SmartBanking

Инструкция по установке SmartBanking Access Control Server (sbACS)

Москва, 2024

Отказ от ответственности

Здесь и далее, название АЦС, как и другие англицизмы, продиктованы исключительно общепринятой терминологией в данной бизнес-области и употребляются для упрощения понимания функционала и спецификации EMV.

АЦС является транслитерацией от акронима ACS на английском языке. Которая, в свою очередь, означает Access Control Server. На русском языке данное название имеет перевод как Сервер Контроля Доступа (СКД). По всем дальнейшим сокращениям и терминологии необходимо обращаться к разделу Акронимы и Терминология.

Кратко о Продукте

Access Control Server компании Smart Banking предназначен для эмитентов, участвующих в программах 3-D Secure международных платежных сетей.

Решение поддерживает регистрацию карт, аутентификацию запросов на совершение операций и уведомление владельцев карт.

sbACS представляет собой систему с несколькими эмитентами и позволяет банкам-эмитентам настраивать каждый параметр для конкретного индивидуального профиля.

Он поддерживает аутентификацию на основе риска (RBA), которая помогает эмитенту сократить число случаев отмены транзакций, внешнюю аутентификацию (OOB), которая повышает удобство работы пользователей и делает платежи удобными, а также множество стандартных и настраиваемых методов аутентификации, таких как OTP (любой канал доставки, как смс, электронная почта, push) и многое другое.

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 инфраструктурой MirAccept, 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, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».
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.

Описание Продукта

sbACS — это программное решение для эмитентов платежных карт, позволяющее безопасно аутентифицировать транзакции без предъявления карты (CNP) через Интернет.

Решение поддерживает регистрацию карт, аутентификацию запросов на оплату и уведомление владельцев карт.

Сертификаты

Поскольку у нас есть много шифрования, такого как TLS и подписанный контент, нам необходимо понять, какой сертификат используется для какого шифрования.

Согласно документации Платёжных систем, для ACS необходимо подготовить следующие сертификаты:

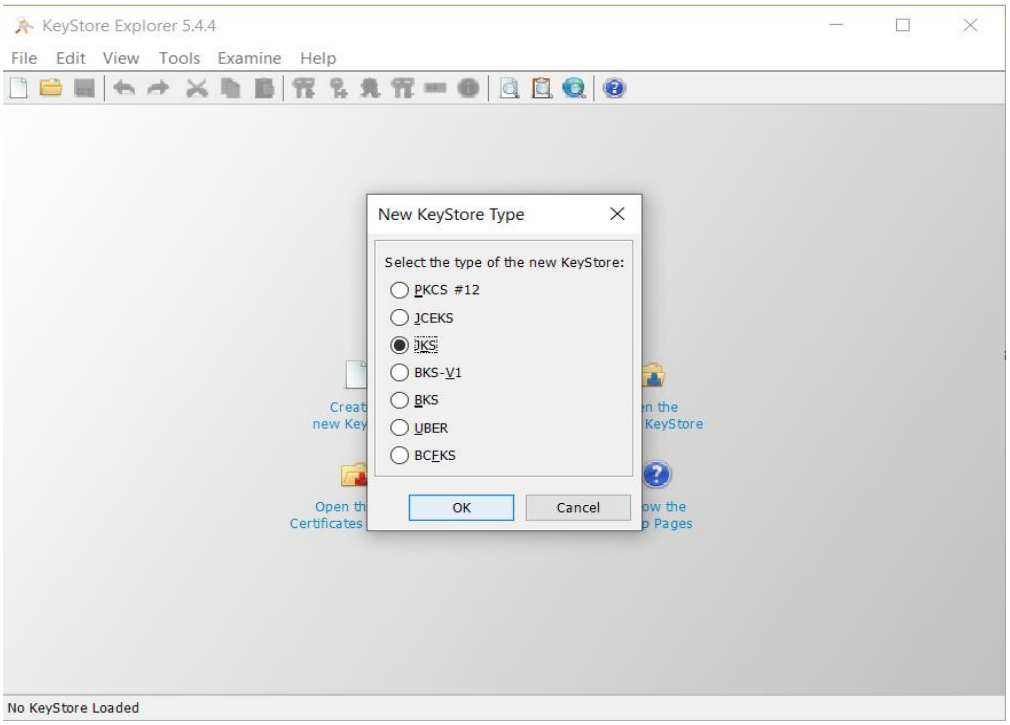
- Сертификат сервера TLS для связи между DS и ACS.
- Сертификат клиента TLS для связи между ACS и DS.
- Сертификат цифровой подписи ACS для подписи контента, подписанного ACS.

