РУТОКЕН

Работа с утилитой "Генератор запросов сертификатов для Рутокен ЭЦП 2.0"

В этом документе

В этом документе описывается процесс работы с утилитой "Генератор запросов сертификатов для Рутокен ЭЦП 2.0".

Описание утилиты

Утилита "Генератор запросов сертификатов для Рутокен ЭЦП 2.0" предназначена для создания запроса на сертификат квалифицированной электронной подписи (КЭП) и записи готового сертификата на устройство Рутокен ЭЦП 2.0.

Запрос на сертификат используется для указания всей необходимой информации для сертификата КЭП.

Процесс создания сертификата КЭП состоит из следующих этапов:

1 этап. Создание запроса на сертификат КЭП и сохранение его на компьютере.

2 этап. Подписание запроса на сертификат КЭП.

3 этап. Создание сертификата КЭП и сохранение его на компьютере.

4 этап. Запись сертификата на устройство Рутокен ЭЦП 2.0.

Краткое описание работы с утилитой

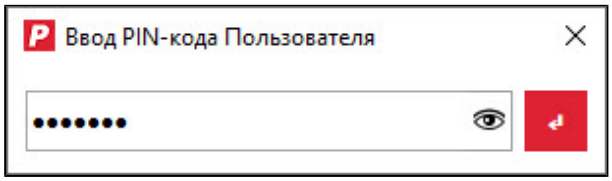
Создание запроса на сертификат КЭП

Для **создания запроса** на сертификат КЭП необходимо выполнить следующие действия:

1. Подключите устройство Рутокен ЭЦП 2.0 к компьютеру.
2. Скачайте архив и распакуйте его.
3. Запустите на исполнение файл **cert-gen-util.exe**. Откроется окно **Генератор запросов сертификатов для Рутокен ЭЦП 2.0**.
4. Заполните вручную все поля запроса (все поля заполняются согласно Приказу ФСБ РФ от 27.12.2011 № 795 "Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи"). Требования к данным, указанным в запросе на сертификат КЭП, смотрите в таблице.

5. Галочку "СКЗИ Рутокен ЭЦП 2.0" стоит снимать только в особых случаях. Когда она установлена, в запросе на сертификат отобразится наименование используемого средства ЭП (OID.1.2.643.100.111).
6. Нажмите на кнопку **[Создать запрос]**.

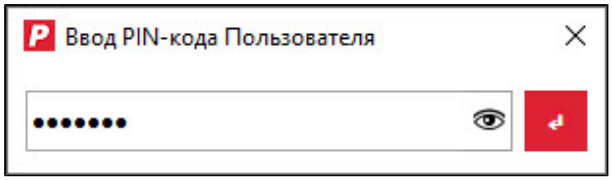
7. Выберите папку для сохранения файла запроса на компьютере и нажмите на кнопку **[Сохранить]**.
8. Укажите PIN-код Пользователя для устройства Рутокен ЭЦП 2.0.
9. Нажмите на кнопку . В результате на компьютере сохранится файл запроса, а на устройстве Рутокен ЭЦП 2.0 сгенерируется ключевая пара.



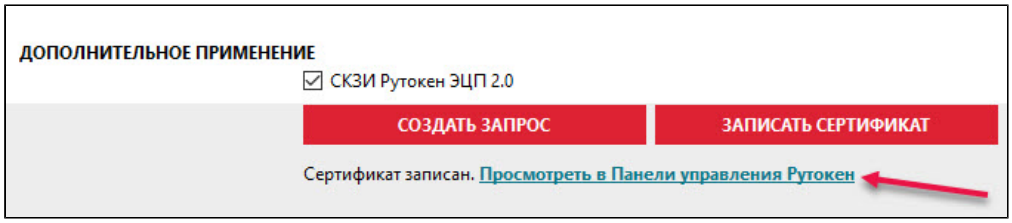
Запись сертификата КЭП на устройство Рутокен ЭЦП 2.0

Для **записи** сертификата КЭП на устройство Рутокен ЭЦП 2.0 необходимо выполнить следующие действия:

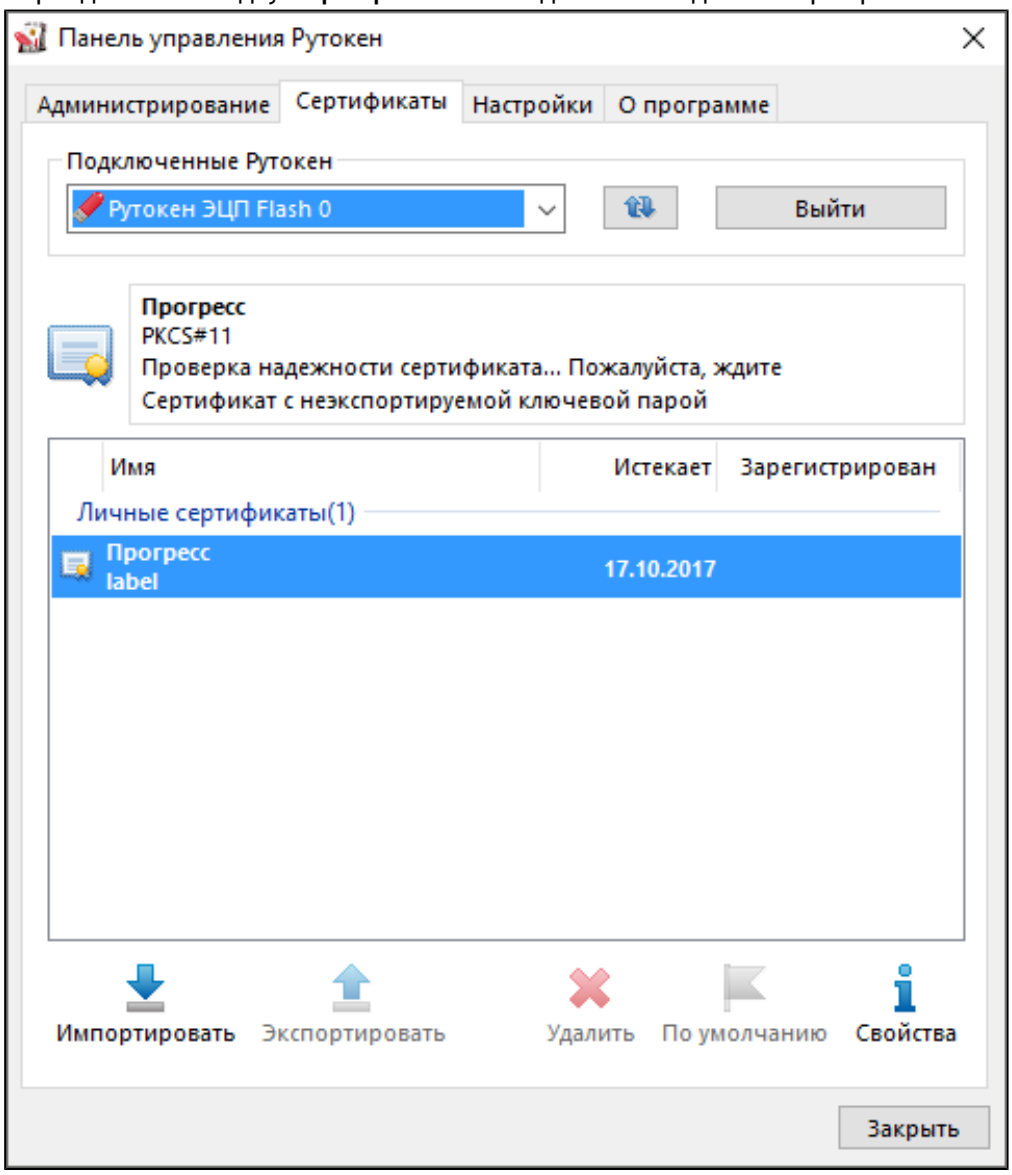
1. Подключите устройство Рутокен ЭЦП 2.0 к компьютеру.
2. Запустите на исполнение файл **cert-gen-util.exe**. Откроется окно **Генератор запросов сертификатов для Рутокен ЭЦП 2.0**.
3. Нажмите на кнопку **[Запись сертификата]**.
4. Выберите файл с сертификатом на компьютере и нажмите на кнопку **[Открыть]**.
5. Укажите PIN-код Пользователя для устройства Рутокен ЭЦП 2.0.
6. Нажмите на кнопку . В результате сертификат запишется на устройство Рутокен ЭЦП 2.0.



7. Для просмотра сертификата, записанного на устройство Рутокен ЭЦП 2.0, пройдите по ссылке "Просмотреть в Панели управления Рутокен". Откроется Панель управления Рутокен.



