e-Commerce Gateway merchant interface

(CGI/WWW forms version)

Contents

Overview

This manual is intended for use by programmers responsible for the merchant payment gateway interface. It describes the interface that merchant systems use to process credit card based e-commerce transactions using the standard CGI/WWW forms posting method. This interface transparently supports various cardholder authentication protocols such as 3-D Secure and Secure Code as well as legacy unauthenticated SSL commerce transactions.

Chapter 1. Retail Transactions Interface

Transaction Flow Scenario

1. After selecting goods and services, the cardholder presses ‘Buy’ or an equivalent button and proceeds to a page where he can enter or modify delivery information and the payment method. Payment method information may offer various payment methods, like ‘Pay by credit card’ or a similar option. This option should not include card number, expiry date, CVC2 or any other card related sensitive information. Because of security risks involved, merchant system should avoid requesting and storing credit card information on the merchant server.

2. If cardholder selects ‘Pay by credit card’ option, merchant system must prepare authorization request fields and redirect the cardholder to an ‘Enter credit card information' page on e-Commerce Gateway CGI URL (https://egateway.victoriabank.md/cgi-bin/cgi_link).

3. After receiving the filled-in form, e-Commerce Gateway validates request information including the message authentication code (field P_SIGN). If the request fails, the validation gateway sends an error response back to merchant system.

4. Upon authorization, reception gateway prepares and sends a transaction response back to the client. Parallel gateway sends response messages to the merchant system to HTTPS url or HTTP url or EMAIL, depending on merchants system.

!!! We strongly recommend to use HTTPS url for receiving response messages.

   Response message will contain message authentication code(field P_SIGN), which is used to prevent spoofing of data in the response message.

   If authorization is successful, the response message will contain the “Internal Reference Number” field, to be used by the merchant system so it can complete or reverse the obtained authorization without the credit card information.

5. After receiving the authorization response (on HTTPS url or HTTP url or EMAIL), the merchant system starts delivery of ordered goods and/or services to the cardholder. At this point, the requested amount is blocked on the cardholder account. Merchant should send an e-mail invoice message to the cardholder with order information and delivery time if applicable.

6. When the merchant has delivered the goods and services to cardholder, the merchant system sends a “Sales completion” transaction directly to the e-Commerce Gateway CGI URL (https://egateway.victoriabank.md/cgi-bin/cgi_link) using an internal reference number to refer to the authorization transaction with its corresponding credit card information. The transaction request should include a message authentication code field (field P_SIGN) for verifying the message's identity.

7. Gateway validates the incoming message and requests financial completion of the transaction from the Way4 card system. At this point, the transaction amount is debited from the cardholder account and the merchant account is credited with the appropriate amount. Gateway sends a response to merchant system within the response document.

8. If the merchant is unable to fulfill the cardholder order or if the cardholder cancels the order at a stage allowed by the merchant, the merchant system must send a “Reversal” message to cancel the pending or completed transaction. The merchant system sends this message directly to the gateway CGI URL. The transaction request should include a message authentication code field for verifying the message's identity.

9. Gateway validates the incoming message and requests a reversal of the pending or completed transaction from the Way4 card system. This may involve transferring funds from the merchant account back to the cardholder account. Gateway sends a reply to the merchant system within the response document.

Authorization Request Format

The following fields set will be posted to e-Commerce Gateway CGI URL through the HTTP POST method.

Table 2. Authorization message visible fields generated by merchant system

Field	**Size**	**Description**
AMOUNT	1-12	Order total amount in float format with decimal point separator
CURRENCY	03	Order currency: 3-character currency code
ORDER	6-32	Merchant order ID
DESC	1-50	Order description
MERCH_NAME	1-50	Merchant name (recognizable by cardholder)
MERCH_URL	1-250	Merchant primary web site URL in format http://www.merchantsitename.domain
MERCHANT	15	Merchant ID assigned by bank
TERMINAL	8	Merchant Terminal ID assigned by bank
EMAIL	80	Client e-mail address
MERCH_ADDRESS	250	Merchant company registered office address

