ИНТЕРФЕЙС E-COMMERCE GATEWAY

1.011 – 15.03.2021

(Версия форм CGI / WWW)

Оглавление

ОБЗОР

Это руководство предназначено для использования программистами, отвечающими за интерфейс торгового шлюза. В нем описывается интерфейс, который используются торговыми системами для обработки транзакций электронной торговли на основе кредитных карт с использованием стандартного метода постинга форм CGI / WWW. Этот интерфейс прозрачно поддерживает различные протоколы аутентификации владельцев карт, такие как 3-D Secure и Secure Code, а также устаревшие неавторизованные торговые транзакции SSL.

ОПРЕДЕЛЕНИЯ

EGW, Шлюз, шлюз электронной коммерции – совокупность программных и аппаратных средств, выполняющих:
- обработку запросов Торговых точек на проведение операций;
- проведение операций;
- передачу результатов проведения операций Торговым точкам.

POST - запрос – один из методов запроса, поддерживаемых HTTP протоколом.
CallBack (Коллбэк) - обратный вызов от EGW электронной коммерции к Торговой точке с результатом операции.
Авторизация – процедура получения разрешения на проведение операции у Банка, выпустившего карту.

ВАЖНЫЕ ЗАМЕЧАНИЯ

- Интеграционное тестирование начинается после согласования коммерческих и организационных вопросов с соответствующей службой Банка.
- Перед проведением интеграционного тестирования на электронный адрес ecom.bin@open.ru необходимо сообщить IP-адрес и URL, на который будет поступать CallBack-ответ. Прислать SSL сертификаты, включая корневой, для приёма callback по https. После предоставления указанных данных Банк высылает по электронной почте номер тестового терминала.
- Поля передаются в запросе HTTP POST.
- Поддерживается только протокол TLSv1.2
- POST-запрос для **тестовых запросов** необходимо направлять на адрес тестового сервера https://3dstest.mdmbank.ru/cgi-bin/cgi_link порт 443.
- Запрос от интернет-магазина ДОЛЖЕН содержать все необходимые поля и МОЖЕТ иметь произвольный порядок полей. Все поля передаются в верхнем регистре.
- В случае отсутствия у торговой точки сертификата соответствия стандарту **PCI DSS** ввод sensitive данных производится на сайте Банка. Передача в запросе от торговой точки параметров: «номер карты», «CVV2» и «expire date» **НЕ ДОПУСКАЕТСЯ**.
- Названия полей в CallBack могут **отличаются от полей в запросе**. Например :Result (=ACTION), RC, Amount, Currency, Order, RRN, IntRef, AuthCode, PAN, BackRef, Terminal, TrType.
- Работа с символами «&», «+» и некоторыми иными математическими символами в полях с URL не гарантируется;
- При отказах значения некоторых полей в CallBack могут отсутствовать;
- **Операция считается успешной при получении в ответе параметров ACTION(Result)=”0” и RC=”00”. При других значениях этих параметров операция не успешна!**
- В CallBack ответе инициатору операции может быть без предупреждения изменён порядок полей. Возможно добавления дополнительных полей

ИНТЕРФЕЙС РОЗНИЧНЫХ ТРАНЗАКЦИЙ

Сценарий потока транзакций

Шлюз электронной торговли поддерживает различные сценарии потока транзакций, но этот документ будет сфокусирован только на рекомендованном сценарии, описанном ниже.

1. Выбрав товары и услуги, владелец карты нажимает кнопку ‘Buy’ (Купить) или эквивалентную кнопку и переходит на страницу, где он может ввести или изменить информацию о доставке и способ оплаты. Информация о способе оплаты может предлагать различные способы оплаты, такие как ‘Pay by credit card’ (Оплата кредитной картой) или аналогичный вариант. Эта опция не должна включать номер карты, дату истечения срока действия, CVC2 или любую другую конфиденциальную информацию, связанную с картой. Из-за связанных с безопасностью рисков система продавца не должна запрашивать и хранить информацию о кредитной карте на сервере продавца.

2. Если владелец карты выбирает опцию ‘Pay by credit card’ (Оплата кредитной картой), торговая система должна подготовить поля запроса авторизации и перенаправить владельца карты на страницу ‘Enter credit card information' (Ввести информацию о кредитной карте) на URL CGI сервера EGW.
   В качестве альтернативы, торговая система сама может представить эту страницу непосредственно владельцу карты. В этом случае URL-адрес публикации для этой формы страницы должен быть установлен на CGI URL-адрес EGW.
   Эта форма должна содержать все поля ввода карты и видимые / скрытые поля, относящиеся к заказу и продавцу в соответствии с форматом запроса на авторизацию.

3. После получения заполненной формы EGW проверяет информацию запроса, включая код аутентификации сообщения. Если запрос не выполняется, EGW отправляет ответ об ошибке обратно в торговую систему.

4. Если предоставленный номер карты относится к диапазону карт с определенным методом аутентификации владельца карты, EGW вызывает соответствующий модуль аутентификации (3-D Secure, MasterCard SPA), который выполняет обработку для конкретного протокола. Если аутентификация владельца карты не удалась, EGW возвращает сообщение об ошибке в торговую систему или использует прежний тип транзакции SSL электронной торговли, чтобы продолжить эту транзакцию.

5. EGW отправляет запрос на авторизацию в платёжную систему. После авторизации EGW готовит и отправляет ответ транзакции обратно в торговую систему. Ответ на транзакцию не содержит информации о кредитной карте или содержит номер карты только в замаскированной форме.
   EGW отправляет ответные сообщения в торговую систему с помощью перенаправления владельца карты. Перенаправление может быть сделано автоматически или в качестве промежуточной формы для размещения на торговом сервере. Ответные сообщения могут также содержать код аутентификации сообщения для проверки подлинности сообщения. Если авторизация прошла успешно, ответное сообщение будет содержать поле “Internal Reference Number” (Внутренний ссылочный номер RRN), которое будет использоваться торговой системой, чтобы она могла завершить или отменить полученную авторизацию без информации о кредитной карте.

6. Кроме того, EGW может отправлять (если предусмотрено конфигурация) уведомление по электронной почте (или направить HTTP) в систему продавца с той же информацией, что и в ответном сообщении онлайн-транзакции. Это делается в случае возможных транспортных проблем при доставке перенаправленного сообщения. Адрес электронной почты или HTTP-URL для уведомлений о транзакциях можно настроить для каждого терминала.

7. После получения онлайнового ответа о транзакции или его уведомления по электронной почте, торговая система начинает доставку заказанных товаров и / или услуг владельцу карты. В этот момент запрашиваемая сумма блокируется на счете держателя карты.

Продавец должен отправить владельцу карты электронное письмо с информацией о заказе и времени доставки, если это применимо.

8. Когда продавец доставил товары и услуги владельцу карты, торговая система отправляет транзакцию “Sales completion” (Завершение продажи) непосредственно на URL CGI EGW, используя внутренний ссылочный номер для ссылки на транзакцию авторизации с соответствующей информацией о кредитной карте. Запрос на транзакцию должен включать в себя поле кода аутентификации сообщения для проверки подлинности сообщения.
9. EGW проверяет входящее сообщение и запрашивает финансовое завершение транзакции из карточной системы. В этот момент сумма транзакции списывается со счета владельца карты, а на счет торговца зачисляется соответствующая сумма. EGW отправляет ответ обратно в торговую систему в ответном документе.
10. Если продавец не может выполнить распоряжение владельца карты или если владелец карты отменяет заказ на стадии, разрешенной продавцом, система продавца должна отправить сообщение “Reversal” (Сторнирование), чтобы отменить отложенную или завершенную транзакцию. Торговая система отправляет это сообщение непосредственно на URL CGI EGW. Запрос на транзакцию должен включать в себя поле кода аутентификации сообщения для проверки подлинности сообщения.
11. EGW проверяет входящее сообщение и запрашивает отмену ожидающей или завершенной транзакции из карточной системы Way4. Это может включать перевод средств со счета продавца на счет держателя карты. EGW отправляет ответ в торговую систему в ответном документе.

Варианты проведения транзакций

Однопроходная схема

В данной схеме от Интернет-магазина отправляется только финансовый запрос (TRTYPE=1). Подтверждения операции не требуется. Денежные средства с карты клиента списываются в момент проведения транзакции.

Двухпроходная схема

В данной схеме первоначально отправляется авторизационный запрос (TRTYPE=0). При проведении данной части, денежные средства на счете клиента блокируются, но не списываются. Вторым шагом необходимо отправить запрос «Завершение продажи» (TRTYPE=21), при успешном выполнении которого будет произведено списание ранее заблокированных средств со счета клиента и перечисление их на счет организации Интернет-магазина.

Формат запроса авторизации

Программное обеспечение Интернет-магазина предоставляет держателю карты HTML-форму, которая будет отправлена на web-сервер CGI EGW с помощью метода HTTP POST.

Набор полей делится на три подмножества: видимые поля, заполненные держателем карты, видимые поля, сгенерированные торговой системой, и скрытые поля, сгенерированные торговой системой. Эта страница может содержать функции JavaScript, которые предварительно проверяют ввод поля держателя карты.

Таблица 1 Поля сообщения авторизации, указанные владельцем карты

Поле	Размер	Описание
CARD	9-19	Номер карты (PAN).
EXP	02	Месяц окончания срока действия карты (двузначное число). Может быть представлено как список значений (01-12) для выбора необходимого значения: <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	Год окончания срока действия карты (двузначное число: 20XX). Может быть представлено как список значений 15-20 ближайших лет для выбора необходимого значения.
CVC2	03	Код проверки карты (CVC; последние три цифры на полосе для подписи)
CVC2_RC	01	Код наличия CVC2. Должен быть представлен в виде списка следующих значений для выбора необходимого значения: <option selected value="1">CVC2 is present</option> (присутствует) <option value="0">CVC2 is not provided</option> (не предоставлен) <option value="2">CVC2 is illegible</option> (неразборчив) <option value="9">No CVC2 on card</option> (не указан на карте)

Таблица 2 Сообщения авторизации видимых полей, сгенерированных торговой системой

Поле	Размер	Описание
AMOUNT	1-12	Общая сумма заказа в формате с плавающей запятой с разделителем десятичных знаков
CURRENCY	03	Валюта заказа: трехзначный код валюты
ORDER	6-20	Идентификатор торгового заказа, числовой. Последние 6 цифр используются в качестве порядкового номера операции с банковской карточкой, который должен быть уникальным в течение дня для терминала.
DESC	1-50	Описание заказа
MERCH_NAME	1-50	Наименование продавца (узнаваемо владельцем карты)
MERCH_URL	1-250	URL основного веб-сайта продавца
TERMINAL	8	Идентификатор торгового терминала, присвоенный банком
EMAIL	80	Адрес электронной почты для уведомления. Если это поле присутствует, шлюз может отправить уведомление о результатах транзакции на указанный адрес электронной почты.

Таблица 3 Скрытые поля сообщения авторизации, сгенерированные торговой системой

Поле	Размер	Описание
TRTYPE	1	Должно быть равно «0» (Авторизация).
COUNTRY	02	2-х значный код страны торгового магазина. Должно быть предоставлено, если торговая система находится в стране, отличной от страны сервера шлюза.
MERCH_GMT	1-5	Смещение часового пояса продавца UTC / GMT (например, -3). Должно быть предоставлено, если система продавца находится в часовом поясе, отличном от часового пояса сервера шлюза.
TIMESTAMP	14	Отметка времени транзакции продавца в GMT: ГГГГММДДЧЧММСС. Разница во времени между торговым сервером и сервером e-Gateway не должна превышать 1 часа, в противном случае e-Gateway отклонит эту транзакцию.
NONCE	1-64	Идентификатор транзакции, задаваемый торговцем в виде случайной комбинации длиной в 8-32 байт в шестнадцатеричном формате. Поле является обязательным, если используется MAC.
BACKREF	1-250	URL продавца для отправки результатов авторизации.
P SIGN	1-256	MAC-код продавца в шестнадцатеричной форме.

Держатель карты заполняет необходимые поля и с помощью кнопки [Submit] отправляет форму на EGW. После проверки значений полей выполняется проверка MAC-кода: все поля двух таблиц, представленных выше, кроме поля MAC, последовательно соединяются в строку с подстановкой перед каждым из них длины поля (см. "Вычисление значения MAC-кода"). Затем полученная строка обрабатывается с помощью криптографического алгоритма. Результат сравнивается с входящим MAC-кодом из поля P_SIGN. Криптографический алгоритм и ключ выбираются с помощью входящего поля "TERMINAL". EGW выполняет дополнительную проверку держателя карты, если это необходимо, а затем преобразует, шифрует и отправляет данную транзакцию в онлайновую карточную систему банка.

