SmartBanking

Инструкция по установке 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 содержимого 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 проверяет, доступна ли аутентификация для 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.
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 Request Message	AReq	Сообщение EMV 3-D Secure, отправленное 3DS Server через DS на ACS для инициирования процесса аутентификации.
Authentication Response Message	ARes	Сообщение EMV 3-D Secure, возвращаемое ACS через DS в ответ на сообщение запроса аутентификации.

Authentication Value	AV	Криптографическое значение, генерируемое ACS для того, чтобы во время обработки авторизации система могла подтвердить полноту результата аутентификации. AV Алгоритм определяется каждой Платёжной системой.
Cardholder		Физическое лицо, которому выдана карта или которое имеет право ее использовать.
Challenge		Процесс, в котором ACS взаимодействует с 3DS Client, для получения дополнительной информации через взаимодействие с держателем карты.
Challenge Request Message	CReq	Сообщение EMV 3-D Secure, отправляемое 3DS SDK или 3DS Server, в котором дополнительная информация передается от держателя карты в ACS для поддержки процесса аутентификации.
Challenge Response Message	CRes	Ответ ACS на сообщение CReq. Он может указывать на результат аутентификации держателя карты или, в случае модели App-based, также указывать на то, что для завершения аутентификации требуется дальнейшее взаимодействие с держателем карты.
Device Channel		Указывает канал, из которого поступила транзакция. Например: • App-based (01-APP) • Browser-based (02-BRW) • 3DS Requestor Initiated (03-3RI)
Payment System	PS IPS	Платежная система, определяющая правила и условия работы, а также требования к выпуску карты и приему торговцами.
Message Category		Указывает тип сообщения EMV 3-D Secure. Например: • Payment (01-PA) • Non-Payment (02-NPA)
Non-Payment Authentication	NPA	
Preparation Request Message	PReq	Сообщение 3-D Secure, отправляемое с 3DS Server на DS для запроса версии (версий) протокола ACS и DS, соответствующих диапазонам карты DS, а также дополнительного 3DS Method

		URL для обновления информации внутреннего хранилища сервера 3DS.
Preparation Response Message	PRes	Ответ на сообщение PReq, содержащий диапазоны карт DS, версии активного протокола для ACS и DS и 3DS Method URL, для обновления внутреннего хранилища 3DS Server.
Results Request Message	RReq	Сообщение, отправляемое ACS через DS для передачи результатов аутентификации держателя карты на сервер 3DS.
Results Response Message	RRes	Сообщение, отправленное 3DS Server в ACS через DS для подтверждения получения сообщения RReq.

Описание продукта

sb3DSS — это программное решение для эквайеров, которым необходимо использовать 3D-Secure аутентификацию держателей карточек для транзакций в сети Интернет, в соответствии с протоколом EMV 3D Secure 2.x.x.

Решение поддерживает регистрацию карт, аутентификацию транзакционных запросов и оповещение владельцев карт.

sb3DSS отвечает за:

- сбор необходимых данных для 3-D Secure сообщения;
- аутентификацию DS;
- валидацию DS, 3DS SDK и 3DS Requestor;
- обеспечение защиты содержимого сообщения.

Сертификаты

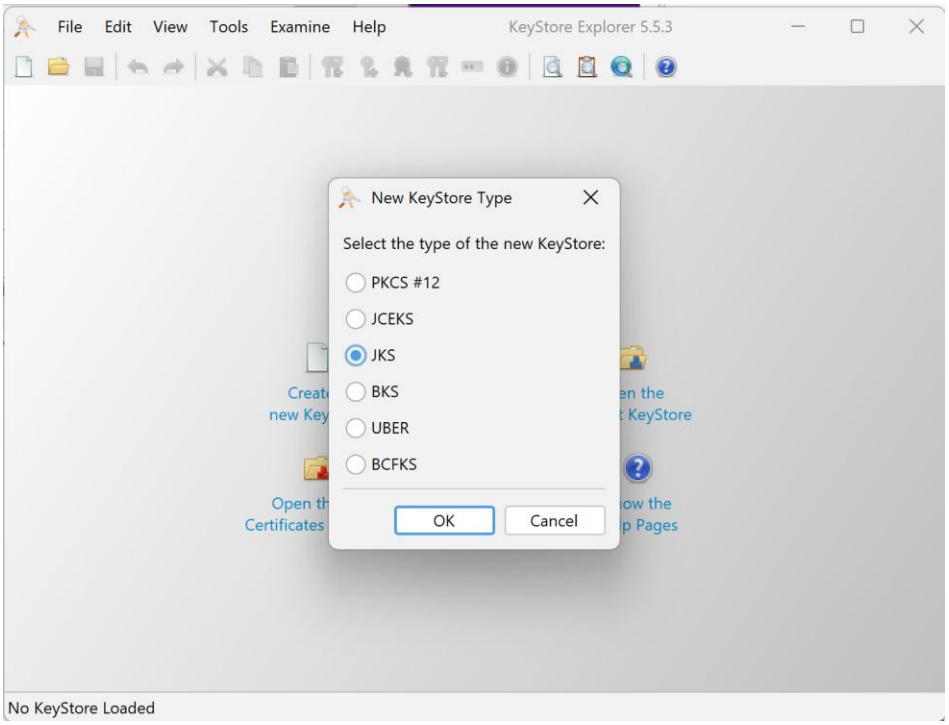
Для работы с 3DSS необходимо подготовить следующие сертификаты:

