Для создания TLS сертификата на Mac OS X и Linux, выполните следующие шаги:

1. Установите OpenSSL:

   - На Mac OS X: OpenSSL уже установлен по умолчанию. Убедитесь, что ваша версия обновлена.

   - На Linux: Откройте терминал и выполните команду `sudo apt-get install openssl` (для систем на основе Debian/Ubuntu) или используйте аналогичную команду для вашего дистрибутива Linux.

2. Сгенерируйте закрытый ключ (private key):
   ```
   openssl genrsa -out private.key 2048
   ```

   Команда `genrsa` используется для генерации RSA закрытого ключа. Флаг `-out` указывает имя файла, в данном случае `private.key`. Значение `2048` определяет длину ключа в битах.

3. Создайте запрос на сертификат (certificate signing request):
   ```
   openssl req -new -key private.key -out request.csr
   ```

   Команда `req` используется для создания запроса на сертификат. Флаг `-key` указывает путь к закрытому ключу, созданному на предыдущем шаге. Флаг `-out` определяет имя файла для сохранения запроса на сертификат.

Введите запрашиваемую информацию, согласно таблице, ниже:

| Атрибут | Значение |
| --- | --- |
| «Общее имя» (Common Name) | Атрибут должен заполняться по шаблону: FINTECH+[KeyNum], где[KeyNum] – номер ключа от 01 до 99, который должен быть уникален для каждого запроса на сертификат.То есть при формировании первого запроса на сертификат пользователь должен указать номер ключа «01», при выпуске следующего запроса указать «02» и т.д.Пример правильного значения поля: FINTECH01 |
| «Электронная почта» (E-mail) | В поле должен указываться действующий электронный адрес сотрудника на стороне клиента, который отвечает за получение TLS сертификатов из УЦ Сбербанка |
| «Страна» (Country/Region) | В поле должен указываться двухбуквенный код страны. Код страны можно узнать в [открытых источниках в сети Интернет](https://en.wikipedia.org/wiki/ISO_3166-1_alpha-2).Для России: RU |
| «Организация» (Company) | В поле должно указываться наименование организации латинскими буквами |
| «Подразделение» (Organizational Unit) | ИНН организации |

4. Отправьте запрос на получение клиентского сертификата по электронной почте на адрес supportdbo2@sberbank.ru. Прикрепите к письму файл `request.csr` для отправки в УЦ Сбербанка и получения клиентского TLS сертификата.

5. Дождитесь получения клиентского сертификата от службы поддержки. Готовый сертификат будет в формате “.cer”

6. Установите полученный клиентский сертификат.

- На Mac OS X: Дважды щелкните файл `certificate.cer`, чтобы добавить его в ключевое хранилище системы.

- На Linux: Поместите файл `certificate.cer` в директорию, используемую вашим веб-сервером для сертификатов.

7. Для проверки установленного сертификата вы можете использовать Swagger.

   Воспользуйтесь отдельным Swagger-интерфейсом, предоставленным для проверки сертификата на странице https://developers.sber.ru/docs/ru/sberbusinessapi/start/tls#proverka-sertifikata