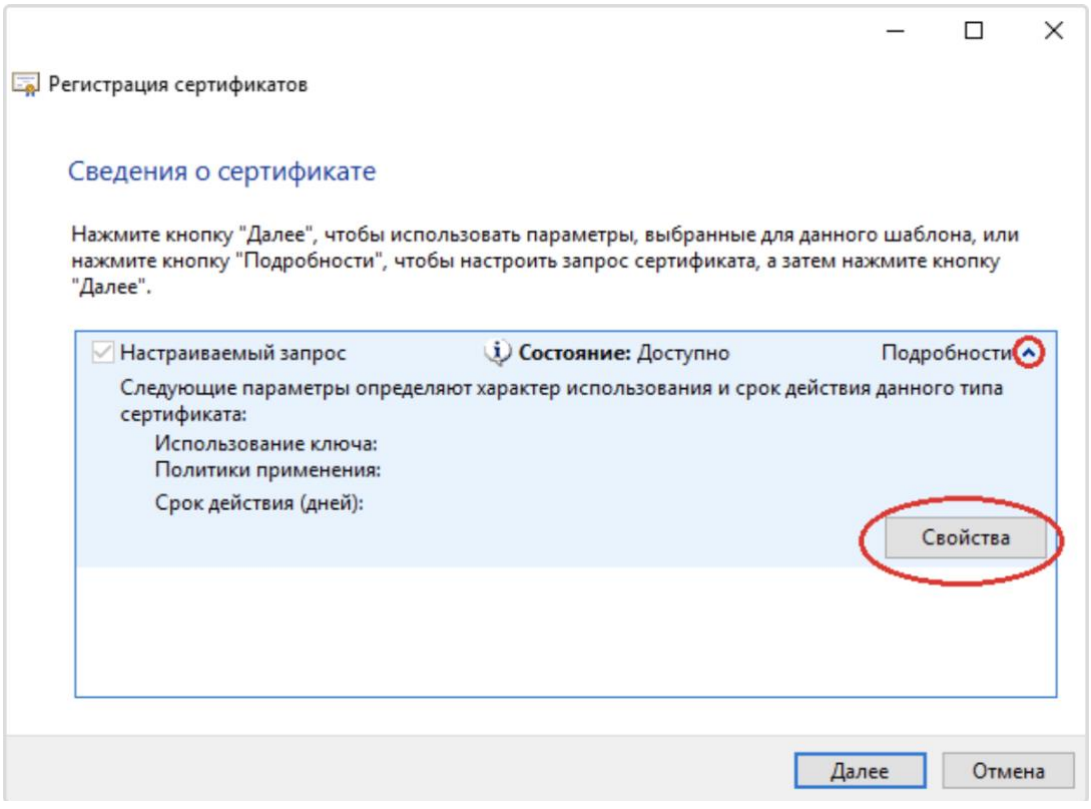
Инструкция по формированию закрытого ключа и запроса на выпуск TLS-сертификата

Генерацию запроса на создание сертификата необходимо выполнить от имени одного конкретного пользователя на одном ПК. После издания банком сертификата его необходимо добавить на ПК, на котором формировался запрос. Изданный ключ и сертификат можно выгрузить в виде файла контейнера, защищенного паролем, и перенести на другой ПК.

Чтобы сформировать запрос на сертификат необходимо выполнить следующие действия:

1. Войти в Windows с правами локального администратора.
2. На рабочем столе Windows нажать кнопку «Пуск».
3. В строке поиска ввести «certmgr.msc».
4. Нажать на найденную программу в верхней части окна.
5. В открывшейся оснастке перейти в папку «Личное».
6. На элемент «Сертификаты» нажать правой кнопкой мыши.
7. В открывшемся меню выбрать Все задачи/Дополнительные операции/Создать настраиваемый запрос.
8. В окне «Перед началом работы» нажать кнопку **Далее**.
9. В окне «Выбор политики регистрации сертификатов» необходимо выбрать пункт «Продолжить без политики регистрации» и нажать кнопку **Далее**.
10. В окне «Пользовательский запрос» выбрать шаблон «Старый ключ (без шаблона)», указать формат запроса «PKCS#10». Нажать кнопку **Далее**.
11. В окне «Сведения о сертификате» необходимо нажать на стрелку рядом с полем «Подробности».
12. В появившемся блоке необходимо нажать кнопку **Свойства**.