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

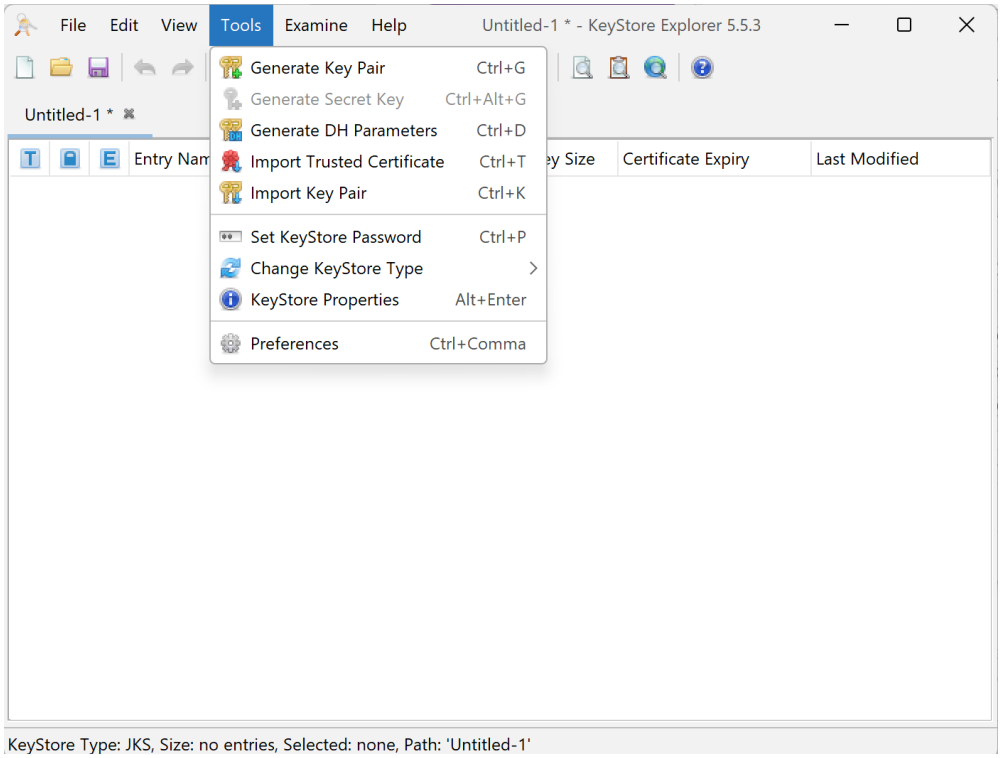
На данный момент sb3DSS поддерживает только один формат хранилища ключей — JKS.

В качестве бесплатного инструмента для работы с ключами и сертификатами мы используем KeyStore Explorer.

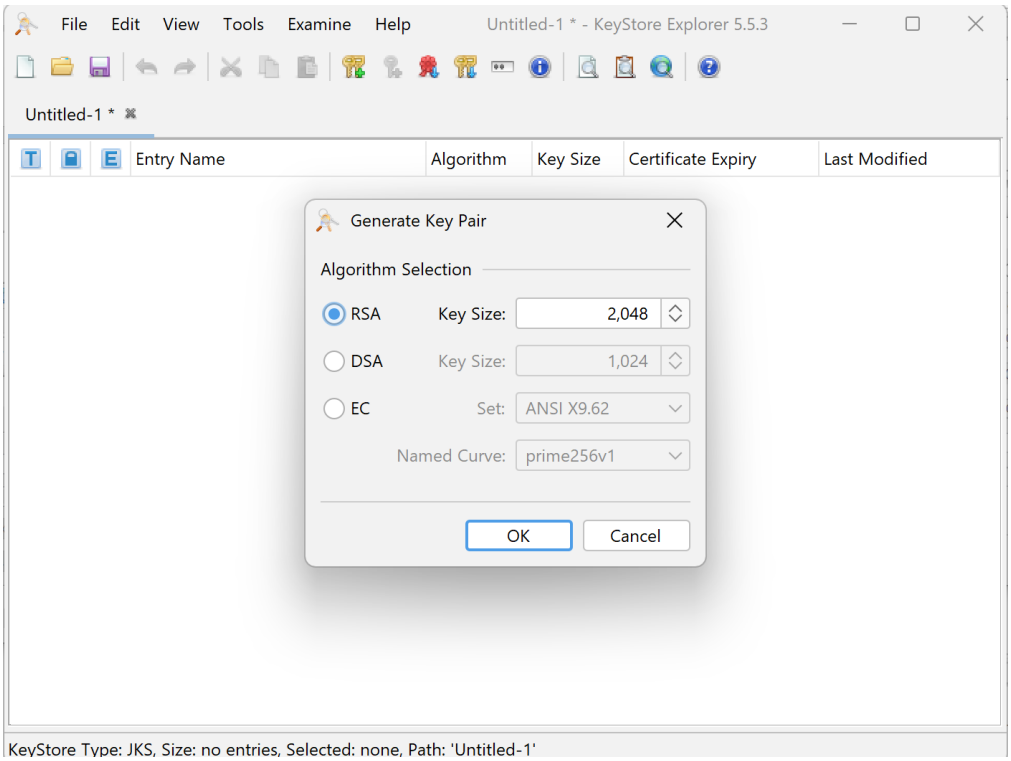
1. Для создания JKS в KeyStore Explorer нажмите кнопку «*Create a new KeyStore*», в открывшемся окне нужно выбрать «*JKS*».