8. Перейдите на вкладку **Сертификаты** и найдите необходимый сертификат КЭП.



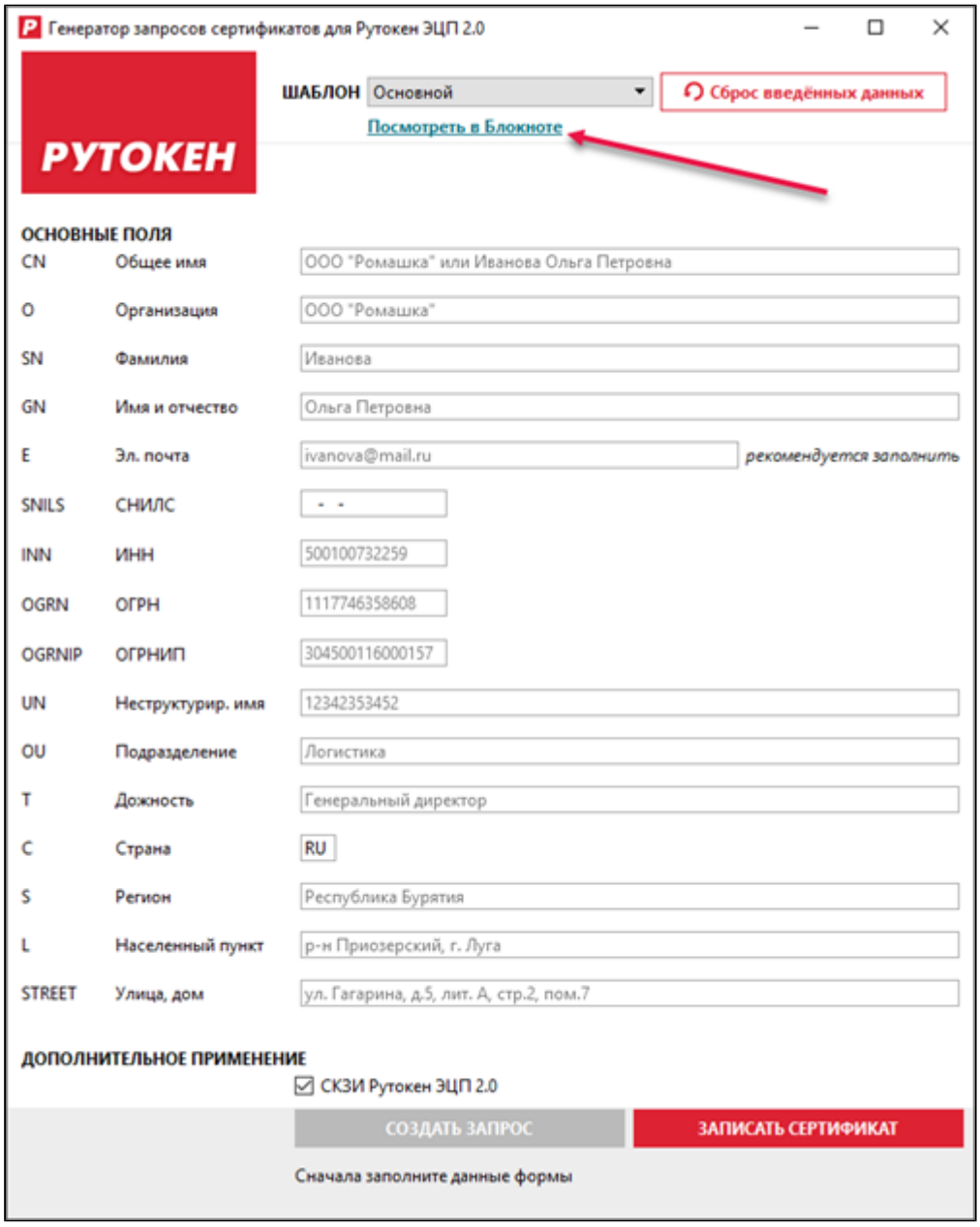
Подробное описание работы с утилитой

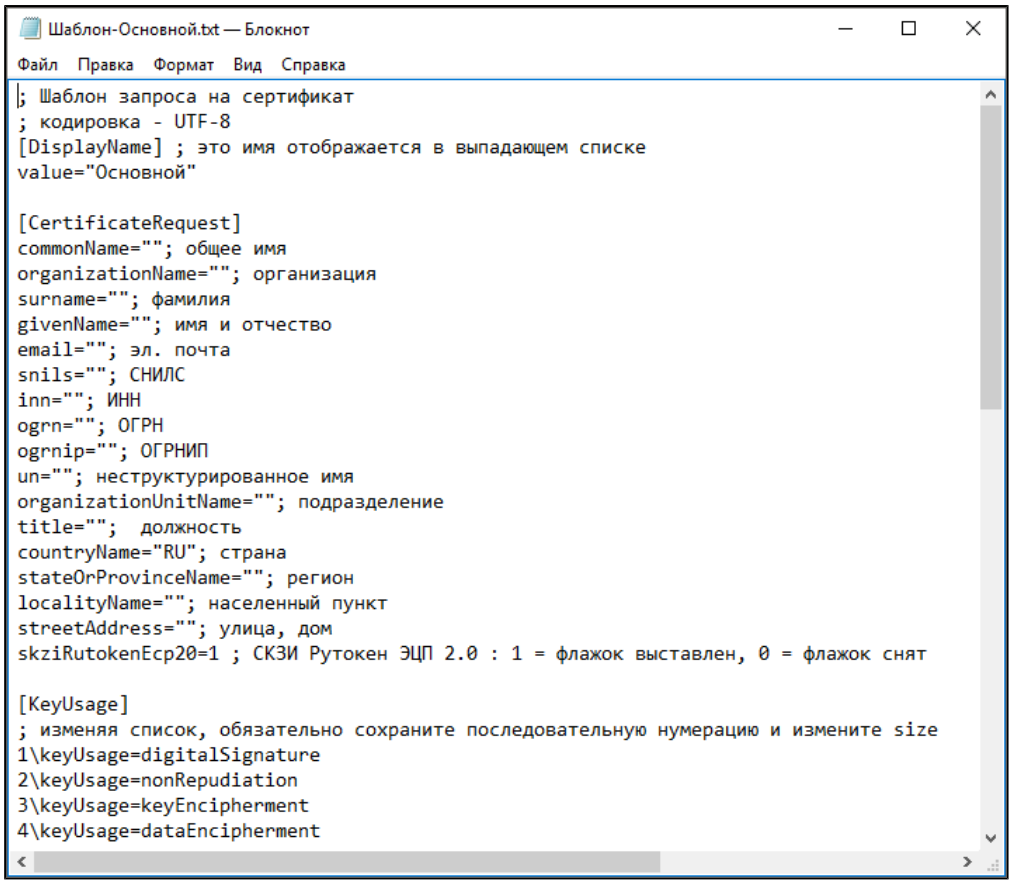
Для пользователя утилиты организованы следующие возможности: изменение параметров шаблона запроса на сертификат КЭП, сохранение нового шаблона на компьютере и его использование.

Изменение параметров шаблона запроса на сертификат КЭП

Для **изменения параметров шаблона** запроса на сертификат КЭП необходимо выполнить следующие действия:

1. Запустите на исполнение файл **cert-gen-util.exe**. Откроется окно **Генератор запросов сертификатов для Рутокен ЭЦП 2.0**.
2. Щелкните по ссылке "Просмотреть в Блокноте". Откроется окно **Шаблон-Основной**.





3. Измените необходимый параметр запроса.
4. В окне **Шаблон-Основной** выберите пункт **Файл** и подпункт **Сохранить как**.
5. Сохраните новый шаблон на компьютере в папке **cert-gen-util**.

Использование нового шаблона запроса на сертификат КЭП

Для **использования нового шаблона** запроса на сертификат КЭП необходимо выполнить следующие действия:

1. Запустите на исполнение файл **cert-gen-util.exe**. Откроется окно **Генератор запросов сертификатов для Рутокен ЭЦП 2.0**.
2. В раскрывающемся списке выберите название созданного шаблона.
3. Следуйте инструкции по созданию запроса на сертификат КЭП.

Структура кода шаблона запроса на сертификат КЭП

Код шаблона запроса на сертификат КЭП состоит из блоков, у каждого из них есть свое назначение.

Блок **[DisplayName]** используется для указания названия шаблона, которое отобразится в раскрывающемся списке в окне **Генератор запросов сертификатов для Рутокен ЭЦП 2.0**.

