Way4™ e-Gateway Module

Overview

Contents

INTRODUCTION 2

CHAPTER 1. OVERVIEW 3

e-Commerce Transaction Process flow 3
Internet P.O.S. Transaction Process flow 6
Connection scheme of high-volume Internet e-Commerce site 8
Connection scheme of Payment e-Gateway site for multiple Internet Merchants e-Commerce sites 8
Connection scheme of Payment e-Gateway for Internet P.O.S. transactions 8

Introduction

This manual is intended for Bank (Processing Center) administrators that will support and maintain the e-Commerce Gateway between Web shops and Way4™ System.

It is also recommended that you read the following guides, included in the set of OpenWay manuals (these manuals are available only with Internet Banking Module):

- "Internet Banking Overview"
- "OpenWay Internet Banking Module. Developer Guide"

The following conventions are used in the manual:

- *Italic* indicates a form field;
- [Square brackets] indicate form buttons, e.g. [Approve];
- → indicates the next item to be selected in the sequence of User Menu items, e.g. "Issuing→Contracts Input & Update";
- ⇒ indicates the next item to be selected in the sequence of System Menu items, e.g. "Database ⇒ Change password";
- <Angle brackets> indicate shortcut keys available in DB Manager, e.g. <Ctrl>+<F3>;
- ☝ indicates a warning of a possible wrong action

Chapter 1. Overview

Secure e-Gateway Module is an open e-Commerce solution for Banks, Internet merchants and ISPs.

It consists of two submodules:

- Secure E-Gateway Client, installed on the Merchant/Bank/ISP Web Server
  - SSL connection with cardholder;
  - CGI or API connection with Internet Shops;
  - Internet P.O.S. authorization and PIN-based transactions processing;
  - Secure connection to PIN pad agent installed at the client side;
  - Transaction pre-validation and logging facility;
  - Secure ISO8583 connection to the e-Gateway Server;
  - Single and Dual transaction message service;
  - Multiple platform support (Windows NT/2000 and UNIX);
- Secure e-Gateway Server, installed at the Authorization Processor
  - Secure ISO8583 connection to the e-Gateway Client;
  - Interface to VISA, Europay and other payment networks;
  - Connection with Host Security Module.

While standard security schemes are supported between Merchant and Cardholder, additional security is implemented on the interface to the authorization host. For that purpose inexpensive hardware security module is installed at the Merchant side. This module stores Zone Master Keys and produces session/transaction cryptographic keys for message exchange with the Secure e-Gateway Server.

Secure e-Gateway Client software supports following schemes:

- Payment e-gateway module for high-volume single Internet e-Commerce site;
- Payment e-gateway for multiple Internet merchants e-Commerce sites;
- Payment e-Gateway server for P.O.S. cardholder present transactions.

e-Commerce Transaction Process flow

An e-Commerce transaction is carried out in the following steps:

- Cardholder makes connection to Merchant Web server via Internet.

- Using content generated by Internet Shop Software cardholder orders goods or services.
- To execute payment Merchant Secure Web Server establishes HTTPS/SSL connection with cardholder and presents Secure e-Gateway Client HTML form (see Fig. 1) including following entry fields:
  - Card primary account number
  - Card expiration date
  - Card CVC2 value (if present on card)

  Optional fields:
  - Cardholder name (as embossed on card)
  - Cardholder e-mail address
  - Cardholder billing address (can be validated by Address Verification Service)

  Following fields to be generated by Internet shop software and are not editable:
  - Order id (can be hidden)
  - Order total amount
  - Order currency
  - Merchant terminal Id (hidden)
  - Time stamp (hidden)
  - Security code (hidden)

  Also this form includes [Submit] or [Approve] button linked with CGI interface of Secure e-Gateway Client located on Merchant Web Server or Bank Web Server.

