRANSACTIONID	VarChar (50)	P	O	Identifier attributed to merchant's transaction
PAY1_COUNTRY	VarChar (30)	P	F	Credit card issuing bank nationality used for the transaction
PAY1_VBV	VarChar (50)	P	F	VBV transaction flag (see VBV Codes table)
PAY1_OTP	Char (32)	P	O	OTP ris

PAY1_CHNAME	VarChar (20)	P	F	Buyer's name and surname
PAY1_CEMAIL	VarChar (50)	I/P	F	Buyer's e-mail address
PAY1_TRANSACTION RESULT	Char (2)	P	O	Transaction result
PAY1_AUTHORIZATIONCODE	VarChar (6)	P	O	Transaction authorizations code
PAY1_BANKTRANSACTIONID	Num (9)	P	O	Identifier attributed to the transaction by GestPay
PAY1_ERRORCODE	Num (9)	P	O	Error code
PAY1_ERRORDESCRIPTION	VarChar (255)	P	O	Error description
PAY1_ALERTCODE	Num (9)	P	F	Alert code
PAY1_ALERTDESCRIPTION	VarChar (255)	P	F	Alert description in language
CustomInfo <sup>(1)</sup>	VarChar (1000)	P	F	String that has the specific information as configured in the merchant's profile

<sup>1</sup> Each field can be maximum 300 characters

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

- Currency (PAY1\_UICCODE)
- Amount (PAY1\_AMOUNT)
- ShopTransactionID (PAY1\_SHOPTRANSACTIONID)
- One Time Password (PAY1\_OTP)
- TransactionResult (PAY1\_TRANSACTIONRESULT)
- AuthorizationCode (PAY1\_AUTHORIZATIONCODE)
- ErrorCode (PAY1\_ERRORCODE)
- ErrorDescription (PAY1\_ERRORDESCRIPTION)
- BankTransactionID (PAY1\_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://ecommm.sella.it/gestpay/login.asp>

for test codes

<https://testecommm.sella.it/gestpay/login.asp>

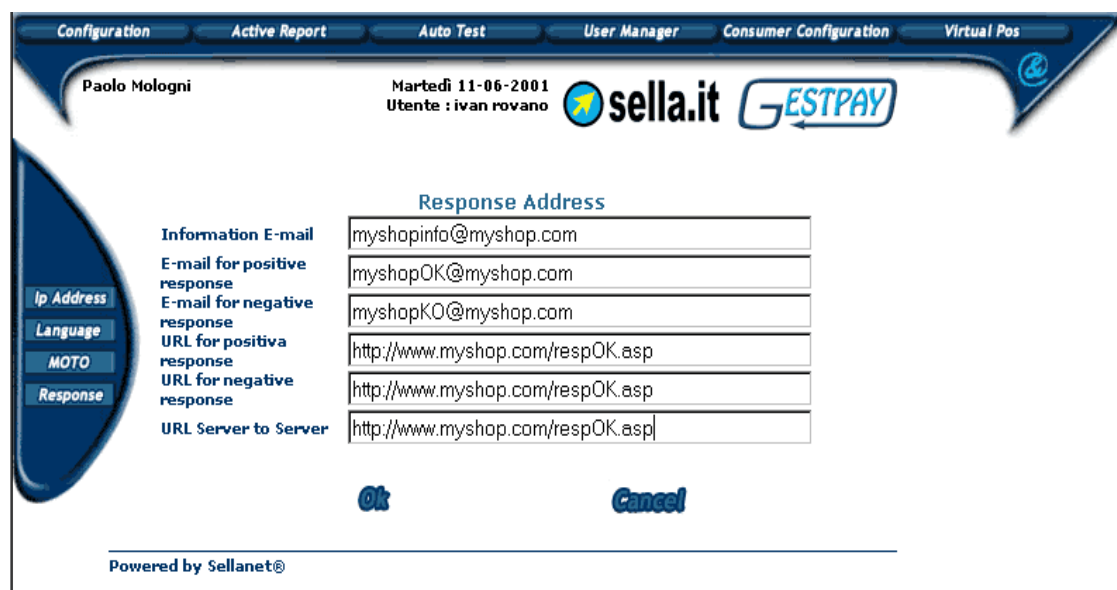
Other settings concern with modality and information that must be sent or that will be returned by GestPay.