Table 3. Authorization message's hidden fields generated by merchant system

Field	**Size**	**Description**
TRTYPE	1	Must be equal to "0" (Authorization).
COUNTRY	02	Merchant shop 2-character country code. Must be provided if merchant system is located in a country other than the gateway server's country.
MERCH_GMT	1-5	Merchant UTC/GMT time zone offset (e.g. –3). Must be provided if merchant system is located in a time zone other than the gateway server's time zone.
TIMESTAMP	14	Merchant transaction timestamp in GMT: YYYYMMDDHHMMSS. Timestamp difference between merchant server and e-Gateway server must not exceed 1 hour, otherwise e-Gateway will reject this transaction.
NONCE	1-64	Merchant nonce. Must be filled with 20-32 unpredictable random bytes in hexadecimal format. Must be present if MAC is used.
BACKREF	1-250	Merchant URL for redirecting the client after receiving transaction result.
P_SIGN	1-256	Merchant MAC in hexadecimal form.
LANG	02	Transaction forms language. By default are available forms in en, ro, ru. If need forms in another languages please contact gateway administrator.

Authorization Response Format

Table 5.E-Commerce Gateway response fields set

Field	**Size**	**Description**
TERMINAL	8	Echo from the request
TRTYPE	2	Echo from the request
ORDER	6-32	Echo from the request
AMOUNT	12	Echo from the request
CURRENCY	3	Echo from the request

ACTION	1	E-Gateway action code:
		🕘 0 – Transaction successfully completed;
		🕘 1 – Duplicate transaction detected;
		🕘 2 – Transaction declined;
		🕘 3 – Transaction processing fault.

RC	02	Transaction response code (ISO-8583 Field 39)
APPROVAL	06	Client bank's approval code (ISO-8583 Field 38). Can be empty if not provided by card management system.
RRN	12	Merchant bank's retrieval reference number (ISO-8583 Field 37).
INT_REF	1-32	E-Commerce gateway internal reference number
TIMESTAMP	14	E-Commerce gateway timestamp in GMT: YYYYMMDDHHMMSS
NONCE	1-64	E-Commerce gateway nonce value. Will be filled with 8-32 unpredictable random bytes in hexadecimal format. Will be present if MAC is used.
P_SIGN	1-256	E-Commerce gateway MAC (Message Authentication Code) in hexadecimal form. Will be present if MAC is used.
ECI	0-02	Electronic Commerce Indicator (ECI): • ECI=empty – Technical fault; • ECI=05 - Secure electronic commerce transaction (fully 3-D Secure authenticated); • ECI=06 - Non-authenticated security transaction at a 3-D Secure-capable merchant, and merchant attempted to authenticate the cardholder using 3-D Secure but was unable to complete the authentication because the issuer or cardholder does not participate in the 3-D Secure program; • ECI=07 - Non-authenticated Security Transaction

Sales Completion Request Format

This transaction shall be sent by the merchant system when goods and/or services are delivered to cardholder. The card system will complete the financial transaction and transfer funds to the merchant account.

All fields are provided by merchant system and the cardholder does not participate in this transaction.

Table 6. Sales completion message fields provided by the merchant system

Field	Size	Description
ORDER	6-32	Merchant order ID from request.
AMOUNT	12	Transaction amount. Float format with decimal point separator.
CURRENCY	3	Currency name. Must be the same as in authorization response.
RRN	12	Retrieval reference number from authorization response.
INT_REF	1-32	Internal reference number from authorization response.
TRTYPE	2	Must be equal to "21" (Sales completion).
TERMINAL	8	Merchant terminal ID assigned by bank. Must be equal to "TERMINAL" field from authorization request.
TIMESTAMP	14	Merchant transaction timestamp in GMT: YYYYMMDDHHMMSS. Timestamp difference between Internet shop and e-Gateway must not exceed 1 hour otherwise e-Gateway will reject this transaction.
NONCE	1-64	Merchant nonce. Must be filled with 8-32 unpredictable random bytes in hexadecimal format. Must be present if MAC is used.
P_SIGN	1-256	Merchant MAC in hexadecimal form.