Давайте разберемся, что, где и как.

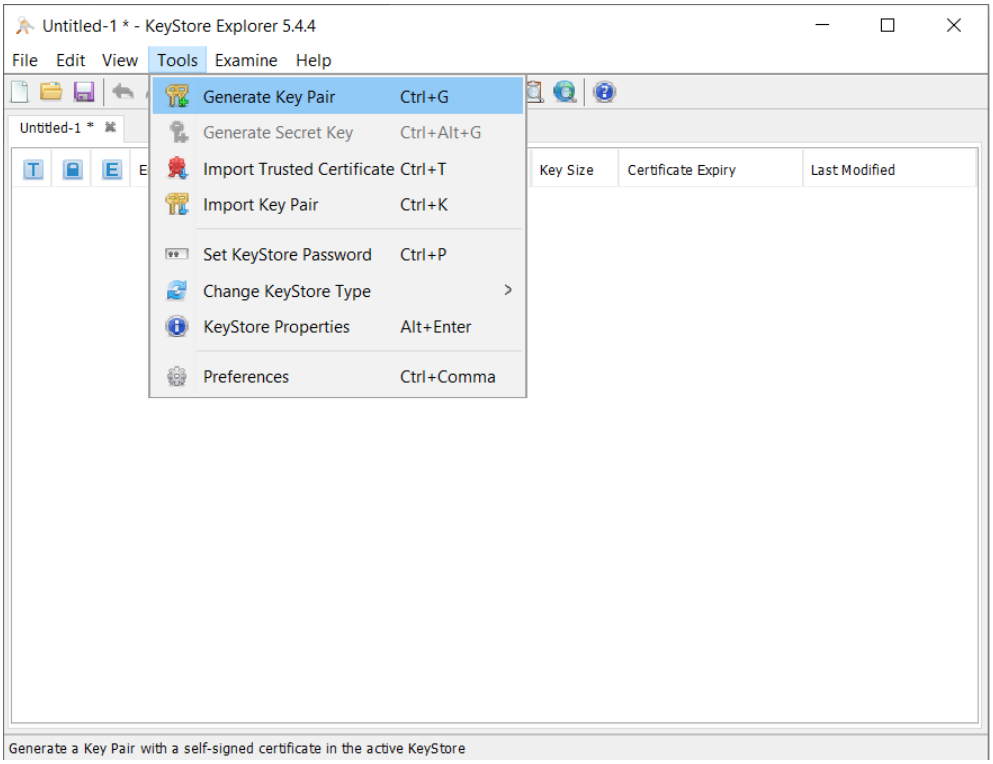
На данный момент sbACS поддерживает только один формат хранилища ключей — JKS.

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

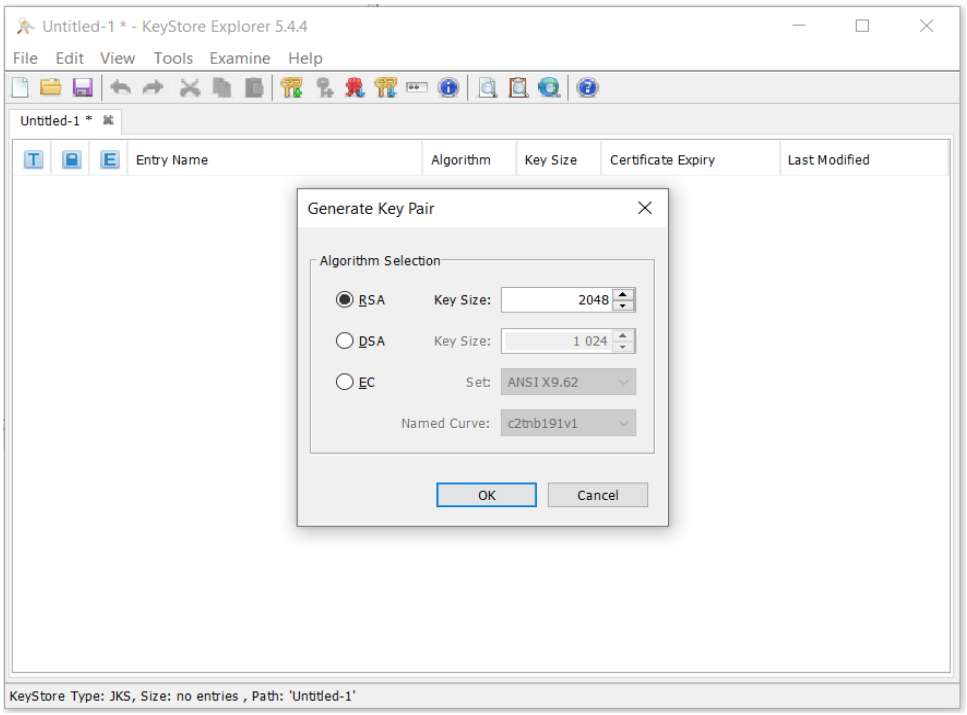
Итак, в KeyStore Explorer нажмите кнопку JKS, чтобы создать соответствующий объект.