Блок **[CertificateRequest]** используется для указания информации о владельце сертификата. Параметры запроса данного блока описаны в **Таблице 1**.

Таблица 1

Название поля (параметр запроса)	**Требования к данным**
Общее имя `(commonName)`	■ для физического лица — имя, фамилия и отчество владельца сертификата ■ для юридического лица — наименование организации владельца сертификата
Организация `(organizationName)`	■ наименование организации владельца сертификата
Фамилия `(surname)`	■ фамилия владельца сертификата с большой буквы в одно слово (без пробелов)
Имя и отчество `(givenName)`	■ имя и отчество владельца сертификата
Эл. почта `(email)`	■ адрес электронной почты владельца сертификата ■ используются только латинские буквы и цифры
СНИЛС `(snils)`	■ строка, состоящая из 11 цифр ■ для физического лица — СНИЛС владельца сертификата ■ для юридического лица — СНИЛС организации владельца сертификата
ИНН `(inn)`	■ строка, состоящая из 12 цифр ■ для физического лица — ИНН владельца сертификата ■ для юридического лица — ИНН организации владельца сертификата

Название поля (параметр запроса)	Требования к данным
ОГРН (ogrn)	■ строка, состоящая из 13 цифр ■ ОГРН организации владельца сертификата
ОГРНИП (ogrnip)	■ строка, состоящая из 15 цифр ■ ОГРНИП владельца сертификата
Неструктурир. имя (un)	■ КПП организации владельца сертификата (для ЕГАИС)
Подразделение (organizationUnitName)	■ подразделение или отдел, в котором работает владелец сертификата
Должность (title)	■ должность владельца сертификата
Страна (countryName)	■ для физического лица — краткое наименование страны, в которой проживает владелец сертификата ■ для юридического лица — краткое наименование страны, в которой находится организация владельца сертификата
Регион (stateOrProvinceName)	■ для физического лица — название региона, в котором проживает владелец сертификата ■ для юридического лица — название региона, в котором находится организация владельца сертификата
Населенный пункт (localityName)	■ для физического лица — название населенного пункта, в котором проживает владелец сертификата ■ для юридического лица — название населенного пункта, в котором находится организация владельца сертификата
Улица, дом (streetAddress)	■ для физического лица — адрес, по которому проживает владелец сертификата ■ для юридического лица — юридический адрес организации владельца сертификата
Галочка "СКЗИ Рутокен ЭЦП 2.0" (subjectSignTool)	■ определяет наличие в сертификате наименования используемого средства ЭП (OID.1.2.643.100.111)

Блок **[KeyUsage]** используется для указания области использования сертификата. Значения, которые можно указать в данном блоке указаны в **Таблице 2.**

Таблица 2

Название	Описание
`digitalSignature`	электронная цифровая подпись
`nonRepudiation`	неотрекаемость от авторства
`keyEncipherment`	шифрование ключей
`dataEncipherment`	шифрование данных
`keyAgreement`	согласование ключей
`keyCertSign`	электронная цифровая подпись сертификатов ключей подписи
`crlSign`	электронная цифровая подпись списков отозванных сертификатов
`encipherOnly`	зашифровывание
`decipherOnly`	расшифровывание

Блок **[ExtendedKeyUsage]** используется для указания параметров расширенного использования сертификата. Здесь указываются идентификаторы необходимых операции, классов пользователей и устройств. Допустимые значения смотрите в **Таблице 3**.

Таблица 3

Значение	Описание
`1.2.643.100.113.1`	класс средства ЭП КС1
`1.2.643.100.113.2`	класс средства ЭП КС2

Значение	Описание
1.3.6.1.5.5.7.3.2	проверка подлинности клиента
1.3.6.1.5.5.7.3.4	защищенная электронная почта
1.2.643.2.2.34.6	пользователь Центра Регистрации, HTTP, TLS клиент
1.2.643.2.2.34.26	пользователь службы актуальных статусов
1.2.643.2.2.34.25	пользователь службы штампов времени

Блок **[CustomExtension]** используется для указания расширений сертификата не предусмотренных в других блоках.

Расширения сертификата — это информационные поля, которые содержат дополнительные сведения о сертификате.

Расширения сертификата задаются следующими параметрами:

- oid — идентификатор расширения;
- value — данные этого расширения в DER-кодировке.
- criticality — критичность наличия данного расширения.

