Открытые
Системы
Транзакций

ПО MPI в составе подсистемы 3-D Secure процессинговой системы ОСТ24.
Руководство по интеграции для интернет-магазина.
Версия 1.4

– Москва * 2018 *

Содержание

Основные принципы функционирования

Взаимодействие компонентов MPI, банка-эмитента и интернет магазина

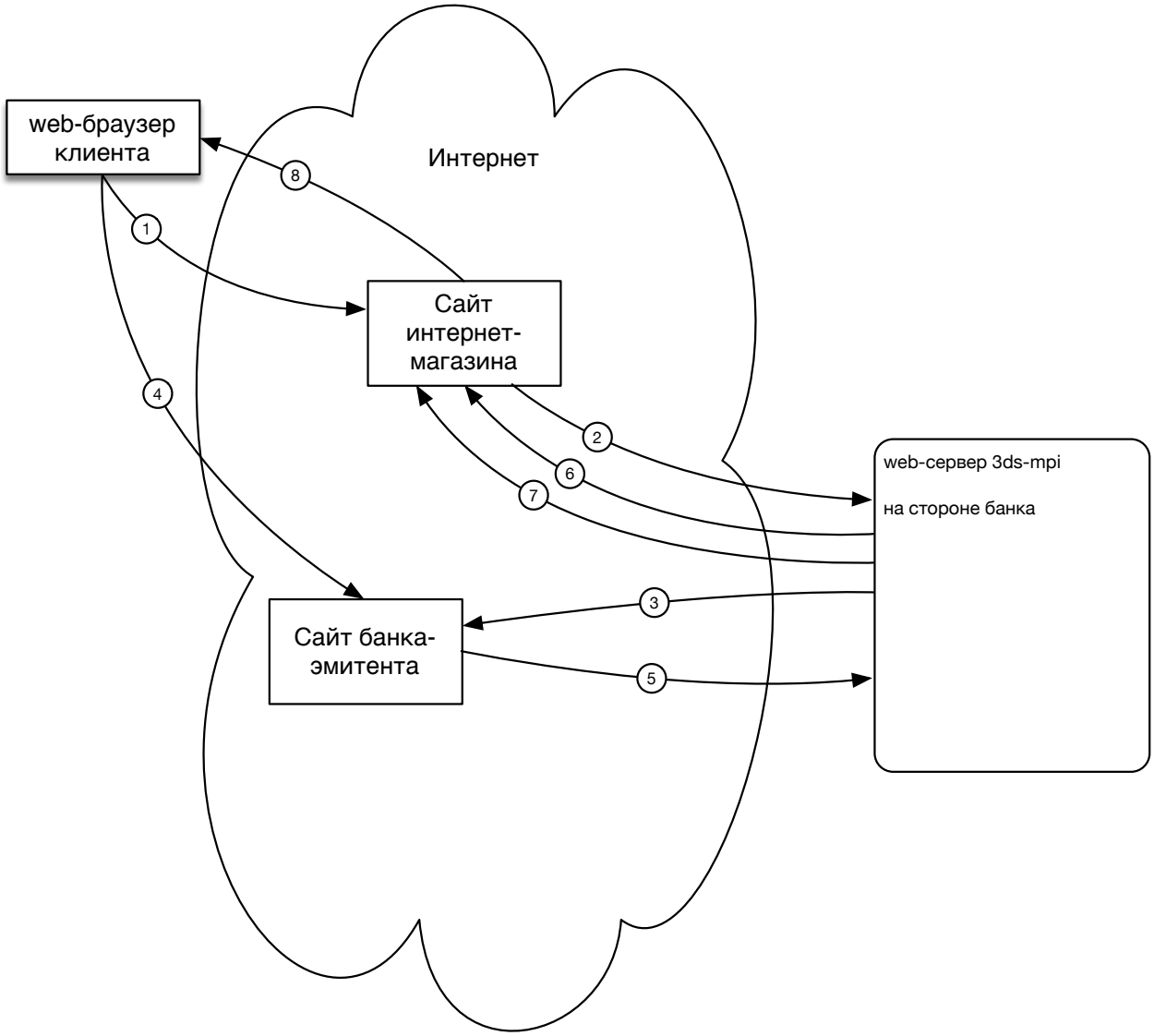

рис. 1 Схема взаимодействия компонентов MPI в составе подсистемы 3-D Secure, платежной системы и банка-эмитента

1. Клиент делает покупки на сайте интернет-магазина – участника 3-D Secure.
2. Интернет-магазин переадресует браузер клиента на web-сервер 3ds-mpi в составе подсистемы 3-D Secure.
3. web-сервер 3ds-mpi переадресует браузер клиента на страницу аутентификации банка-эмитента.
4. Клиент проходит аутентификацию на сайте своего банка.
5. Банк-эмитент переадресует браузер клиента на web-сервер 3ds-mpi в составе подсистемы 3-D Secure.
6. web-сервер 3ds-mpi осуществляет доставку результатов аутентификации и авторизации на выделенный адрес интернет-магазина.
7. web-сервер 3ds-mpi переадресует браузер клиента на сайт интернет-магазина.
8. Интернет-магазин информирует клиента о результате аутентификации.

