SmartBanking

Описание процессов и архитектуры решения SmartBanking 3DS Server (sb3DSS)

2025

Кратко о продукте

Smart Banking 3DS Server (sb3DSS) – это программное решение для поставщиков платёжных услуг, которым необходимо в момент совершения операций электронной коммерции выполнять аутентификацию клиента в соответствии с протоколом EMV 3D-Secure 2.x.

sb3DSS – автономный компонент, который может быть интегрирован с любым платёжным решением электронной коммерции эквайера или, например, сервис-провайдера.

Для осуществления аутентификации клиента sb3DSS собирает данные как о платеже, либо переводе, так и об устройствах, на которых они осуществляются.

СОДЕРЖАНИЕ

Акронимы и Терминология

Термин	Акроним	Описание
3DS Server	3DSS	Компонент Домена Эквайрера, который обеспечивает взаимодействие между средой 3DS Requestor Environment и компонентом DS для аутентификации Держателя карты. Компонент 3DS Server отвечает за: • сбор необходимых элементов данных для сообщений протокола EMV 3-D Secure; • аутентификацию компонента DS; • валидацию компонента DS, компонента 3DS SDK и компонента 3DS Requestor; • обеспечение защиты содержания сообщений.
3-D Secure Software Development Kit	3DS SDK	Компонент, который встроен в 3DS Requestor App (приложение ТСП, установленное на средстве персональной коммуникации Держателя карты).
3DS Requestor Initiated	3RI	Подтверждение платежного средства Эмитентом, инициированное ТСП электронной коммерции или его сервис провайдером, которое выполняется без непосредственного участия в этом процессе Держателя карты.
Access Control Server	ACS	Компонент Домена Эмитента, который взаимодействует с DS платёжной системы, проверяет, доступна ли аутентификация для номера карты и типа устройства, а также аутентифицирует Держателя карты.
Directory Server	DS	Компонент Домена платежной системы, выполняющий ряд функций, включая маршрутизацию аутентификационных сообщений и аутентификацию серверов в Доменах Эквайрера и Эмитента.
3-D Secure	3DS	Совокупность открытых спецификаций протокола надежной аутентификации Держателя карты при проведении операции в сети Интернет, разработанных EMVCo. Термин может использоваться в сочетании с мажорными версиями спецификации 2.1.0 и 2.2.0.

EMVCo	EMVCo	Организация, способствующая разработке стандартов в области платежных технологий.
Сервис-провайдер (Internet Payment Service Provider)	IPSP	Сторонняя организация, привлеченная Участником с целью обеспечения взаимодействия с Операционным центром ПС для оказания Участнику услуг по аутентификации Держателей карт при выполнении Операций в сети Интернет с использованием технологии надежной аутентификации. Организация, выполняющая функции IPSP, должна иметь действующий сертификат соответствия требованиям Стандарта PCI DSS.
Сертификат		Электронный документ, выданный УЦ ПС. Здесь и далее под сертификатом понимается не являющийся квалифицированным сертификат ключа проверки электронной подписи формата X.509 v.3 (https://tools.ietf.org/html/rfc5280), содержащий открытый ключ владельца, идентификатор владельца, срок действия сертификата, условия использования закрытого ключа, соответствующего сертификату, идентификатор УЦ.
Удостоверяющий центр Certificate Authority	УЦ CA	Юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, выполняющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей.
3DS Requestor		Инициатор запроса аутентификации EMV 3-D Secure. Например, это может быть продавец или цифровой кошелек, запрашивающий аутентификацию внутри потока покупок.
3DS Method		Вызов сценария, предоставляемый интегратором 3DS и размещаемый на сайте 3DS Requestor. Опционально используется для получения дополнительной информации о браузере держателя карты, для облегчения принятия решений, основанных на риске.
Authentication		В контексте 3-D Secure, процесс подтверждения того, что человек, совершая транзакцию электронной коммерции, имеет право использовать платежную карту.

Authentication Value	AV	Криптографическое значение, генерируемое ACS, для обеспечения возможности проверки авторизационной системой целостности результата аутентификации. Алгоритм AV определяется каждой Платежной системой.
Authorisation		Процесс, посредством которого Эмитент или обработчик от имени Эмитента, утверждает транзакцию к оплате.
Authorisation System		Системы и услуги, посредством которых Платежная система осуществляет свою деятельность: онлайн- услуги финансовой обработки, авторизации, клиринга и расчетов эмитентам и эквайерам.
Bank Identification Number	BIN	Первые шесть или восемь цифр номера платежной карты, которые однозначно идентифицируют финансовое учреждение-эмитент.
Base64		Кодирование, применяемое к элементу данных «Authentication Value», как определено в RFC 2045.
Base64url		Кодирование, применяемое к данным 3DS Method Data, Device Information и сообщениям CReq/CRes, как определено в RFC 7515.
Cardholder		Физическое лицо, которому выдана карта или которое имеет право ее использовать.
Challenge Flow		Поток 3-D Secure, включающий взаимодействие с держателем карты.
Electronic Commerce Indicator	ECI	Значение, специфичное для платежной системы, предоставляемое ACS для обозначения результатов аутентификации держателя карты.
Frictionless Flow		Поток 3-D Secure, который не предполагает взаимодействия с держателем карты.
One-Time Passcode	OTP	Код доступа, действительный только для одной попытки аутентификации.
Out-of-Band	OOB	Процесс аутентификации, выполняемый вне основного потока, но параллельно с ним. Последний запрос не используется для передачи данных в ACS, но сигнализирует только о том, что аутентификация завершена. Методы аутентификации не определяются спецификацией 3-D Secure.