Блок **[Criticality]** используется для указания критичности наличия параметров сертификата, указанных в блоках **[KeyUsage]** и **[ExtendedKeyUsage]**.

Дополнительная информация об утилите

Изменение параметра запроса на сертификат КЭП

Для изменения параметра запроса на сертификат КЭП необходимо выполнить следующие действия:

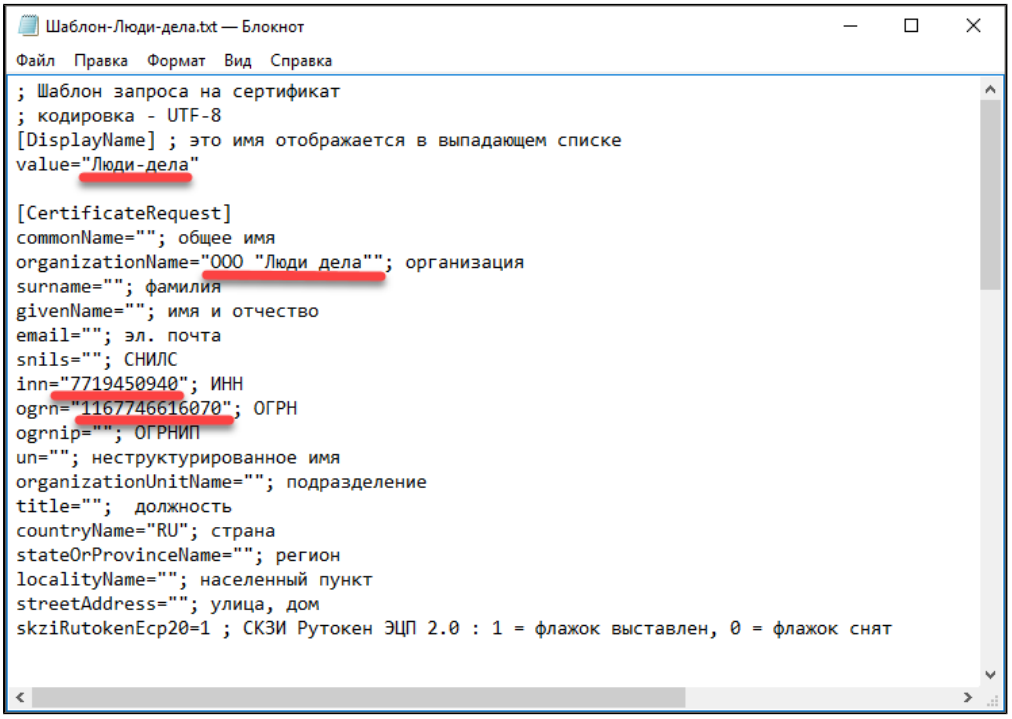
1. Запустите на исполнение файл **cert-gen-util.exe**. Откроется окно **Генератор запросов сертификатов для Рутокен ЭЦП 2.0**.
2. Щелкните по ссылке "Просмотреть в блокноте". Откроется окно **Шаблон-Основной**.
3. Поставьте курсор мыши в необходимой строке между кавычками и укажите значение параметра.

Пример 1:

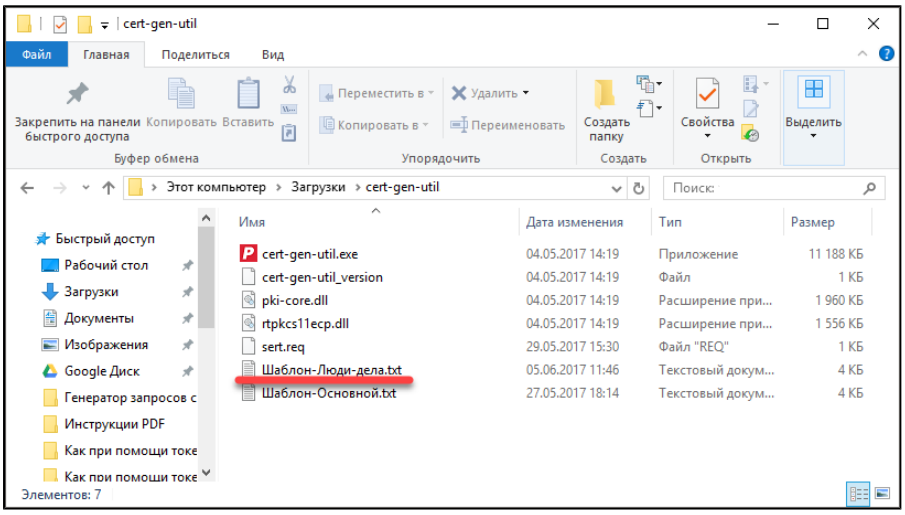
Изменения в блоке **[CertificateRequest]**.