Формат ответа на авторизацию

После получения ответа из карточной системы EGW направляет держателю карты ответ в виде HTML-формы (см. Таблица 4), которая должна быть отправлена в Интернет-магазин (URL для

отправки содержится в поле "BACKREF"). Кроме того, тот же набор полей может быть отправлен в торговую систему по электронной почте на адрес, указанный во входящем поле EMAIL, в случае возможных проблем с соединением с браузером держателя карты.

Таблица 4 Набор полей ответа шлюза электронной коммерции

Поле	Размер	Описание
TERMINAL	8	Эхо от запроса
TRTYPE	2	Эхо от запроса
ORDER	6-20	Эхо от запроса
AMOUNT	12	Авторизованная сумма. Как правило, будет равна первоначальной сумме плюс комиссия эквайрера
CURRENCY	3	Эхо от запроса
ACTION	1	Код действия электронного шлюза: ■ 0 - Транзакция успешно завершена; ■ 1 - Обнаружена повторяющаяся транзакция; ■ 2 - Транзакция отклонена; ■ 3 - Ошибка обработки транзакции.
RC	02	Код транзакционного ответа (поле 39 протокола ISO-8583)
RRN	12	Уникальный ссылочный номер транзакции, заданный банком торговца (поле 37 протокола ISO-8583)
INT_REF	1-32	Внутренний ссылочный номер шлюза электронной коммерции
TIMESTAMP	14	Метка времени шлюза электронной торговли в GMT: ГГГГММДДЧЧММСС
NONCE	1-64	Значение одноразового номера шлюза электронной коммерции. Будет заполнено 8-32 непредсказуемыми случайными байтами в шестнадцатеричном формате. Будет присутствовать, если используется MAC.
P_SIGN	1-256	MAC-код шлюза электронной коммерции (MAC -код аутентификации сообщения) в шестнадцатеричной форме. Будет присутствовать, если используется MAC.

После получения данного сообщения Интернет-магазин должен проверить MAC-код и поставить товары и/или услуги держателю карты.

Формат запроса на завершение продажи

Для получения оплаты после доставки держателю карты товаров и/или услуг Интернет-магазин должен завершить транзакцию с помощью сообщения "Sales completion". Необходимо отправить следующие поля HTML-формы (см. Таблица 5) на EGW по протоколу HTTPS. Карточная система завершит финансовую транзакцию и переведет средства на торговый счет.

Таблица 5 Поля сообщения о завершении продаж, предоставленные торговой системой

Поле	Размер	Описание
ORDER	6-20	Идентификатор заказа продавца из запроса
AMOUNT	12	Сумма сделки. Формат с плавающей запятой с разделителем десятичных знаков.
CURRENCY	3	Название валюты. Должен быть таким же, как в отклике на авторизацию.
RRN	12	Поисковый ссылочный номер из отклика на авторизацию.
INT REF	1-32	Внутренний ссылочный номер из отклика на авторизацию.
TRTYPE	2	Должно быть равно "21" (завершение продаж).
TERMINAL	8	Идентификатор торгового терминала, присвоенный банком. Должно быть равно полю "TERMINAL" из запроса на авторизацию.
TIMESTAMP	14	Отметка времени транзакции продавца в GMT: ГГГГММДДЧЧММСС. Разница во времени между интернет-магазином и e-Gateway не должна превышать 1 часа, в противном случае e-Gateway отклонит эту транзакцию.

NONCE	1-64	Одноразовый номер продавца. Должно быть заполнено 8-32 непредсказуемыми случайными байтами в шестнадцатеричном формате. Должен присутствовать, если используется MAC.

Формат ответа о завершении продажи

После получения ответа из карточной системы EGW направляет держателю карты ответ в виде HTML-формы, которая должна быть отправлена в Интернет-магазин (URL для отправки содержится в поле "BACKREF") или в виде специальной страницы (в зависимости от настроек, заданных для данного терминала), содержащей поля см. Таблица 4.

Формат запроса отмены

Если товары и/или услуги не могут быть доставлены держателю карты или транзакция была выполнена на сумму, отличающуюся от фактической, Интернет-магазин должен отменить транзакцию на полную сумму или на часть суммы с помощью сообщения "Reversal request". Необходимо отправить на EGW по протоколу HTTPS следующие поля HTML-формы (см. Таблица 5 и Таблица 6).

Таблица 6 Изменённые поля для запроса отмены

Поле	Размер	Описание
TRTYPE	2	Должно быть равно «24» (см. раздел «Использованию различных видов операций отмен/возвратов»)
ORG_AMOUNT	12	Исходная сумма транзакции
AMOUNT	12	Сумма транзакции, подлежащая отмене. Если значение AMOUNT равно значению ORG_AMOUNT, выполняется отмена полной суммы, в противном случае выполняется частичная отмена (Partial Reversal).

В разных случаях используются различные значения TRTYPE (более подробно см. раздел «Использование различных видов операций отмен/возвратов»).

Формат ответа на запрос отмены

После получения ответа из карточной системы EGW направляет держателю карты ответ в виде HTML-формы, которая должна быть отправлена в Интернет-магазин (URL для отправки содержится в поле "BACKREF") или в виде специальной страницы (в зависимости от настроек, заданных для данного терминала). Ответная страница будет содержать тот же набор полей, что и сообщение ответа на запрос о завершении торговой операции (см. "Формат ответа о завершении продажи "). Поле "TRTYPE" будет содержать то же значение, что и аналогичное поле запроса.

Использование различных видов операций отмен/возвратов

Отмены (TRTYPE=22, TRTYPE=24) рекомендуется использовать для оригинальных операций, прошедших в день X, до 00:00 дня X+1.

Возвраты (TRTYPE=174) рекомендуется использовать для оригинальных операций, прошедших в день X, начиная с 00:00 Мск дня X+1 и т.д.

Отмены.

TRTYPE=22 - Запрос отмены вторичной операции со ссылкой на первичную транзакцию.
TRTYPE=24 - Уведомление об отмене вторичной операции со ссылкой на первичную транзакцию.

Являются операциями отмен, которые отправляются в онлайне.
Основное отличие заключается в том, что в случае trtype=22 отправляется запрос к эмитенту и торговец будет получать результат в зависимости от результата обработки транзакции. А в случае trtype=24 отправляется уведомление об отмене.

Возврат.

TRTYPE=174 - Запрос на возврат покупки, раннее совершенной через канал электронной коммерции (поиск сведений об оригинальной операции осуществляется по уникальному внутреннему номеру, сформированному шлюзом электронной коммерции)
TRTYPE=14 - Транзакция по возмещению со ссылкой на первичную транзакцию.

В данном случае основное отличие заключается в том, что при использовании trtype=174 запрос отправляется в онлайне, а в случае trtype=14 в оффлайне.

С 1.07.2020 г. для карт Visa и MC вместо обычной операции возврата TRTYPE=14 должен использоваться запрос на возврат покупки TRTYPE=174.

В платежной системе МИР нет операций возвратов в онлайне. Для карт МИР используется операция возврата в оффлайне (в клиринге) trtype=14.

Если использовались операции с trtype=0 или trtype=12 в указанных условиях, то предлагаем использовать для отмены trtype=22/24.

Для отмены AFT операций, используется отдельный тип операций отмены:
TRTYPE=28 - отмена AFT Auth
TRTYPE=32 - отмена AFT Completion

Периодические платежи

Периодические платежи - это регулярно запланированные транзакции, которые используются в различных ситуациях, таких как ежемесячные подписки, аренды и др.

Первая операция должна содержать план платежей.

Формат запроса «Периодический платеж» аналогичен формату финансового запроса. Первая операция (**TRTYPE**=1) должна содержать план платежей, задаваемый значениями дополнительных полей:
- **RECUR_FREQ** (формат числовой) - частота платежей указывает минимальное количество дней между авторизациями, обычно это значение задается равным 28;
- **RECUR_EXP** (формат ГГГГММДД) - дата окончания периодических платежей. После этой даты ни одна авторизация не будет обслужена.
- **MERCH_RN_ID** (Текстовое 16 знаков) – символьный уникальный идентификатор, который формируется мерчантом для связывания первичной и последующий операций.
- **MERCH_TRAN_STATE** (Текстовое 1 знак) – идентификатор инициированности операции. В первичной операции всегда «S»

Последующие операции (TRTYPE=171) должны содержать поля аналогичные операции **TRTYPE**=1, номер карты и срок ее действия исключаются из запроса.

- **RECUR_REF** со значением номера ссылки (RRN) первой авторизации
- **MERCH_RN_ID** – соответствует значению из первичной операции
- **MERCH_TRAN_STATE** – принимает значение «M» или «C»

Где:
«M» - инициированные ТСП без участия клиента (Merchant Initiated Transaction) / MIT
«C» - инициированные клиентом, т.е. с его участием (Cardholder Initiated Transaction) / CIT

Самая ранняя возможная дата для каждой операции основывается на фактической дате выполнения предыдущей операции. Последующие авторизации принимаются до истечения срока. Контроль полей **“RECUR_FREQ”** и **“RECUR_EXP”** осуществляется на стороне эмитента.

Передача дополнительной комиссии ecom в МПС НСПК

Размер и валюту комиссии торговец должен передавать в элементах SURCHARGE_AMOUNT и SURCHARGE_CURR

SURCHARGE_AMOUNT – указывается в рублях

SURCHARGE_CURR - можно задавать в виде числового кода или строкового кода валюты

Для простоты обработки сообщения допускается передача только суммы комиссии, тогда валюта будет браться равной валюте операции

ИНТЕРФЕЙС ОПЕРАЦИЙ ПЕРЕВОДОВ

Перевод денежных средств “Person-to-Person”

Перевод денежных средств (P2P) обеспечивает держателю карты возможность направить средства на счет другой карты в любой точке мира. С точки зрения шлюза это очень похоже на обычные розничные платежи (см. «Формат запроса авторизации»), за исключением того, что необходимо предоставить номер карты, на которую осуществляется перевод. Обычно P2P сделки осуществляются со сбором комиссии со стороны эквайера, которую держатель карты должен подтвердить или отклонить (см. «Подтверждение суммы комиссии»).

Таблица 7 Специфичные для P2P транзакций поля

Поле	Описание
TRTYPE	Этот параметр должен быть установлен в 8
PAYMENT_TO	Номер карты для перевода

Ответ EGW на запрос имеет тот же формат что и «Формат ответа на авторизацию» (см. Таблица 4).

Операция перевода P2P не требует завершения и её нельзя отменить.

Подтверждение суммы комиссии

Комиссия эквайера это дополнительная наценка на сумму транзакции при совершении сделки, добавляемая банком-эквайером, может быть разной по усмотрению эквайера. Информация о сумме комиссии может быть предоставлена в качестве пояснительного текста или может быть предоставлена держателю карты в отдельной форме. В последнем случае реализуется в виде транзакции на странице подтверждения. После получения запроса о прохождении транзакции EGW запрашивает точную сумму комиссии, посылая сообщение “Transaction Check” на хост эквайера и получает точное значение от суммы вознаграждения, а также суммы сделки. После этого, держателю карты будет показана страница с полной суммой и запросом подтверждения. Если держатель карты подтверждает детали сделки (сумму комиссии, полную сумму сделки) транзакция продолжается, в противном случае она завершается с ошибкой -25 “Сделка отменяется”.

Пример формы с подтверждением транзакции:

```
<input TYPE="HIDDEN" NAME="CONFIRM_ID" VALUE="%188"/>
<input TYPE="HIDDEN" NAME="CONFIRM" VALUE="Y"/>
<input TYPE="HIDDEN" NAME="TERMINAL" VALUE="1111111"></input>
<input TYPE="HIDDEN" NAME="TRTYPE" VALUE="8"></input>
```

Переводы денежных средств с карты на счет терминала (AFT)

Для осуществления операции AFT первоначально отправляется запрос «AFT PreAuth авторизация/ предавторизация» (TRTYPE=27). При проведении данной части, денежные средства на карте клиента блокируются, но не списываются.

Вторым шагом необходимо отправить запрос «AFT Completion подтверждение (завершение расчета)» (TRTYPE=29), при успешном выполнении которого будет произведено списание ранее заблокированных средств со счета клиента и перечисление их на счет организации Интернет-магазина.

Для отмены операции AFT PreAuth используется операция AFT Completion Reversal отмена предавторизации (TRTYPE = 28).

Для отмены подтверждённой операции AFT Completion используется операция AFT Auth Reversal отмена подтверждённой операции (TRTYPE = 32).

Формат запросов и ответов по операциям описан ниже.

AFT PreAuth авторизация/ предавторизация (TRTYPE = 27).

Торговая точка формирует POST – запрос и отправляет его на EGW.

