

**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".

Что необходимо установить на компьютер для работы с утилитой? (см. стр. [3](#))

Как запустить утилиту? (см. стр. [7](#))

Как создать запрос на сертификат квалифицированной электронной подписи? (см. стр. [10](#))

Как записать сертификат квалифицированной электронной подписи на устройство Рутокен? (см. стр. [11](#))

Как изменить, существующий в утилите шаблон запроса на сертификат? (см. стр. [13](#))

Как воспользоваться измененным шаблоном запроса на сертификат? (см. стр. [14](#))

Общая информация

Эту инструкцию можно использовать, если вы работаете с устройствами:

- Рутокен ЭЦП 2.0;
- Рутокен ЭЦП 2.0 micro;
- Рутокен ЭЦП 2.0 Touch;
- Рутокен ЭЦП 2.0 Flash;
- Рутокен ЭЦП 2.0 Type-C;
- Рутокен PINPad.

У каждого устройства Рутокен есть PIN-код Пользователя и PIN-код Администратора.

PIN-код Пользователя является паролем, который используется для реализации основных функций устройства Рутокен.

PIN-код Пользователя по умолчанию – 12345678.

PIN-код Администратора является паролем, который используется для доступа к административным функциям устройства Рутокен.

PIN-код Администратора по умолчанию – 87654321.

Процесс создания сертификата квалифицированной электронной подписи состоит из следующих этапов:

- 1 этап.** Создание запроса на сертификат квалифицированной электронной подписи и сохранение его на компьютере.
- 2 этап.** Подписание запроса на сертификат квалифицированной электронной подписи.
- 3 этап.** Создание сертификата квалифицированной электронной подписи и сохранение его на компьютере.
- 4 этап.** Запись сертификата на устройство Рутокен ЭЦП 2.0.

Утилита "Генератор запросов сертификатов для Рутокен ЭЦП 2.0" предназначена:

- для создания запроса на сертификат квалифицированной электронной подписи;
- для записи готового сертификата на устройство Рутокен.

Запрос на сертификат используется для указания всей необходимой информации для сертификата квалифицированной электронной подписи.

Доступ к утилите возможен из Панели управления Рутокен, которая устанавливается в систему при установке комплекта "Драйверы Рутокен для Windows".

Установка комплекта "Драйверы Рутокен для Windows"

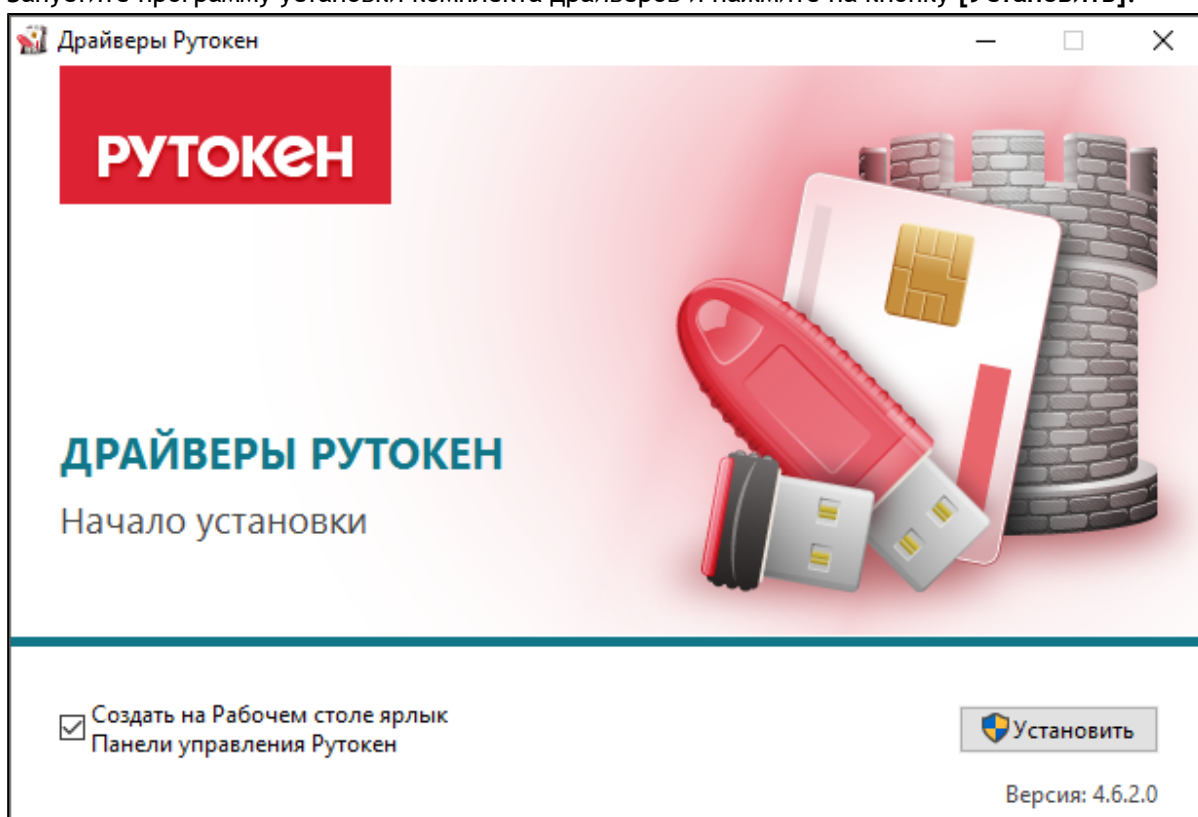
Актуальная версия комплекта драйверов доступна по ссылке:

<https://www.rutoken.ru/support/download/drivers-for-windows/>

1. Перед началом установки комплекта драйверов рекомендуется закрыть все работающие приложения и отсоединить Рутокен от компьютера.
2. Для установки комплекта драйверов необходимы права администратора системы.

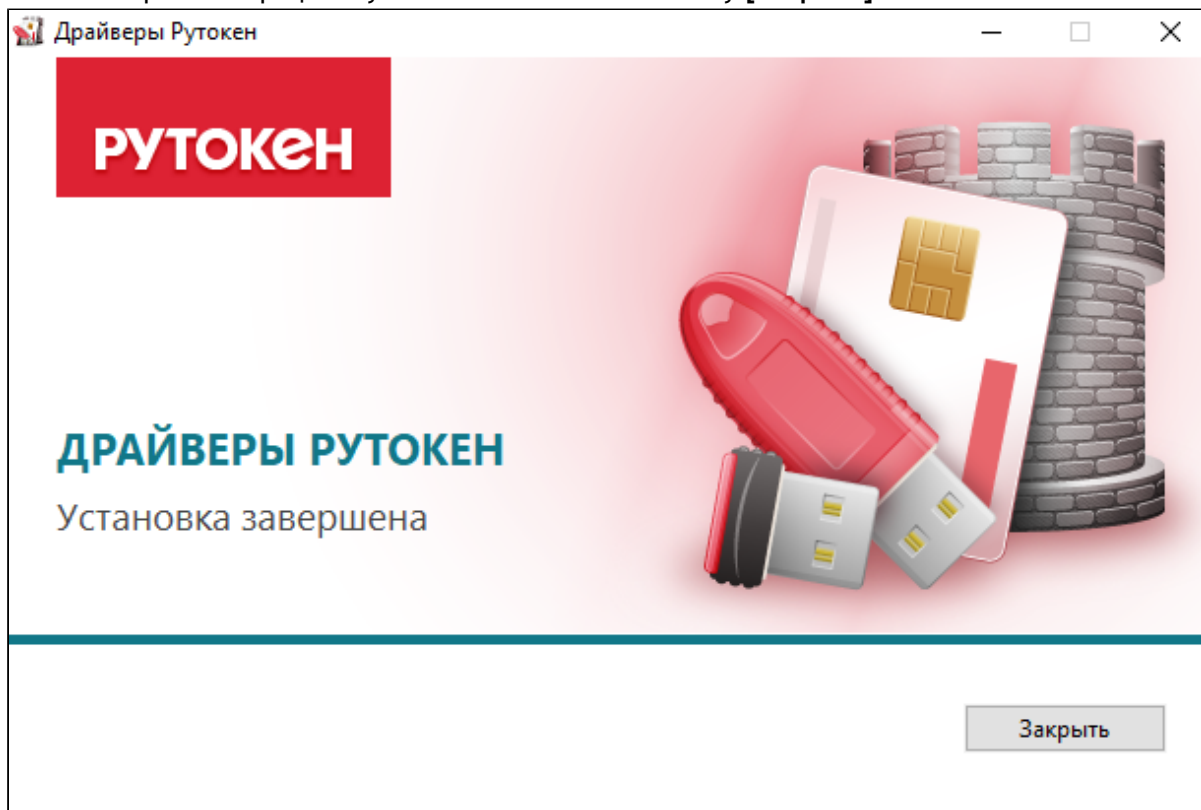
Для установки комплекта драйверов:

1. Запустите программу установки комплекта драйверов и нажмите на кнопку **[Установить]**.



