Платежный шлюз eCommerceConnect Gateway.

Интеграция и тестирование.

Руководство разработчика торговой системы

Український процесінговий центр

Содержание

1. Использование тестовой версии платежного шлюза 3
2. Описание выполняемых тестов 4
3. Оценка результатов тестирования 6

1. Использование тестовой версии платежного шлюза

Перед началом реального функционирования электронной торговой системы разаработчикам этой системы необходимо выполнить работы по программированию интерфейса взаимодействия с платежным сервером, а также произвести установку и подключение модуля генерации MAC-кода.
После того как указанные работы будут выполнены, необходимо:

- получить в процессинговом центре URL тестового платежного сервера;
- предоставить администратору платежного сервера такие параметры как адрес страницы (**SUCCESS_URL**) для редиректа браузера пользователя в случае успешного проведения транзакции, адрес страницы (**FAILURE_URL**) для редиректа браузера пользователя в случае неуспешного проведения транзакции и адрес страницы (**NOTIFY_URL**) для передачи результата транзакции от шлюза напрямую электронному магазину;

2. Описание выполняемых тестов.

Задача предлагаемых тестов сводится к тому, чтобы убедиться:

- в корректности формирования электронной торговой системой авторизационых запросов;
- в правильности функционирования механизмов приема и обработки авторизационных ответов при различных значениях кода завершения транзакции (TranCode);
- в правильности функционирования механизмов вычисления и проверки MAC-кодов.

Разработчик самостоятельно может инициировать получение от тестового платежного сервера тех или иных кодов завершения транзакции путем использования номеров тестовых карт в соответствии с таблицей, приведенной ниже:

Таблица 1

Коды на основе ответов авторизацинного хоста банка		Комментарий
Обобщенные коды ответа для магазина	Примерная интерпретация ответа на странице возврата электронного магазина	Номер карты (срок действия 12/2012; CVV2 - 999)
000	Сделка авторизована	4999999999990011
105	Транзакция не разрешена банком-эмитентом	4999999999990029
116	Недостаточно средств	4999999999990037
111	Несуществующая карта	4999999999990045
108	Карта утеряна или украдена	4999999999990052
101	Неверный срок действия карты	4999999999990060
130	Превышен допустимый лимит расходов	4999999999990078
290	Банк-издатель недоступен	4999999999990086
291	Техническая или коммуникационная проблема	4999999999990094
Коды на основе ответов генерируемых платежным сервером без обращения к хосту банка		
Внутренние коды ошибок платежного сервера в соответствии со способом обработки		
401	Ошибки формата	*
402	Ошибки в параметрах Acquirer/Merchant	*
403	Ошибки при соединении с ресурсом платежной системы (DS)	4999999999990102
404	Ошибка аутентификации покупателя	4999999999990110
405	Ошибка подписи	*
501	Транзакция отменена пользователем	*
502	Сессия браузера устарела	*

Первая часть таблицы предназначена для тестирования ситуаций, которые возникают за пределами участка «торговая система-браузер покупателя-платежный сервер». Другими словами, в ней приводятся коды завершения транзакции, основанные на данных, полученных либо от банка-эмитента в результате проведения последним процесса авторизации карты, либо от банка-эквайрера в случае, если банк-эквайрер по каким-либо причинам не может связаться с банком-эмитентом.

В любом случае это означает, что интерфейс с платежным шлюзом функционирует нормально и задачей торговой системы является лишь корректное продолжение/завершение операции покупки товара или услуги, либо вежливое информирование покупателя о причине отказа, полученного от платежного шлюза с предложением попробовать приобрести товар или услугу позднее, или использовать другую платежную карту.

Вторая часть таблицы отображает те коды завершения транзакции, которые характерны для ситуаций, в которых платежный сервер не смог сформировать полноценный авторизационный запрос и направить его в авторизационный хост банка-эквайрера.

Поскольку причины двух таких ситуаций (TranCode = 403 или 404) находятся за пределами платежного сервера, получение таких кодов завершения можно инициировать с использованием соответствующих номеров тестовых карт.

Тестирование других ошибочных ситуаций (TranCode = 401, 402, 405) и способов их обработки можно провести путем искусственного моделирования соответствующих ситуаций на торговой системе (убрав, например, какой-либо параметр из первичного запроса – Currency, OrderID или любой другой для получения TranCode = 401; исказив значения параметра MerchantID/TerminalID для получения TranCode = 402; исказив значение сгенерированого MAC-кода - для получения TranCode = 405).

При этом, для получения кода ошибки 501 необходимо произвести отмену операции оплаты, нажав на соответствующую клавишу на странице ввода реквизитов карты платежного сервера.

Ситуация с кодом ошибки 502 возникает (и может быть смоделирована) в случае, если покупатель, находясь на странице для ввода реквизитов карты платежного сервера, не завершает свою работу в течение 15...20 минут.

3. Оценка результатов тестирования.

Разработчикам торговой системы рекомендуется создавать в рамках реализации интерфейса взаимодействия с платежным шлюзом (а также с программным модулем генерации MAC -кода) механизм журналирования, облегчающих сопровождение системы и быструю диагностику возникающих проблем.

Оценка корректности реализации проводится:

- разработчиком электронной торговой системы – на основании оценки корректности кодов ответов, полученных при выполнении тестов с применением всех номеров карт согласно табл. 1 , а также анализа журналов электронной торговой системы;

- службами процессингового центра – на основании анализа журналов платежного сервера