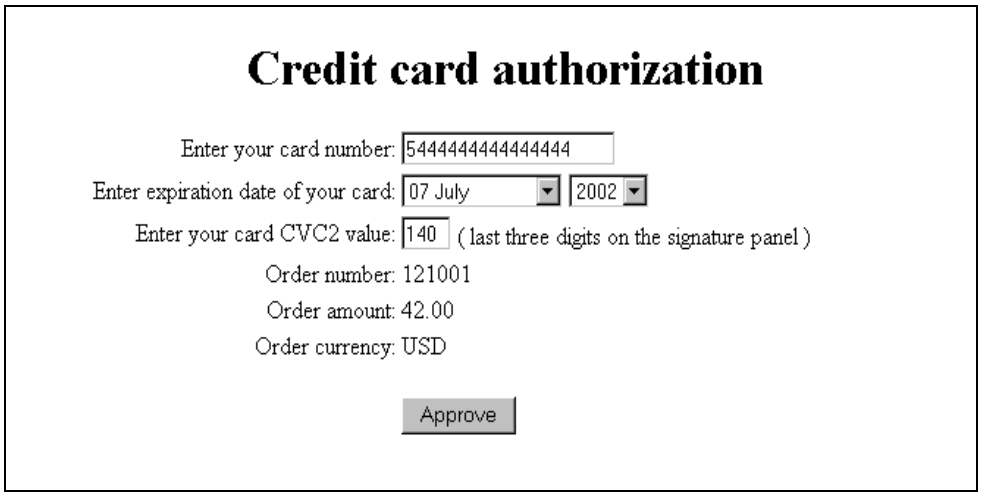


Fig. 1. Sample Internet Shop authorization request screen.

Cardholder fills in payments form and press [Approve] button. Submitted fields are parsed and pre-validated by CGI e-Gateway Client interface

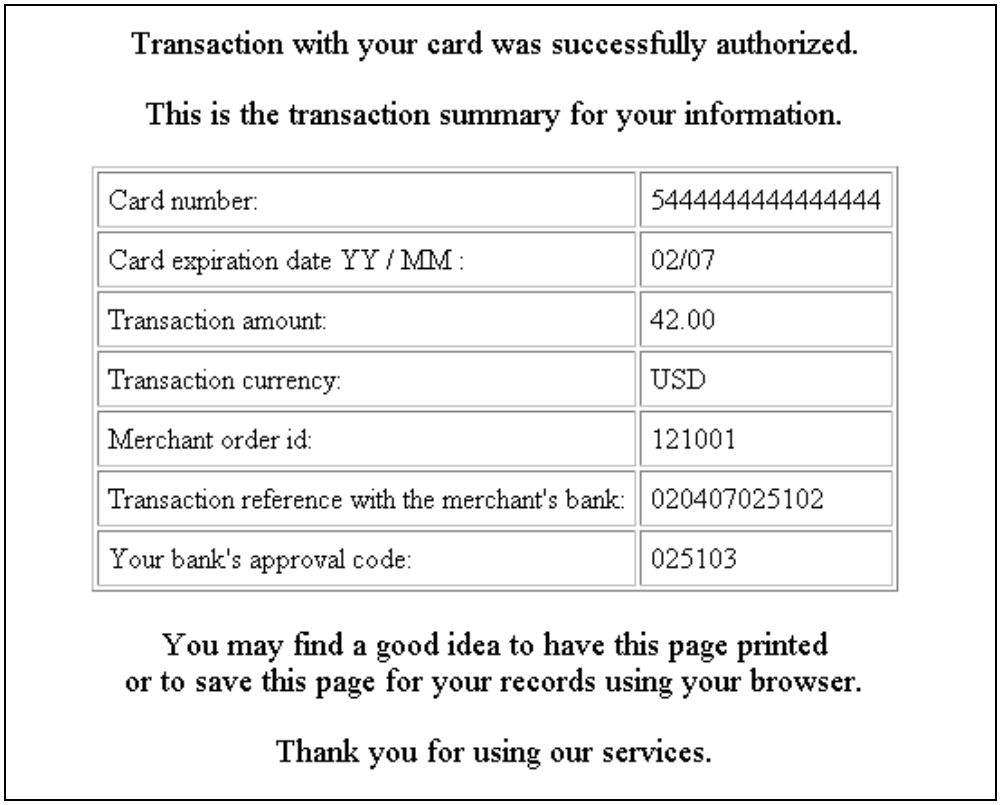
program. Alternatively input fields may be parsed by Internet Shop Software and passed to e-Gateway Client via API call.

Secure e-Gateway Client program performs key management with security device to get session/transaction cryptographic keys.

Secure e-Gateway Client program assembles ISO-8583 OpenWay dialect message, encrypts it with session key and transmit over dedicated TCP/IP link to Secure e-Gateway Server.

Secure e-Gateway Server makes all necessary steps to authorize this transaction and sends reply to Secure e-Gateway Client.

Upon reception of this message Secure e-Gateway Client CGI interface program generates HTML page for cardholder and Internet Shop software with results of authorization and stores results locally on e-Gateway/Merchant Web Server (see Fig. 2). Those results include order id, response code, authorization code and retrieval reference number (RRN) assigned to the message by NetServer.



Transaction with your card was successfully authorized.

This is the transaction summary for your information.

