ПАО «СДМ-Банк»

Инструкция подключения торговой точки

Версия 0.8

3dsecure
2.10.2018

Оглавление

Описание механизма взаимодействия

Процедура взаимодействия интернет магазина и банка при совершении операции покупки включает в себя следующие этапы:

1. Покупатель подключается сайту интернет-магазина.
2. Покупатель заказывает необходимые товары/услуги на сайте интернет-магазина.
3. Покупатель выбирает способ оплаты товаров/услуг банковской картой.
4. Интернет магазин отправляет данные о покупке (см *Исходящее сообщение*) и переводит покупателя на платежный шлюз банка.
5. Платежный шлюз проверяет данные о покупке, подпись MAC (см. *Механизм формирования цифровой подписи MAC)*. Выводит основную информацию о совершаемой транзакции покупателю и предлагает безопасно ввести карточные данные (номер карты, срок действия, имя держателя, cvv2).
6. Покупатель вводит карточные данные и нажимает оплатить.
7. Платежный шлюз выводит все существенные данные и условия проведения операции для окончательного подтверждения покупателем.
8. Покупатель подтверждает.
9. В случае поддержки картой покупателя технологии 3dsecure платежный шлюз переводит покупателя на сайт эмитента банковской карты для проведения авторизации.
10. Покупатель проводит 3dsecure проверку.
11. Платежный шлюз проводит списание денежных средств с карты покупателя.
12. Платежный шлюз отправляет интернет магазину информацию о результатах операции на заранее согласованный адрес URL (см. *Входящее сообщение*).
    Интернет магазин отдельно и заранее передает в Банк ссылку для получения ответов, а та ссылка которая передается в запросах - это просто ссылка для возврата на страницу магазина на которую ничего не передается.
13. Платежный шлюз выводит информацию о результатах операции покупателю и предлагает вернуться в интернет магазин.
14. Интернет магазин проверяет принятую от платежного шлюза информацию, проверяет подпись MAC (см. *Механизм формирования цифровой подписи MAC).*
15. В случае успешного проведения и списания денежных средств с карты покупателя интернет-магазин оказывает услуги / отправляет товары покупателю.
16. Если по каким-то причинам оказание услуг/отправка товаров невозможно интернет магазин самостоятельно проводит операции отмены покупки или частичного возврата денежных средств на карту покупателя (см. *Формат операции отмены* и *Формат операции частичного возврата*).
17. Банк возмещает интернет-магазину денежные средства за совершенные операции в соответствии с договором обслуживания.

Описание технологии токенизации.

Технология токенизации позволяет сохранить на стороне магазина уникальный номер (токен) для использования в последующих покупках. Это позволяет не вводить клиенту магазина данные карты при каждой транзакции.

Возможность сохранения данных карты для последующих покупок реализована на странице ввода данных карты при совершении платежа на стороне банка. В случае выбора клиентом данной опции магазину в ответе, в специальных поля, будет возвращен токен и маскированный номер карты.

При последующих покупках, магазин должен в операции покупки присылать номер токена в специальном поле.

Поле, содержащее номер токена, не будет возвращено если клиент не воспользовался данной опцией.

Полученный токен магазин должен хранить на своей стороне в связке- маскированный номер карты- номер токена. Необходимость хранения данных именно в данной связке, обусловлена возможностью наличия у клиента более чем одной карты.

Ответственность за сохранность базы данных токенов лежит на магазине. В случае утери базы данных токенов банк не передаёт магазину информацию о уже сгенерированных токенах.

Описание механизма взаимодействия с использованием технологии токенизации.