Payment System	PS IPS	Платежная система, определяющая правила и условия работы, а также требования к выпуску карты и приему торговцами.
Whitelisting		Процесс ACS, позволяющий держателю карты поместить запрашивающую сторону 3DS в список доверенных бенефициаров.

Версия 3-D Secure

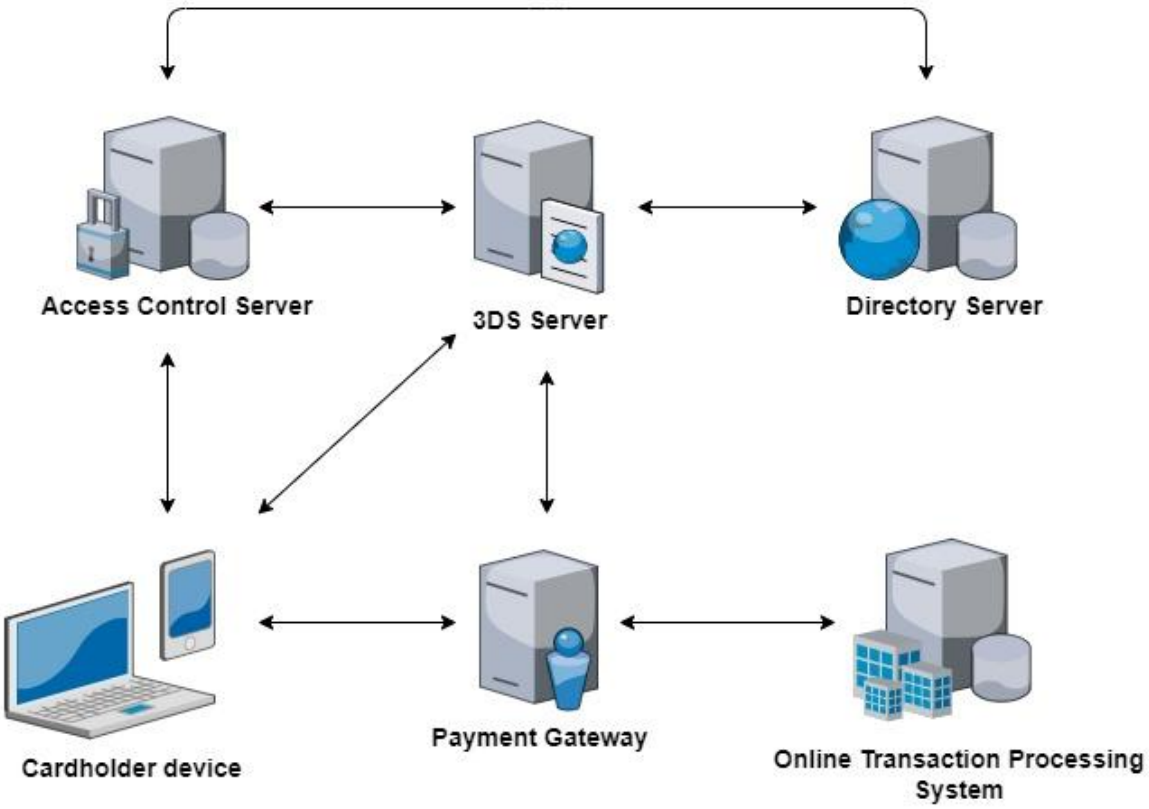
Если вы не знакомы с технологией 3-D Secure, ознакомьтесь со спецификацией протокола EMV 3-D Secure и основных функций (https://www.emvco.com/specifications/emv-3-d-secure-protocol-and-core-functions-specification-2/).