Card number:	5444444444444444
Card expiration date YY / MM :	02/07
Transaction amount:	42.00
Transaction currency:	USD
Merchant order id:	121001
Transaction reference with the merchant's bank:	020407025102
Your bank's approval code:	025103

You may find a good idea to have this page printed or to save this page for your records using your browser.

Thank you for using our services.

Fig. 2. Sample Internet Shop authorization response screen.

After this page cardholder is redirected back to merchant Web server. Internet shop software will retrieve from redirected form "Internet Transaction Reference number" assigned to the message by NetServer. This unique transaction reference allows Merchant software to send transaction completion advice to secure e-Gateway client without knowledge of cardholder account information.

In case of single message scheme the transaction is completed. Secure e-Gateway Client program allows generating of transaction reversal (using "Internet Transaction Reference number") if merchant cannot fulfill order.

In case of Online Dual scheme, merchant software (using unique transaction reference) must complete transaction by sending "Sales completion" or "Reversal" advice to secure e-Gateway.

Offline Dual message scheme assumes generating transaction batch file by Internet Shop software with results of goods and services delivery using "Internet Transaction Reference number" of transactions.

Internet P.O.S. Transaction Process flow

Merchant establishes HTTPS/SSL connection with Payment e-Gateway Web server via Internet.

Payment e-Gateway Secure Web Server presents P.O.S. transaction HTML form (see Fig. 3) including following entry fields:

- Card primary account number;
- Card expiration date;
- Card CVC2 value (if present on card);
- Transaction amount;
- Transaction currency;
- Transaction terminal (if assigned more than one);
- Also this form includes "Authorize" button linked with CGI interface of Secure e-Gateway Client located on Payment e-Gateway Web Server.

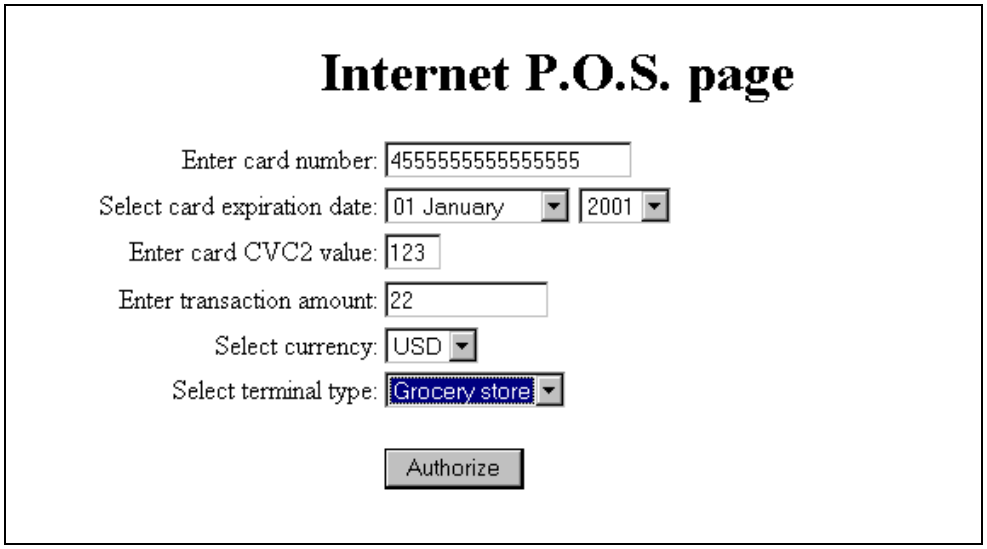


Fig. 3. Internet POS sample screen.

Merchant cashier/operator fills in payments form and press "Authorize" button. Submitted fields are parsed and pre-validated by CGI e-Gateway Client interface program.

In case of PIN pad enabled merchant, e-Gateway requests PIN pad agent software to input cardholder card tracks and PIN. Encrypted information is sent back to e-Gateway Client Web Server.

Secure e-Gateway Client program performs key management with security device to get session/transaction cryptographic keys.

Secure e-Gateway Client program assembles ISO-8583 OPENWAY dialect message, encrypts it with session key and transmit over dedicated TCP/IP link to Secure e-Gateway Server.

Secure e-Gateway Server makes all necessary steps to authorize this transaction and sends reply to Secure e-Gateway Client.

Upon reception of this message Secure e-Gateway Client CGI interface program generates HTML page for merchant and cardholder with results of authorization and stores results locally on e-Gateway Web Server. Those results include response code, authorization code and retrieval reference number assigned to the message by the NetServer.

Secure e-Gateway Client program allows generating of transaction reversal if merchant cannot fulfill order.