Процедура взаимодействия интернет магазина и банка при совершении операции покупки по токену включает в себя следующие этапы:

1. Покупатель подключается сайту интернет-магазина.
2. Покупатель заказывает необходимые товары/услуги на сайте интернет-магазина.
3. Покупатель выбирает способ оплаты товаров/услуг сохраненной банковской картой.
4. Интернет магазин отправляет данные о покупке (см *Исходящее сообщение*) переводит покупателя на платежный шлюз банка. В случае если магазин уже имеет сгенерированый токен, то его номер должен быть передан в соответствующем поле.
5. Платежный шлюз проверяет данные о покупке, подпись MAC (см. *Механизм формирования цифровой подписи MAC)*. Выводит основную информацию о совершаемой транзакции покупателю и предлагает безопасно ввести карточные данные (номер карты, срок действия, имя держателя, cvv2). Данный пункт выполняется в случае, если операция была выполнена без указания токена.
6. Покупатель вводит карточные данные и нажимает оплатить. Данный пункт выполняется в случае, если операция была выполнена без указания токена. На данном этапе клиент может выбрать опцию «сохранить данные карты для последующих покупок».
7. Платежный шлюз выводит все существенные данные и условия проведения операции для окончательного подтверждения покупателем.
8. Покупатель подтверждает.
9. В случае поддержки картой покупателя технологии 3dsecure платежный шлюз переводит покупателя на сайт эмитента банковской карты для проведения авторизации.
10. Покупатель проводит 3dsecure проверку.
11. Платежный шлюз проводит списание денежных средств с карты покупателя.
12. Платежный шлюз отправляет интернет магазину информацию о результатах операции на заранее согласованный адрес URL (см. *Входящее сообщение*). В случае выбора клиентом опции «сохранить карту для последующих покупок», в ответе будет содержаться специальное поле с номером токена и маскированый номер карты.

    Внимание! В случае, если клиент отказался от опции «сохранить карту для последующих покупок» данное поле в ответе передаваться не будет.
    Интернет магазин отдельно и заранее передает в Банк ссылку для получения ответов, а та ссылка которая передается в запросах - это просто ссылка для возврата на страницу магазина на которую ничего не передается.
13. Платежный шлюз выводит информацию о результатах операции покупателю и предлагает вернуться в интернет магазин.

14. Интернет магазин проверяет принятую от платежного шлюза информацию, проверяет подпись MAC (см. *Механизм формирования цифровой подписи MAC).*
15. В случае успешного проведения и списания денежных средств с карты покупателя интернет-магазин оказывает услуги / отправляет товары покупателю.
16. Если по каким-то причинам оказание услуг/отправка товаров невозможно интернет магазин самостоятельно проводит операции отмены покупки или частичного возврата денежных средств на карту покупателя (см. *Формат операции отмены* и *Формат операции частичного возврата*).
17. Банк возмещает интернет-магазину денежные средства за совершенные операции в соответствии с договором обслуживания.

Описание механизма взаимодействия при отменах.

В случае, если клиент отказался от товар или оплаченная услуга не была оказана, магазин может выполнить операцию отмены. Данная операция может быть осуществлена как на полную сумму, так и на часть суммы. В данном случае предусмартивается следующий механизм взаимодействия:

1. Интернет магазин формирует операцию отмены\возврата
2. Платежный шлюз проверяет формат сообщения и подпись MAC
3. Платежный шлюз проводит отмену операции списания денежных средств с карты покупателя.
4. Платежный шлюз отправляет интернет магазину информацию о результатах операции на заранее согласованный адрес URL.
5. Интернет магазин проверяет принятую от платежного шлюза информацию, проверяет подпись MAC (см. *Механизм формирования цифровой подписи MAC*).
6. Банк производит расчёты в соответствии с договором обслуживания.

Внимание! Операции отмены и возврата имеют одинаковые форматы как для работы с токенизацией так и без неё.

Формат операции покупки

Данные необходимо передать методом HTTP POST на платежный шлюз Банка:

https://3ds.sdm.ru/cgi-bin/cgi_link – промышленный шлюз

https://3dst.sdm.ru/cgi-bin/cgi_link – тестовый шлюз

Исходящее сообщение

Поле OW	Имя поля	Формат	Размер	Описание
227	MERCH_TOKEN_ID	символьное	32	Номер токена. Необязятельное поле. Значение заполняется только в случае выполенения операции по токену.
25	AMOUNT	цифровое	12	Общая сумма заказа.
26	CURRENCY	цифровое, фиксированное значение	3	Валюта заказа, 3-символьный код валюты Задать равным “643”
27	ORDER	цифровое,	6-32	Номер заказа интернет-магазина. Должно быть уникально в течении суток.
58	DESC	символьное	1-50	Описание заказа интернет-магазина
53	MERCH_NAME	символьное	1-50	Имя торговца
55	MERCH_URL	символьное	1-250	URL сайта торговца
29	MERCHANT	символьное	15	Идентификатор торговца, заданный банком
21	TERMINAL	символьное	8	Идентификатор терминала торговца, заданный банком
47	TIMESTAMP	цифровое, ГГГГММДДЧЧММСС	14	Временная отметка проведения операции интернет-магазином по времени GMT: ГГГГММДДЧЧММСС. Разница времени не должна превышать 1 час с реальным, иначе платежный шлюз отклонит транзакцию.
56	MERCH_GMT	цифровое	1-5	Сдвиг часового пояса интернет магазина относительно UTC/GMT (например, "–3")
37	EMAIL	символьное	80	Зарезервировано, не используется
22	TRTYPE	цифровое, фиксированное значение	2	Тип операции. Задать равным "1"
41	BACKREF	символьное	1-250	URL куда возвращать пользователя после проведения операции
61	NONCE	символьное	16-64	Идентификатор транзакции, задаваемый интернет-

				магазином в виде случайной комбинации длиной в 8-32 байт в шестнадцатеричном формате.
44	P_SIGN	символьное	1-256	MAC-код торговца в шестнадцатеричном формате, подробнее см. *Механизм формирования цифровой подписи MAC*

Входящее сообщение

Данные отправляются методом HTTP POST на заранее предоставленный интернет-магазином URL-адрес.

Поле OW	Имя поля	Формат	Размер	Описание
25	AMOUNT	цифровое	12	Сумма операции.
26	CURRENCY	цифровое, фиксированное значение	3	Валюта заказа, 3-символьный код валюты Фиксированное значение “643”
27	ORDER	цифровое	6-32	Номер заказа интернет-магазина, полученный во входящем сообщении
22	TRTYPE	цифровое, фиксированное значение	2	Тип операции. Фиксированное значение “1”
1	RESULT	цифровое	1	Код ответа шлюза, подробнее см. *Коды ответа шлюза 3DSecure*
2	RC	цифровое	2	Код транзакционного ответа (поле 39 протокола ISO-8583), подробнее см. *Коды ответа шлюза 3DSecure*
4	AUTHCODE	символьное	6	Код положительного ответа банка клиента (код авторизации) (поле 38 протокола ISO-8583)
12	MASKEDPAN	символьное	9-19	Маска номера карты. Возвращается только магазинам работающим с токенами.
28	RRN	символьное	12	Уникальный ссылочный номер СДМ-БАНКа (поле 37 протокола ISO-8583)
51	INTREF	символьное	1-12	Внутренний ссылочный номер шлюза
227	MERCHTOKENID	символьное	32	Номер сгенерированного токена. Возвращается только магазинам работающим с токенами.
157	FEE	цифровое	12	Дополнительная комиссия банка.
44	P_SIGN	символьное	1-256	MAC-код ответа в шестнадцатеричном формате, подробнее см. *Механизм формирования цифровой подписи MAC*

Формат операции отмены

Исходящее сообщение

Данные необходимо передать методом HTTP POST на платежный шлюз Банка:

https://3ds.sdm.ru/cgi-bin/cgi_link – промышленный шлюз

https://3dst.sdm.ru/cgi-bin/cgi_link – тестовый шлюз

Поле OW	Имя поля	Формат	Размер	Описание
25	AMOUNT	цифровое	12	Сумма отмены, должна совпадать с суммой оригинальной операции
26	CURRENCY	цифровое, фиксированное значение	3	Валюта заказа, 3-символьный код валюты Задать равным “643”
27	ORDER	цифровое	6-32	Номер заказа интернет-магазина. Долен совпадать с оригинальным номером заказа
21	TERMINAL	символьное	8	Идентификатор терминала торговца, заданный банком
28	RRN	символьное	12	Уникальный ссылочный номер СДМ-БАНКа (поле 37 протокола ISO-8583), полученный в ответ на оригинальную операцию
51	INT_REF	символьное	1-32	Внутренний ссылочный номер шлюза, полученный в ответ на оригинальную операцию
47	TIMESTAMP	цифровое, ГГГГММДДЧЧММСС	14	Временная отметка проведения операции интернет-магазином по времени GMT: ГГГГММДДЧЧММСС. Разница времени не должна превышать 1 час с реальным, иначе платежный шлюз отклонит транзакцию.
56	MERCH_GMT	цифровое	1-5	Сдвиг часового пояса интернет магазина относительно UTC/GMT (например, "–3")
22	TRTYPE	цифровое, фиксированное значение	2	Тип операции. Задать равным "14"
61	NONCE	символьное	16-64	Идентификатор транзакции, задаваемый интернет-магазином в виде случайной комбинации длиной в 8-32 байт в шестнадцатеричном формате.
44	P_SIGN	символьное	1-256	MAC-код торговца в шестнадцатеричном формате, подробнее см. *Механизм формирования цифровой подписи MAC*

Входящее сообщение

Данные отправляются методом HTTP POST на заранее предоставленный интернет-магазином URL-адрес.

Поле OW	Имя поля	Формат	Размер	Описание
25	AMOUNT	цифровое	12	Сумма операции.
26	CURRENCY	цифровое, фиксированное значение	3	Валюта заказа, 3-символьный код валюты Фиксированное значение “643”
27	ORDER	цифровое	6-32	Номер заказа интернет-магазина, полученный во входящем сообщении
22	TRTYPE	цифровое, фиксированное значение	2	Тип операции. Фиксированное значение “14”
1	RESULT	цифровое	1	Код ответа шлюза, подробнее см. *Коды ответа шлюза 3DSecure*
2	RC	цифровое	2	Код транзакционного ответа (поле 39 протокола ISO-8583), подробнее см. *Коды ответа шлюза 3DSecure*
4	AUTHCODE	символьное	6	Код положительного ответа банка клиента (код авторизации) (поле 38 протокола ISO-8583)
12	MASKEDPAN	символьное	9-19	Маска номера карты. Возвращается только магазинам работающим с токенами.
227	MERCHTOKENID	символьное	32	Номер токена. Возвращается только магазинам работающим с токенами.
28	RRN	символьное	12	Уникальный ссылочный номер СДМ-БАНКа (поле 37 протокола ISO-8583)
51	INF_REF	символьное	1-12	Внутренний ссылочный номер шлюза
157	FEE	цифровое	12	Дополнительная комиссия банка.
44	P_SIGN	символьное	1-256	MAC-код торговца в шестнадцатеричном формате, подробнее см. *Механизм формирования цифровой подписи MAC*

Формат операции частичного возврата

Исходящее сообщение

Данные необходимо передать методом HTTP POST на платежный шлюз Банка:

https://3ds.sdm.ru/cgi-bin/cgi_link – промышленный шлюз

https://3dst.sdm.ru/cgi-bin/cgi_link – тестовый шлюз

Поле OW	Имя поля	Формат	Размер	Описание
25	AMOUNT	цифровое	12	Сумма для возврата на карту клиента
26	CURRENCY	цифровое, фиксированное значение	3	Валюта заказа, 3-символьный код валюты Задать равным “643”
27	ORDER	цифровое	6-32	Номер операции возврата интернет-магазина. Должен быть уникален в течение суток, и не должен совпадать с оригинальным номером заказа.
21	TERMINAL	символьное	8	Идентификатор терминала торговца, заданный банком
28	RRN	символьное	12	Уникальный ссылочный номер СДМ-БАНКа (поле 37 протокола ISO-8583), полученный в ответ на оригинальную операцию
51	INT_REF	символьное	1-32	Внутренний ссылочный номер шлюза, полученный в ответ на оригинальную операцию
47	TIMESTAMP	цифровое, ГГГГММДДЧЧММСС	14	Временная отметка проведения операции интернет-магазином по времени GMT: ГГГГММДДЧЧММСС. Разница времени не должна превышать 1 час с реальным, иначе платежный шлюз отклонит транзакцию.
56	MERCH_GMT	цифровое	1-5	Сдвиг часового пояса интернет магазина относительно UTC/GMT (например, "–3")
22	TRTYPE	цифровое, фиксированное значение	2	Тип операции. Задать равным "14"
61	NONCE	символьное	16-64	Идентификатор транзакции, задаваемый интернет-магазином в виде случайной комбинации длиной в 8-32 байт в шестнадцатеричном формате.
44	P_SIGN	символьное	1-256	MAC-код торговца в шестнадцатеричном формате, подробнее см. *Механизм*

