

Модуль e-Gateway системы Way4™

Общие сведения

Содержание

ВВЕДЕНИЕ	2
ГЛАВА 1. ОБЩИЕ СВЕДЕНИЯ	3
Процедура выполнения транзакции e-Commerce	4
Процедура выполнения транзакции Интернет-терминалом	7
Архитектура сайта e-Commerce с большим числом транзакций	8
Архитектура шлюза e-Commerce для обслуживания нескольких сайтов Интернет-торговли	9
Архитектура шлюза e-Commerce для обработки транзакций Интернет терминала	9


Введение

Настоящий документ предназначен для системных администраторов банков (процессинговых центров), осуществляющих техническую поддержку модулей e-Commerce (Шлюзов Интернет-торговли между Интернет-магазинами и системой Way4™).

При работе с данным документом рекомендуется пользоваться следующими источниками из комплекта документации OpenWay (поставляемого только с модулем Internet Banking):

- "Internet Banking. Общие сведения";
- "Модуль OpenWay Internet Banking. Руководство разработчика".

В руководстве используются следующие обозначения:

- названия полей экранных форм выделяются *курсивом*;
- названия кнопок экранных форм приводятся в квадратных скобках, например, [Approve];
- последовательность выбора пункта в меню пользователя отображается с помощью стрелок следующим образом: "Issuing→Contracts Input & Update";
- последовательность выбора пункта в системном меню отображается с помощью стрелок следующим образом: "Database ⇒ Change password";
- комбинации клавиш, используемые при работе с DB Manager, приводятся в угловых скобках, например <Ctrl>+<F3>;
- предостережения в связи с возможностью совершения неправильных действий отмечены знаком ;

Глава 1. Общие сведения

Модуль e-Gateway (Защищенный шлюз Интернет-торговли) – это открытая система для торговли по сети Интернет, предназначенная для использования банками, предприятиями Интернет-торговли и провайдерами Интернет-услуг.

Система состоит из двух подмодулей:

- Клиент модуля e-Gateway, устанавливаемый на сервере торгового предприятия, банка или Интернет-провайдера. Данный подмодуль обеспечивает:
 - ♦ SSL-соединения с держателями карт;
 - ♦ CGI- или API-соединения с Интернет-магазинами;
 - ♦ авторизацию Интернет-терминалов и обработка транзакций с проверкой ПИН-кода;
 - ♦ защищенное соединение с программным обеспечением для ввода ПИН-кода, установленным у клиента (держателя карты);
 - ♦ средства предварительной проверки и регистрации транзакций;
 - ♦ защищенное соединение с сервером e-Gateway на основе протокола ISO 8583;
 - ♦ обслуживание единичных и парных транзакционных сообщений;
 - ♦ поддержку различных платформ (Windows NT/2000 и UNIX).
- Сервер модуля e-Gateway, представляющий собой канал коммуникационного сервера (NetServer). Данный подмодуль обеспечивает:
 - ♦ защищенное соединение с Клиентом e-Gateway на основе протокола ISO 8583;
 - ♦ Обеспечение интерфейса с VISA, Europay и другими платежными системами;
 - ♦ Соединение с аппаратным модулем безопасности (HSM).

При поддержке стандартных средств защиты обмена данными между торговцем и держателем банковской карты, дополнительные средства реализованы в интерфейсе сервера авторизации. Для этого у торговца устанавливается недорогое аппаратное средство защиты. Такой модуль хранит зональные мастер-ключи и генерирует сессионные/транзакционные ключи шифрования для обмена данными с сервером модуля e-Gateway.

- Клиент модуля e-Gateway может быть использован как:
 - ♦ модуль e-Commerce (модуль шлюза Интернет-торговли) для обслуживания отдельного сайта Интернет-торговли с большим числом транзакций;
 - ♦ модуль e-Commerce для обслуживания нескольких сайтов Интернет-торговли;
 - ♦ сервер e-Commerce для обработки транзакций Интернет-терминала, генерируемых в присутствии держателя карты.

Процедура выполнения транзакции e-Commerce

Процедура выполнения транзакции e-Commerce включает в себя следующие этапы:

- Держатель карты подключается к Web-серверу Интернет-торговца.
- С помощью экранных сообщений, генерируемых программным обеспечением Интернет-магазина, держатель карты заказывает необходимые товары и услуги.
- Для осуществления платежа защищенный Web-сервер торговца устанавливает HTTPS/SSL-соединение с держателем карты и выводит на экран HTML-форму клиентской части модуля e-Gateway, содержащую следующие поля ввода данных (см. Рис. 1):
 - ♦ номер карты;
 - ♦ дата истечения срока действия карты;
 - ♦ CVC2 карты; данное поле формы заполняется, если соответствующее значение указано на карте.