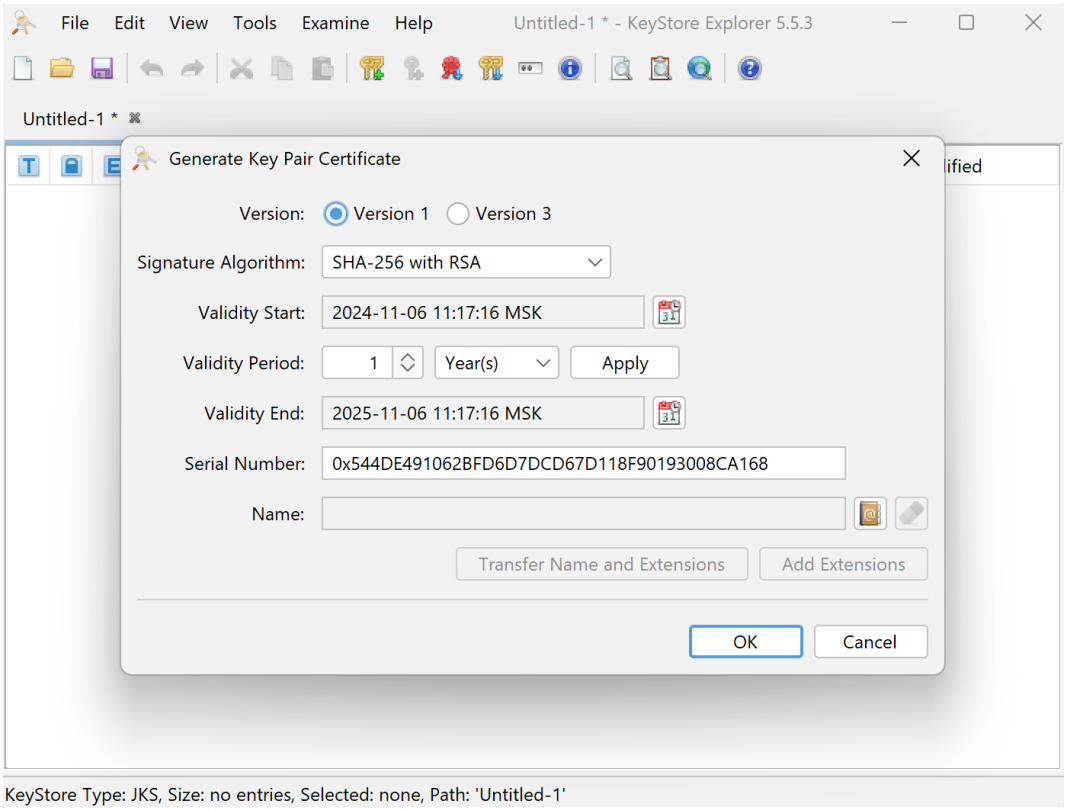
2. На следующем этапе нужно создать ключевую пару. Для этого необходимо перейти в пункт меню «*Tools*» и «*Generate Key Pair*»



3. Затем в открывшемся окне выбираем алгоритм шифрования, в соответствии с требованиями, например, платёжных систем. Как правило, используется RSA с Key Size минимум 2048 bit. Выбираем, нажимаем «*OK*»:



4. Следующим шагом нам необходимо создать запрос на выпуск сертификата (csr-файл). Для этого в открывшемся окне выбираем Version 1 / Version 3, Signature Algorithm по умолчанию SHA-256 with RSA и нажимаем на возле поля «*Name*»:

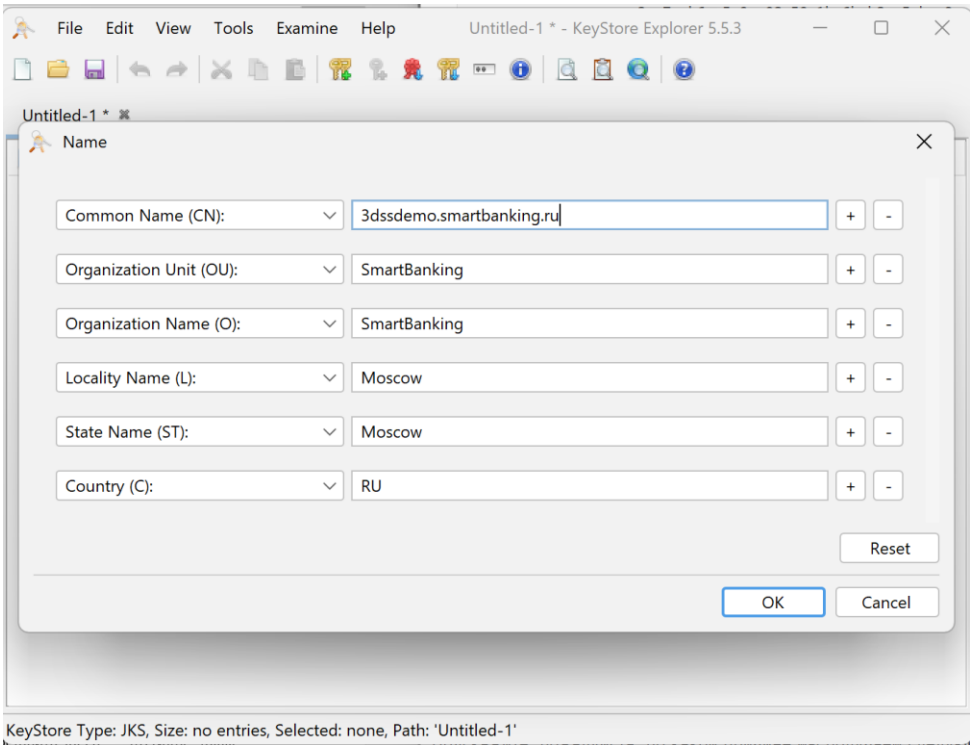


Автоматически будет проставлен срок действия сертификата в 1 год. При необходимости можно указать другой срок.

Серийный номер будет сформирован автоматически.

5. В открывшемся окне необходимо заполнить все поля для запроса на выпуск сертификата (csr).

Например, выглядеть это может следующим образом:

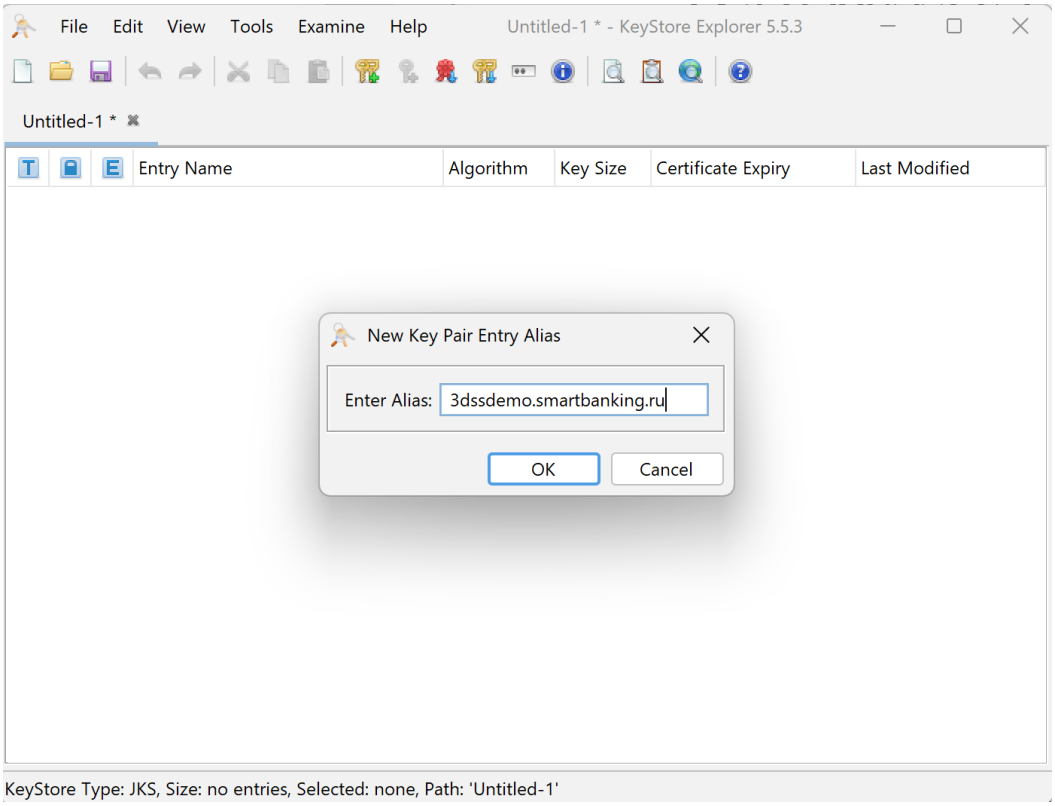


У разных Платёжных систем есть свои требования по заполнению полей при генерации csr-запросов на выпуск сертификатов.

В связи с этим, если запрос сертификата не требует указания дополнительных расширений (Extensions) – можно использовать Version 1.

Если запрос сертификата требует указания дополнительных расширений (Extensions) – используйте Version 3, предварительно перейдя в секцию для ввода данных по расширению – Add Extension.

6. Теперь для создаваемой ключевой пары необходимо задать Alias (он же - Entry Name). Задаём, нажимаем «*OK*»:

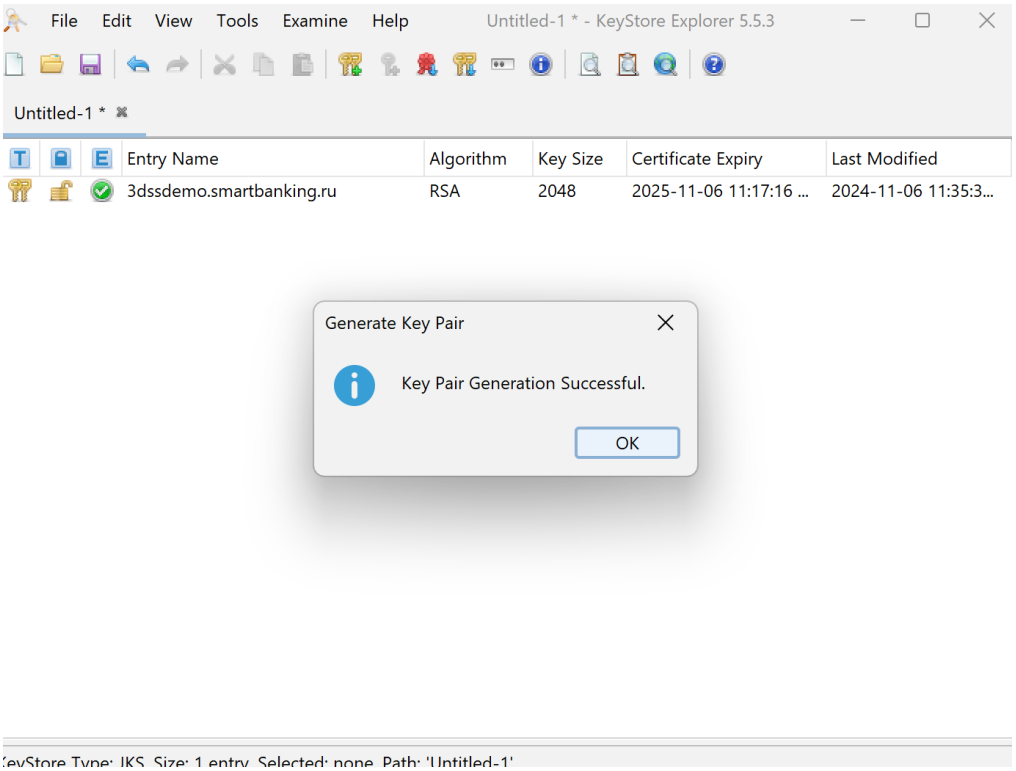


Именно этот алиас будет использоваться в конфигурационном файле sb3DSS.

7. Далее необходимо задать пароль для создаваемого JKS. Задаём пароль, повторяем его, нажимаем «*OK*».

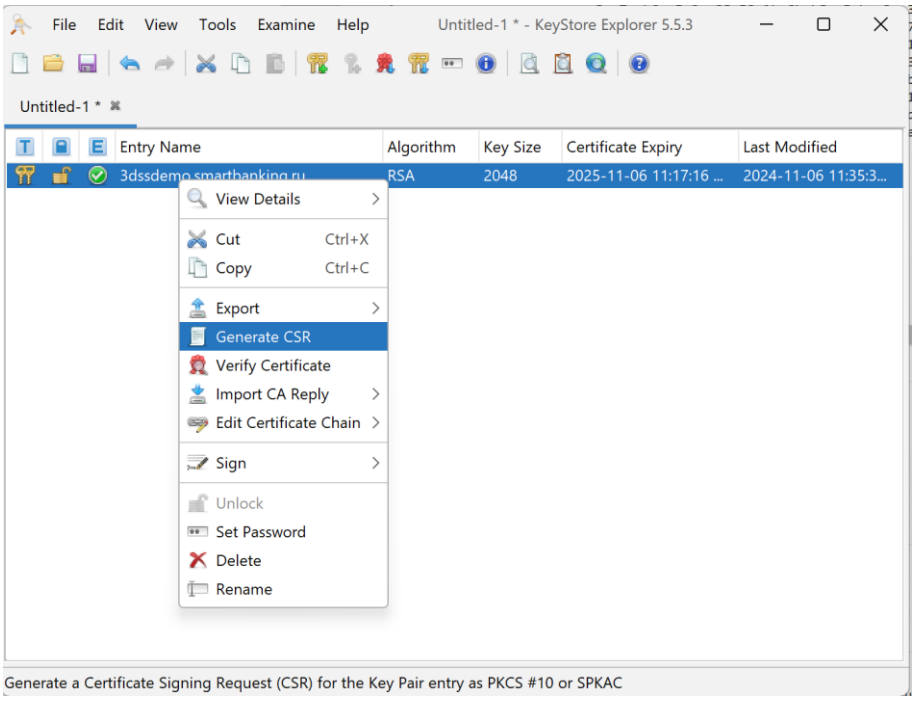
Заданный пароль необходимо обязательно сохранить, так как он в последующем будет использоваться для импорта в JKS полученного от платёжной системы сертификата, а также при загрузке в последующем JKS с клиентским сертификатом в конфигурацию sb3DSS.