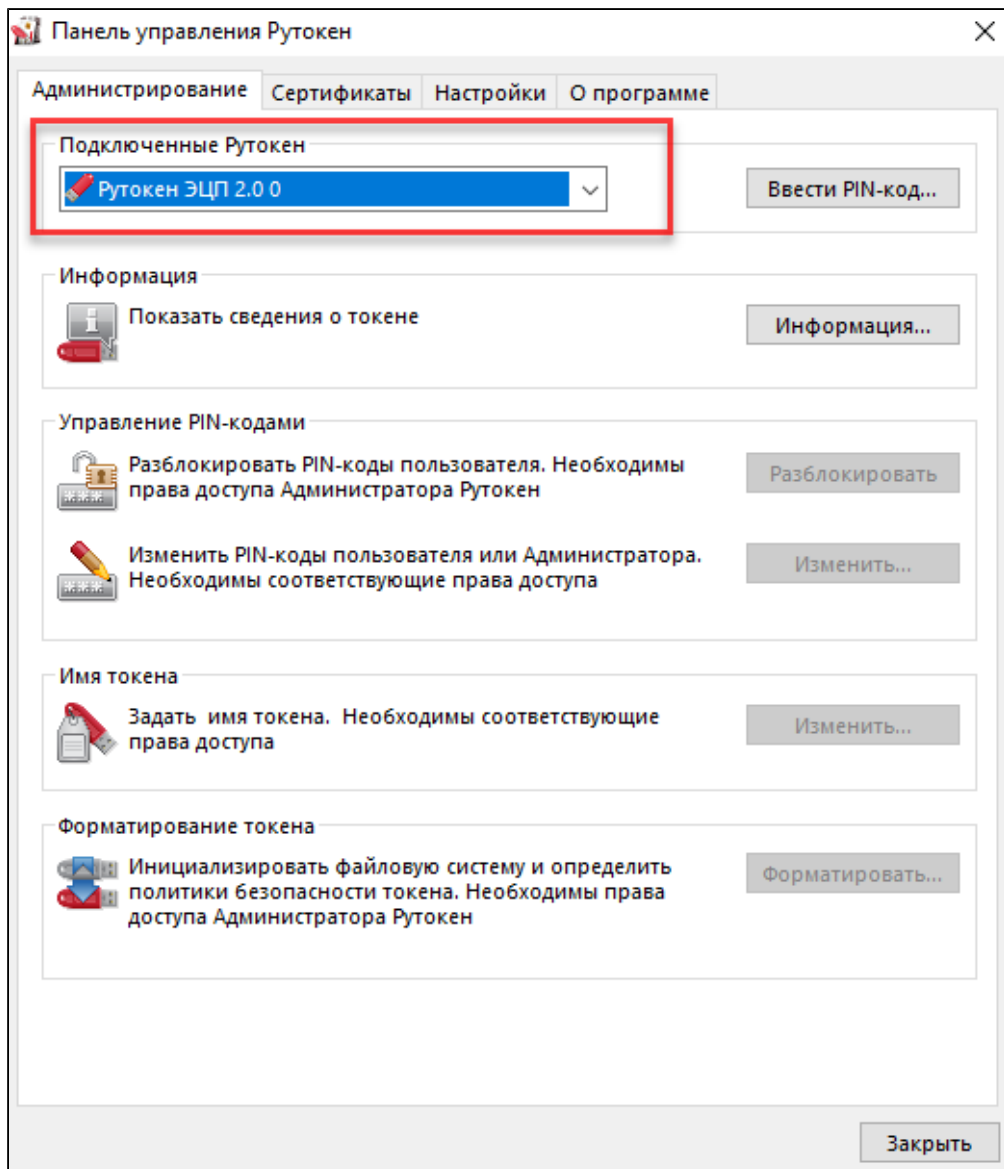
2. В окне с запросом на разрешение изменений на компьютере нажмите на кнопку **[Да]**. В результате запустится процесс установки комплекта драйверов.