Указанная форма может также содержать следующие поля:

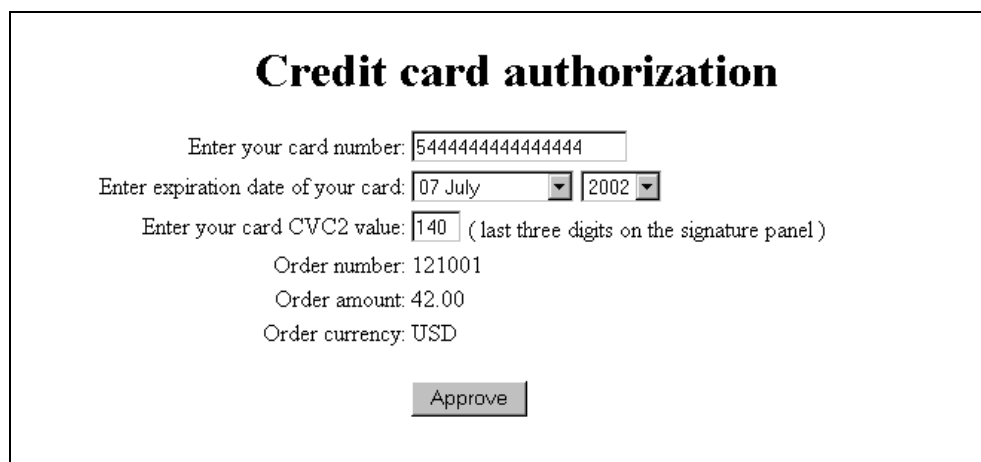
- ♦ имя держателя карты; данное поле формы заполняется, если соответствующая информация указана на карте;
- ♦ адрес электронной почты держателя карты;
- ♦ адрес держателя карты, подлинность которого может быть проверена Службой проверки адресов (VISA AVS) платежной системы VISA.

Значения следующих полей, генерируемые программным обеспечением Интернет-магазина, недоступны для редактирования держателем карты:

- ♦ Номер заказа (может не выводиться на экран);
- ♦ Общая сумма заказа;
- ♦ Валюта заказа;
- ♦ Идентификатор торговца (не выводится на экран);
- ♦ Отметка времени (не выводится на экран);

- ♦ Защитный код (не выводится на экран).

Кроме того, в данной форме имеется кнопка [Submit] или [Approve], связанная с CGI-интерфейсом клиентской части модуля e-Gateway, установленной на Web-сервере торговца или банка.



Credit card authorization

Enter your card number:

Enter expiration date of your card:

Enter your card CVC2 value: (last three digits on the signature panel)

Order number: 121001
Order amount: 42.00
Order currency: USD

Рис. 1. Пример экрана авторизационного запроса Интернет-магазина

Держатель карты заполняет форму платежа и нажимает кнопку [Approve]. Существует две схемы проверки введенных данных. В одном случае, данные полей анализируются и предварительно проверяются CGI-интерфейсом клиентской части модуля e-Gateway. В другом случае, они анализируются программным обеспечением Интернет-магазина и передаются клиентской части модуля e-Gateway через вызов API.

При помощи устройства защиты данных, клиентская часть Secure e-Gateway генерирует сессионные/транзакционные ключи шифрования.

Клиентская часть модуля e-Gateway формирует сообщение стандарта ISO-8583 диалекта OpenWay, шифрует его с помощью сессионного ключа и передает по выделенному каналу TCP/IP на сервер модуля e-Gateway.

Сервер модуля e-Gateway выполняет все необходимые для авторизации этой транзакции действия и передает ответ клиентской части модуля e-Gateway.

После получения данного сообщения программа CGI-интерфейса клиентской части модуля e-Gateway генерирует для держателя карты и Интернет-магазина HTML-страницу, содержащую результаты авторизации, и сохраняет результаты локально на WEB-сервере шлюза/торговца. Данные результаты включают в себя номер заказа, код ответа, авторизационный код и уникальный номер цепочки операции (Retrieval Reference Number, RRN), присваиваемый сообщению коммуникационным сервером.

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.

Рис. 2. Пример экрана авторизационного ответа Интернет-магазина

После этого страница держателя карты передается обратно на Web-сервер торговца. Программное обеспечение Интернет-магазина извлекает из полученной формы Internet Transaction Reference number, присваиваемый сообщению коммуникационным сервером. Данный уникальный номер операции позволяет программному обеспечению торговца дать команду клиентской части модуля e-Gateway о выполнении транзакции, не располагая информацией о счете держателя карты.

В случае применения схемы единичных транзакционных сообщений, транзакция на этом шаге считается завершенной. Если торговец не может выполнить заказ, то программа клиентской части модуля e-Gateway позволяет выполнять отмену транзакции (с помощью Internet Transaction Reference number).