### 6.1 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 – 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 by 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

Ok Cancel

Powered by Sellanet®



### 6.2 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.

[Configuration](#)
[Active Report](#)
[Auto Test](#)
[User Manager](#)
[Consumer Configuration](#)
[Virtual Pos](#)

Paolo Mologni
Martedì 11-06-2001  
Utente : ivan rovano



[Page Edit](#)
[Fields&Parameters](#)
[Setting Languages](#)
[Risk Restriction](#)

### Configure Input & Parameters

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

[Select Page](#)
[New](#)
[Preview](#)

Powered by Sellanet®

## 7 Software Qualifications

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

### 7.1 Buyer's Browser Qualifications

Domain <https://ecommerce.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.

### 7.2 Merchant's Server Qualifications

Server that hosts virtual shop doesn't need particular requirements.

Only if merchant decides to forward directly to GestPay the buyer's credit card number, will have to realize a site protected by digital certificate (buyer's sensible data must be protected when communicated via the Internet).

This situation is typical of merchants that hold customers' details including credit card number or that decide to acquire it directly on their own site.

## 8 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

### 8.1 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

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

Result	
Authorization code	54e813
Bank transaction ID	216
OTP ris	9ljds548yyH23d7thGs43ug122y6w6ur

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

Buyer's browser 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 the data string :

#### Payment page Url

```
Https://ecomm.sella.it/gestpay/pagam.asp?
a=9000001&b=PAY1_UICCODE=242*P1*PAY1_AMOUNT=1828.45*PAY1_SH
OPTRANSACTIONID=34az85ord19*P1*PAY1_OTP=34gJkui8326Fbs08uwe6387
hlmKasfr8
```

GestPay will make verification controls on Shop login (parameter a) and security controls on the 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 II

After you have processed transaction, GestPay communicates transaction result to merchant.

#### Server to server communication

```
http://www.mionegozio.com/s2s.asp?
a=9000001&b=PAY1_UICCODE=242*P1*PAY1_AMOUNT=1828.45*P1*PAY1_SHOPTRAN
SACTIONID=34az85ord19*P1*PAY1_OTP=34gJkui8326Fbs08uwe6387hlmKasfr8*P1*PAY1
_TRANSACTIONRESULT=OK*P1*PAY1_AUTHORIZATIONCODE=54e813*P1*PAY1_BAN
KTRANSACTIONID=216*P1*PAY1_ERRORCODE=0*P1*PAY1_ERRORDescription=Tr
ansazione%20eseguita
```

GestPay will address buyer's browser on merchant's server (in this case positive response url) communicating the result string.

#### Buyer's Redirect Client

```
http://www.mionegozio.com/rispOK.asp?
a=9000001&b=PAY1_UICCODE=242*P1*PAY1_AMOUNT=1828.45*P1*PAY1_SHOPTRAN
SACTIONID=34az85ord19*P1*PAY1_OTP=9ljds548yyH23d7thGs43ug122y6w6ur*P1*PAY1
_TRANSACTIONRESULT=OK*P1*PAY1_AUTHORIZATIONCODE=54e813*P1*PAY1_BAN
KTRANSACTIONID=216*P1*PAY1_ERRORCODE=0*P1*PAY1_ERRORDescription=Tr
ansazione%20eseguita
```

Transaction result is also notified to merchant via e-mail

#### Send E-mail

```
result_OK@myshop.com
```

## 8.2 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
OTP ric	34gJkui8326Fbs08uwe6387hlmKasfr8
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
OTP ris	9ljds548yyH23d7thGs43ug122y6w6ur
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

Buyer's browser 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 data string received in the previous phase by GestPay:

#### Payment page Url

<https://ecommm.sella.it/gestpay/pagam.asp?>

```
a=9000001&b=PAY1_UICCODE=18*P1*PAY1_AMOUNT=450600*P1*PAY1_SHOPTRANSA
CTIONID=Or784sR71*P1*PAY1_OTP=34gJkui8326Fbs08uwe6387hlmKasfr8*P1*PAY1_CAR
DNUMBER=4321432143214321*P1*PAY1_EXPMONTH=12*P1*PAY1_EXPYEAR=01*P1*PA
Y1_CHNAME=Paolo%20Rossi*P1*PAY1_CEMAIL=paolo.rossi@isp.it
```

GestPay will make verification controls on Shop login (parameter a) and security controls on the 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 II

After you have processed transaction, GestPay communicates transaction result to merchant.

### Server to server communication

```
http://www.mionegozio.com/s2s.asp?
a=9000001&b=PAY1_UICCODE=18*P1*PAY1_AMOUNT=450600*P1*PAY1_SHOPTRANSA
CTIONID=Or784sR71*P1*PAY1_OTP=9ljds548yyH23d7thGs43ug122y6w6ur*P1*PAY1_TRA
NSACTIONRESULT=KO*P1*PAY1_AUTHORIZATIONCODE=*P1*PAY1_BANKTRANSACTI
ONID=3861*P1*PAY1_ERRORCODE=1024*P1*PAY1_ERRORDescription=Carta
%20non%20riconosciuta
```

GestPay will address buyer's browser on merchant's server (in this case negative response url) communicating the result string.

### Buyer's Redirect Client

```
http://www.mionegozio.com/ rispKO.asp?
a=9000001&b=PAY1_UICCODE=18*P1*PAY1_AMOUNT=450600*P1*PAY1_SHOPTRANSA
CTIONID=Or784sR71*P1*PAY1_OTP=9ljds548yyH23d7thGs43ug122y6w6ur*P1*PAY1_TRA
NSACTIONRESULT=KO*P1*PAY1_AUTHORIZATIONCODE=*P1*PAY1_BANKTRANSACTI
ONID=3861*P1*PAY1_ERRORCODE=1024*P1*PAY1_ERRORDescription= Carta
%20non%20riconosciuta
```

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

### Send E-mail

```
result_KO@myshop.com
paolo.rossi@isp.it
```

## 8.3 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
OTP ric	34gJkui8326Fbs08uwe6387hlmKasfr8
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
OTP ris	9ljds548yyH23d7thGs43ug122y6w6ur

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

Buyer's browser 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 data string received in the previous phase by GestPay:

### Payment page Url

```
https://ecommm.sella.it/gestpay/pagam.asp?
a=9000001&b=PAY1_UICCODE=242*P1*PAY1_AMOUNT=1245.6*P1*PAY1_SHOPTRANS
ACTIONID=34az85ord19*P1*PAY1_OTP=34gJkui8326Fbs08uwe6387hlmKasfr8*P1*PAY1_I
DLANGUAGE=3*P1*PAY1_CHNAME=Mario
%20Bianchi*P1*PAY1_CHEMAIL=mario.bianchi@isp.it*P1*BV_CODCLIENTE=12*P1*BV_S
```

SESSIONID=398
---------------

GestPay will make verification controls on Shop login (parameter a) and security controls on the 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 II

After you have processed transaction, GestPay communicates transaction result to merchant.

### Server to server communication

```
http://www.mionegozio.com/s2s.asp?
a=9000001&b=PAY1_UICCODE=242*P1*PAY1_AMOUNT=1245.6*P1*PAY1_SHOPTRANS
ACTIONID=34az85ord19*P1*PAY1_OTP=9ljds548yyH23d7thGs43ug122y6w6ur*P1*PAY1_T
RANSACTIONRESULT=OK*P1*PAY1_AUTHORIZATIONCODE=9823y5*P1*PAY1_BANKT
RANSACTIONID=860*P1*PAY1_ERRORCODE=0*P1*PAY1_ERRORDESCRIPTION=Transa
zione%20eseguita*P1*BV_CODCLIENTE=12*P1*BV_SESSIONID=398
```

GestPay will address buyer's browser on merchant's server (in this case positive response url) communicating the same result string.