Список отправляемых Торговой точкой параметров: **AMOUNT, CURRENCY, ORDER, DESC, TERMINAL, TRTYPE, CARD, EXP, EXP_YEAR, CVC2, CVC2_RC, PAYMENT_TYPE_ID, TIMESTAMP.**

Описание параметров POST – запроса и допустимых значений см. Таблица 8.

Для операций с MCC, указанными ниже, требуется заполнение дополнительного cgi параметра 'PAYMENT_TO', в котором указывается определенный параметр назначения:

- для MCC=6538 в формате: A + 9 символов БИК + 20 символов счет - при переводе на счет,
- для MCC=4814 в формате: T+ номер телефона получателя, без требований к формату - при переводе по номеру телефона,
- для MCC=6050, 6051 в формате: W + номер электронного кошелька получателя, без требований к формату - при переводе на электронный кошелек.

Если операция является родительской для AFT Auth Recur (Периодическая операция АФТ), то необходимо передавать дополнительные поля (см. «Периодические платежи»)

AFT Completion Reversal отмена предавторизации (TRTYPE = 28).

Отмену операции можно провести только на всю сумму предавторизации.

Торговая точка формирует POST – запрос и отправляет его на EGW. Список отправляемых Торговой точкой параметров:

PAYMENT_TYPE_ID, ORDER, AMOUNT, CURRENCY, RRN, INT_REF, TRTYPE, TERMINAL, TIMESTAMP.

Описание параметров POST – запроса и допустимых значений см. Таблица 8.

Названия параметров передаются в верхнем регистре. Порядок передачи параметров не важен.

AFT Completion подтверждение (завершение расчета) (TRTYPE = 29).

Завершение расчета можно провести на сумму равную предавторизованной ранее сумме.

Торговая точка формирует POST – запрос и отправляет его на EGW.

Список отправляемых Торговой точкой параметров:

PAYMENT_TYPE_ID, ORDER, AMOUNT, CURRENCY, RRN, INT_REF, TRTYPE, TERMINAL, TIMESTAMP.

Описание параметров POST – запроса и допустимых значений см. Таблица 8

Названия параметров передаются в верхнем регистре. Порядок передачи параметров не важен.

AFT Auth Reversal отмена подтверждённой операции (TRTYPE = 32).

Отмену операции можно провести только на всю сумму.

Торговая точка формирует POST – запрос и отправляет его на EGW.

Список отправляемых Торговой точкой параметров:

PAYMENT_TYPE_ID, ORDER, AMOUNT, CURRENCY, RRN, INT_REF, TRTYPE, TERMINAL, TIMESTAMP.

Описание параметров POST – запроса и допустимых значений см. Таблица 8.

Названия параметров передаются в верхнем регистре. Порядок передачи параметров не важен.

AFT Completion Auth Recur (Периодическая операция АФТ) предавторизации (TRTYPE = 29).

Торговая точка формирует POST – запрос и отправляет его на EGW.

Список отправляемых Торговой точкой параметров: **PAYMENT_TYPE_ID, ORDER, AMOUNT, CURRENCY, RECUR_REF, INT_REF, TRTYPE, TERMINAL, TIMESTAMP.**

Описание параметров POST – запроса и допустимых значений см. Таблица 8.

PAYMENT_TYPE_ID - значение поля обязательно должно быть "PAA" (Индентификатор AFT операции, согласован с МПС)

Формат ответа на AFT запросы.

После получения ответа из карточной системы EGW направляет держателю карты ответ в виде HTML-формы, которая должна быть отправлена в Интернет-магазин (URL для отправки содержится в поле "BACKREF") или в виде специальной страницы (в зависимости от настроек, заданных для данного терминала). Ответная страница будет содержать тот же набор полей, что и сообщение ответа на запрос о завершении торговой операции (см. Таблица 4 Набор полей ответа шлюза электронной коммерции) Поле "TRTYPE" будет содержать то же значение, что и аналогичное поле запроса.

Таблица 8 Описание параметров AFT POST – запроса и допустимых значений

Название параметра	Формат данных / длина *	Значения для запросов от Торговой точки	Значения для ответов от Банка	Описание
AMOUNT	числовой с десятичной точкой / 1-11	Для всех запросов формирует Торговая точка	Транслируется из запроса Торговой точки	Сумма операции
CURRENCY	символьный / 3	Для всех запросов RUB	Транслируется из запроса Торговой точки	Валюта операции
ORDER	числовой / 6-20	**Предавторизация** - формирует Торговая точка **Отмена и завершение расчетов** - транслируется из запроса на предавторизацию	Транслируется из запроса Торговой точки	Уникальный номер заказа.
DESC	символьный / 50	**Предавторизация** - формирует Торговая точка **Отмена и завершение расчетов** - не используется	Транслируется из запроса Торговой точки	Описание заказа
TERMINAL	числовой / 8	Для всех запросов Торговая точка передает значение , присвоенное банком	Транслируется из запроса Торговой точки	Уникальный номер виртуального терминала торговой точки.

Название параметра	Формат данных / длина *	Значения для запросов от Торговой точки	Значения для ответов от Банка	Описание
TRTYPE	числовой / 1-2	**Предавторизация** – 27 **Отмена** – 28 **Завершение расчетов** – 29 **Отмена завершение расчетов** – 32 **Совершение операции** – 70	Транслируется из запроса Торговой точки	Тип запрашиваемой операции
MERCH_NAME	символьный / 22	**Предавторизация** - формирует Торговая точка **Отмена и завершение расчетов** - не используется	Транслируется из запроса Торговой точки	Название Торговой точки
TIMESTAMP	числовой / 14	Для всех запросов формирует Торговая точка	Для всех ответов формирует Банк	UTC время проведения/обработки операции в формате YYYYMMDDHHMISS (Московское время - 3 часа)
RRN	числовой / 12	**Предавторизация** – не используется **Отмена и завершение расчетов** - транслируется из ответа на предавторизацию	Для всех ответов формирует Банк	Retrieval Reference Number – Уникальный идентификатор запроса на списание средств с карты.
INT_REF	символьный / 1-32	**Предавторизация** – не используется **Отмена и завершение расчетов** - транслируется из ответа на предавторизацию	Для всех ответов формирует Банк	Internal Reference – Уникальный идентификатор операции на платежном шлюзе.
CARD	Числовой/16-19	**Предавторизация** – Формирует Торговая точка **Отмена и завершение расчетов** - не используется	Транслируется из запроса Торговой точки	Номер карты
EXP	Числовой / 2	**Предавторизация** – Формирует Торговая точка **Отмена и завершение расчетов** - не используется	Не используется	Срок действия карты (MM)

Название параметра	Формат данных / длина *	Значения для запросов от Торговой точки	Значения для ответов от Банка	Описание
EXP_YEAR	Числовой / 2	**Предавторизация** – Формирует Торговая точка **Отмена и завершение расчетов** - не используется	Не используется	Срок действия карты (ГГ)
CVC2	Числовой / 3	**Предавторизация** – Формирует Торговая точка **Отмена и завершение расчетов** - не используется	Не используется	Дополнительный код безопасности, печатаемый на оборотной стороне карты (может отсутствовать)
CVC2_RC	Числовой / 1	**Предавторизация** – Формирует Торговая точка **Отмена и завершение расчетов** - не используется	Не используется	CVC2_RC Код наличия CVV2/CVC2: "0" – CVC2 намеренно не предоставлен; "1" – CVC2 присутствует; "2" – CVC2 присутствует, но неразборчив; "9" – CVC2 не указан на карте.
***PAYMENT_TYPE_ID**	Символьный / 3	Константа	Транслируется из запроса Торговой точки	PAA - тип платежа для транзакции
****MK_TOKEN**	Символьный / 5	**Предавторизация** Константа **MERCH** **Отмена и завершение** Не используется	Не используется	MERCH –значение параметра для генерации токена карты
MERCH_TOKEN_ID	Символьный	**Предавторизация** – не используется **Отмена и завершение расчетов** - транслируется из ответа на предавторизацию	Не используется	Токен карты, содержит номер карты, срок действия карты

Перевод средств со счетов зарегистрированного у эквайра контракта Торговой точки на карты любого банка(OCT).

Формат запроса на операцию OCT (TRTYPE = 70)

Для выполнения OCT перевода Торговая точка формирует POST – запрос, затем отправляет его на EGW. В предоставленном запросе должны содержаться следующие параметры:
AMOUNT, CURRENCY, ORDER, DESC, TERMINAL, TRTYPE, CARD, PAYMENT_TYPE_ID, TIMESTAMP
Описание параметров POST – запроса и допустимых значений см. Таблица 8.

Кроме указанных полей ожидаются следующие поля:

Таблица 9 Дополнительные CGI поля информации о получателе.

CGI поле	Описание	Формат	Номер CGI поля
PAYMENT_RECEIVER_FIRST_NAME	Receiver First name	ANS ...35	390
PAYMENT_RECEIVER_MIDDLE_NAME	Receiver Middle name	ANS 1	391
PAYMENT_RECEIVER_LAST_NAME	Receiver Last name	ANS ...35	392
PAYMENT_RECEIVER_STREET	Street Address	ANS ...50	393
PAYMENT_RECEIVER_CITY	City	ANS ...25	394
PAYMENT_RECEIVER_STATE_CODE	State/Province Code	AN ...2	395
PAYMENT_RECEIVER_COUNTRY	Country	ANS 3	396
PAYMENT_RECEIVER_POSTAL_CODE	Postal Code	ANS ...10	397
PAYMENT_RECEIVER_PHONE	Phone Number	ANS ...20	398
PAYMENT_RECEIVER_DATE_OF_BIRTH	Date of Birth	N 8	399
PAYMENT_RECEIVER_IDENTITY_TYPE	Identification Type	N 2	400
PAYMENT_RECEIVER_IDENTITY_ID	Identification Number	ANS ...25	401
PAYMENT_RECEIVER_IDENTITY_COUNTRY	Identification Country code	ANS 3	402
PAYMENT_RECEIVER_IDENTITY_EXP_DATE	Identification expiration date	N 8	403
PAYMENT_RECEIVER_NATIONALITY	Nationality	ANS 3	404
PAYMENT_RECEIVER_COUNTRY_OF_BIRTH	Country of Birth	ANS 3	405

Таблица 10 Таблица дополнительные CGI поля информации о отправителе.

CGI поле	Описание	Формат	Номер CGI поля
PAYMENT_SENDER_FIRST_NAME	Receiver First name	ANS ...35	406
PAYMENT_SENDER_MIDDLE_NAME	Receiver Middle name	ANS 1	407

CGI поле	Описание	Формат	Номер CGI поля
PAYMENT_SENDER_LAST_NAME	Receiver Last name	ANS ...35	408
PAYMENT_SENDER_STREET	Street Address	ANS ...50	409
PAYMENT_SENDER_CITY	City	ANS ...25	410
PAYMENT_SENDER_STATE_CODE	State/Province Code	AN ...2	411
PAYMENT_SENDER_COUNTRY	Country	ANS 3	412
PAYMENT_SENDER_POSTAL_CODE	Postal Code	ANS ...10	413
PAYMENT_SENDER_PHONE	Phone Number	ANS ...20	414
PAYMENT_SENDER_DATE_OF_BIRTH	Date of Birth	N 8	415
PAYMENT_SENDER_IDENTITY_TYPE	Identification Type	N 2	416
PAYMENT_SENDER_IDENTITY_ID	Identification Number	ANS ...25	417
PAYMENT_SENDER_IDENTITY_COUNTRY	Identification Country code	ANS 3	418
PAYMENT_SENDER_IDENTITY_EXP_DATE	Identification expiration date	N 8	419
PAYMENT_SENDER_NATIONALITY	Nationality	ANS 3	420
PAYMENT_SENDER_COUNTRY_OF_BIRTH	Country of Birth	ANS 3	421
PAYMENT_SENDER_ACCOUNT_NUMBER	Payment sender account number	ANS ...32	422

В случае если параметр **PAYMENT_TYPE_ID** = **PSR**
- обязательны следующие данные о получателе:

PAYMENT_RECEIVER_FIRST_NAME
PAYMENT_RECEIVER_LAST_NAME
PAYMENT_SENDER_ACCOUNT_NUMBER

Поле **PAYMENT_SENDER_ACCOUNT_NUMBER** обязательное.

Формат ответа на OCT запрос.

После получения ответа из карточной системы EGW направляет держателю карты ответ в виде HTML-формы, которая должна быть отправлена в Интернет-магазин (URL для отправки содержится в поле "BACKREF") или в виде специальной страницы (в зависимости от настроек, заданных для данного терминала). Ответная страница будет содержать тот же набор полей, что и сообщение ответа на запрос о завершении торговой операции (см. Таблица 4 Набор полей ответа шлюза электронной коммерции) Поле "TRTYPE" будет содержать то же значение, что и аналогичное поле запроса.