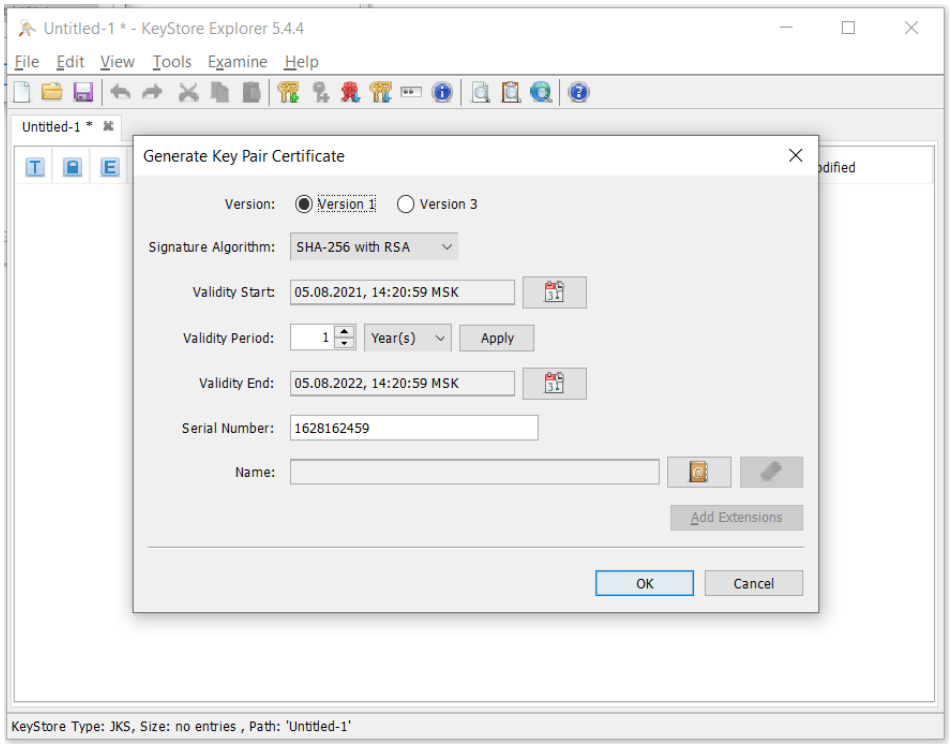
Следующим шагом будет создание пары ключей.



Согласно документам Платёжных Систем, для 3DS2 используется криптографический алгоритм RSA с минимальным размером ключа 2048 бит.



На следующем шаге потребуются данные, необходимые для запроса сертификата.