1) Изменим следующие параметры запроса на сертификат КЭП:

- `value;`
- `organizationName;`
- `inn;`
- `ogrn.`

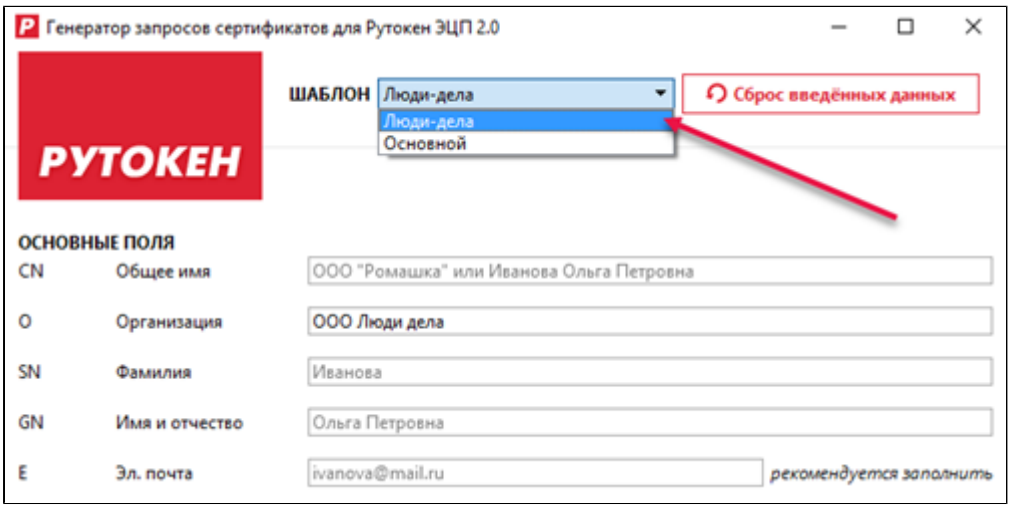


2) Сохраним новый шаблон на компьютере в папке **cert-gen-util** и назовем его **Шаблон-Люди-дела**.