Сервис для получения суммы доступного лимита списания:

Владелец терминала может получить сумму доступного лимита сделав запрос на URL:
https://3ds.mdmbank.ru/proxy_frm/service

Параметры, которые должен содержать запрос:
SERVS=AMOUNT_OCT
ID=OCTXXXXX – идентификатор терминала

Пример запроса:
https://3ds.mdmbank.ru/proxy_frm/service?SERVS=AMOUNT_OCT&ID=OCT99999
Ответ от сервиса выдаётся в формате json.

Пример ответа на запрос:

```
{
        "SERVS" : "AMOUNT_OCT",
        "VALUES" : [{id: "OCT99999", amount: "1.11", curr: "810"}]
}
```

Где:
id: "OCT99999" – идентификатор терминала
amount: "1.11" – сумма доступных средств
curr: "810" – код валюты в ISO

ОБЩИЕ ЭЛЕМЕНТЫ

Вычисление значения MAC-кода

Чтобы аутентифицировать сообщения транзакций на шлюзе к / от канала продавца, система продавца должна иметь возможность рассчитывать и проверять коды аутентификации сообщений, по крайней мере, для транзакций, передаваемых через перенаправление браузера владельца карты. Для сообщений, которые отправляются непосредственно в EGW («Завершение продаж» и «Сторнирование»), MAC является обязательным.

MAC рассчитывается по всем полям, сгенерированным торговой системой, как определено в соответствующих таблицах формата (видимые и скрытые поля, сгенерированные торговой системой), за исключением самого поля MAC («P_SIGN»). Список полей для MAC согласовывается при подключении терминала.

Чтобы сгенерировать или проверить поле аутентификации сообщения, система продавца должна собрать исходную строку MAC; все значения полей из таблиц форматирования имеют префикс десятичной длины поля в ASCII и объединяются в указанном порядке. Если сообщение не содержит необязательных полей, однако они присутствуют в списке полей, заданном для вычисления MAC-кода, в соответствующей позиции MAC-строки в качестве префикса поля должен использоваться символ "-". Все сообщения, для которых вычисляется MAC-код, должны содержать поля TIMESTAMP и NONCE, являющиеся обязательными для всех списков полей. Поле NONCE всегда должно содержать только что сгенерированное значение (не менее 8 байт) в шестнадцатеричном формате. Поле TIMESTAMP должно содержать временную отметку отправителя (по времени GMT, в формате ГГГГММДДЧЧММСС).

Пример сообщения об авторизации: исходная строка MAC будет содержать следующие значения полей - AMOUNT, CURRENCY, ORDER, DESC, MERCH_NAME, MERCH_URL, MERCHANT, TERMINAL, EMAIL, TRTYPE, COUNTRY, MERCH_GMT, TIMESTAMP, NONCE, BACKREF. Предположим, что у нас есть транзакция со следующими полями:

Поле	Размер	Описание
AMOUNT	5	11.48
CURRENCY	3	USD - валюта
ORDER	6	771446 - № заказа
DESC	16	Книги по IT. Кол-во: 2
MERCH_NAME	17	Books Online Inc. - продавец
MERCH URL	14	www.sample.com – сайт продавца
MERCHANT	15	123456789012345 - продавец
TERMINAL	8	99999999 - теминал
EMAIL	19	pgw@mail.sample.com
TRTYPE	1	1
COUNTRY	0	страна
MERCH GMT	0	
TIMESTAMP	14	20030105153021 отметка времени
NONCE	16	F2B2DD7E603A7ADA одноразовый код
BACKREF	33	https://www.sample.com/shop/reply - ответ с сайта продавца

Исходная строка MAC для этого примера:

```
511.483USD677144616IT Books. Qty: 217Books Online Inc.14www.sample.com
151234567890123458999999991 9pgw@mail.sample.com11--1420030105153021
16F2B2DD7E603A7ADA33https://www.sample.com/shop/reply
```

Разрывы строк вставляются только для наглядности. Длина этой строки составляет 190 байт.

После того как исходная строка MAC собрана, торговая система должна применить криптографический алгоритм для генерации кода аутентификации сообщения. Система продавца должна реализовывать алгоритм в виде аппаратного или программного обеспечения и нести полную ответственность за безопасное хранение и использование соответствующих криптографических ключей. Эффективная длина ключа должна быть не менее 112 бит для симметричных криптографических алгоритмов.

Алгоритм MAC - HMAC_SHA1.

Для нашего примера исходной строки MAC и алгоритма HMAC_SHA1 с шестнадцатеричным секретным ключом «00112233445566778899AABBCCDDEEFF» поле MAC-адреса результата («P_SIGN») должно быть равно: «FACC882CA67E109E409E3974DDEDA8AAB13A5E48». Допускается наличие в поле MAC-кода шестнадцатеричных символов как нижнего, так и верхнего регистра, но обычно создает его из символов верхнего регистра без разделителей)

Специфические отраслевые дополнения

От торговой системы может потребоваться предоставление отраслевых данных транзакций, чтобы соответствовать правилам клиринга и расчетов в банке-эквайере и платежных системах. Следующее поле должно быть установлено для указания типа дополнительных данных:

Поле	Размер	Описание
ADDENDUM	2	Тип отраслевого приложения. Когда это поле присутствует, EGW (шлюз электронной коммерции) будет читать и обрабатывать дополнительный набор полей (см. Поля дополнения ниже). В настоящее время определены типы: «AI» - авиакомпания, маршрут передвижения пассажира

Дополнительные бизнес-специфичные поля

«AI» - авиакомпания, маршрут передвижения пассажира

В настоящее время все поля дополнения являются необязательными в интерфейсе EGW, но система продавца должна предоставить всю доступную информацию. Формат полей - буквенно-цифровой (AN), цифровой (N) или буквенно-цифровой, пробелы (ANS), допускаются только латинские буквы.

Общая подробная информация о билете

Поле	Формат	Описание
AI.TICKET.NAME	ANS(20)	Имя пассажира
AI.TICKET.NUMBER	AN(13)	Номер билета
AI.TICKET.RESTRICTED	N(1)	Указывает, является ли билет невозвратным. 0 = Без ограничений 1 = Ограниченный (невозвратный) билет
AI.TICKET.SYSTEM	AN(4)	Обозначает компьютеризированную систему бронирования, которая использовалась для бронирования и покупки билета: DATS = Delta SABR = Sabre и т. д..
AI.TICKET.AGENCY.CODE	AN(8)	Код турагентства
AI.TICKET.AGENCY.NAME	ANS(25)	Название турагентства

Данные о пересадках (стыковках)

На данный момент поддерживается информация не более чем о 4 пересадках (стыковках). Символ ‘#’ должен быть заменен номером пересадки (стыковки).

Поле	Формат	Описание
AI.TRIPLEG#.DATE	YYYY-MM-DD	Дата отправления пассажира
AI.TRIPLEG#.CARRIER	AN(2)	Код с указанием названия перевозчика (United Airlines, Jet Blue и т. д.)
AI.TRIPLEG#.CLASS	AN(1)	Указывает класс обслуживания (первый класс, бизнес-класс и т. д.)
AI.TRIPLEG#.FROM	AN(3)	Код города отправления
AI.TRIPLEG#.TO	AN(3)	Код города назначения
AI.TRIPLEG#.STOP	AN(1)	Указывает, разрешена ли промежуточная остановка в этом билете. O = остановка разрешена X = остановка не разрешена
AI.TRIPLEG#.FARE	AN(6)	Код тарифа
AI.TRIPLEG#.FLIGHT	AN(5)	Номер рейса

Дополнительная информация для протокола EMVCo 3DS v2

Торговая система может предоставлять конкретные данные транзакции для расширенной обработки 3DS v2. Отправка этих данных является необязательной, MPI должен проверить версию протокола 3DS и соответственно применить эти данные.

Поле	Размер	Описание
M_INFO	35000	Дополнительный набор данных, относящихся к 3DS v2, отправленных продавцом. Должна быть строкой в кодировке Base64 в формате JSON “parameter”:”value data” ("параметр":"данные значения"). Полный набор доступных данных можно найти на веб-сайте EMVCo, в документе “3-D Secure - Protocol and Core Functions Specification” (Защищенный протокол 3-D и спецификация основных функций), в описании сообщений AReq. Все параметры этого набора являются дополнительными.

Ниже приведен пример данных, подготовленных для поля M_INFO. Приведенные ниже данные должны быть преобразованы в одну строку и закодированы в Base64

```
{
"browserLanguage":"en",
"browserColorDepth":"32",
"browserScreenHeight":"1920",
"browserScreenWidth":"1080",
"browserTZ":"0",
"browserUserAgent":"Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0)
Gecko/20100101 Firefox/47.0"
}
```

Ниже приведен список параметров, которые можно отправить для обработки 3DS v2. Отправка этих данных является необязательной, MPI должен проверить версию протокола 3DS и соответственно применить эти данные.

Поле	Описание
threeDSRequestorAuthenticationInfo	Тип данных JSON: Объект Примечание. Данные будут отформатированы в объект JSON до помещения их в информационное поле аутентификации сообщения запросчика 3DS..
Метка времени аутентификации запросчика 3DS. Имя поля: threeDSReqAuthTimestamp	Дата и время в UTC для аутентификации владельца карты.
Индикатор запросчика 3DS. Имя поля: threeDSRequestorChallengeInd	Указывает, произведен ли запрос для этой транзакции.
Информация о предварительной аутентификации запросчиком 3DS Имя поля: threeDSRequestorPriorAuthenticationInfo	Информация о том, как запросчик 3DS аутентифицировал владельца карты как часть предыдущей транзакции 3DS
Тип счета. Имя поля: acctType	Указывает тип счета. Например, для карточного продукта с несколькими счетами.
Индикатора соответствия адреса. Имя поля: addrMatch	Указывает, совпадают ли адрес доставки держателя карты и платежный адрес держателя карты.

Поле	Описание
Заголовки приёма браузера. Имя поля: browserAcceptHeader	Точное содержимое HTTP-заголовков приема, отправленных в запросчик 3DS из браузера держателя карты.
IP-адрес браузера.Имя поля: browserIP	IP-адрес браузера, возвращаемый заголовками HTTP запросчику 3DS.
Браузер Java включен. Имя поля: browserJavaEnabled	Логическое значение, представляющее способность браузера держателя карты выполнять Java. Значение возвращается из свойства navigator.javaEnabled.
Язык браузера. Имя поля: browserLanguage	Значение, представляющее язык браузера, как определено в IETF BCP47. Возвращается из свойства navigator.language.
Глубина цвета экрана браузера. Имя поля: browserColorDepth	Значение, представляющее битовую глубину цветовой палитры для отображения изображений, в битах на пиксель. Получено из браузера держателя карты с помощью свойства screen.colorDepth
Высота экрана браузера. Имя поля: browserScreenHeight	Общая высота экрана владельца карты в пикселях. Значение возвращается из свойства screen.height.
Ширина экрана браузера. Имя поля: browserScreenWidth	Общая ширина экрана владельца карты в пикселях. Значение возвращается из свойства screen.width.
Часовой пояс браузера. Имя поля: browserTZ	Разница во времени между временем UTC и местным временем браузера держателя карты, в минутах.
Пользовательский агент браузера. Имя поля: browserUserAgent	Точное содержание заголовка пользовательского агента HTTP.
Информация о счете владельца карты. Имя поля: acctInfo	Дополнительная информация о счете владельца карты.
Город расчетного адреса владельца карты. Имя поля: billAddrCity	Город расчетного адреса владельца карты, связанного с картой, использованной для этой покупки.
Страна расчетного адреса владельца карты. Имя поля: billAddrCountry	Страна расчетного адреса владельца карты, связанного с картой, использованной для этой покупки.
Первая строка расчетного адреса владельца карты. Имя поля: billAddrLine1	Первая строка адреса улицы или эквивалентной локальной части расчетного адреса владельца карты, связанного с картой, использованной для этой покупки.
Вторая строка расчетного адреса владельца карты. Имя поля: billAddrLine2	Вторая строка адреса улицы или эквивалентной локальной части расчетного адреса владельца карты, связанного с картой, использованной для этой покупки.
Третья строка расчетного адреса владельца карты. Имя поля: billAddrLine3	Третья строка адреса улицы или эквивалентной локальной части расчетного адреса владельца карты, связанного с картой, использованной для этой покупки.
Почтовый индекс владельца карты. Имя поля: billAddrPostCode	ZIP или иной почтовый индекс расчетного адреса держателя карты, связанный с картой, использованной для этой покупки.
Штат расчетного адреса держателя карты. Имя поля: billAddrState	Штат или провинция расчетного адреса держателя карты, связанный с картой, использованной для этой покупки.
Адрес электронной почты владельца карты. Имя поля: email	Адрес электронной почты, связанный с учетной записью, который был введен владельцем карты.
Номер домашнего телефона владельца карты. Имя поля: homePhone	Номер домашнего телефона, предоставленный владельцем карты.
Номер мобильного телефона владельца карты. Имя поля: mobilePhone	Номер мобильного телефона, предоставленный владельцем карты.
Имя владельца карты. Имя поля: cardholderName	Имя владельца карты

