e-Commerce Gateway merchant interface

(CGI/WWW forms version)

Contents

OVERVIEW 2

CHAPTER 1. RETAIL TRANSACTIONS INTERFACE 3

Transaction Flow Scenario 3
Authorization Request Format 4
Authorization Response Format 6
Sales Completion Request Format 7
Sales Completion Response Format 8
Reversal Request Format 8
Reversal Response Format 8

CHAPTER 2. COMMON ELEMENTS 9

Merchant MAC – Message Authentication Code 9

REVISIONS HISTORY 11

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 3D-Secure and Secure Code as well as legacy unauthenticated SSL commerce transactions.

Chapter 1. Retail Transactions Interface

Transaction Flow Scenario

Way4 e-Commerce gateway supports various transaction flow scenarios, but this document will focus only on the recommended scenario, described below.

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.

   Alternatively, the merchant system itself may present this page directly to cardholder. In this case posting URL for this page form must be set to e-Commerce Gateway CGI URL.

   This form shall contain all card entry fields and visible/hidden fields relating to the order and merchant as required by the authorization request format.
3. After receiving the filled-in form, e-Commerce Gateway validates request information including the message authentication code. If the request fails, the validation gateway sends an error response back to merchant system.
4. If the provided card number belongs to a card range with a defined cardholder authentication method, gateway calls the corresponding authentication module (3D Secure, MasterCard SPA, e-Token, etc.), which performs protocol-specific processing. If cardholder authentication is unsuccessful, Gateway returns an error message to the merchant system or falls back on a legacy e-Commerce SSL transaction type to continue this transaction.
5. Gateway sends an authorization request to the Way4 card system. Upon authorization, reception gateway prepares and sends a transaction response back to the merchant system. The transaction response contains no credit card information or contains the card number in blinded form only.

   Gateway sends response messages to the merchant system using cardholder redirect. Redirect may be done automatically or as an intermediate form to be posted on the merchant server. Response messages may also contain a message authentication code in order to verify the message's identity.

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.

6. Additionally the e-commerce gateway may send (if requested by the configuration) an e-mail notification to the merchant system with the same information as the online transaction response message. This is done in case of possible transport problems while delivering a redirected message.
7. After receiving the online transaction response or its e-mail notification, 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.
8. 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 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 for verifying the message's identity.
9. 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 back to merchant system within the response document.
10. 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.
11. 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. The set of field is divided into three subsets: visible fields filled by cardholder, visible fields generated by the merchant system and hidden fields generated by the merchant system. The page may contain JavaScript functions that pre-validate cardholder field input.

Table 1. Authorization message fields specified by the cardholder

Field	Size	Description
CARD	9-19	Card number (Primary account number).
EXP	02	Card expiration month (Numeric 2 digit value). Can be presented as "select" field (01-12): <option value="01">01 January</option> <option value="02">02 February</option> <option value="03">03 March</option> <option value="04">04 April</option> <option value="05">05 May</option> <option value="06">06 June</option> <option value="07">07 July</option> <option value="08">08 August</option> <option value="09">09 September</option> <option value="10">10 October</option> <option value="11">11 November</option> <option value="12">12 December</option>
EXP_YEAR	02	Card expiration year (Numeric 2 digit value: 20XX). Can be presented as "select" field for 15-20 years ahead.
CVC2	03	Card verification code (last three digits on the signature panel).
CVC2_RC	01	CVC2 reason code. Must be presented as "select" field with following values: <option selected value="1">CVC2 is present</option> <option value="0">CVC2 is not provided</option> <option value="2">CVC2 is illegible</option> <option value="9">No CVC2 on card</option>
ZIP	6	Cardholder billing ZIP code. Can be present if Address verification service is used.
AVS	80	Cardholder billing address. Can be present if Address verification service is used.
CVC3	03	Cardholder verification code. Must be present if requested by local banks.

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
MERCHANT	15	Merchant ID assigned by bank
TERMINAL	8	Merchant Terminal ID assigned by bank
EMAIL	80	E-mail address for notification. If this field is present Gateway may send transaction results notification to specified e-mail 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 8-32 unpredictable random bytes in hexadecimal format. Must be present if MAC is used.
BACKREF	1-250	Merchant URL for posting authorization result.
P_SIGN	1-256	Merchant MAC in hexadecimal form.

Additionally, the credit card information entry page may contain two empty hidden fields reserved for MasterCard SPA support.