### Buyer's Redirect Client

```
http://www.mionegozio.com/s2s.asp?
a=9000001&b=PAY1_UICCODE=242*P1*PAY1_AMOUNT=1245.6*P1*PAY1_SHOPTRANS
ACTIONID=34az85ord19*P1*PAY1_OTP=9ljds548yyH23d7thGs43ug122y6w6ur*P1*PAY1_T
RANSACTIONRESULT=OK*P1*PAY1_AUTHORIZATIONCODE=9823y5*P1*PAY1_BANKT
RANSACTIONID=860*P1*PAY1_ERRORCODE=0*P1*PAY1_ERRORDESCRIPTION=Transa
zione%20eseguita*P1*BV_CODCLIENTE=12*P1*BV_SESSIONID=398
```

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

### Send E-mail

result_OK@myshop.com
mario.bianchi@isp.it



## 9 Examples of Implementation

In this chapter it is described an example of interfacing to GestPay realized using HTML language.

HTML Example

CODE TO MAKE A CONNECTION TO PAYMENT PAGE (PAYMENT REQUEST)

```
<form action="https://ecommm.sella.it/gestpay/pagam.asp">
<input type="hidden" name="a" value="90000001">
<input type="hidden" name="b" value="PAY1_AMOUNT=3400...">
</form>
```

for test codes

```
<form action="https://testecommm.sella.it/gestpay/pagam.asp">
<input type="hidden" name="a" value="90000001">
<input type="hidden" name="b" value="PAY1_AMOUNT=3400...">
</form>
```

## 10 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	<i>Authorization denied</i>
907	<i>Authorization denied</i>
908	<i>Authorization denied</i>
910	<i>Authorization denied</i>
911	<i>Authorization denied</i>
913	<i>Authorization denied</i>
914	<i>Authorization denied</i>
915	<i>Authorization denied</i>
916	<i>Authorization denied</i>
917	<i>Authorization denied</i>
918	<i>Authorization denied</i>
919	<i>Authorization denied</i>
920	<i>Authorization denied</i>
950	<i>Not qualified credit card</i>
951	<i>Wrong merchant configuration in bank authorizative system</i>
998	<i>Credit card with wrong check-digit</i>
999	<i>Operation not performed</i>
1100	<i>Empty parameter string</i>
1101	<i>Invalid format of parameter string</i>
1102	<i>No parameter name precedes = symbol</i>
1103	<i>Parameter string ending with a separator</i>
1104	<i>Invalid parameter name</i>
1105	<i>Invalid parameter value</i>
1106	<i>Repeated parameter name</i>
1107	<i>Unexpected parameter name. Please double check "Fields and Parameters" configuration in Back Office.</i>
1108	<i>Compulsory parameter not set</i>
1109	<i>Missing parameter</i>
1110	<i>Missing PAYI_UICCODE parameter</i>
1111	<i>Invalid currency code</i>
1112	<i>Missing PAYI_AMOUNT parameter</i>
1113	<i>Not numeric amount</i>
1114	<i>Amount with a wrong number of decimal digits</i>
1115	<i>Missing PAYI_SHOPTRANSACTIONID parameter</i>
1116	<i>Too long PAYI_SHOPTRANSACTIONID parameter</i>
1117	<i>Invalid language identifier</i>
1118	<i>Not numeric characters in credit card number</i>
1119	<i>Credit card number with wrong length</i>
1120	<i>Credit card with wrong check-digit</i>
1121	<i>Credit card belongs to a Company not enabled</i>
1122	<i>Expiry year without expiry month</i>
1123	<i>Expiry month without expiry year</i>
1124	<i>Invalid expiry month</i>
1125	<i>Invalid expiry year</i>
1126	<i>Expired expiry date</i>
1127	<i>Invalid cardholder email address</i>
1128	<i>Too long parameter string</i>
1129	<i>Too long parameter value</i>
1130	<i>Not accepted call: missing parameter A</i>
1131	<i>Not accepted call: Shop not recognized</i>
1132	<i>Not accepted call: shop is not in active state</i>
1133	<i>Not accepted call: missing parameter B</i>
1134	<i>Not accepted call: empty parameter B</i>
1135	<i>Not accepted call: other parameters beside A and B are present</i>
1136	<i>Not accepted call: transaction did not begin with a call to server-server cryptography system</i>
1137	<i>Not accepted call: transaction already processed before</i>
1138	<i>Not accepted call: card number or expiry date are missing</i>