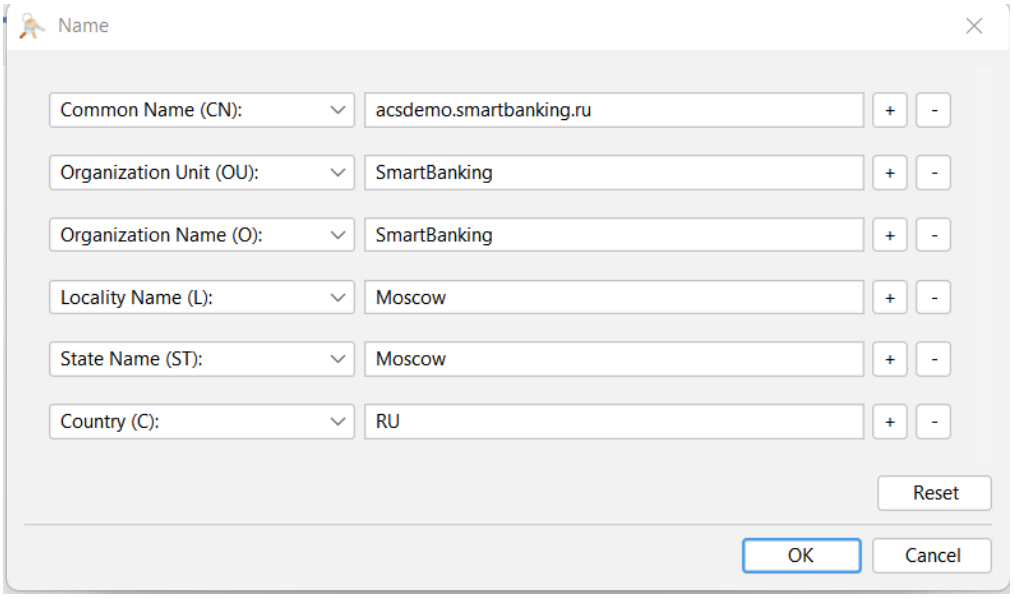
Поскольку нам не нужны расширения для сертификатов, достаточно выбрать Версию 1.

Алгоритм подписи по умолчанию установлен на SHA-256, это приемлемо для нашего примера, поэтому сохраните его.

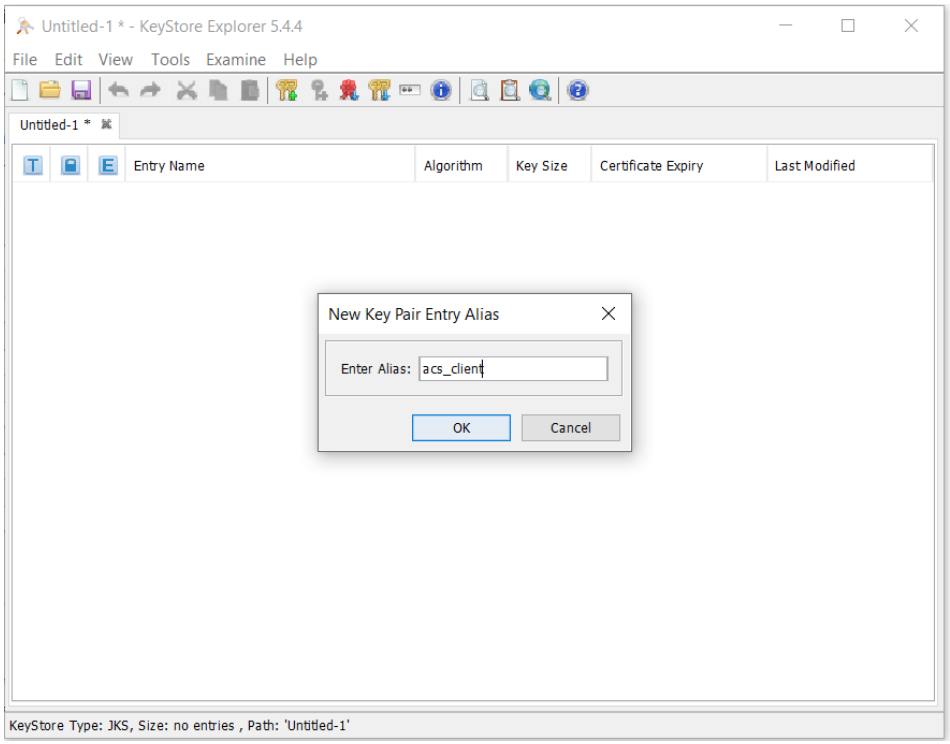
Кроме того, вы можете не изменять срок действия, который по умолчанию составляет 1 год.

Серийный номер будет указан по умолчанию, давайте его тоже сохраним.