				формирования цифровой подписи MAC

Входящее сообщение

Данные отправляются методом HTTP POST на заранее предоставленный интернет-магазином URL-адрес.

Поле OW	Имя поля	Формат	Размер	Описание
25	AMOUNT	цифровое	12	Сумма операции.
26	CURRENCY	цифровое, фиксированное значение	3	Валюта заказа, 3-символьный код валюты Фиксированное значение “643”
27	ORDER	цифровое	6-32	Номер заказа интернет-магазина, полученный во входящем сообщении
22	TRTYPE	цифровое, фиксированное значение	2	Тип операции. Фиксированное значение “14”
1	RESULT	цифровое	1	Код ответа шлюза, подробнее см. *Коды ответа шлюза 3DSecure*
2	RC	цифровое	2	Код транзакционного ответа (поле 39 протокола ISO-8583), подробнее см. *Коды ответа шлюза 3DSecure*
4	AUTHCODE	символьное	6	Код положительного ответа банка клиента (код авторизации) (поле 38 протокола ISO-8583)
28	RRN	символьное	12	Уникальный ссылочный номер СДМ-БАНКа (поле 37 протокола ISO-8583)
12	MASKEDPAN	символьное	9-19	Маска номера карты. Возвращается только магазинам работающим с токенами.
227	MERCHTOKENID	символьное	32	Номер токена. Возвращается только магазинам работающим с токенами.
51	INF_REF	символьное	1-12	Внутренний ссылочный номер шлюза
157	FEE	цифровое	12	Дополнительная комиссия банка.
44	P_SIGN	символьное	1-256	MAC-код ответа в шестнадцатеричном формате, подробнее см. *Механизм формирования цифровой подписи MAC*

Формат операции удаления токена по карте.

Исходящее сообщение

Данные необходимо передать методом HTTP POST на платежный шлюз Банка:

https://3ds.sdm.ru/cgi-bin/cgi_link – промышленный шлюз

https://3dst.sdm.ru/cgi-bin/cgi_link – тестовый шлюз

Поле OW	Имя поля	Формат	Размер	Описание
227	MERCH_TOKEN_ID	символьное	32	Номер токена.
27	ORDER	цифровое,	6-32	Номер заказа интернет-магазина. Должно быть уникально в течении суток.
58	DESC	символьное	1-50	Описание заказа интернет-магазина
53	MERCH_NAME	символьное	1-50	Имя торговца
55	MERCH_URL	символьное	1-250	URL сайта торговца
29	MERCHANT	символьное	15	Идентификатор торговца, заданный банком
21	TERMINAL	символьное	8	Идентификатор терминала торговца, заданный банком
47	TIMESTAMP	цифровое, ГГГГММДДЧЧММСС	14	Временная отметка проведения операции интернет-магазином по времени GMT: ГГГГММДДЧЧММСС. Разница времени не должна превышать 1 час с реальным, иначе платежный шлюз отклонит транзакцию.
56	MERCH_GMT	цифровое	1-5	Сдвиг часового пояса интернет магазина относительно UTC/GMT (например, "–3")
37	EMAIL	символьное	80	Зарезервировано, не используется
22	TRTYPE	цифровое, фиксированное значение	2	Тип операции. Задать равным "82"
41	BACKREF	символьное	1-250	URL куда возвращать пользователя после проведения операции
61	NONCE	символьное	16-64	Идентификатор транзакции, задаваемый интернет-магазином в виде случайной комбинации длиной в 8-32 байт в шестнадцатеричном формате.
44	P_SIGN	символьное	1-256	MAC-код торговца в шестнадцатеричном формате, подробнее см. *Механизм*

				формирования цифровой подписи MAC

Входящее сообщение

Данные отправляются методом HTTP POST на заранее предоставленный интернет-магазином URL-адрес.