Поле	Описание
Город адреса доставки владелца карты. Имя поля: shipAddrCity	Городская часть адреса доставки, запрошенного владельцем карты.
Страна адреса доставки владелца карты. Имя поля: shipAddrCountry	Страна адреса доставки, запрошенного владельцем карты.
Первая строка адреса доставки владельца карты. Имя поля: shipAddrLine1	Первая строка адреса улицы или эквивалентной локальной части адреса доставки, запрошенная владельцем карты.
Вторая строка адреса доставки владельца карты. Имя поля: shipAddrLine2	Вторая строка адреса улицы или эквивалентной локальной части адреса доставки, запрошенная владельцем карты.
Третья строка адреса доставки владельца карты. Имя поля: shipAddrLine3	Третья строка адреса улицы или эквивалентной локальной части адреса доставки, запрошенная владельцем карты.
Почтовый индекс адреса доставки владельца карты. Имя поля: shipAddrPostCode	ZIP или иной почтовый индекс адреса доставки, запрошенный владельцем карты.
Штат адреса доставки владельца карты. Имя поля: shipAddrState	Штат или провинция адреса доставки, связанного с картой, используемой для этой покупки.
Рабочий номер телефона владельца карты. Имя поля: workPhone	Рабочий номер телефона, предоставленный владельцем карты.
Данные по рассрочке платежа. Имя поля: purchaseInstalData	Указывает максимальное количество авторизаций, разрешенных для платежей в рассрочку.
Код категории продавца. Имя поля: mcc	Специфичный DS код, описывающий тип бизнеса, продукта или услуги продавца.
Индикатор торгового риска. Имя поля: merchantRiskIndicato	Оценка продавцом уровня риска мошенничества для конкретной аутентификации, как для владельца карты, так и для проводимой аутентификации.
Расширение текста сообщения. Имя поля: messageExtension	Данные, необходимые для поддержки требований, не определенных иным образом в сообщении 3-D Secure, передаются в расширении сообщения.

Приложение 1. Коды ответа на запрос проведения операции

Коды действия модуля e-Gateway

Значения поля «RESULT» «ACTION» в HTML-форме ответа на запрос проведения операции:

Код	Описание
0	Транзакция успешно завершена
1	Обнаружена повторная транзакция
2	Транзакция отклонена
3	Ошибка обработки транзакции

Коды транзакционного ответа

Значения поля «RC» в HTML-форме ответа на запрос проведения операции (соответствует полю «39» ISO8583):

Код	Описание	
0	Завершено успешно	Approved
1	Отказ обратитесь в банк	Call your bank
2	Отказ спец. условие	Call your bank
3	Недействительный ПТС	Invalid merchant
4	Карточку изъять	Your card is restricted
5	Не оплачивать	Transaction declined
6	Ошибка	Error - retry
7	Карточку изъять (спец)	Your card is disabled
8	Оплатить с идентификацией	Additional identification required
9	Запрос не завершен	Request in progress
10	Разрешено для частичной суммы	Partially approved
11	Одобрено (VIP)	Approved (VIP)
12	Транзакция не выполнена	Invalid transaction
13	Неверная сумма	Invalid amount
14	Недействительная карточка	No such card
15	Нет связи с банком клиента	No such card/issuer
16	Одобрено, запись дорожки 3	Approved, update track 3
17	Отменено клиентом	Customer cancellation
18	Не подтвеждено клиентом	Customer dispute
19	Повторите транзакцию	Re-enter transaction
20	Неправильный ответ	Invalid response

Код	Описание	
21	Операция не выполнена	No action taken
22	Сбой системы	Suspected malfunction
23	Неприемлемый размер налога	Unacceptable fee
24	Операция не поддерживается	Update not supported
25	Нет исходной операции	No such record
26	Дублирование записи	Duplicate update/replaced
27	Ошибка изменения записи	Field update error
28	Файл блокирован	File locked out
29	Ошибка обновления файла	Error, contact acquirer
30	Неправильный формат	Format error
31	Банк клиента недоступен	Issuer signed-off
32	Завершено частично	Completed partially
33	Карточка просрочена	Expired card
34	Подозрительная карточка	Suspected fraud
35	Свяжитесь с банком	Acceptor contact acquirer
36	Карточку изъять (блок.)	Restricted card
37	Карточку изъять (банк)	Call your bank
38	Карточку изъять (ПИН)	PIN tries exceeded
39	Нет кредитного счета	No credit account
40	Функция недоступна	Function not supported
41	Карточку изъять/утеряна	Lost card
42	Нет общего счета	No universal account
43	Карточку изъять/украдена	Stolen card
44	Нет инвестиционного счета	No investment account
51	Недостаточно средств	Not sufficient funds
52	Нет счета	No chequing account
53	Нет счета для сбережений	No savings account
54	Карточка просрочена	Expired card
55	Неверный ПИН	Incorrect PIN
56	Неизвестная карточка	No card record
57	Транзакция запрещена	Not permitted to client
58	Транзакция запрещена	Not permitted to merchant
59	Подозрительная операция	Suspected fraud
60	Позвоните в банк	Acceptor call acquirer
61	Превышен лимит на сумму	Exceeds amount limit

Код	Описание	
62	Карточка запрещена	Restricted card
63	Ошибка шифрования	Security violation
64	Неправильная сумма	Wrong original amount
65	Превышен лимит операций	Exceeds frequency limit
66	Позвоните в банк	Acceptor call acquirer
67	Карточку изъять/банкомат	Pick up at ATM
68	Ответ получен поздно	Reply received too late
75	Лимит ввода ПИН исчерпан	PIN tries exceeded
76	Неверный ПИН. Лимит исчерпан	Wrong PIN,tries exceeded
77	Операция не доступна	Wrong Reference No.
79	Эта сумма уже отменена	Already reversed
80	Ошибка в сети	Network error
81	Ошибка в зарубежной сети	Foreign network error
82	Недоступен банк клиента	Time-out at issuer
83	Невозможно завершить	Transaction failed
84	Таймаут пре-авторизации	Pre-authorization timed out
85	Выполнена проверка счета	Account verification required
86	Не могу проверить ПИН	Unable to verify PIN
88	Ошибка шифрования	Cryptographic failure
89	Ошибка идентификации	Authentication failure
90	Неопределенная ошибка	Cutoff is in progress
91	Недоступен банк клиента	Issuer unavailable
92	Ошибка в сети банка	Router unavailable
93	Нарушение закона	Violation of law
94	Двойная передача	Duplicate transmission
95	Транзакция не найдена	Reconcile error
96	Неисправность в системе	System malfunction
99	Транзакция прервана	Aborted
100	Неопределенный отказ	General fault
101	Обязательное поле отсутствует	Mandatory field is empty
102	Ошибка в формате запроса	Bad CGI request
103	Ответ не получен	No or Invalid response received
104	Сервер не отвечает	Server is not responding
105	Ошибка подключения	Connect failed
106	Ошибка конфигурации	Configuration error

Код	Описание	
107	Ошибка формата ответа	Invalid response
108	Ошибка в номере карты	Error in card number field
109	Ошибка в сроке действия карты	Error in card expiration date field
110	Ошибка в сумме	Error in amount field
111	Ошибка в валюте	Error in currency field
112	Ошибка в номере терминала	Error in merchant terminal field
113	Неизвестный источник операции	Unknown referer
114	Ошибка ПИН клавиатуры или драйвера	PINpad agent/device error
115	Ошибка в номере RRN	Invalid Retrieval reference number
116	Терминал занят, пробуйте еще	Terminal is locked, please try again
117	Отказано в доступе	Access denied
118	Ошибка кода CVC2 или его описания	Error in CVC2 or CVC2 Description fields
119	Ошибка аутентификации	Authentication failed
120	Транзакция просрочена	Expired transaction
121	Повторная транзакция	Duplicate transaction
122	Ошибка аутентификации	Invalid authentication information
123	Ошибка в контексте транзакции	Invalid transaction context
124	Несоответствие в контексте транзакции	Transaction context mismatch
125	Транзакция прервана	Transaction canceled
126	Неверный BIN карты	Invalid action BIN
127	Ошибка в имени продавца	Invalid merchant name
128	Ошибка в дополнительных данных	Invalid incoming addendum(s)
129	Ошибка в ссылке аутентификации (повреждена или дублируется)	Invalid/duplicate authentication reference
130	Подозрительная транзакция	Transaction fraud declined

Дополнительные коды ответа модуля e-Gateway

Код ответа	Описание
-1	В запросе не заполнено обязательное поле
-2	Запрос не прошел CGI-проверку
-3	Хост эквайрера (NS) не отвечает либо неверный формат файла шаблона ответа модуля e-Gateway
-4	Нет соединения с хостом эквайрера (NS)
-5	Ошибка соединения с хостом эквайрера (NS) во время обработки транзакции
-6	Ошибка настройки модуля e-Gateway
-7	Некорректный ответа хоста эквайрера (NS), например, отсутствуют обязательные поля
-8	Ошибка в поле "Card number" запроса
-9	Ошибка в поле "Card expiration date" запроса
-10	Ошибка в поле "Amount" запроса
-11	Ошибка в поле "Currency" запроса
-12	Ошибка в поле "Merchant ID" запроса
-13	IP-адрес источника транзакции (обычно IP торговца) не соответствует ожидаемому
-14	Нет соединения с PIN-клавиатурой Интернет-терминала либо программа-агент на компьютере/рабочей станции Интернет-терминала не запущена
-15	Ошибка в поле "RRN" запроса
-16	На терминале выполняется другая транзакция
-17	Терминалу отказано в доступе к модулю e-Gateway
-18	Ошибка в поле "CVC2" или "CVC2 Description" запроса
-19	Ошибка в запросе на аутентификационную информацию либо аутентификация неуспешна
-20	Превышен допустимый временной интервал (по умолчанию – 1 час) между значением поля "Time Stamp" запроса и временем модуля e-Gateway
-21	Транзакция уже выполнена
-22	Транзакция содержит ошибочную аутентификационную информацию
-23	Ошибка в контексте транзакции
-24	Несоответствие в контексте транзакции
-25	Транзакция прервана пользователем
-26	Неверный BIN карты
-27	Ошибка в имени продавца
-28	Ошибка в дополнительных данных
-29	Ошибка в ссылке аутентификации (повреждена или дублируется)
-30	Транзакция отклонена как мошенническая
-31	Транзакция в процессе выполнения
-32	Повторная отклоненная транзакция
-33	Транзакция в процессе аутентификации клиента с помощью авторизации случайной суммы или одноразового случайного кода
-34	MasterCard Installment транзакция в процессе выбора пользователем способа оплаты
-35	MasterCard Installment транзакция в процессе выбора пользователем способа оплаты была отклонена автоматически после превышения лимита времени на эту операцию
-36	MasterCard Installment транзакция в процессе выбора пользователем способа оплаты была отклонена самим пользователем

Приложение 2. Параметры тестового EGW и список тестовых карт

Тестовый шлюз e-Gateway*
https://3dstest.mdmbank.ru/cgi-bin/cgi_link

Тестовые карты			
PAN (Номер карты)	CVC(Код проверки подлинности карты)	Expire (Срок действия)	3DS (Код подтверждения)
5543 7Зпять4 8четыре62 6654	852	22-01	123456
2200 2два01 1759 3три58	858	22-01	123456
4652 0три56 3304 2два38	973	20-12	123456
42два1 0455 66пять7 8282	748	20-12	Без 3DS
554три 7256 6091 7три40	087	22-01	Без 3DS

Тестовый ключ макирования
Предоставляется уникальный каждому мерчанту или агрегатору при необходимости

Приложение 3. Пример взаимодействия “Интернет–магазин» - «Банк»

На примере trtype=1 (Финансовый запрос).