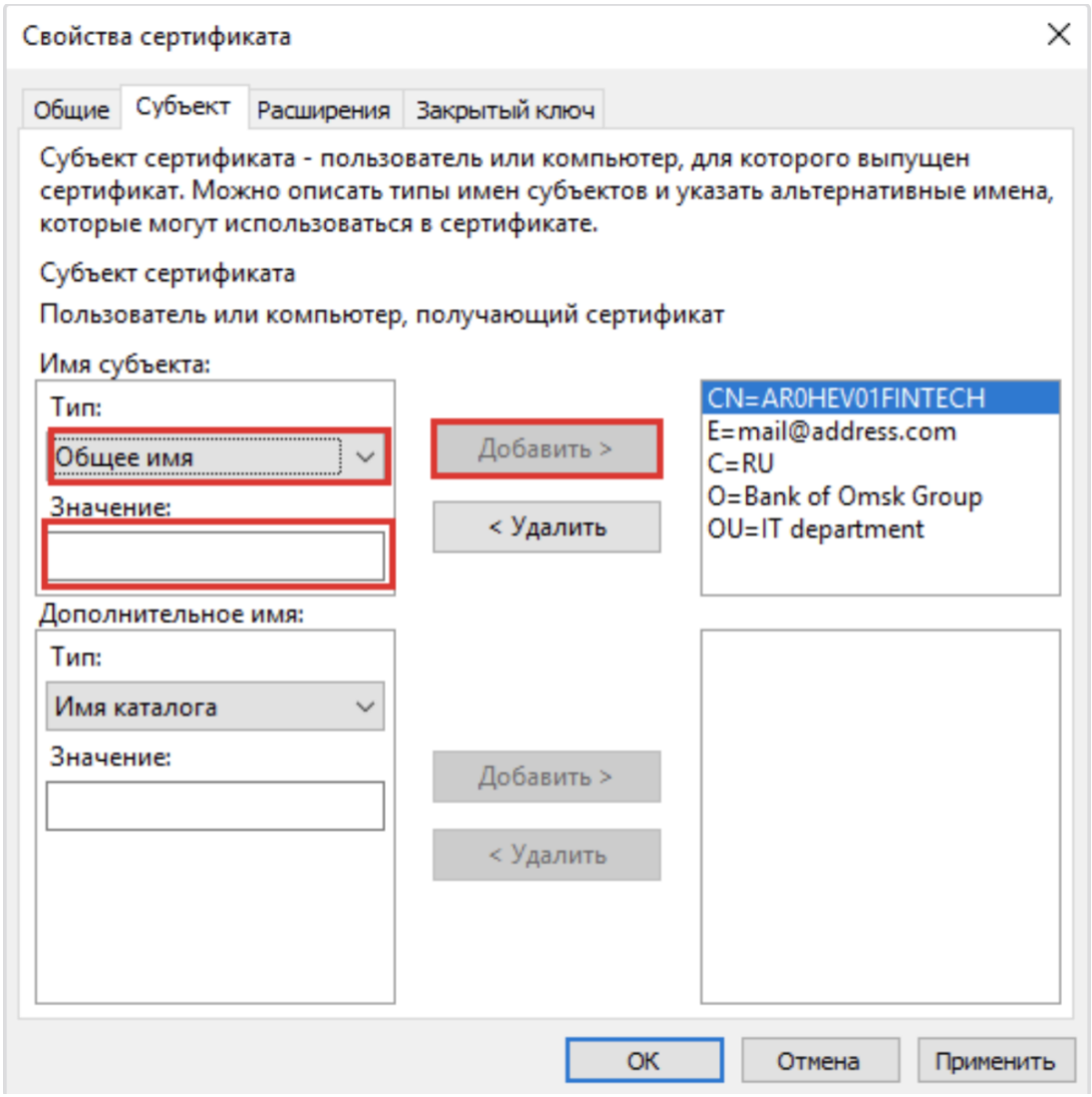


13. В окне «Свойства сертификата» необходимо заполнить атрибуты запроса на сертификат согласно требованиям УЦ, предъявляемым к запросам на TLS сертификат.
    Все атрибуты должны заполняться **только латинскими буквами.**
    На вкладке «Общие», в поле «Понятное имя» ввести удобное для пользователя название сертификата.

14. На вкладке «Субъект» требуется заполнить следующие атрибуты:

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. Для России: RU
«Организация» (Company)	В поле должно указываться наименование организации латинскими буквами
«Подразделение» (Organizational Unit)	ИНН организации

В блоке «Имя субъекта» необходимо по очереди выбирать названия нужных атрибутов в ниспадающем списке «Тип», вводить значение атрибута в поле «Значение», а затем нажать кнопку **Добавить** .
Ниже представлен пример заполнения атрибутов сертификата:



15. На вкладке «Расширения» необходимо в разделе «Использование ключа» добавить элементы «Шифрование данных» и «Цифровая подпись».

16. В разделе «Расширенное использование ключа (политики применения)» добавить элемент «Проверка подлинности клиента».

17. На вкладке «Закрытый ключ» в разделе «Поставщик службы шифрования» необходимо выбрать элемент «Microsoft RSA SChannel Cryptographic Provider (Шифрование)».

> «Microsoft RSA SChannel Cryptographic Provider» должен быть единственным выбранным поставщиком.

18. В разделе «Параметры ключа» установить «Размер ключа» равный 2048 и параметр «Сделать закрытый ключ экспортируемым».

19. После установки всех параметров нажать кнопку **ОК**.

20. В окне «Сведения о сертификате» нажать кнопку **Далее**.