В случае применения схемы парных транзакционных сообщений, программное обеспечение торговца (с помощью уникального номера операции) должно завершить транзакцию, направив модулю e-Gateway команду "Sales completion" или "Reversal".

Парные транзакционные сообщения предполагают генерирование программным обеспечением Интернет-магазина пакетного файла транзакций, в который входят результаты поставки товаров и услуг.

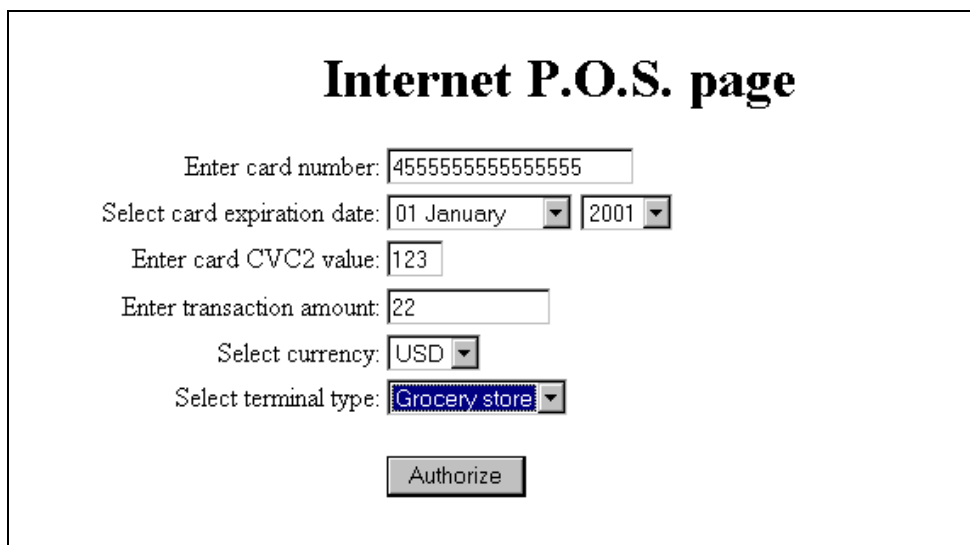
Процедура выполнения транзакции Интернет-терминалом

Торговец устанавливает HTTPS/SSL-соединение через Интернет с WEB-сервером шлюза e-Commerce.

Защищенный WEB-сервер e-Commerce выводит на экран транзакционную HTML-форму Интернет-терминала, содержащую следующие поля (см. Рис. 3):

- номер карты;
- дата истечения срока действия карты;
- CVC2 карты; данное поле формы заполняется, если соответствующее значение указано на карте;
- сумма транзакции;
- валюта транзакции;
- идентификатор терминала, с помощью которого проведена транзакция (если у торговца более одного терминала);

Кроме того, данная форма имеет кнопку [Authorize], связанную с CGI-интерфейсом клиентской части модуля e-Gateway, установленной на WEB-сервере шлюза e-Commerce.



The screenshot displays a web form titled "Internet P.O.S. page". The form contains the following fields and controls:

- Enter card number:** A text input field containing the value "4555555555555555".
- Select card expiration date:** Two dropdown menus. The first shows "01 January" and the second shows "2001".
- Enter card CVC2 value:** A text input field containing the value "123".
- Enter transaction amount:** A text input field containing the value "22".
- Select currency:** A dropdown menu showing "USD".
- Select terminal type:** A dropdown menu showing "Grocery store".
- Authorize:** A button located at the bottom center of the form.

Рис. 3. Пример экрана Интернет-терминала

Кассир/оператор торговца заполняет платежную форму и нажимает кнопку [Authorize]. Данные полей анализируются и предварительно проверяются CGI-интерфейсом клиентской части модуля e-Gateway.

Если Интернет-терминал торговца оснащен дополнительной клавиатурой для чтения магнитной полосы карты и ввода ПИН-кода, модуль e-Gateway запрашивает у программы-агента по вводу ПИН-кода данные, записанные на магнитной полосе карты, и ПИН-код. Зашифрованная информация передается обратно на WEB-сервер клиентской части модуля e-Gateway.

При помощи устройства защиты данных клиентская часть модуля e-Gateway генерирует сессионные/транзакционные ключи шифрования.

Клиентская часть Secure e-Gateway формирует сообщение стандарта ISO-8583 диалекта OpenWay, шифрует его с помощью сессионного ключа и передает по выделенному каналу TCP/IP на сервер Secure e-Gateway.

Сервер Secure e-Gateway выполняет все необходимое для авторизации этой транзакции и передает ответ клиентской части модуля e-Gateway.

После получения данного сообщения программа CGI-интерфейса клиентской части модуля e-Gateway генерирует для держателя карты и Интернет-магазина HTML-страницу, содержащую результаты авторизации и сохраняет результаты локально на WEB-сервере шлюза/торговца. Данные результаты включают в себя номер заказа, код ответа, авторизационный код и уникальный номер цепочки операции (RRN), присваиваемый сообщению коммуникационным сервером.