1139	<i>Not accepted call: missing published payment page</i>
1140	<i>Transaction cancelled by buyer</i>
1141	<i>Not accepted call: input parameter string not acceptable</i>
1142	<i>Not accepted call: invalid IP Address</i>
1143	<i>Transaction abandoned by buyer</i>
1144	<i>Compulsory field not set</i>
1145	<i>Invalid OTP</i>
1146	<i>Too small amount</i>
1147	<i>Too big amount</i>
1148	<i>Invalid cardholder name</i>
1150	<i>IPIN must be set</i>
1151	<i>Parameters error</i>
1999	<i>Technical error in connection with Credit Card Company network</i>
2000	<i>Transaction exceeds maximum operations number in time period</i>
2001	<i>Transaction exceeds maximum number of operations performed by the same buyer in time period</i>
2002	<i>Transaction exceeds maximum amount in time period</i>
2003	<i>Transaction exceeds maximum amount payable by same buyer in time period</i>
2004	<i>Transaction contains a field value that had been declared not acceptable</i>
2005	<i>Buyer abandoned the transaction because it was double</i>
2006	<i>Wrong line length</i>
2007	<i>Wrong value in SHOPTRANSACTIONID field</i>
2008	<i>Wrong value in CURRENCY field</i>
2009	<i>Wrong value in AMOUNT field</i>
2010	<i>Wrong value in AUTHORIZATION DATE field</i>
2011	<i>Transaction not found</i>
2012	<i>Transaction ambiguous</i>
2013	<i>Text file contains more rows related to the same transaction</i>
2014	<i>You requested a refund operation with an amount exceeding transaction balance</i>
2015	<i>Wrong value in BANKTRANSACTIONID field</i>
2016	<i>Fields BANKTRANSACTIONID and SHOPTRANSACTIONID are empty</i>
2017	<i>Transacion can not be deleted</i>
2018	<i>Transacion can not be refunded</i>
2019	<i>Transacion can not be settled</i>
2020	<i>Transacion can not be renounced</i>
7401	<i>Authorization refused by credit card companies</i>
7402	<i>Card not qualified</i>
7403	<i>Card not recognized</i>
7404	<i>Card expired</i>
7405	<i>Call credit card company</i>
7406	<i>Wrong card date</i>
7407	<i>Wrong transaction date</i>
7408	<i>System error</i>
7409	<i>Merchant not recognized</i>
7410	<i>Invalid format</i>
7411	<i>Amount not available</i>
7412	<i>Not settled</i>
7413	<i>Operation not allowed</i>
7414	<i>Network not available</i>
7415	<i>Collect card</i>
7416	<i>PIN attempts exhausted</i>
7417	<i>Blocked terminal</i>
7418	<i>Forcedly Closed terminal</i>
7419	<i>Not permitted transaction</i>
7420	<i>Not authorized transaction</i>
7421	<i>Servizio sospeso il 01/01/2002.</i>
9997	<i>Phase with error</i>
9998	<i>Phase correctly ended</i>

9999	System Error
------	--------------

## 11 Currency codes table

Currency code is managed by GestPay through currency attribute

Code UIC	Description
18	Italian lira
242	Euro
1	Dollar
2	Pound
71	Yen
103	Hong Kong Dollar
234	Real

## 12 Language codes table

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

## 13 Payment Orders made on Gestpay Test Codes

We remind you that also the payment orders you made through a Gestpay Test Code, using a real credit card, book the amount on the credit card plafond (but no amount will be charged after the booking).

Therefore we suggest you to make payment orders on Gestpay test code only for minimum amounts.