1. Магазин отправляет страницу, в которой заполняются форма с полями см. Таблица 2, Таблица 3 (в примере ввод данных производится на стороне Банка). Форма постируется на адрес Банка Открытие (далее - Банк).
2. Банк отправляет клиенту страницу tranform.html, в которой клиент заполняет поля формы EXP, EXP_YEAR, CVC2, CVC2_RC. Форма постируется в банк. Банк формирует запрос VeReq в Платежную систему (DS). Если карта не подписана на 3ds (enroll=n), то осуществляется переход на этап 6, иначе - этап 3.
3. Банк отправляет пустую страницу cardauth.html с невидимой формой, которая автоматически постирует PaReq на адрес банка-эмитента, который Банку вернула Платежная система, параметр %126. При этом в параметр TermUrl ставится адрес Банка %124, куда банк-эмитент должен направить PaRes через клиента.
4. Банк-эмитент отправляет клиенту страницу ввода пароля. Клиент вводит пароль.
5. Банк-эмитент отправляет пустую страницу с невидимой формой, которая автоматически постирует PaRes в Банк.
6. Если аутентификация проходит успешно, то Банк в зависимости от TRTYPE проводит либо блокировку, либо списание средств с карты, либо осуществляется отмена операции.
7. Банк отправляет одну из страниц ответа.
8. Банк отправляет CallBack магазину о результатах операции.

	Мага-зин	Браузер (клиент)	Банк Открытие (EGW)	Банк-Эмитент (ACS)
1		<form action="http://3ds2.mmbank.ru/cgi-bin/cgi_link" method="POST"> <input name="AMOUNT" …. type="TEXT"> ……name="CURRENCY"…… ……name="ORDER"…… ……name="DESC"…… ……name="MERCH_NAME"…… ……name="MERCH_URL"…… ……name="MERCHANT"…… ……name="TERMINAL"…… ……name="EMAIL"…… ……name="TRTYPE"…… ……name="COUNTRY"…… ……name="MERCH_GMT"…… ……name="TIMESTAMP"…… ……name="NONCE"……		

		……name="BACKREF"…… ……name="P_SIGN"…… <input value="Approve" name="SEND_BUTTON" type="SUBMIT">		
2		tranform.html <form ACTION="/cgi-bin/cgi_link" METHOD="POST"> <input …. name ="CARD" ……> ……name="EXP" …… ……name="EXP_YEAR"…… ……name="CVC2"…… ……name="CVC2_RC"…… …….. <input type="hidden" name ="TRTYPE" VALUE="%22"></input> ……name="CURRENCY"…… ……name="ORDER"…… ……name="DESC"…… ……name="MERCH_NAME"…… ……name="MERCH_URL"…… ……name="MERCHANT"…… ……name="TERMINAL"…… ……name="EMAIL"…… ……name="TRTYPE"…… ……name="COUNTRY"…… ……name="MERCH_GMT"…… ……name="TIMESTAMP"…… ……name="NONCE"…… ……name="BACKREF"…… ……. input type="submit" name ="SEND_BUTTON"></input>		
3		cardauth.html <body OnLoad="OnLoadEvent();"> <FORM ACTION="%126" METHOD="post"> <input name="PaReq" type="hidden" value="%125">		

		<input name="TermUrl" type="hidden" value="%124"> <input name="MD" type="hidden" value="%39"> </FORM> <SCRIPT> function OnLoadEvent () { document.forms[0].submit(); } </SCRIPT> </body>		
4		Страница ввода пароля Ввод пароля		
5		<body onLoad="onLoadHandler();"> < form name ="PAResForm" METHOD="post" action ="{TermUrl}"> < input name ="PaRes" TYPE="hidden" VALUE="…"> < input name ="MD" TYPE="hidden" VALUE="{MD}"> </ form > </body> < script >function onLoadHandler(){document["PAResForm"].submit();} </script >		
6			Блокировка, списание денег с карты	
7		success.html …… <tr><td >Номер карты:</td><td>%23</td></tr> <tr><td>Срок действия карты:</td><td>%14</td></tr> <tr><td>Сумма операции:</td><td>%8</td></tr> <tr><td>Валюта операции:</td><td>%7</td></tr> <tr><td>Номер заказа:</td><td>%27</td></tr> <tr><td>RRN:</td><td>%28</td></tr>		

		<tr><td>INT_REF:</td><td>%51</td></tr> <tr><td>Код авторизации:</td><td>%4</td></tr> …… ИЛИ decline.html duplicate.html fault.html		
8	Формат ответа: Function=TransResponse&AMOUNT=%25&CURRENCY=%26&ORDER=%27&DESC=%58&MERCH_NAME=%53&MERCH_URL=%55&MERCHANT=%29&TERMINAL=%21&EMAIL=%37&TRTYPE=%22&COUNTRY=%54&MERCH_GMT=%56&TIMESTAMP=%47&NONCE=%61&BACKREF=%41&P_SIGN=%44&CARD=%12&EXP=%14&RRN=%28&INT_REF=%51&APPROVAL=%4&RC=%2&MESSAGE=%3&CODE=%39&RESULT=%1&Payment_Text=%70		CallBack	

Приложение 4. Пример взаимодействия «Интернет–магазин» – «Агрегатор» - «Банк»

На примере trtype=1 (Финансовый запрос)

1. Магазин (ТСП) вводит поля из Таблицы 1.
2. Агрегатор формирует и отправляет запрос в Банк с полями Таблицы 1,2,3. Банк делает запрос VeReq в Платежную систему (DS). Если карта не подписана на 3ds (enroll=n), то идет этап 8, иначе этап 3.
3. Банк отправляет агрегатору xml-страницу cardauth.html с параметрами для формирования запроса в банк-эмитент через клиента. В параметре {TERMURL} возвращается адрес Банка, куда агрегатору нужно ответить PaRes.
4. Банк отправляет пустую страницу с невидимой формой, которая автоматически постирует PaReq на адрес банка-эмитента {ACSURL}, который прислал Банк в cardauth.html. При этом в параметр TermUrl ставится адрес агрегатора {MURL}, куда банк-эмитент должен направить PaRes через клиента.
5. Банк-эмитент отправляет клиенту страницу ввода пароля. Клиент вводит пароль.
6. Банк-эмитент отправляет клиенту пустую страницу с невидимой формой, которая автоматически постирует PaRes агрегатору на адрес {MURL}.
7. Агрегатор отправляет запрос PaRes на адрес Банка {TERMURL}, который он присылал в cardauth.html.
8. Если аутентификация проходит успешно, то Банк в зависимости от TRTYPE проводит либо блокировку, либо списание денег с карты, либо reverse операции.
9. Банк отправляет одну из xml-страниц результата операции.
10. Агрегатор отправляет результат операции клиенту.

	Клиент	Агрегатор (ПО)	Банк Открытие (EGW)	Банк-Эмитент (ACS)
1.				
2.		Формирует и отправляет запрос в Банк с полями Таблицы 1,2,3 		
3.				

		cardauth.html Content-type: text/html <RESPONSE> <ACSURL>%126</ACSURL> <PAREQ>%125</PAREQ> <MD>%39</MD> <TERMURL>%124</TERMURL> </RESPONSE>		
4.	<body OnLoad="OnLoadEvent();"> <FORM ACTION="{ACSURL}" METHOD="post"> <input name="PaReq" type="hidden" value="{PAREQ}"> <input name="TermUrl" type="hidden" value="{MURL}"> <input name="MD" type="hidden" value="{MD}"> </FORM> <SCRIPT> function OnLoadEvent () { document.forms[0].submit(); } </SCRIPT> </body>			
5.				

	Страница ввода пароля Ввод пароля			
6.	<body onLoad="onLoadHandler();"> < form name ="PAResForm" METHOD="post" action ="{MURL}"> < input name ="PaRes" TYPE="hidden" VALUE=""> < input name ="MD" TYPE="hidden" VALUE=""> </ form > </body> < script >function onLoadHandler(){document["PAResForm"].submit();} </script >			
7.		<body onload="document.getElementById('3dsform').submit();"> <form action="{TERMURL}" id="3dsform" method="post"> <input type="hidden" name="PaRes" value="{PaRes}">		

		<input type="hidden" name="MD" value="{MD}"> </form> </body>		
8.			Блокировка, списание денег с карты	
9.		success.html Content-type: text/html <RESPONSE> <AMOUNT>%25</AMOUNT> <CURRENCY>%26</CURRENCY> <ORDER>%27</ORDER> <DESC>%58</DESC> <MERCH_NAME>%53</MERCH_NAME> <MERCH_URL>%55</MERCH_URL> <MERCHANT>%29</MERCHANT> <TERMINAL>%21</TERMINAL> <EMAIL>%37</EMAIL> <TRTYPE>%22</TRTYPE> <COUNTRY>%54</COUNTRY>		

		<MERCH_GMT>%56</MERCH_GMT> <TIMESTAMP>%47</TIMESTAMP> <NONCE>%61</NONCE> <BACKREF>%41</BACKREF> <P_SIGN>%44</P_SIGN> <CARD>%12</CARD> <EXP>%14</EXP> <RRN>%28</RRN> <INT_REF>%51</INT_REF> <APPROVAL>%4</APPROVAL> <RC>%2</RC> <MESSAGE>%3</MESSAGE> <CODE>%39</CODE> <RESULT>%1</RESULT> <PAYMENT_TEXT>%70</PAYMENT_TEXT> </RESPONSE> ИЛИ decline.html duplicate.html fault.html		
10.	Вывод клиенту результатов операции.			

Приложение 5. Пример взаимодействия «Интернет–магазин» – «Агрегатор» - «Банк» с 3DS 2.0

Форматы запросов и ответов даны для примера. Форматы ответов от Банка (json, xml, html) согласовываются во время интеграции.

На примере trtype=1 (Финансовый запрос) и он-лайн сообщений от Банка json.

1. Клиент вводит поля из Таблицы 1.
2. Агрегатор формирует и отправляет **POST**-запрос в Банк с полями Таблицы 1,2,3. *Для получения результата авторизации* "***CRes***" *(аналог PaRes) и "threeDSSessionData" в запрос необходимо добавить поле* "**MERCH_3D_TERM_URL**" *(аналог "TERMURL" в PAReq), это URL, куда ответит Банк-эмитент* "***Cres***" *и "threeDSSessionData".*
3. Если карта подписана эмитентом в МПС на дополнительный **3ds method**, Банк отправляет Агрегатору json страницу с параметрами для формирования запроса в банк-эмитент через браузер клиента. В параметре "**THREEDSMETHODURL**" содержится URL эмитента, на который необходимо переслать запрос для проведения 3DS method. В параметре "**TERMURL**" содержится URL Банка, на который необходимо отправлять запросы для проведения 3ds method. В параметре "**THREEDSMETHODDATA**" содержатся шифрованные BASE64 вложения:
   "threeDSMethodNotificationURL" – URL , куда вернется ответ от эмитента через браузер клиента.

   "threeDSServerTransID" – идентификатор транзакции.

Если карта не подписана эмитентом в МПС на дополнительный 3ds method, Банк сразу формирует запрос **AReq** (аналог VeReq) в Платежную систему (**DS**). Подробности в пункте 6.

4. Агрегатор в параметре "**THREEDSMETHODDATA**" **подменяет** threeDSMethodNotificationURL на **свой URL**, на который придет ответ эмитента через браузер клиента о прохождении **3ds Method**.
5. Агрегатор отправляет html страницу **acs_fingerprint.html** (или аналог страницы, сделанный самим Агрегатором) с невидимой формой в браузер клиента, которая автоматически постирует "**threeDSMethosdData**" на URL банка-эмитента из "**THREEDSMETHODURL**".
6. После отправки страницы **acs_fingerprint.html** (или аналога страницы, сделанного самим Агрегатором) в браузер клиента, Агрегатор получает от эмитента "**threeDSMethosdData**" и методом Post на CGI Банка из "**TERMURL**" отправляет "**threeDSMethosdData**" и получает «OK» от Банка.

7. Агрегатор методом Post на CGI Банка из "TERMURL" отправляет "threeDSMethosdData" и "threeDSMethodState=N" . Проведение **3DS Method** завершено.

8. После завершения **3DS Method,** Банк формирует запрос **AReq** (аналог VeReq) в Платежную систему. Если эмитент запрашивает дополнительный **CHALLENGE** (**ARes** содержит "transStatus": "**C**"), то осуществляется переход на этап 9. Если эмитент считает, что операцию по данной карте можно провести по упрощенной схеме 3ds аутентификации (**ARes** содержит "transStatus": "**Y**"), то следует этап 13.
9. Банк отправляет Агрегатору параметры "redirect": "%126", "Creq": "%125", "threeDSSessionData": "%39". Агрегатор запоминает у себя значение параметра "threeDSSessionData".
10. Агрегатор отправляет в браузер клиента пустую html страницу **cardauth2.html** с невидимой формой (или аналог страницы, сделанный самим Агрегатором), которая из браузера клиента автоматически постирует **CReq** (аналог PaReq) и "threeDSSessionData" на URL эмитента из параметра "**redirect**".
11. Банк-эмитент отправляет клиенту страницу ввода пароля. Клиент вводит пароль.