В случае, если торговец не может выполнить заказ, клиентская часть модуля e-Gateway позволяет выполнять отмену операции.

Архитектура сайта e-Commerce с большим числом транзакций

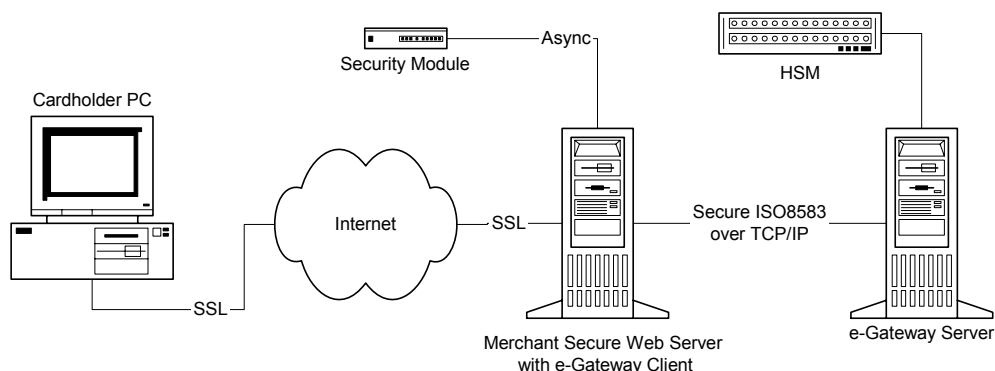


Рис. 4. Архитектура сайта e-Commerce с большим числом транзакций

Архитектура шлюза e-Commerce для обслуживания нескольких сайтов Интернет-торговли

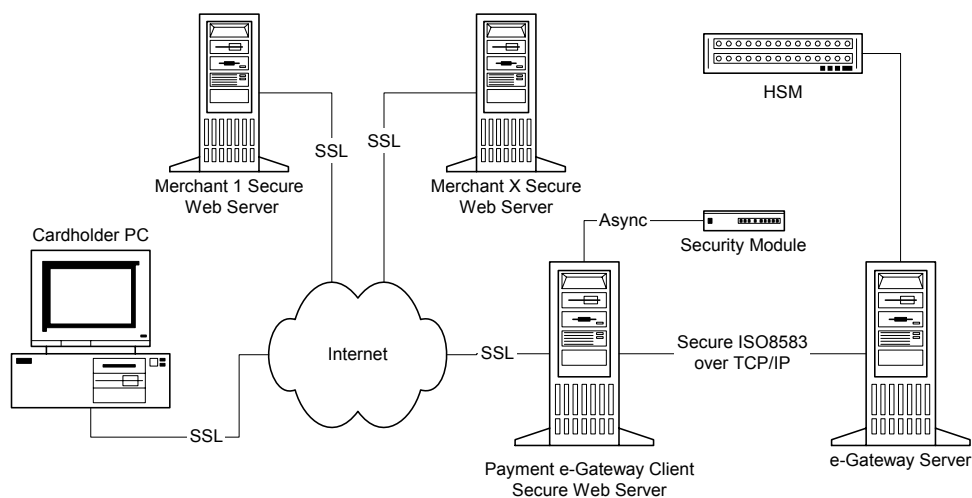


Рис. 5. Архитектура шлюза e-Commerce для обслуживания нескольких сайтов Интернет-торговли

Архитектура шлюза e-Commerce для обработки транзакций Интернет терминала

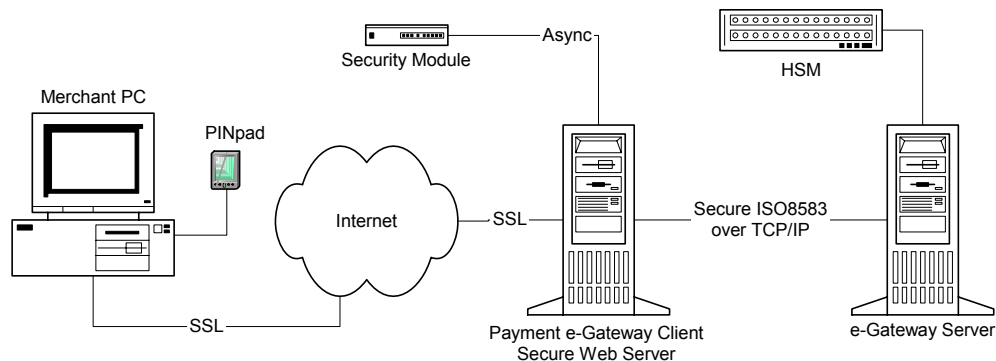


Рис. 6. Архитектура шлюза e-Commerce для обработки транзакций Интернет терминала