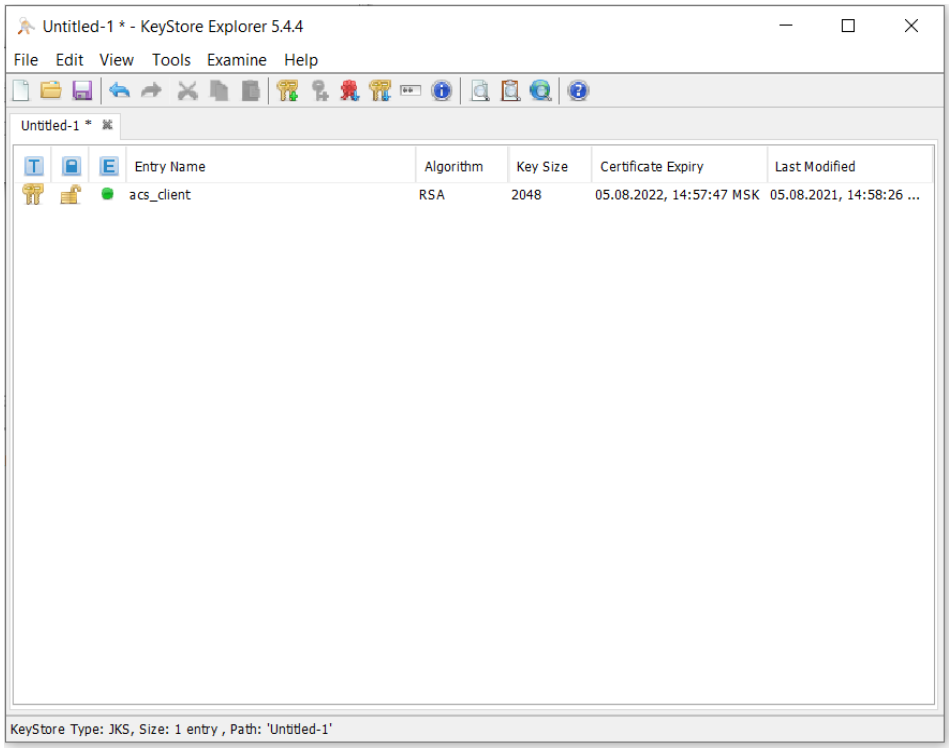
Итак, единственные данные, которые мы должны предоставить здесь, — это Name, также известное как Subject сертификатов:

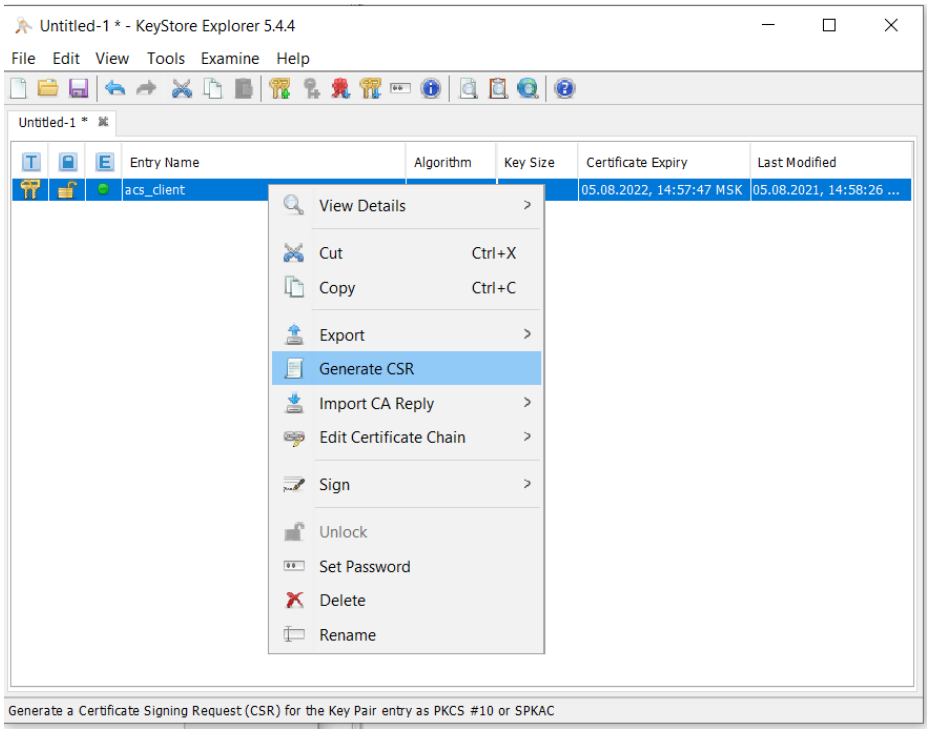


Введите псевдоним для конкретной пары ключей и пароль, если требуется.