Конфигурационные параметры ПО ОСТ24, предоставляемые интернет-магазином

Для того, чтобы ПО 3-D Secure в составе процессинговой системы ОСТ24 могло обрабатывать транзакции от интернет-магазинов, требуется выполнить конфигурирование интернет-магазина в БД подсистемы 3-D Secure в составе процессинговой системы ОСТ24.
Заполнение полей следующее:

- **NAME** – название интернет-магазина латиницей;
- **COUNTRY** – ISO-код страны интернет-магазина;
- **URL** – URL-адрес страницы интернет-магазина;
- **URL_APPROVE** – URL-адрес страницы интернет-магазина, на которую будет переадресован браузер клиента после успешного завершения транзакции;
- **URL_DECLINE** – URL-адрес страницы интернет-магазина, на которую будет переадресован браузер клиента после получения отказа при обработке транзакции (как на этапе аутентификации клиента, так и авторизации);
- **URL_ERROR** – URL-адрес страницы интернет-магазина, на которую будет переадресован браузер клиента в случае возникновения при обработке транзакции ошибки в подсистеме 3-D Secure MPI в составе процессинговой системы ОСТ24.

Интерфейс взаимодействия интернет-магазина с MPI

Шаг №2 – переадресация клиента на web-сервер 3ds-mpi

Взаимодействие между интернет-магазином и MPI на этом этапе осуществляется посредством передачи данных транзакции в формате CGI-формы в кодировке «**application/x-www-form-urlencoded**» при помощи метода POST протокола HTTP на URL «**https://***адрес-сервера-3ds-mpi***/3dsmpi.php**».
Спецификация полей данных формы приведена в таблице ниже.

Поле CGI	Формат	Присутствие	Описание
STORE_ID	N..8	Обязательно	Уникальный идентификатор интернет-магазина, присвоенный интернет-магазину банком-эквайером

Поле CGI	Формат	Присутствие	Описание
LANG	AN3	Необязательно	Код языка. RUS – русский; ENG – английский. Возможно использование других значений в рамках отдельных проектов.
DESCR	ANS..256	Необязательно	Описание транзакции в кодировке UTF8. Передается банку-эмитенту.
ORDER_ID	B20 под BASE64	Обязательно	20-разрядный уникальный номер заказа, закодированный при помощи алгоритма BASE64. Передается банку-эмитенту.
AMOUNT	N9.3	Обязательно	Сумма операции. Передается банку-эмитенту.
CURR	N3	Обязательно	ISO-код валюты операции. Передается банку-эмитенту.

Шаг №6 – доставку результатов аутентификации и авторизации на сайт интернет-магазина

Взаимодействие между интернет-магазином и MPI на этом этапе осуществляется посредством передачи данных результата аутентификации и авторизации при помощи метода POST протокола HTTP.

URL-адрес страницы, на которую MPI производит отправку данных, предоставляется интернет-магазином банку на этапе регистрации.

Внимание! Доставка результатов аутентификации и авторизации осуществляется при помощи защищенного соединения по протоколу HTTPS с обязательной проверкой клиентского сертификата на стороне интернет-магазина. Интересантом выполнения данной проверки является интернет-магазин, поскольку, это позволяет снизить риски убытков магазина вследствие действий кибер-преступников, осуществляющих кражи товара путем подстановки ложных результатов аутентификации и авторизации, если магазин принимает результаты транзакции при использовании неверного сертификата.