Поле OW	Имя поля	Формат	Размер	Описание
27	ORDER	цифровое	6-32	Номер заказа интернет-магазина, полученный во входящем сообщении
22	TRTYPE	цифровое, фиксированное значение	2	Тип операции. Фиксированное значение “81”
1	RESULT	цифровое	1	Код ответа шлюза, подробнее см. *Коды ответа шлюза 3DSecure*
2	RC	цифровое	2	Код транзакционного ответа (поле 39 протокола ISO-8583), подробнее см. *Коды ответа шлюза 3DSecure*
44	P_SIGN	символьное	1-256	MAC-код ответа в шестнадцатеричном формате, подробнее см. *Механизм формирования цифровой подписи MAC*

Механизм формирования цифровой подписи MAC

Для подтверждения подлинности входящих и исходящих сообщений используется механизм цифровой подписи MAC – Message Authentication Code. Для формирования подписи интернет-магазин должен сформировать исходную строку из следующих полей сообщения (порядок важен):

Внимание! Формирование MAC производится только по полям описанным в таблице. Остальные поля запроса не участвуют в расчёте MAC.

Тип операции	Список полей
Исходящее покупка	AMOUNT, CURRENCY, ORDER, DESC, MERCH_NAME, MERCH_URL, MERCHANT, TERMINAL, EMAIL, TRTYPE, TIMESTAMP, NONCE, BACKREF
Исходящее отмена	AMOUNT, CURRENCY, ORDER, TERMINAL, TRTYPE, TIMESTAMP, NONCE,BACKREF,RRN,INT_REF
Исходящее частичный возврат	AMOUNT, CURRENCY, ORDER, TERMINAL, TRTYPE, TIMESTAMP, NONCE, BACKREF, RRN,INT_REF
Входящее (для всех)	AMOUNT, CURRENCY, ORDER, TRTYPE, RESULT, RC, AUTHCODE, RRN, INF_REF

Исходная строка формируется путем последовательной записи длины текста каждого поля (в байтах) и его значения в кодировке UTF-8. Если поле пустое, то на место поля необходимо вставить символ '-'.

Пример формирования подписи MAC для следующих тестовых данных:

Имя поля	Размер	Значение
AMOUNT	5	11.48
CURRENCY	3	USD
ORDER	6	771446
DESC	12	Книги: 2 шт.
MERCH_NAME	17	Books Online Inc.
MERCH_URL	14	www.sample.com
MERCHANT	15	123456789012345
TERMINAL	8	99999999
EMAIL	19	pgw@mail.sample.com
TRTYPE	1	1
TIMESTAMP	14	20030105153021
NONCE	16	F2B2DD7E603A7ADA
BACKREF	33	https://www.sample.com/shop/reply

Исходная строка MAC для вышеприведенного примера (без переноса строк):

> *511.483USD677144612Книги: 2 шт.17Books Online Inc.14www.sample.com15123456789012345899999999919pgw@mail.sample.com11142003010515302116F2B2DD7E603A7ADA33https://www.sample.com/shop/reply*

После формирования MAC строки необходимо применить стандартный криптографический механизм HMAC_SHA1 (подробнее https://ru.wikipedia.org/wiki/HMAC) используя заранее полученный секретный ключ и данную строку. Секретный ключ в функцию получения MAC необходимо подставлять в бинароном виде.