12. Банк-эмитент отправляет в браузер клиента пустую страницу с невидимой формой, которая автоматически постирует **CRes** (аналог PaRes) на URL , полученный в **AReq** от Платежной системы.
    *Если в первоначальном запросе п.2, был указан параметр "**MERCH_3D_TERM_URL**" с отличным от Банковского значения "**TERMURL**", то ответ с "**CRes**" и "threeDSSessionData" придёт на этот адрес. В этом случае полученный Агрегатором "**CRes**" и "threeDSSessionData" с оригинальным значением (см. п.9) нужно без изменения переслать в банк на URL переданный в запросе из п.3 "**TERMURL**".*
13. Если аутентификация проходит успешно, то Банк проводит списание денежных средств с карты.
14. Банк отправляет Агрегатору одну из страниц ответа. Страница будет содержать набор полей для Агрегатора
15. Агрегатор отправляет результат операции клиенту.

	Клиент	Агрегатор (ПО)	Банк Открытие (EGW)	Банк-Эмитент (ACS)
1.	→			
2.		Формирует и отправляет запрос в Банк с полями Таблицы 1,2,3	→	
3.		Если карта зарегистрирована эмитентом с дополнительным 3ds method		

		acs_finger.html Content-type: text/html <RESPONSE> <TERMURL>%124</TERMURL> <THREEDSMETHODURL> %463 </THREEDSMETHODURL > <THREEDSMETHODDATA> %464 <THREEDSMETHODDATA> </RESPONSE>		
4.	acs_finger.html в браузер клиента <html> <head><title>Waiting for fingerprint</title></head> <body onload="javascript:OnLoadEvent();"> <iframe name="iframe1" style="display:none;"> <P>Please use a browser which supports IFrames!</P> </iframe>	acs_finger.html		

	<form id="formID" name="FingerPrintForm" target="iframe1" action="{THREEDSMETHODURL}" method="POST"> <input name="threeDSMethodData" type="hidden" value="{THREEDSMETHODDATA}"> </form> Please wait We are getting a fingerprint of your browser... </body> … <html>			
5.	в браузер клиента <body onload="document.getElementById('3dsform').submit();">			

	<form action="{threeDSMethodNotificationURL}" id="3dsform" method="post"> <input type="hidden" name="threeDSMethodData" value="{THREEDSMETHODDATA}"> </form> </body>			
6.	из браузера клиента → <body onload= "document.getElementById('3dsform').submit();"> <form action="{threeDSMethodNotificationURL}" id="3dsform" method="post"> <input type="hidden" name="threeDSMethodData" value="{THREEDSMETHODDATA}"> </form> </body>	→		
7.		После отправки страницы acs_fingerprint.html в браузер клиента, Агрегатор на CGI Банка из <TERMURL> отправляет методом Post "threeDSMethosdData" , полученный от эмитента. →		

		Для завершения 3DS method Агрегатор на CGI Банка из <TERMURL> отправляет методом Post "threeDSMethosdData" и "threeDSMethodState=N"		

8.	cardauth2.html
	
	<BODY ONLOAD="javascript:OnLoadEvent();">
	<FORM ACTION="{ACSURL}" METHOD="post" NAME="ThreeDform" target="_self">
	<input name="creq" type="hidden" value="{CREQ}">
	<input name="threeDSSessionData" type="hidden" value="{MD}">
	<input name="termURL" type="hidden" value="{notificationURL}"
	</FORM>
	<SCRIPT>
	function OnLoadEvent () {
	document.forms[0].submit();
	}
	</SCRIPT>
	</BODY>
		cardauth2.html		

9.				

	Страница ввода пароля Ввод пароля			
10.	<html> <head> <META http-equiv="Content-Type" content="text/html; charset=UTF-8"> <title>Return to Merchant's site</title> <SCRIPT> function onLoadHandler() { document["CResForm"].submit(); } </SCRIPT> </head> <body onLoad="onLoadHandler();"> Processing... FORM NAME="CResForm" METHOD="post" ACTION="NotificationURL from AREQ" > INPUT NAME="notificationURL"			

	TYPE="hidden" VALUE="NotificationURL from AREQ"> < INPUT NAME="cres" TYPE="hidden" VALUE="{CRES}" > <INPUT NAME="threeDSSessionData" TYPE="hidden" VALUE="{MD}"> </FORM> </body> </html>	Cres и "threeDSSessionData" 		
11.			Списание денег с карты	
12.		success.html Pragma: no-cache Cache-Control: no-store Content-type: text/html; charset=UTF-8		

		Strict-Transport-Security: max-age=31536000; includeSubDomains ….. <!--Content-type: text/html--> <!--RESPONSE> <AMOUNT>%25</AMOUNT> <CURRENCY>%26</CURRENCY> <ORDER>%27</ORDER> <DESC>%58</DESC> <MERCH_NAME>%53</MERCH_NAME> <MERCH_URL>%55</MERCH_URL> <MERCHANT>%29</MERCHANT> <TERMINAL>%21</TERMINAL> <EMAIL>%37</EMAIL> <TRTYPE>%22</TRTYPE> <COUNTRY>%54</COUNTRY> <MERCH_GMT>%56</MERCH_GMT> <TIMESTAMP>%47</TIMESTAMP> <NONCE>%61</NONCE> <BACKREF>%41</BACKREF> <P_SIGN>%44</P_SIGN> <CARD>%12</CARD> <EXP>%14</EXP>		

		<RRN>%28</RRN> <INT_REF>%51</INT_REF> <APPROVAL>%4</APPROVAL> <RC>%2</RC> <MESSAGE>%3</MESSAGE> <CODE>%39</CODE> <ACTION>%1</ACTION> <PAYMENT_TEXT>%70</PAYMENT_TEXT> </RESPONSE--> ИЛИ decline.html duplicate.html fault.html		
13.	Вывод клиенту результатов операции. ←			

Приложение 6. Использование собственного дизайна Интернет-магазина

Для использования собственного дизайна для страниц ввода данных карты и показа ответов необходимо предоставить в Банк следующие html-страницы:

Имя файла	**Описание**
cardauth.html	Шаблон для ввода пароля на сайте эмитента
decline.html	Шаблон для вывода информации по отклоненным эмитентом операциям
duplicate.html	Шаблон для вывода информации по повторным операциям
fault.html	Шаблон для вывода информации об операциях, завершившихся с ошибкой
success.html	Шаблон для вывода информации об успешно завершившихся операциях.
tranform.html	Форма для ввода карточных данных на стороне банка (при выборе этого варианта ввода карточных данных)

Каждый шаблон должен начинаться со строки:

Content-type: text/html

После данной строки должна идти пустая строка.

При создании собственных шаблонов для отправки данных на URL e-Gateway необходимо использовать имена полей, указанные в разделе «Поля транзакционного сообщения E-Gateway» в колонке **Field Name.** Для отображения на странице значений, полученных от модуля e-Gateway используется конструкция «%N», где %N – номера полей, указанные в поле **Field.**

Дополнительно необходимо указать ссылки к картинкам, css и пр. в относительном виде, используя конструкцию /organization_name/folder, где

- organization_name – интуитивно понятное название организации (возможно, предварительно согласованное с Банком);
- folder – название каталога, указывающее на его содержимое (css, image и т.д.)

Примеры:

- <link rel="stylesheet" href="/ow/superpay_ru/css/our_css.css" type="text/css">
-

Примеры построения данных шаблонов предоставляются Банком при необходимости по запросу.

Шаблон carduth.html

В данном шаблоне для переадресации на сайт банка-эмитента для ввода 3DS-пароля рекомендуется использовать следующую конструкцию:

```
<body OnLoad="OnLoadEvent();">
…
        <IFRAME name="iframe1" align="top" height="410" width="420" align="middle">
            <P>Please use a browser which supports IFrames!</P>
        </IFRAME>
        <FORM ACTION="%126" METHOD="post" target="iframe1">
```

```
        <input name="PaReq"   type="hidden" value="%125">
        <input name="TermUrl" type="hidden" value="%124">
        <input name="MD"      type="hidden" value="%39">
    </FORM>
    <SCRIPT>
        function OnLoadEvent () { document.forms[0].submit(); }
    </SCRIPT>
</body>
```

Описание используемых полей описаны в таблице в разделе «Поля транзакционного сообщения E-Gateway».

Шаблон tranform.html

В данном шаблоне рекомендуется с помощью скриптов проводить следующие проверки:

- Заполнение поля «Номер карты»
- Выбор срока действия карты
- Соответствие значения поля CVC2_RC и CVC2

Шаблоны вывода результатов операции

Для корректного отображения результатов операции после проведения 3DS-операции в данных шаблонах рекомендуется «упаковывать» html-код в java-скрипт, используя следующую конструкцию:

```
Content-type: text/html
<HTML>
<HEAD><TITLE>  </TITLE>
<SCRIPT>
function OnLoadEvent()
{
var msg = '<html>\
            <head>\
                    …\
                    …\
            </head>\
            <body>\
                    …\
                    <!-- html-код, каждая строка заканчивается символом «\» -->
                    …\
            </body>\
        </html>';
    var doc = parent.document;
    doc.open();
    doc.writeln(msg);
```

```
            doc.close();
        }
</SCRIPT>
</HEAD>
<BODY ONLOAD="javascript:OnLoadEvent();">
</BODY>
</HTML>
```

Использование данной конструкции позволяет освободиться от фрейма после ввода клиентом 3DS пароля.

Таблица 11 Рекомендуемые поля для вывода результата выполнения операции

Шаблон	**N поля**	**Описание**
decline.html	%2	Код возврата
	%3	Текстовое описание кода возврата
	%28	RRN
duplicate.html	%23	Номер карты
	%14	Срок действия карты
	%8	Сумма операции
	%7	Валюта операции
	%27	Номер заказа
	%28	RRN
	%4	Код авторизации
fault.html	%2	Код возврата
	%3	Текстовое описание кода возврата
	%17	Расширенное диагностическое сообщение
tranform.html	%23	Номер карты
	%14	Срок действия карты
	%8	Сумма операции
	%7	Валюта операции
	%27	Номер заказа
	%28	RRN
	%4	Код авторизации

Приложение 7. Поля транзакционного сообщения e-Commerce Gateway

Поля, отправляемые модулем e-Commerce Gateway в ответ на запросы Интернет-магазина.

Данные поля возможно определить на web-странице в виде %Field

Пример:

```
<IFRAME name="iframe1" align="top" height="410" width="420" align="middle">
<P>Please use a browser which supports IFrames!</P>
</IFRAME>
<FORM ACTION="%126" METHOD="post" target="iframe1">
<input name="PaReq"   type="hidden" value="%125">
<input name="TermUrl" type="hidden" value="%124">
<input name="MD"      type="hidden" value="%39">
</FORM>
<SCRIPT>
function OnLoadEvent () { document.forms[0].submit(); }
</SCRIPT>
```

Field	Format (Length)	Description
1	Numeric (1)	This field contains e-gateway action code. Action codes are: 0 – Transaction successfully completed; 1 – Duplicate transaction detected; 2 – Transaction declined; 3 – Transaction processing fault; 4 – Information message.
2	Numeric (2)	This field contains ISO-8583 Field 39: Response code or additional e-Gateway Response Code
3	String (3)	This field contains text message corresponding to the Response code (Field 2). Text message is retrieved from "rctext.ext" file by line number. Extension of this file name equals to e-gateway field 31 or "def" if this field is absent.
4	Numeric (6)	Client bank's approval code (ISO-8583 Field 38)
5	YYMM	Card expiration date (ISO-8583 Field 14).
6	Numeric (3)	Transaction currency code.
7	String (3)	Transaction currency name.
8	Numeric	Authorized transaction amount. (ISO-8583 Field 4).
9	MMDDHHMMSS	Transaction transmission time stamp. (ISO-8583 Field 7).

Field	Format (Length)	Description
10	MMDDHHMMSS	Transaction processing time stamp (ISO-8583 Fields 12,13).
11		Reserved for future use.
12	String(9-19)	Masked PAN (e.g. 4XXXXXXX1111)
13	String	Decoded value of Field 1.
14	YY/MM	Different format of Field 5.
15	String	Interface mode. Reserved for future use.
16	String	Extended diagnostic code
17	String	Extended diagnostic message
18-20		Reserved for future use.
21-120		Source Transaction Fields. See next Table below.
121	String	Web master e-mail address.
122	String	Transit variables for "GET" method.
123	String	The text message corresponding to the Response Code. The same as field 3 but URL encoded.
124	String	“OUR_URL” parameter from [MAIN] section
125	String	XML message body. Used by 3D Secure MPI module.
126	String	ACS URL. Used by 3D Secure MPI module.
127-153		Reserved for future use.
151	Char(1)	Card channel. Used by 3D Secure MPI module: E – MasterCard V – VISA
152	Char(1)	Own card flag. Used by 3D Secure MPI module: Y – Existing own card. R – Own card range. Card is absent. N – Non-own card range.
153	String	Card Brand. Used by 3D Secure MPI module.
154	String	Member ID. Used by 3D Secure MPI module.
155	String	iPOS Mini-statement
156	String	iPOS Account Balances List
157	Amount	Acquirer’s fee. Positive amount is cardholder debit fee; negative amount is cardholder credit fee (acquirer’s bonus).
158	Numeric(6)	iPOS Batch ID.
159	String	iPOS Batch processing type. Reserved.
160	String	iPOS Batch totals.
161	String	Cardholder verification/authentication type: PBT – PIN based authentication. TDS – 3D Secure authentication.
162	Amount	Transaction amount without fee. This field is set when acquirer fee is used.