При организации проверки клиентского сертификата интернет-магазинам следует выполнять настройку web-сервера таким образом, чтобы принимались соединения только от HTTPS-клиентов, содержащих в пути подписанных сертификатов определенный сертификат, определяемый банком-эквайером. Это может быть как корневой сертификат, промежуточный сертификат доверенного центра, так и конечный клиентский сертификат. На практике проверка клиентского сертификата выполняется средствами web-сервера на уровне отдельного web-сайта, который идентифицируется связкой доменного имени сайта и опционального номера порта. Таким образом, чтобы обеспечить проверку клиентского сертификата для механизма доставки результатов транзакции, но не нарушить возможность доступа пользователей, не имеющих установленного клиентского сертификата, к другим страницам сайта, URL, используемый для отправки результатов транзакции, должен содержать адрес хоста или (и) номер порта web-сайта, отличные от страниц, доступных пользователям. В противном случае, пользователи-клиенты интернет-магазина не смогут пользоваться страницами сайта ввиду отсутствия закрытого ключа соответствующего сертификата в локальной базе данных браузера.

Спецификация полей данных формы приведена в таблице ниже.

Поле CGI	Формат	Присутствие	Описание
PAResVerified	A..5	Обязательно	«true» - аутентификация прошла успешно «false» - аутентификация не прошла

AuthResult	AN..7	Необязательно	Результат авторизации. Поле присутствует только для транзакций, для которых аутентификация прошла успешно. «approve» - авторизовано; «decline» - получен отказ; «error» - в процессе авторизации произошла ошибка.
AuthCode	AN..6	Необязательно	Поле присутствует только для успешно авторизованных транзакций и содержит код авторизации. В случае неуспешной аутентификации или отказа банка-эмитента авторизовать транзакцию поле отсутствует.
ORDER_ID	B20 под BASE64	Обязательно	20-разрядный уникальный номер заказа, закодированный при помощи алгоритма BASE64. Содержит значение, полученное от интернет-магазина на шаге №2.

Шаг №7 – переадресация клиента на сайт интернет-магазина

Взаимодействие между интернет-магазином и MPI на этом этапе осуществляется при помощи переадресации браузера клиента на одну из страниц интернет-магазина в соответствии с результатом аутентификации и предоставленными при регистрации интернет-магазином URL-адресами (URL_APPROVE, URL_DECLINE, URL_ERROR) с добавлением к URL дополнительных полей, перечисленных в таблице ниже.

Поле CGI	**Формат**	**Присутствие**	**Описание**
PAResVerified	A..5	Обязательно	«true» - аутентификация прошла успешно «false» - аутентификация не прошла
AuthResult	AN..7	Необязательно	Результат авторизации. Поле присутствует только для транзакций, для которых аутентификация прошла успешно. «approve» - авторизовано; «decline» - получен отказ; «error» - в процессе авторизации произошла ошибка.
AuthCode	AN..6	Необязательно	Поле присутствует только для успешно авторизованных транзакций и содержит код авторизации. В случае неуспешной аутентификации или отказа банка-эмитента авторизовать транзакцию поле отсутствует.
ORDER_ID	B20 под BASE64	Обязательно	20-разрядный уникальный номер заказа, закодированный при помощи алгоритма BASE64. Содержит значение, полученное от интернет-магазина на шаге №2.

Поле CGI	Формат	Присутствие	Описание
PAResVerified	A..5	Обязательно	«true» - аутентификация прошла успешно «false» - аутентификация не прошла
AuthResult	AN..7	Необязательно	Результат авторизации. Поле присутствует только для транзакций, для которых аутентификация прошла успешно. «approve» - авторизовано; «decline» - получен отказ; «error» - в процессе авторизации произошла ошибка.
AuthCode	AN..6	Необязательно	Поле присутствует только для успешно авторизованных транзакций и содержит код авторизации. В случае неуспешной аутентификации или отказа банка-эмитента авторизовать транзакцию поле отсутствует.
Signature	BASE64	Обязательно	Электронная подпись в формате PKCS#1, выполненная при помощи алгоритмов SHA1/RSA. В качестве объекта электронной подписи используется сцепка присутствующих в форме полей PAResVerified, AuthResult, AuthCode, ORDER_ID в следующем формате: *поле=значение* с разделителем NL (LF, ASCII-код 0x10).

Внимание! Переадресация браузера клиента на сайт интернет-магазина сопровождается передачей результатов аутентификации и авторизации, сопровождаемых электронной подписью, выполненной банком-эквайером при помощи закрытого RSA-ключа. Проверка электронной подписи должна производиться публичным RSA-ключом, предоставляемым магазину банком-эквайером. Интересантом проверки электронной подписи является интернет-магазин, поскольку, это позволяет снизить риски убытков магазина вследствие действий кибер-преступников, осуществляющих кражи товара путем подстановки ложных результатов аутентификации и авторизации, если магазин принимает результаты транзакции при использовании фальсифицированной электронной подписи.