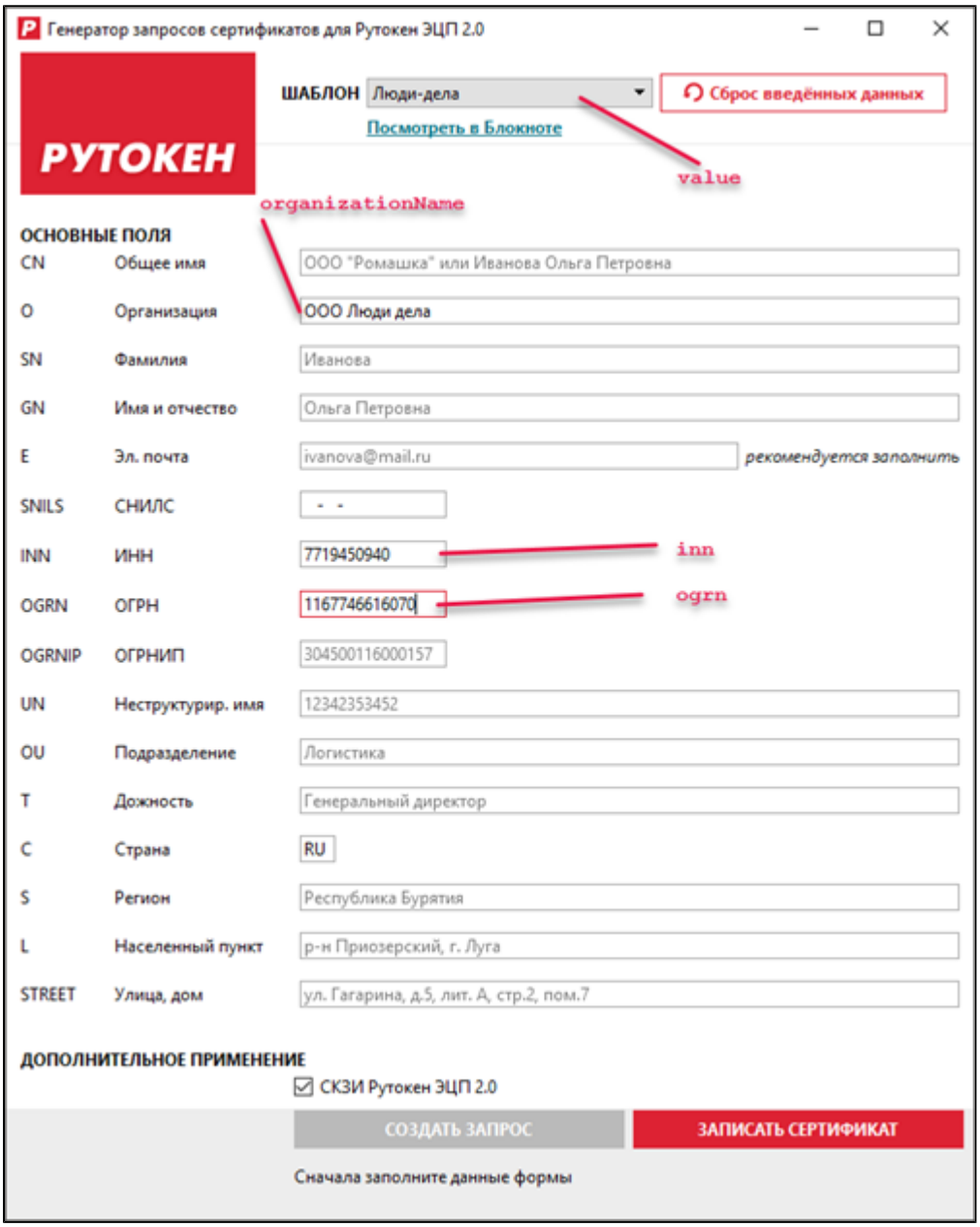


3) Запустим на исполнение файл **cert-gen-util.exe**. Откроется **Генератор запросов сертификатов для Рутокен ЭЦП 2.0**.

4) В раскрывающемся списке выберем название шаблона.



5) Заданные параметры отобразятся в окне **Генератор запросов сертификатов для Рутокен ЭЦП 2.0**.



Пример 2:

Изменения в блоке **[CustomExtension]**.

1) Добавим следующие расширения для сертификата:

- `1\oid=1.3.6.1.4.1.311.21.7`
- `1\value=@ByteArray(\x30\x0D\x06\x08\x2A\x85\x03\x02\x02\x2E\x00\x08\x02\x01\x01)`
- `1\criticality=non critical`

```
[CustomExtensions]
1\oid=1.3.6.1.4.1.311.21.7
1\value=@ByteArray(\x30\x0D\x06\x08\x2A\x85\x03\x02\x02\x2E\x00\x08\x02\x01\x01)
1\criticality=non critical
size=1
```

Каждое расширение для сертификата может быть обозначено, как критическое или некритическое (параметр criticality). Сертификат должен быть отвергнут при отсутствии критических расширений (если параметр у расширения criticality=critical).

Отсутствие некритических расширений может быть проигнорировано (если параметр у расширения critikality= non critical).

2) Сохраните шаблон на компьютере. В результате для сертификата будет задано следующее расширение:

```
SEQUENCE {
 OBJECTIDENTIFIER 1.2.643.2.2.46.0.8
 INTEGER 1
 }
```

Дополнительные источники информации

При возникновении вопроса, на который вам не удалось найти ответ в этой инструкции, рекомендуем обратиться к следующим дополнительным источникам информации:

- **WWW:** https://rutoken.ru
  Наш веб-сайт содержит большой объем справочной информации об устройствах Рутокен.
- **WWW:** https://dev.rutoken.ru
  Портал разработчика содержит техническую информацию об устройствах Рутокен и руководства по их интеграции.
- **Форум**: https://forum.rutoken.ru
  Форум содержит ответы на часто задаваемые вопросы. Кроме того, здесь вы можете задать свой вопрос разработчикам и сотрудникам Службы технической поддержки Рутокен.
- **Служба технической поддержки Рутокен:**
  www: https://www.rutoken.ru/support/feedback/
  сервис диагностики: https://help.rutoken.ru
  e-mail: hotline@rutoken.ru
  тел.: +7(495)925-77-90