Field	Format (Length)	Description
163	Numeric(6)	iPOS transaction number in batch.
164	String	Enrollment form identification.
170	String	Application specific tags. (OW POS ISO Field 63.29)
171	String	Last login information. As received from Authentication server.

Поля, отправляемые в запросах со стороны системы Интернет-магазина.

С web-страницы поля постируются на адрес e-Gateway по **Field Name.**

Пример:

```
<td><div align="right">Enter your card number:</div></td>
<td><input name="CARD" value="5417I5IO364766O1" size="16" maxlength="16" type="TEXT">
</td>
```

На web-странице вывода результатов данные поля определяются в виде %**Field**.

Пример:

```
<input TYPE="HIDDEN" NAME="AMOUNT" VALUE="%25"></input>
<input TYPE="HIDDEN" NAME="CURRENCY" VALUE="%26"></input>
<input TYPE="HIDDEN" NAME="ORDER" VALUE="%27"></input>
```

Field	Format and Presence	Field Name	Description
21	String Conditional	TERMINAL	Merchant Terminal ID. Field is optional if Terminal Id can be detected by IP address, otherwise mandatory
22	Numeric Conditional	TRTYPE	E-Gateway Transaction type (See "E-Gateway Transaction Types" table). Field is optional if configuration defines default transaction type
23	Numeric Conditional	CARD	Card Number (ISO-8583 Field 2). Optional for PBT transactions
24	String Conditional	EXP	Source card expiration date or month. E.g. "0101" or "01" or "Jan". Optional for PBT transactions.
25	Numeric Mandatory	AMOUNT	Source transaction amount.
26	String (3) Mandatory	CURRENCY	Source transaction currency. Must be valid currency name or code.
27	Numeric Conditional	ORDER	Source e-Merchant Order Id. Mandatory for Retail transactions.
28	Numeric 12 Conditional	RRN	Retrieval reference number (ISO-8583 Field 37). Mandatory for reversal operations
29	Numeric Optional	MERCHANT	Source e-Merchant Id
30	Numeric 4 Conditional	CVC2	Card CVV2/CVC2
31	Numeric 3 Conditional	LANG	Transaction language. The value of this field will be used as extension for message file.

Field	Format and Presence	Field Name	Description
32	Numeric Conditional	EXP_YEAR	Card expiration year if Field 24 doesn't contain it
33	Numeric 1 Conditional	PINPAD	Merchant PIN pad type for PBT. 2 – PIN pad agent connection (obsolete) 3 – Authentication service compatible PIN pad (iPOS).
34	Numeric Optional	BANK	Source Merchant Acquirer Id
35	Numeric Optional	ZIP	Client ZIP code (to be verified by AVS)
36	String Optional	AVS	Client billing address (to be verified by AVS)
37	E-mail Optional	EMAIL	Client e-mail address
38	String Optional	NAME	Client card name (as embossed on card)
39	String Conditional	CODE	Message reference/security code (used in the multiphase transactions)
40	Numeric Conditional	PAYMENT	Utility payment code. Mandatory for payment transaction types.
41	URL Optional	BACKREF	Merchant site URL to return response back
42	String Optional	P_SES_ID	Internet Banking Session Id
43	String Optional	JSERVSESSIONID ROOT	Internet Banking Security Id
44	String Conditional	P_SIGN	Message authentication code (MAC). Mandatory if required by terminal configuration
45	String Optional	P_CURR_JOB	Internet Banking Job Id
46	String Optional	PASSWORD	Client password, if password authentication is used.
47	YYYYMMDDHHMMSS Conditional	TIMESTAMP	Transaction timestamp. Mandatory if message authentication code (MAC) is used.
48	Numeric Optional	P_ID	Internet Banking Reference Id
49	Numeric Conditional	ACCNT_SEL	Account selector. Identifies account (credit, checking, default, etc.) within PAN.
50	Numeric (1) Optional	CVC2_RC	CVV2/CVC2 Reason Code: 0 – CVC2 is intentionally not provided 1 – CVC2 is present 2 – CVC2 is present but illegible 9 – No CVC2 is imprinted

Field	Format and Presence	Field Name	Description
51	Numeric	INT_REF	Internal Reference. Mandatory for reference based transactions. Must match INT_REF from original response.
52	Numeric Optional	ORG_AMOUNT	Original transaction amount. Must be present for partial reversals.
53	String(80)	MERCH_NAME	Merchant name.
54	String (3)	COUNTRY	Merchant 2-character country code.
55	String(250)	MERCH_URL	Merchant Internet Shop URL.
56	Sign and Number(1)	MERCH_GMT	Merchant UTC/GMT time zone offset.
57	String(80)	BRANDS	Merchant accepted comma-separated brands list.
58	String(80)	DESC	Merchant order description
59	String(32)	SERVICE	Requested service name
60	String(32)	USER	User name for requested service
61	String(64)	NONCE	Transaction nonce. Must be filled with 8-32 unpredictable random bytes in hexadecimal form. Mandatory if message authentication code (MAC) is used.
62	String(2-36)	PAYMENT_TO	“Payment to” details (e.g. phone number)
63-64		Ucaf_flag, Ucaf_Authentication_Data	Reserved for UCAF data
65	String(16)	FORM_ID	Form reference ID (used for transaction forms, i.e. when HTML form for entering card data generated by e-Gateway)
66	String	AUTH_TYPE	Authentication method or type
67	String	AUTH_DATA	Authentication data (depends on AUTH_TYPE)
68	String(1-25)	PAYMENT_FROM	“Payment from” details (e.g. account number)
69	Numeric(8-14)	PAYMENT_DATE	Payment period (field format depends on payment type)
70	String(1-100)	PAYMENT_TEXT	Payment text details
71-100	String		Administrator defined fields.
101-121	String		These fields are retrieved from CGI Environment
101	IP Address Mandatory	REMOTE_ADDR	Client CGI source IP address
102	URL Mandatory	HTTP_REFERER	Client Browser Referrer Page
103	String Mandatory	HTTP_USER_AGENT	Client Browser Software

Field	Format and Presence	Field Name	Description
104	String Mandatory	HTTPS	SSL Switch
105	String	ACCEPT	User accepted mime types.
106	String Optional	Authorization	Web server authorization code
107- 121			Reserved for future use.
171	Char(1), Optional	DELIVERY	Delivery method. When field is absent, delivery type is unknown. Defined values: 'S' - Electronic delivery, 'T' - Physical delivery.
177	String(2), Optional	ADDENDUM	Type of industry specific addendum. When this field is present, EGW will read and process additional set of fields (See addendum fields below). Currently defined types: “AI” - Airline, Passenger Itinerary

Приложение 8. Дополнительные атрибуты операции при использовании внешнего MPI.

Для 3DS v1

Для проведения операций 3DS v1 Торговой точкой должны быть использованы параметры, полученные в результате обмена запросами между MPI Торговой точки и платежной системой, эмитентом.

Все приведенные ниже параметры берутся из ответа PARes, который получает MPI в результате прохождения процедуры 3DS.

- **EXT_MPI_XID=** XID параметр из ответа внешнего MPI;
- **EXT_MPI_CAVV=** CAVV параметр из ответа внешнего MPI;
- **EXT_MPI_CAVV_ALG=** CAVVALGORITHM параметр из ответа внешнего MPI;
- **EXT_MPI_ECI=ECI** параметр из ответа внешнего MPI.

Для 3DS v2

Для проведения операций 3DS v2 Торговой точкой должны быть использованы приведенные ниже параметры. Как и в случае с операциями 3DS v1, необходимая информация берется из обмена запросами между MPI Торговой точки и платежной системой, эмитентом.

Все приведенные ниже параметры берутся из запроса RRec, который получает 3DSServer в результате прохождения процедуры 3DS.

- **EXT_MPI_CAVV** = authenticationValue
- **EXT_MPI_ECI** = eci
- **EXT_MPI_TRN_ID** = dsTransID
- **EXT_MPI_3D_VER** = **2**
- **EXT_AUTH_METHOD** = authenticationMethod

Поддержка ApplePay, SamsungPay или GooglePay server на E-Commerce Acquiring

Протоколом взаимодействия с Торговой точкой, обсуживающийся в Банке, определяется ниже приведенный набор признаков, передаваемых Торговой точкой на платежный шлюз Банка для определения платежей с использованием платёжных сервисов.

При проведении операции ApplePay\SamsungPay\GooglePay Торговой точке необходимо отправить на шлюз Банка два параметра, которые были получены от платежного сервиса.

POST CGI variable	Description
EXT_MPI_ECI	Response ECI variable from ApplePay or SamsungPay or GooglePay server
TAVV	Response CAVV variable from ApplePay or SamsungPay or GooglePay server

Длина входящего параметра EXT_MPI_ECI составляет два символа.
В случае, если хотя бы один из перечисленных параметров не получен, получено пустое значение или пропущен, транзакция будет отклонена и в ответном сообщении в поле "EXT_XID_CAVV" будет указан код диагностического отказа.

Пример HTLM страницы с использованием параметров EXT_MPI:

POST request

...

<input TYPE="HIDDEN" NAME="EXT_MPI_XID" VALUE="70Irdm3Nmmc1XnnJFxCn+yCIs8I="></input>

<input TYPE="HIDDEN" NAME="EXT_MPI_CAVV" VALUE="AAABBGQSkRcGdjI3aBKRAAAAAAA="></input>

<input TYPE="HIDDEN" NAME="EXT_MPI_CAVV_ALG" VALUE="2"></input>

<input TYPE="HIDDEN" NAME="EXT_MPI_ECI" VALUE="06"></input>

...

Приложение 9. Типы транзакций модуля e-Commerce Gateway

Тип	Описание
0	Запрос на выполнение авторизации
1	Запрос на выполнение финансовой части торговой операции
8	“Person-to-Person” платеж (Перевод денежных средств)
12	Предварительная авторизация
14	Транзакция по возмещению со ссылкой на первичную транзакцию
21	Завершение вторичной торговой операции со ссылкой на первичную транзакцию
22	Запрос отмены вторичной операции операции со ссылкой на первичную транзакцию (возврат)
24	Уведомление об отмене вторичной операции со ссылкой на первичную транзакцию (возврат)
81	Запрос на создание токена (регистрация карты)
82	Запрос на удаление токена (удаление зарегистрированной карты)
171	Вторичная операция периодического платежа. Обязательные поля RECUR_REF(RRN из первой(оригинальной) транзакции) и INT_REF(ссылка на внутренний номер транзакции из первой(оригинальной) транзакции). Номер карты PAN и срок действия карты не участвуют в проведении данной транзакции.

История изменений

Номер документа	Описание
1.002 - 23.06.2020	Внесены изменения в главу «Использованию различных видов операций отмен/возвратов»
1.003 – 26.06.2020	Добавлено описание заполнения поля PAYMENT_TO для AFT PreAuth в зависимости от MCC. Добавлен комментарий о возврате для карт МИР операцией trtype=14(в клиринге).
1.004 – 16.07.2020	Внесено уточнение в описание параметра EXT_MPI_ECI в пункте «Поддержка ApplePay, SamsungPay или GooglePay server на E-Commerce Acquiring»
1.005 – 23.07.2020	Откорректировано описание Вычисление значения MAC-кода
1.006 – 24.07.2020	Откорректировано описание Вычисление значения MAC-кода. Обязательность полей TIMESTAMP и NONCE
1.007 – 11.11.2020	Откорректировано описание операции OCT. Обязательность полей о получателе и отправителе при типе операции «PSR»
1.008 – 19.11.2020	Откорректировано описание операции OCT. Поле PAYMENT_SENDER_ACCOUNT_NUMBER обязательное.
1.008 – 04.02.2021	Дополнено описание полей об получателе и отправителе для OCT операций.
1.010 – 05.02.2021	Скорректировано описание операций AFT. Карточные данные не нужны для вторичных операций AFT.
1.011 – 15.03.2021	Добавлено Приложение 5. Пример взаимодействия «Интернет–магазин» – «Агрегатор» - «Банк» с 3DS 2.0
1.012 – 11.05.2021	Добавлено описание «Передача дополнительной комиссии ecom в МПС НСПК»