Пример для PHP:

```
String = '511.483USD677144618Книги: 2 шт.17Books Online
Inc.14www.sample.com15123456789012345899999999919pgw@mail.sample.com11--
142003010515302116F2B2DD7E603A7ADA33https://www.sample.com/shop/reply';
$skey = '00112233445566778899AABBCCDDEEFF';
echo  hash_hmac('sha1',$String,hex2bin($skey));
```

Пример для Java (https://3dsdemo.sdm.ru):

```
DATA.value = '511.483USD677144618Книги: 2 шт.17Books Online
Inc.14www.sample.com15123456789012345899999999919pgw@mail.sample.com11--
142003010515302116F2B2DD7E603A7ADA33https://www.sample.com/shop/reply';
KEY.value = '00112233445566778899AABBCCDDEEFF';
P_SIGN.value = hex_hmac_sha1(hex2bin(KEY.value),MAC_DATA.value);
```

Обращаем внимание, что предоставляемый Банком в ТСП секретный ключ является единственным механизмом проверки подлинности отправителя. Поэтому хранение и использование секретного ключа на серверах ТСП должно быть реализовано так, чтобы секретный ключ не мог быть скомпрометирован злоумышленником. Например обработку ключей, подписей и входящих и исходящих сообщений нельзя делать в JavaScript выполняемом на клиенте (язык на котором сделана библиотека mac.js, библиотека приведена только в качестве демонстрации алгоритма расчета подписи).

Для вышеприведенной строки и секретного ключа “00112233445566778899AABBCCDDEEFF”, результирующая подпись MAC (поле “P_SIGN”) должна равняться “e89371772f1504f6a48992b8b2c00b55d4f84779”.

Приложение 1. Описание подключения к тестовому стенду

Демонстрационный стенд для самостоятельной проверки, настроенный на взаимодействия с тестовым шлюзом, находится по адресу https://3dsdemo.sdm.ru

Реквизиты необходимые для подключения к тестовому стенду:

Поле	Значение
MERCHANT	123456789012345
TERMINAL	10008888 (для примера)
TRTYPE	1 – покупка, 14 – отмена/частичный возврат
ключ	466B3FE46B9D6030B322EEFAB03BE966
адрес шлюза	https://3dst.sdm.ru

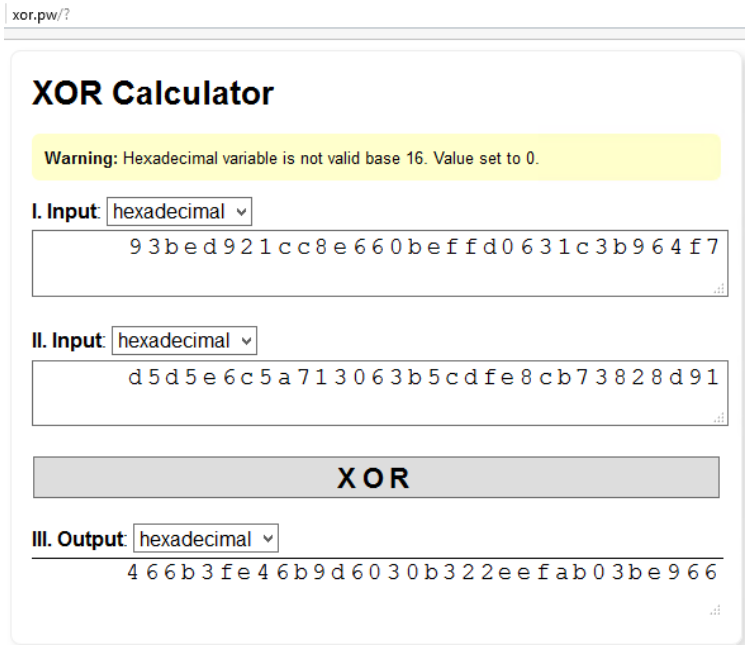
Ключ передается в виде двух компонент. Итоговый ключ получается объединением этих 2-х компонент методом XOR.