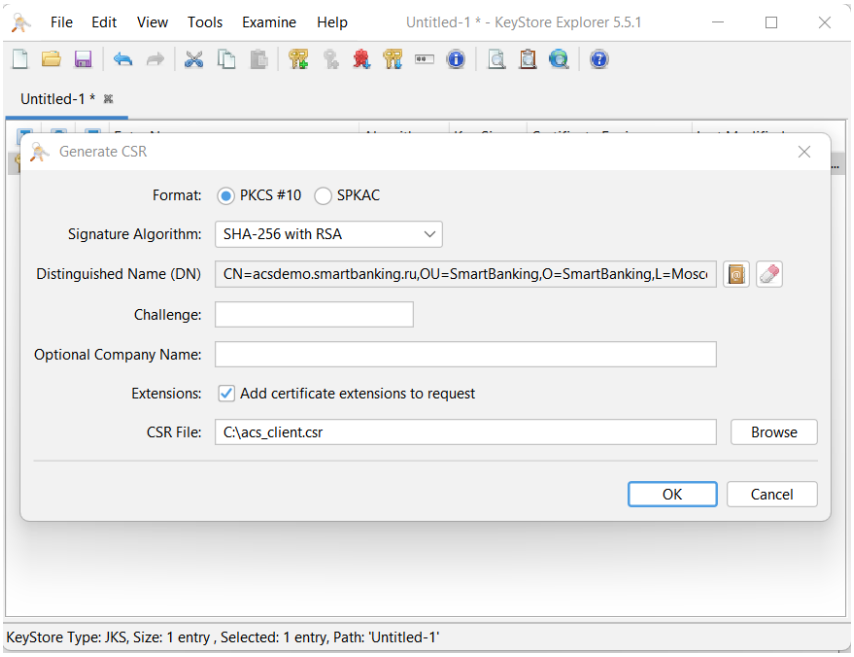
Итак, мы создали ключевую пару (и сертификат), назвали ее псевдонимом и готовы генерировать CSR.



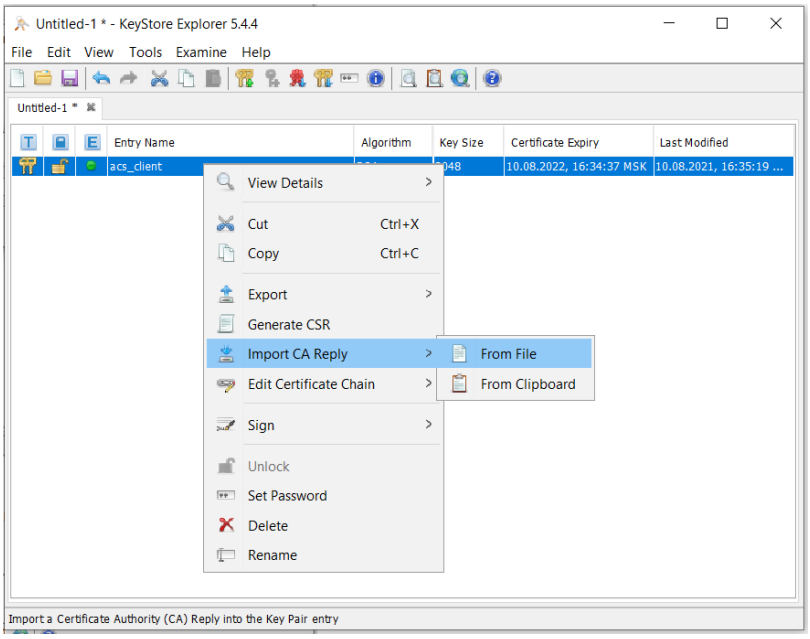


Для формирования запроса на подпись сертификата необходимо:

- выберите формат PKCS#10, который соответствует требованиям Платёжных сетей
- выберите алгоритм подписи или оставьте его по умолчанию
- исправьте данные имени, если необходимо
- расширения можно не задавать
- и укажите путь к файлу CSR



Все запросы на сертификаты должны быть отправлены в соответствующий центр сертификации платежной системы для обработки.