Поддерживаемая версия протокола 3-D Secure — 2.2.0

Поддерживаемые программы платёжных систем:

- Mastercard Identity Check
- Visa Secure
- НСПК MirAccept
- UnionPay 3-D Secure
- Discover Diners ProtectBuy

Архитектура решения



В зависимости от требований проекта sb3DSS может быть интегрирован со следующими системами:

- DS (сервер каталогов) — сервер платежной схемы (PS) для выполнения 3DS, часть общей инфраструктуры 3DS. Соединение с DS устанавливается обычным способом через обратный прокси-сервер (например, nginx или аналогичный), поскольку требуются сертификаты, подписанные PS, размещенные на прокси. Но также возможно установить соединение из самого приложения sb3DSS.
- Устройства держателей карт — это может быть браузер или мобильное устройство, соединение устанавливается так же, как и для DS, но вместо этого с соответствующими сертификатами, подписанными коммерческими CA.

- ➢ Платежный шлюз — что касается платежной операции или операции перевода денег, требующей аутентификации держателя карты с помощью 3D-Secure, sb3DSS может быть интегрирован с любым платежным шлюзом. Соответствующий API разрабатывается и используется для выполнения 3DS.
- ➢ ACS — может быть ситуация, когда sb3DSS напрямую интегрирован с ACS того же банка или поставщика услуг. В случае локальных операций (например, когда эмитентом и экватором является один и тот же банк), не требующих участия платёжной системы, используется прямая интеграция и конкретная конфигурация.

Управление сертификатами

Для работы с sb3DSS необходимы следующие сертификаты:

- Сертификат сервера TLS для связи между DS и 3DSS.
- Сертификат клиента TLS для связи между 3DSS и DS.

PCI DSS compliance

Компания Smart Banking гарантирует безопасность своего продукта sb3DSS и соответствие международным стандартам PCI 3DS и PCI DSS.

Метрики

Метрики — это количественные показатели событий в системе.

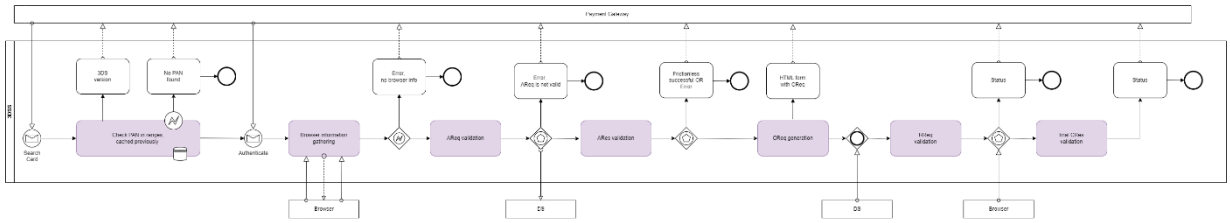
Метрики можно использовать для мониторинга и анализа доступности и производительности системы.

Sb3DSS предоставляет всю необходимую информацию и данные для мониторинга любым популярным инструментам.

Технологический стек

OpenJDK, PostgreSQL

Описание процесса



В первой итерации взаимодействия с 3DS Server необходимо вызвать сервис проверки карты.

3DSS проверяет, участвует ли номер карты в программе 3DSS 2.x, сравнивая его с интервалами номеров карт, полученными ранее с сервера каталогов, в противном случае процесс завершается с ошибкой.

Следующий шаг требуется от платежного шлюза для начала аутентификации. Для этого вызывается соответствующая служба из 3DSS.

Для завершения форматирования AReq 3DSS должен выполнить сбор информации браузера. Если, по какой-либо причине, это невозможно, 3DSS не может завершить AReq и завершает обработку.

Если нет причин для завершения процесса с ошибкой, AReq отправляется в соответствующий DS.

В случае возникновения проблем с сетью или другой причины, препятствующей процессу, 3DSS завершает обработку.

В ответ 3DSS получает ARes и выполняет проверку. В случае Frictionless flow процесс аутентификации завершается.

Если эмитент решил аутентифицировать держателя карты, 3DSS генерирует CReq и предоставляет его в виде HTML платежному шлюзу. Сам Challenge находится вне поля зрения 3DSS. Но его результат 3DSS получает из RReq, полученного от DS.

Также результат операции может быть получен в CRes (final), переданном в 3DSS посредством соответствующего API из браузера или платёжного шлюза. В этом случае оба значения статуса операции обрабатываются 3DSS, а финальный результат платежа предоставляется платежному шлюзу.

Условия использования

Аппаратные требования

- минимум: 4 ядра процессора i3, 8 ГБ ОЗУ, 50 ГБ жесткого диска
- средний: 4–8 процессорных ядер i5, 8–16 ГБ ОЗУ, 50–100 ГБ HDD/SSD
- максимум: 8 процессорных ядер i7, 16 ГБ ОЗУ, 100 ГБ SSD

Среда

Для установки требуется только Java 11-ой версии.

База данных

Для базы данных необходима единственная пустая схема, все необходимые объекты создаются Flywaydb в процессе установки.

Поддерживаются следующие версии баз данных:

- PostgreSQL 9.6+

Система

sb3DSS поставляется как автономное приложение, которое не занимает много ресурсов и не требует отдельного сервера приложений.