Connection scheme of high-volume Internet e-Commerce site

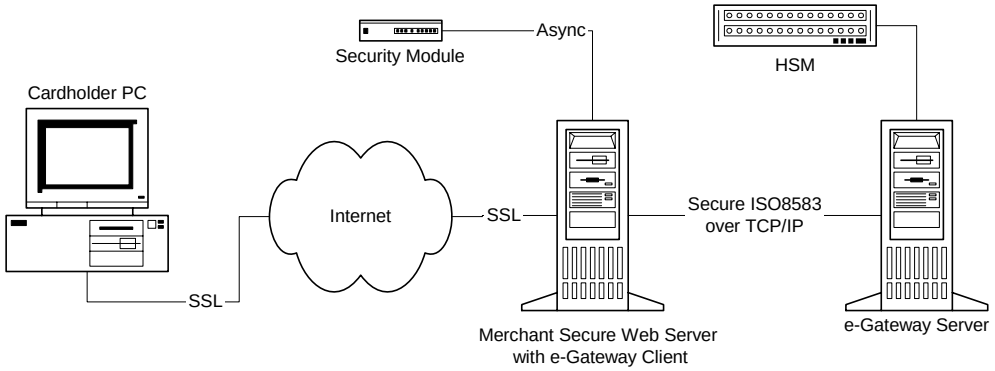


Fig. 4.High-volume Internet e-Commerce site connection scheme.

Connection scheme of Payment e-Gateway site for multiple Internet Merchants e-Commerce sites

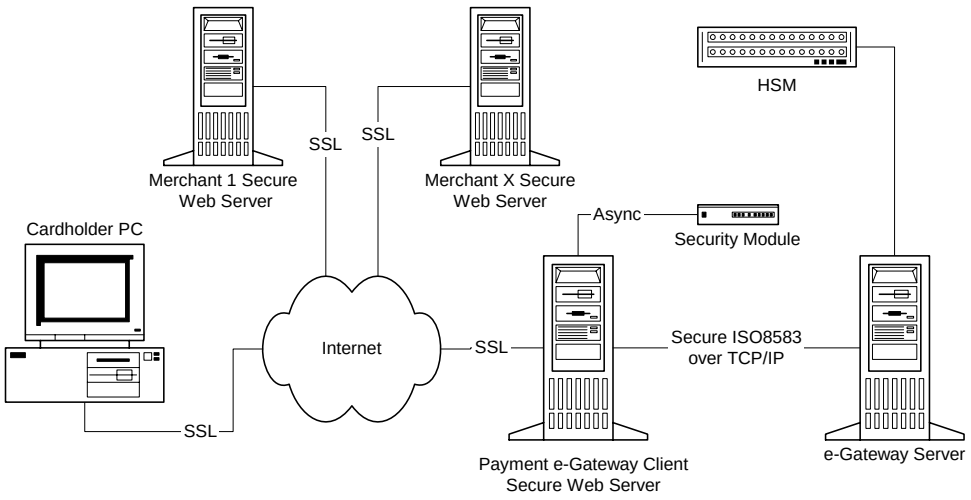


Fig. 5.Payment e-Gateway site for multiple Internet Merchants connection scheme.

Connection scheme of Payment e-Gateway for Internet P.O.S. transactions

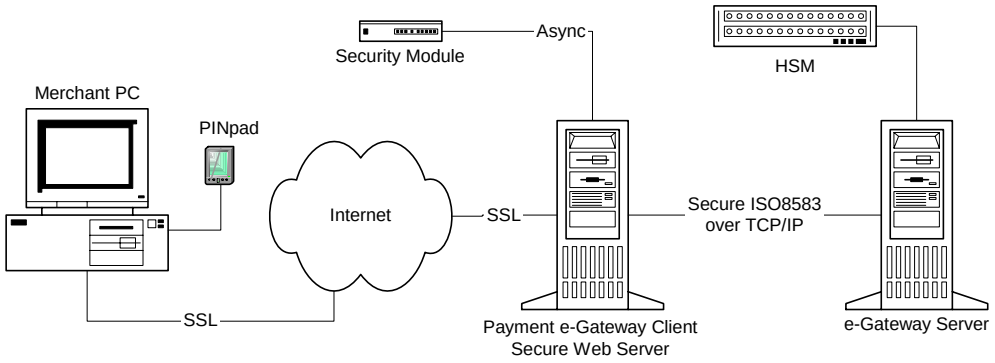


Fig. 6.Payment e-Gateway site for Internet POS transactions connection scheme.