8. Видим сообщение о том, что ключевая пара успешно сгенерирована, нажимаем «*OK*»:



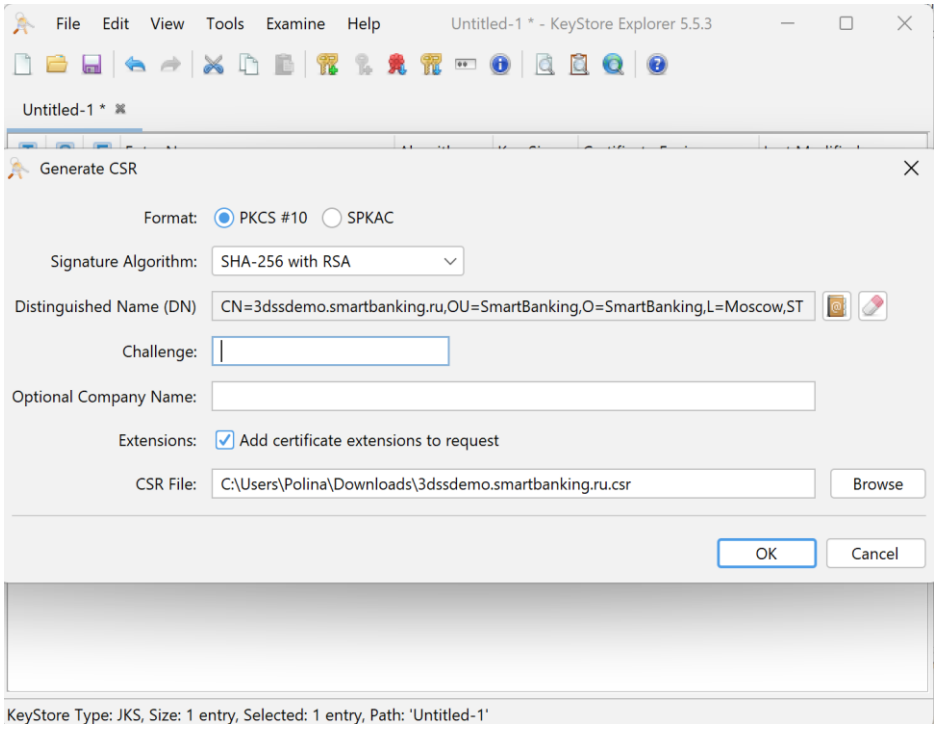
9. Следующим этапом будет генерация csr-запроса на выпуск сертификата, который в последующем будет отправляться в платёжную систему.

Для этого правой кнопкой мыши нажимаем на созданную ключевую пару и в открывшемся меню выбираем «*Generate CSR*»:

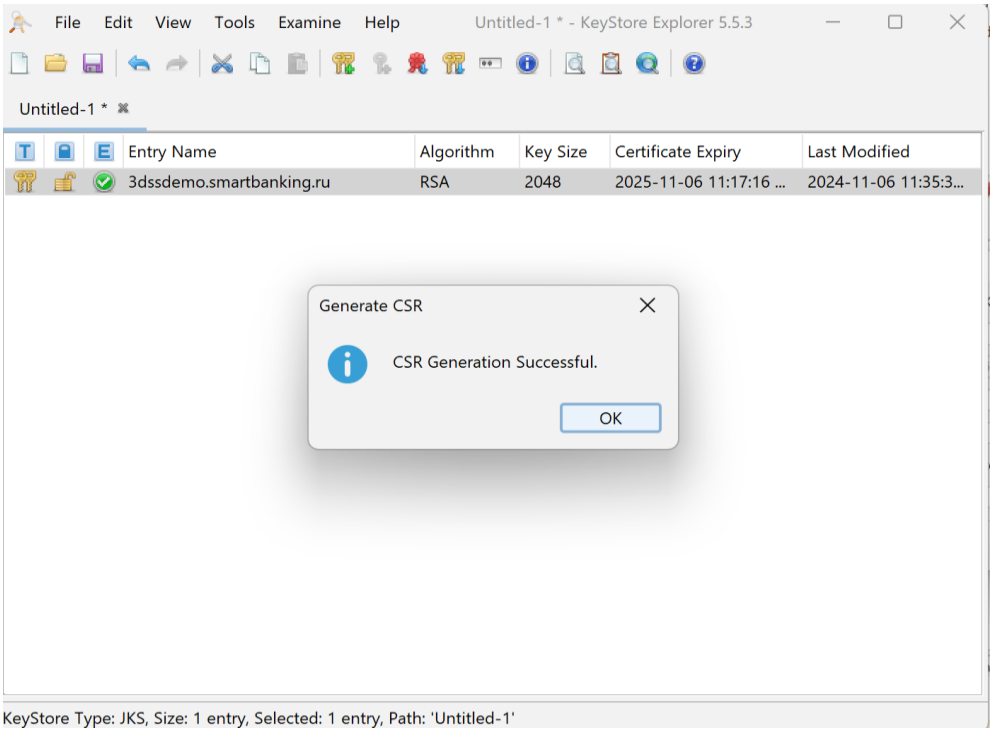


10. Для формирования запроса на подпись сертификата (csr-файла) необходимо:

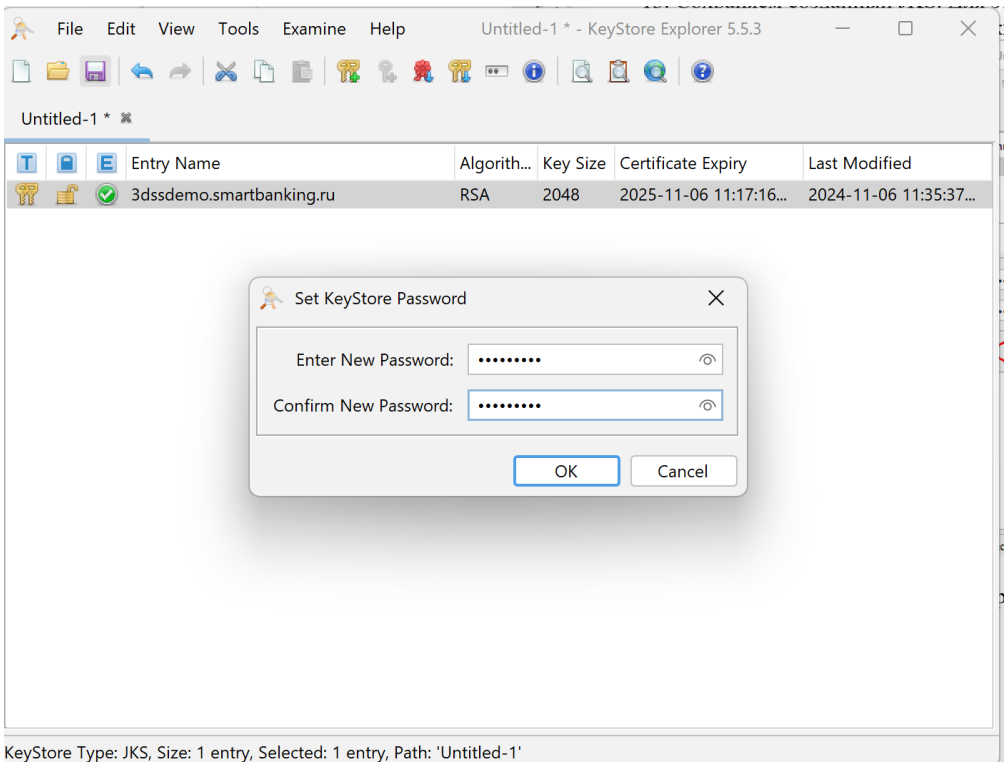
- выбрать формат PKCS#10, который соответствует требованиям конкретной Платёжной системы;
- выбрать алгоритм подписи или оставить его по умолчанию;
- исправить данные имени, если необходимо;
- расширения можно не задавать, если это не требуется, согласно документации Платёжной системы;
- указать путь сохранения файла CSR.



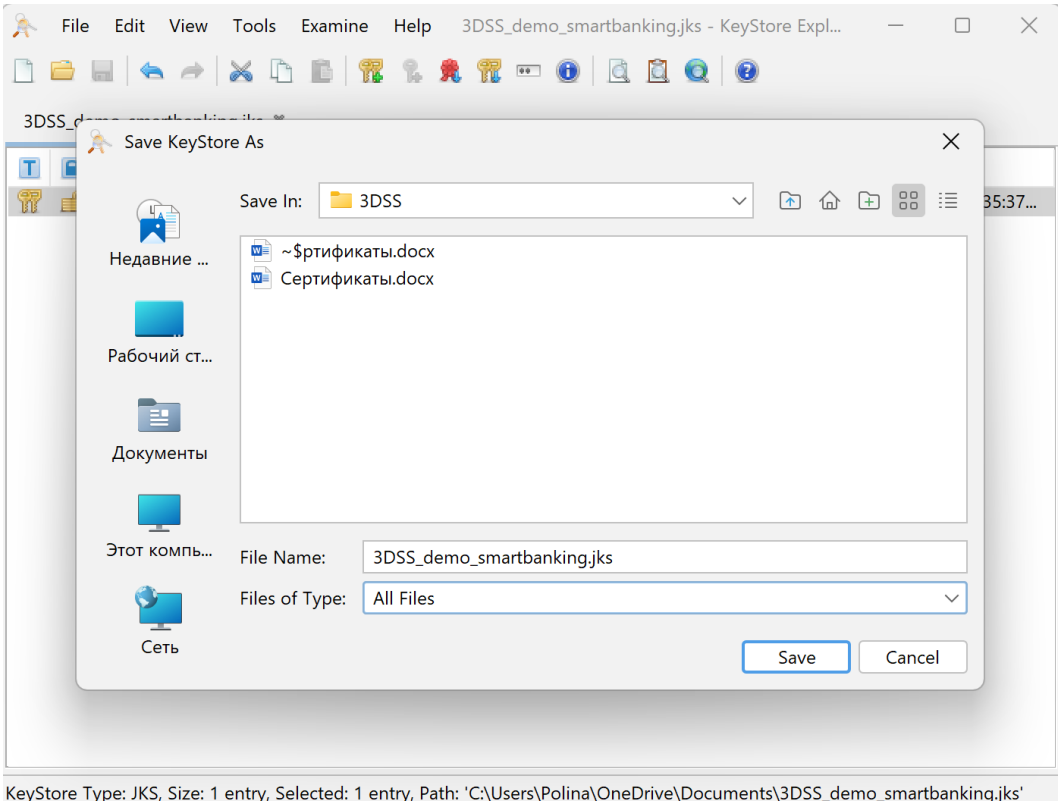
Получаем сообщение об успешной генерации csr-запроса, нажимаем «*OK*»:



11. Сохраняем созданный JKS. Для этого нажимаем на кнопку , вводим заданный ранее пароль, повторяем его, нажимаем «*OK*»:



Выбираем директорию, куда сохраняем JKS, задаём ему имя, обязательно указываем расширение .jks и нажимаем «*Save*»:

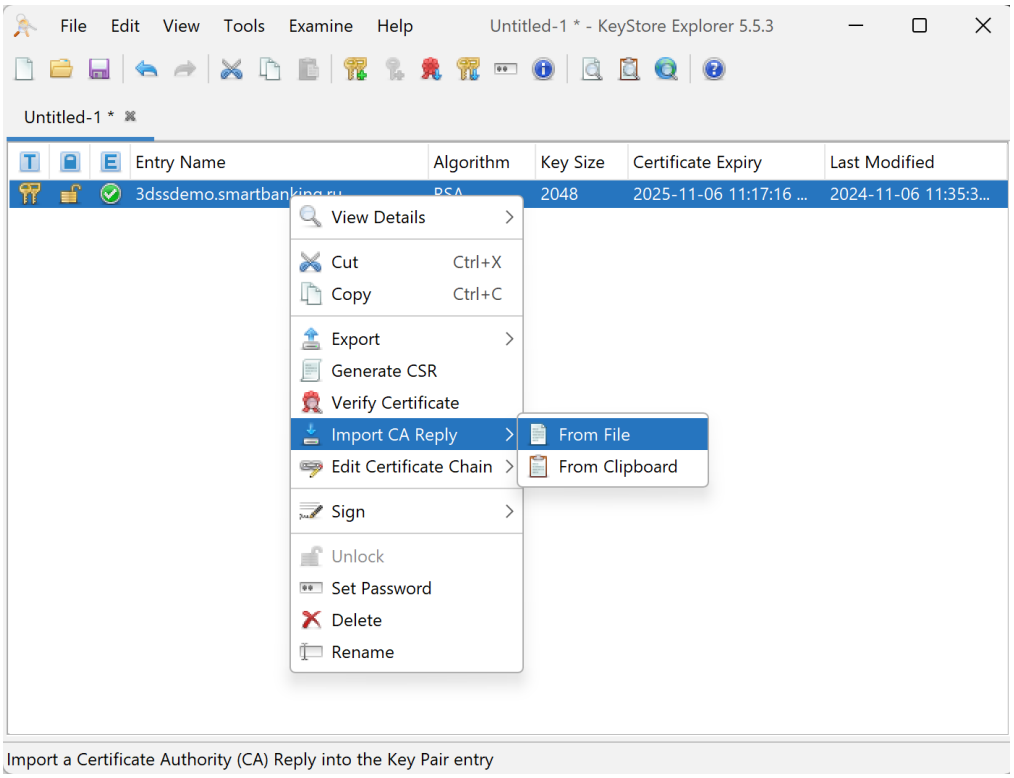


12. Все запросы на выпуск сертификатов должны быть отправлены в соответствующий центр сертификации Платёжной системы для обработки.

13. При получении сертификата от Платёжной системы необходимо его импортировать в созданный ранее JKS.

По умолчанию все сертификаты будут возвращены в форматах Privacy Enhanced Mail (PEM), PKCS#7 или Distinguished Encoding Rules (DER).

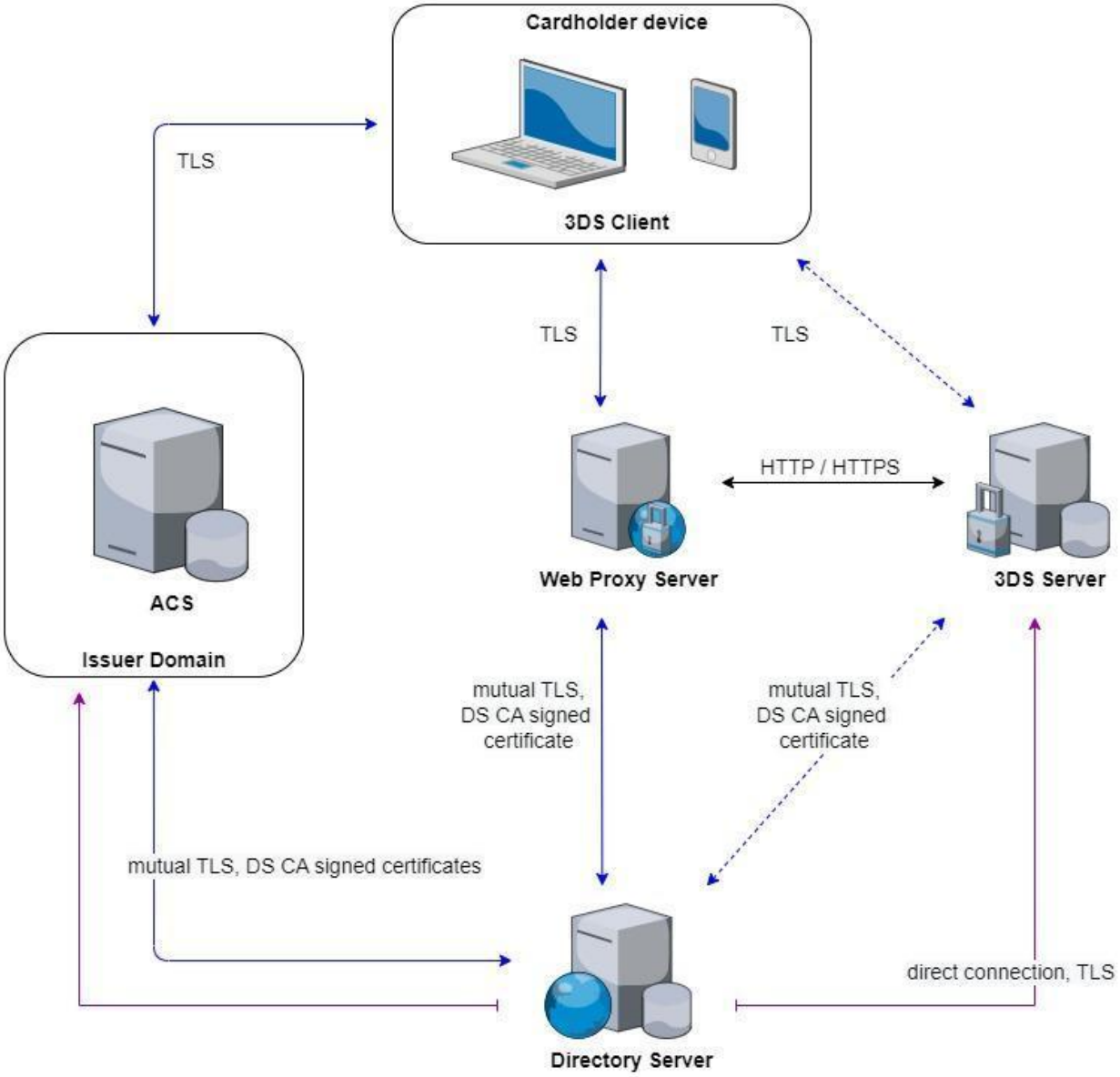
Для этого открываем сам JKS, который сохраняли в п.11, правой кнопкой мыши нажимаем на ключевую пару, в открывшемся меню выбираем «*Import CA Reply*» → «*From file*»:



Готово! Поздравляем, вы успешно загрузили сертификат и готовы к работе.