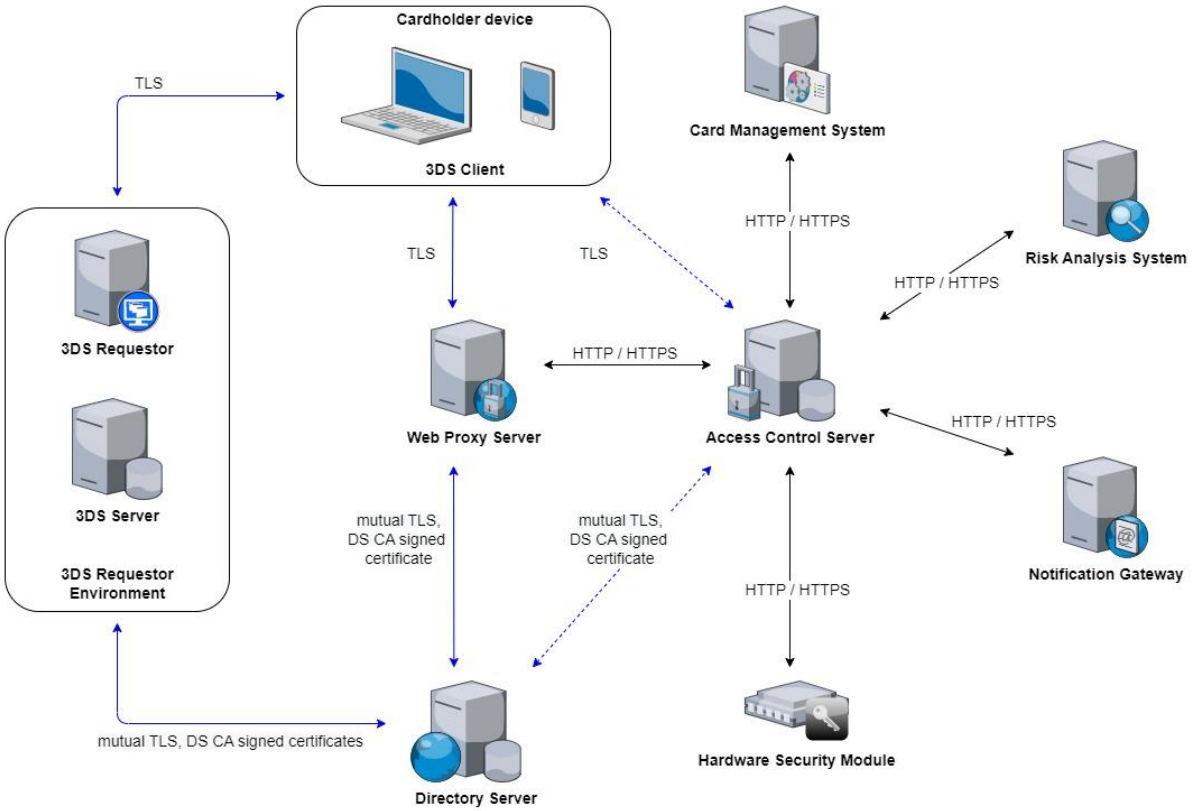


По умолчанию все сертификаты будут возвращены в форматах Privacy Enhanced Mail (PEM), PKCS#7 и Distinguished Encoding Rules (DER).

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

Инфраструктура

Взаимодействие ACS с другими объектами инфраструктуры 3-D Secure изображено на рисунке ниже.



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

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

Для протоколов 3DS2 прямая связь между браузером или 3DS SDK и ACS устанавливается только в том случае, если транзакция требует вызова.

Вызов инициируется:

- браузером из iframe, предоставленного в ARes
- с помощью SDK, используя URL-адрес, указанный в ARes

Соединение устанавливается с использованием протокола TLS с аутентификацией ACS (сервера) браузером (или 3DS SDK). Сертификат открытого ключа ACS подписывается коммерческим центром сертификации.

Данные запроса и ответа владельца карты шифруются и обрабатываются с использованием сессионных ключей, ранее установленных между ACS и 3DS SDK. Используя данные, передаваемые в сообщениях AReq/ARes, 3DS SDK и ACS выполняют протокол обмена ключами DiffieHellman для создания ключей для безопасного канала, которые позже будут использоваться для защиты сообщений CReq/CRes в потоке Challenge.