Table 4. MasterCard SPA hidden fields

Field	Size	Description
Ucaf_Flag	1	UCAF Security Level Indicator.
Ucaf_Authentication_Data	2-32	UCAF Authentication Data Field.

Authorization Response Format

E-Commerce Gateway processes the authorization request and returns an HTML page containing a web form with result fields, listed in the next table. The web form will be manually or automatically posted (depending on configuration) via cardholder browser to a merchant system URL provided in the BACKREF incoming field. Additionally, the same field set may be sent to the merchant system via e-mail to the address provided in the EMAIL incoming field in case of possible connection problems with the cardholder browser.

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.

Sales Completion Request Format

The following fields set shall be posted to e-Commerce Gateway CGI URL using HTTP POST method over SSL (HTTPS). The Message Authentication Code can be omitted if using mutual authenticated SSL (SSL with client certificate).

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

Gateway processes the sales completion request and returns result fields to merchant system within the response document. Response fields are formatted in URL-encoded form. 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

Gateway processes a reversal request and returns the result fields to the merchant system within a response document. Response fields are formatted in URL-encoded form. The field set and format are the same as for the authorization response. See *Table 5* for details.

Chapter 2. Common Elements

Merchant MAC – Message Authentication Code

To authenticate transaction messages on gateway to/from the merchant link, the merchant system should be able to calculate and verify message authentication codes for at least the transactions passed through cardholder browser redirects. Messages that are sent directly to e-Commerce Gateway ("Sales completion" and "Reversal") may be mutually authenticated with SSL client/server certificates and does not require MAC; if they are not mutually authenticated, MAC for these messages is mandatory.

MAC is calculated over all fields generated by the merchant system as defined in corresponding format tables (visible and hidden fields generated by the merchant system) except the MAC field ("P_SIGN") itself.

In order to generate or verify the message authentication field, the merchant system must assemble a MAC source string; all field values from the format tables are prefixed with the decimal field length in ASCII and concatenated in a specified order. If the field is not present, the '-' character is added to the message in its place.

Authorization message example: MAC source string will contain the following field values - AMOUNT, CURRENCY, ORDER, DESC, MERCH_NAME, MERCH_URL, MERCHANT, TERMINAL, EMAIL, TRTYPE, COUNTRY, MERCH_GMT, TIMESTAMP, NONCE, BACKREF. Suppose that we have a transaction with following fields:

Field	Length	Value
AMOUNT	5	11.48
CURRENCY	3	USD
ORDER	6	771446
DESC	16	IT Books. Qty: 2
MERCH_NAME	17	Books Online Inc.
MERCH_URL	14	www.sample.com
MERCHANT	15	123456789012345
TERMINAL	8	99999999
EMAIL	19	pgw@mail.sample.com
TRTYPE	1	1
COUNTRY	0	
MERCH_GMT	0	
TIMESTAMP	14	20030105153021
NONCE	16	F2B2DD7E603A7ADA
BACKREF	33	https://www.sample.com/shop/reply

MAC source string for this example is:

```
511.483USD677144616IT Books. Qty: 217Books Online Inc.14www.sample.com
15123456789012345899999999919pgw@mail.sample.com11--1420030105153021
16F2B2DD7E603A7ADA33https://www.sample.com/shop/reply
```

Line breaks are inserted for visibility only. This string is 190 bytes long.

After the MAC source string is assembled, the merchant system must apply a cryptographic algorithm to generate the message authentication code. Gateway supports various cryptographic algorithms and the system administrator may specify which algorithm will be used for a particular merchant terminal.

The merchant system must implement a chosen algorithm either in hardware or software form and be fully responsible for the secure storage and usage of corresponding cryptographic keys. An effective key length must be at least 112 bits for symmetric cryptographic algorithms and 1024 bits for RSA algorithm.

The default MAC algorithm is HMAC_SHA1. Standard options include Triple DES ABA/ABC CBC MAC, AES 128 CBC MAC and RSA/SHA1 signature. Additional options may be available on demand.

For our MAC source string example and HMAC_SHA1 algorithm with hexadecimal secret key “00112233445566778899AABBCCDDEEFF”, the result MAC (“P_SIGN”) field must be equal to: “FACC882CA67E109E409E3974DDEDA8AAB13A5E48”. MAC field value can be either an upper case or lower case hexadecimal string.

Revisions History

Reference number	Description
03.15.10-00001-15.10.2003	Extracted from “e-Commerce Gateway Module” document.
03.15.10-00002-05.01.2004	Minor clarifications added.
03.22.19-00003-03.08.2006	Fixed error with TRTYPE=0 – authorization.