21. В окне «Где вы хотите сохранить автономный запрос?» необходимо:

- в поле «Имя файла» указать имя файла, в который будет сохранен запрос на сертификат,

- выбрать формат файла «Base64»,
- нажать кнопку **Готово**.

Окно регистрации сертификата будет закрыто, а система сформирует файл с запросом, с именем файла указанном на предыдущем шаге.

Далее пользователю необходимо файл с запросом на сертификат передать на п/я сопровождения **supportdbo2@sberbank.ru**, для отправки в УЦ Сбербанка и получения клиентского TLS сертификата.

Установка сертификата

После того, как УЦ выпустит TLS сертификат, необходимо:

1. Получить сертификат от **supportdbo2@sberbank.ru**
2. Установить цепочку доверенных сертификатов Сбербанка (если их еще нет) в каталог «Доверенные корневые центры сертификации».
3. Установить полученный TLS сертификат (в каталог «Личные») на том же компьютере и под тем же пользователем, под которыми создавался запрос на этот сертификат.
4. Для установки сертификата и закрытого ключа на ОС Linux необходимо экспортировать установленный сертификат из каталога "Личные" на ПК Windows в контейнере в формате .PFX
5. Полученный файл в формате .PFX конвертируйте в формат .PEM с помощью OPENSSL

Команды openssl для конвертации:

To convert a PFX file to a PEM file that contains both the certificate and private key, the following command needs to be used:
 # openssl pkcs12 -in filename.pfx -out cert.pem -nodes

Conversion to separate PEM files
We can extract the private key form a PFX to a PEM file with this command:
openssl pkcs12 -in filename.pfx -nocerts -out key.pem

Exporting the certificate only:

openssl pkcs12 -in filename.pfx -clcerts -nokeys -out cert.pem