Инфраструктура

Взаимодействие между sb3DSS и другими объектами инфраструктуры 3D-Secure показано на рисунке ниже.



TLS-соединение может быть установлено через обратный прокси-сервер или напрямую к 3DSS. Это зависит от инфраструктурной реализации.

TLS-соединения

Связь между DS и sb3DSS для обмена сообщениями устанавливается с использованием протокола TLS с взаимной аутентификацией. Сертификаты открытых ключей обеих сторон подписываются DS CA. Сертификаты для безопасного соединения с DS и браузера держателя карты могут храниться на веб-прокси-сервере. Эти сертификаты настраиваются независимо от sb3DSS.

Устройство держателя карты — 3DS Requestor

При взаимодействии держателя карты с 3DS Requestor, в соответствии с протоколом EMV 3D-Secure 2.x, ссылки должны быть защищены. Это зависит от конкретного 3DS Requestor, и предполагается, что он соответствует требованиям безопасности Платёжной системы, по крайней мере, по протоколу TLS с аутентификацией 3DS Requestor (сервера) приложением 3DS Requestor или браузером.

Если 3DS Requestor и 3DS Server являются отдельными компонентами, данные, передаваемые между компонентами, должны быть защищены на уровне, удовлетворяющем требованиям безопасности Платёжной системы с взаимной аутентификацией обоих серверов.

3DS Server — DS

Связь 3DS Server с DS для сообщений AReq/ARes устанавливается с использованием протокола TLS с взаимной аутентификацией. Сертификаты открытых ключей обеих сторон подписываются DS CA, при этом 3DS Server делает необходимый выбор, если он подключается к более чем одному DS.

Связь DS с 3DS Server для сообщений RReq/RRes устанавливается с использованием протокола TLS с взаимной аутентификацией. Сертификаты открытых ключей обеих сторон подписываются DS CA.

3DSS – ACS

Возможно связать 3DS Server с ACS напрямую. Когда Эмитент и Эквайер разместили свои 3DS -модули в одном месте и нет необходимости посещать DS Платёжной системы, то для установки такого соединения необходимо настроить соответствующие параметры.

sb3DSS URLs

Для правильной работы 3DSS должны быть доступны следующие URL-адреса.

Метод	URL	Взаимодействие с
POST	/api/3dsmethod	Payment Gateway Browser
GET	/api/browserinfo/[threeDSServerTransID]	Browser
POST	/3dsmethod/collect	Browser
POST	/3dsmethod/handle-acs-notification	ACS
POST	/api/pArq	Payment Gateway
GET	/api/challenge/[threeDSServerTransID]	Payment Gateway
POST	/rreq	DS
POST	/api/cresponse	Payment Gateway Browser ACS

sb3DSS API

Описание полного набора параметров, связанных с передачей данных между системами в рамках интеграции с sb3DSS представлено в документе «API 3DSS».

Установка

Для работы программы необходимо предварительно установить Java 11

Для запуска sb3DSS на этапе установки необходимо:

выполнить команду:

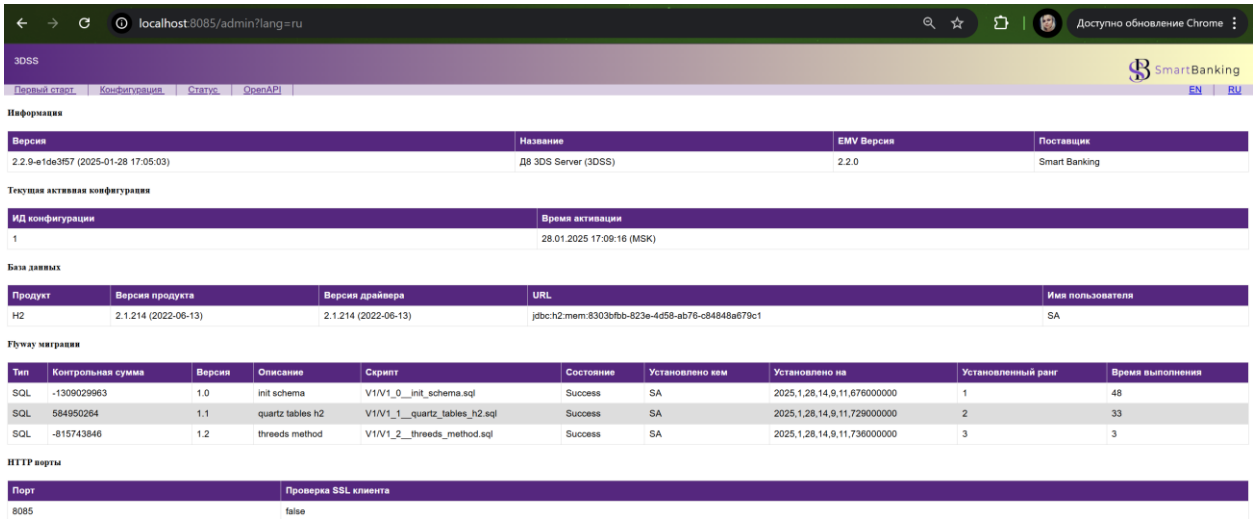
java -jar <наименование jar-файла>.jar --server.port=<порт>

Пример команды: java -jar sb3dss-2.2.9-6da2ed00.jar --server.port=8085

В команде можно указать свободный порт, который будет использоваться для sb3DSS. По умолчанию sb3DSS будет работать на порту 8080, и этот параметр можно опустить.

Чтобы открыть консоль администратора приложения sb3DSS нужно перейти в браузер и в адресной строке ввести http://host:port/admin

Например: http://localhost:8085/admin



Далее следуйте по документу «Инструкция по тестированию функционала sb3DSS».