3DS Метод

Связь между Браузером и ACS для 3DS Метода открывается из скрытого iframe, загружаемого Сервером 3DS как часть страницы оформления заказа. Он используется ACS для загрузки JavaScript, который собирает информацию об устройстве и возвращает ее в ACS. Сюда входит идентификатор транзакции сервера 3DS, который позволяет ACS сопоставить информацию с правильной транзакцией.

URL-адрес ACS, используемый для метода 3DS, рассматривается как URL-адрес, который отличается от URL-адреса ACS для потока вызова, и для 3DS Метода и для любого потока вызова будут установлены отдельные ссылки TLS.

Соединение устанавливается по протоколу TLS с аутентификацией сервера ACS браузером. Сертификат открытого ключа ACS подписывается коммерческим центром сертификации.

URL-адреса ACS

Для правильной работы ACS должны быть доступны следующие URL-адреса.

/auth

Этот URL-адрес описывает основной сервис, принимающий AReq. При этом он должен быть доступен для подключения к ДС и защищен сертификатом (Серверным), подписанным Платежной системой.

Соединение от DS к ACS (AReq) должно быть защищено серверным сертификатом. В то время как обратное направление (RReq) защищено клиентским сертификатом.

/challenge

URL-адрес для взаимодействия с держателем карты. Поскольку эти действия выполняются через браузер или мобильный SDK, сертификаты, необходимые для установки защищенного соединения, должны быть подписаны центром сертификации, доступным для Интернет-пользователей.

Обратите внимание, что можно настроить URL-адреса запроса отдельно для каждого конкретного случая, например потока на основе приложения или браузера:

- /challenge/app
- /challenge/browser
- /challenge/browser/data (этот URL-адрес описывает конечную точку, куда будет отправлена форма с OTP)

/3dsmethod

URL-адрес функциональности 3DS Метода, позволяющий ACS собирать дополнительную информацию о браузере до получения сообщения AReq, чтобы облегчить оценку риска транзакции. Использование 3DS Метода системой ACS не является обязательным.

Сертификаты должны быть подписаны центром сертификации, доступным для потребителей Интернета.

Существует дополнительный URL-адрес, который эмитент должен применить, если поддерживается функциональность метода 3DS — **/3dsmethod/collect**.

Установка

Автономный вариант

Для работы программы необходимо предварительно установить Java 11

Для запуска ACS на этапе инициализации необходимо выполнить следующую команду:

```
java -jar sbacs.jar --server.port=<порт>
```

Здесь вы можете настроить порт, который будет использоваться для ACS. По умолчанию ACS будет работать на порту 8080, и этот параметр можно опустить.

Затем откройте Консоль администратора в браузере.

```
http:// host:port/admin
```

Следуйте инструкциям по тестированию приложения.

В контейнере

Чтобы запустить ACS в качестве образа Docker, вам необходимо выполнить следующие команды:
Вход в Docker

```
docker login registry.smartbanking.ru:5050
```

Затем вам понадобится docker-compose.yml, где настроен образ ACS.
Пример такого файла размещен ниже:

```
version : "3.9"

services :
 acs :
```

```
  privileged : true
  image : registry.smartbanking.ru:5050/ecom/acs/acs:latest
  ports :
   - "8080:8080"
  environment :
   - JVM_OPTS=-Xmx150m -Xms150m
   - SPRING_BOOT_APPLICATION_ARGS=>
     --logging.file.name=/opt/app/logs/acs.log
     --logging.logback.rollingpolicy.file-name-
pattern=/opt/app/logs/acs.log.%d{yyyy-MM-dd}.%i.gz
     --logging.logback.rollingpolicy.max-file-size=30MB
  restart : always
  deploy :
   resources :
    limits :
     memory : 500M
  networks :
   - acsNetwork
  logging :
   driver : "json-file"
   options :
    max-file : "20"
    max-size : "30m"
  volumes :
   - //c/deploy/logs:/opt/app/logs
   - //c/deploy/config:/app/config

networks :
 acsNetwork :
  driver : bridge
```

Наконец, давайте запустим контейнер.

```
docker-compose -f docker-compose.yml up --force-recreate -d
```

Docker загрузит и развернет контейнер, описанный и настроенный в yaml-файле docker-compose.

Если все в порядке, у вас должен быть доступ к консоли администратора через порт, описанный в файле конфигурации docker-compose.

Перейдите на вкладку «Начало работы» и следуйте инструкциям, чтобы инициировать соединение с БД и

предоставить секреты для шифрования всех конфиденциальных данных.