Пример генерации:
cmpt 1: 93BED921CC8E660B EFFD0631C3B964F7
cmpt 2: D5D5E6C5A713063B 5CDFE8CB73828D91

Чистый ключ из этих компонент, полученный методом XOR:
clear key: 466B 3FE4 6B9D 6030 B322 EEFA B03B E966

Для объединения компонент методом XOR можно использовать любой калькулятор, в котором есть данная функция. Например, такой калькулятор есть на сайте http://xor.pw/

Вводим значения 2-х компонент и нажимаем кнопку XOR, в нижней части получаемый итоговое значение ключа:



Приложение 2. Примеры и коды html страниц для работы с тестовым стендом

Библиотека для расчета MAC (mac.js)

mac_js.txt

Библиотека для работы с форматами времени (moment.js)

moment_js.txt

Операция покупки (payment.html)

payment_html.txt

Операция отмены (full_reversal.html)

full_reversal_html.txt

Операция частичного возврата (partial_reversal.html)

Partial_reversal_html.txt

Приложение 3. Расшифровка кодов ошибок

Коды ответа шлюза 3DSecure

поле Result исходящих сообщений

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

Детализированная расшифровка кодов ответа

поле RC исходящих сообщений (поле 39 протокола ISO-8583)

Код	Описание
00	Successfully completed
01	Refer to card issuer
02	Refer to card issuer's special condition
03	Invalid merchant / source
04	PICK UP
05	Do not Honour
06	Error
07	Pick-up card, special condition
08	Honour with identification
09	Request in progress
10	Approved for partial amount
11	Approved (VIP)
12	Invalid transaction
13	Invalid amount
14	No such card
15	No such issuer
16	Approved, update track 3
17	Customer cancellation
18	Customer dispute
19	Re-enter transaction
20	Invalid response
21	No action taken
22	Suspected malfunction
23	Unacceptable transaction fee
24	File update not supported by receiver
25	No such record
26	Duplicate record update, old record replaced

27	File update field edit error
28	File locked out while update
29	File update error, contact acquirer
30	Format error
31	Issuer signed-off
32	Completed partially
33	Pick-up, expired card
34	Suspect Fraud
35	Pick-up, card acceptor contact acquirer
36	Pick up, card restricted
37	Pick up, call acquirer security
38	Pick up, Allowable PIN tries exceeded
39	No credit account
40	Requested function not supported
41	Pick up, lost card
42	No universal account
43	Pick up, stolen card
44	No investment account
45	Reserved for ISO use
46	Reserved for ISO use
47	Reserved for ISO use
48	Reserved for ISO use
49	Reserved for ISO use
50	Do not renew
51	Not sufficient funds
52	No chequing account
53	No savings account
54	Expired card / target
55	Incorrect PIN
56	No card record
57	Transaction not permitted to cardholder
58	Transaction not permitted to terminal
59	Suspected fraud
60	Card acceptor contact acquirer
61	Exceeds withdrawal amount limit
62	Restricted card
63	Security violation
64	Wrong original amount
65	Exceeds withdrawal frequency limit
66	Call acquirers security department
67	Card to be picked up at ATM
68	Response received too late
69	Reserved
70	Invalid transaction; contact card issuer

71	Decline PIN not changed
72	Reserved
73	Reserved
74	Reserved
75	Allowable number of PIN tries exceeded
76	Wrong PIN, number of PIN tries exceeded
77	Wrong Reference No.
78	Record Not Found
79	Already reversed
80	Network error
81	Foreign network error / PIN cryptographic error
82	Time-out at issuer system / Bad CVV (VISA)
83	Transaction failed
84	Pre-authorization timed out
85	No reason to decline
86	Unable to validate PIN
87	Purchase Approval Only
88	Cryptographic failure
89	Authentication failure
90	Cutoff is in progress
91	Issuer or switch is inoperative
92	Unable to route at acquirer module
93	Cannot be completed, violation of law
94	Duplicate Transmission
95	Reconcile error / Auth Not found
96	System Malfunction
97	Reserved
98	Reserved
99	Reserved

Дополнительные коды ответа.

Код	**Описание**
-1	В запросе не заполнено обязательное поле
-2	Запрос не прошел CGI-проверку
-3	Хост эквайрера (NS) не отвечает либо неверный формат файла шаблонаответа 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, отсутствуютобязательные 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