Sales Completion Response Format

The field set and format are the same as for the authorization response. See *Table 5* for details.

Reversal Request Format

The reversal transaction request shall be sent by the merchant system to e-Commerce Gateway in order to cancel previously authorized or completed transactions. The request format and transmission method are the same as for the sales completion request except the TRTYPE field (See *Tables 6* and *7*).

All fields are provided by merchant system and the cardholder does not participate in this transaction.

Table 7. Amended field for reversal request

Field	Size	Description
TRTYPE	2	Must be equal to “24” (Reversal advice)

Reversal Response Format

The field set and format are the same as for the authorization response. See Table 5 for details.

Appendix A

P_SIGN creation/verification in the Merchant System

1. Settings on the merchant side

Merchant system must form digital signature (P_SIGN) as follows:
1) Merchant system assemble a control string on which a digital signature will be generated.
Example:
If
ORDER = 100001
NONCE = 11111111000000011111
TIMESTAMP = 20110627060100
TRTYPE = 0
AMOUNT=34.99
Then a control string will be: **61000012011111111000000011111142011062706010010534.99**
Where 6, 20, 14, 1, 5 are the lengths of content of the corresponding fields.

2) This string is hashed by MD5 (16 bytes) in HEX format
The result for this example will be:
MD5 hash: 8530fae8c7ca6d3e7294763ecb0f3c59
3) To the md5 hash is added HEX prefix:
«003020300C06082A864886F70D020505000410»
4) The result string is added in front with "0001" then "FF" to a length equal to the length of the RSA key, by which all will be encrypted. The result is a HEX string of the form:
0001FFFFFFF….FFFFFF003020300C06082A864886F70D020505000410[MD5HASH]
5) The string is converted into a binary buffer (HEX to BIN conversion) and then is encrypted with a merchant private RSA key.
6) The resulting binary buffer is converted to the hexadecimal form (BIN to HEX conversion) and then sent as a digital signature in P_SIGN field.

!!! The signature, which E-Gateway sends back to the merchant system in response message is formed in the same way automatically.
E-Gateway forms P_SIGN using the following fields:
ACTION, RC, RRN, ORDER, AMOUNT
Merchant system must decrypt P_SIGN field received in response message from E-Gateway using bank public RSA key.
Merchant system must compare MD5HASH from decrypted p_sign with MD5HASH formed using received response message fields(ACTION, RC, RRN, ORDER, AMOUNT).

2. Key Generation and transmission

1) To generate a new RSA key should be used the OpenSSL utility.
The command for key generation is as follows.

```
openssl genrsa -f4 -out key.pem 2048
```

Where the parameter specifies the open-f4 exponent equal to 63 537. May be omitted.
Parameter-out key.pem specifies the output file name and the last parameter specifies the key length in bits.

The successful execution of the command creates the file key.pem

⚠ Formed file contains the value of the secret part of the RSA key, and should not be transmitted in the clear. With this key (private parts) Merchant system should create a digital signature (P_SIGN).

2) To create a public key for e-gateway system, merchant must execute the command:

```
openssl rsa -pubout -in key.pem -out pubkey.pem
```

The successful execution of the command creates a file pubkey.pem.

3) Formed public-key file is transmitted to the servicing bank.

Appendix B

Test Cases

Before starting work in production environment merchant system should execute a set of tests.

Test case No	Transaction types to execute	Description
1	Authorization request	Merchant system perform Authorization request transaction(TRTYPE=0), then using data received in Authorization response perform Sales completion request(TRTYPE=21)
	Sales completion request	
2	Authorization request	Merchant system perform Authorization request transaction(TRTYPE=0), then using data received in Authorization response perform Reversal request(TRTYPE=24)
	Reversal request	
3	Authorization request	Merchant system perform Authorization request transaction(TRTYPE=0), then using data received in Authorization response perform Sales completion request(TRTYPE=21). After receiving Sales completion response PSP system should perform Reversal request(TRTYPE=24).
	Sales completion request	
	Reversal request	

For each test case please provide RRN for checking.