3. После завершения процесса установки нажмите на кнопку **[Закреть]**.



4. Подключите Рутокен к компьютеру.

5. Запустите Панель управления Рутокен. В результате откроется главное окно панели управления и в поле Подключенные Рутокен отобразится название подключенного устройства.



Генератор запросов сертификатов работает со следующими устройствами Рутокен:

- Рутокен ЭЦП 2.0;
- Рутокен ЭЦП 2.0 micro;
- Рутокен ЭЦП 2.0 Touch;
- Рутокен ЭЦП 2.0 Flash;
- Рутокен ЭЦП 2.0 Type-C;
- Рутокен PINPad.

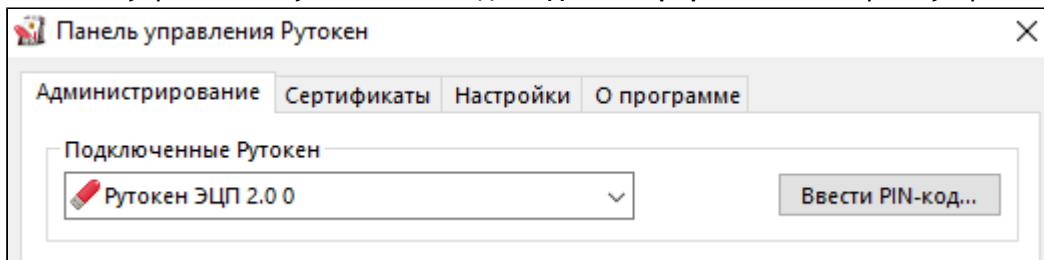
Запуск утилиты "Генератор запросов сертификатов для Рутокен ЭЦП 2.0"

Чтобы генератор запросов стал доступен в Панели управления Рутокен необходимо ввести PIN-код Администратора.

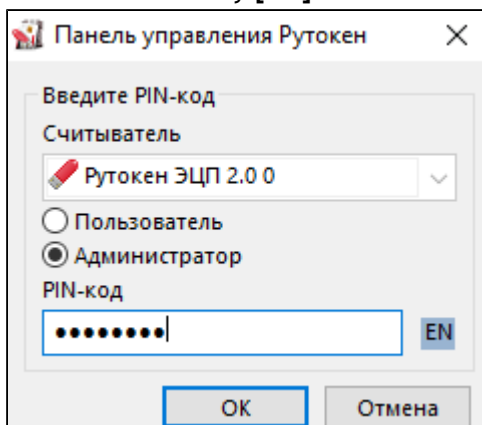
Если вы не знаете PIN-кода Администратора, то обратитесь к тому, кто выдал вам устройство Рутокен.

Чтобы запустить утилиту:

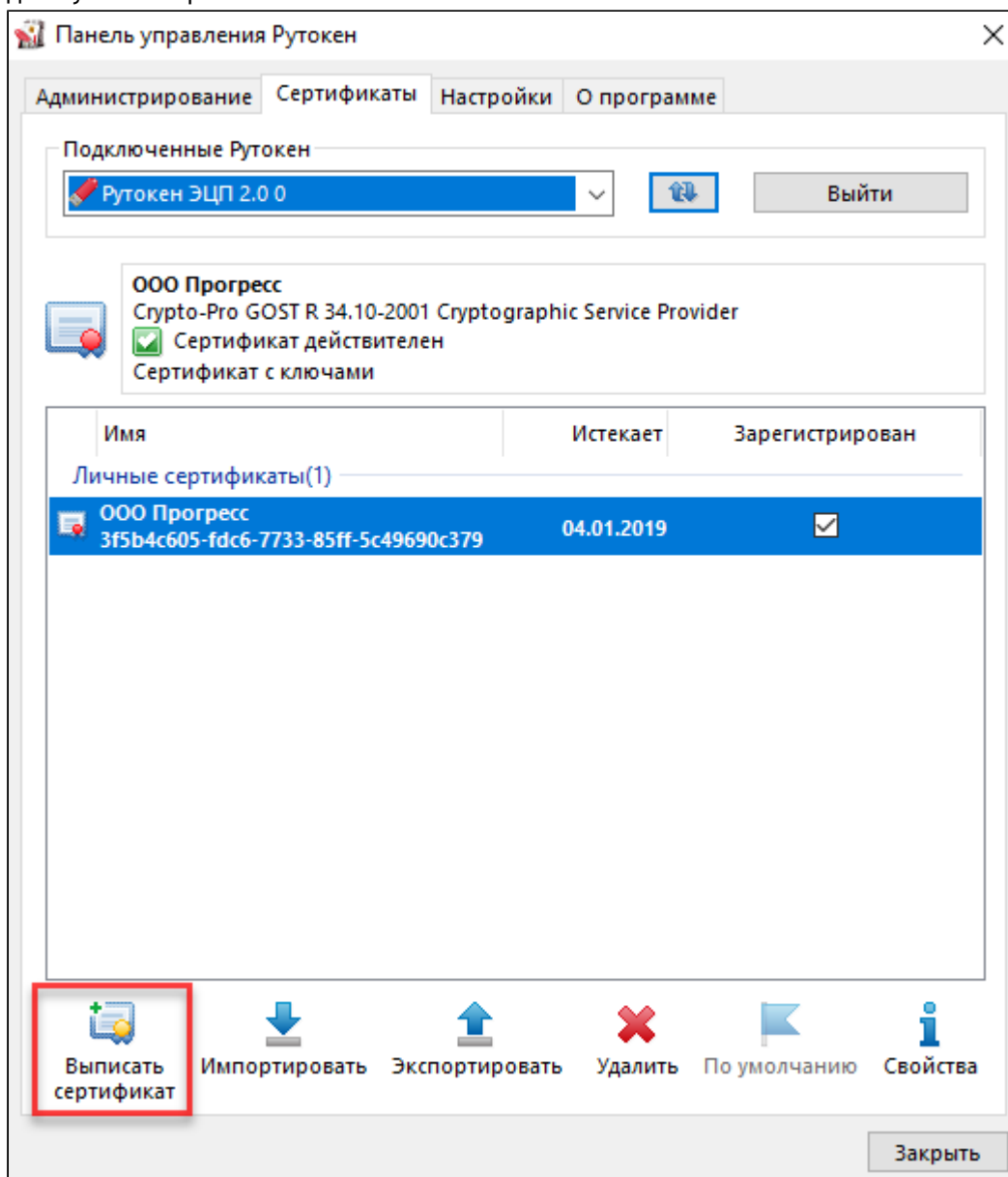
1. В Панели управления Рутокен на вкладке **Администрирование** выберите устройство.



2. Нажмите на кнопку **[Ввести PIN-код]**.
3. Установите переключатель в положение **Администратор** и введите PIN-код Администратора.
4. Нажмите на кнопку **[OK]**.



5. Перейдите на вкладку **Сертификаты**.
6. Нажмите на кнопку **[Выписать сертификат]** (эта кнопка станет активной, если вы ввели корректный PIN-код Администратора). В результате откроется окно утилиты "Генератор запросов сертификатов для Рутокен ЭЦП 2.0".



Р Генератор запросов сертификатов для Рутокен ЭЦП 2.0

РУТОКЕН

ШАБЛОН Пример для ГОСТ 2001 Сброс введённых данных

[Посмотреть в Блокноте](#)

ОСНОВНЫЕ ПОЛЯ

CN	Общее имя	<input type="text" value="ООО " иванова="" или="" ольга="" петровна"="" ромашка"=""/>
O	Организация	<input type="text" value="ООО " ромашка""=""/>
SN	Фамилия	<input type="text" value="Иванова"/>
GN	Имя и отчество	<input type="text" value="Ольга Петровна"/>
E	Эл. почта	<input type="text" value="ivanova@mail.ru"/> <i>рекомендуется заполнить</i>
SNILS	СНИЛС	<input type="text" value="- -"/>
INN	ИНН	<input type="text" value="006104001458"/>
OGRN	ОГРН	<input type="text" value="1117746358608"/>
OGRNIP	ОГРНИП	<input type="text" value="304500116000157"/>
UN	Неструктурир. имя	<input type="text" value="12342353452"/>
OU	Подразделение	<input type="text" value="Логистика"/>
T	Должность	<input type="text" value="Генеральный директор"/>
C	Страна	<input type="text" value="RU"/>
S	Регион	<input type="text" value="03 Республика Бурятия"/>
L	Населенный пункт	<input type="text" value="р-н Приозерский, г. Луга"/>
STREET	Улица, дом	<input type="text" value="ул. Гагарина, д.5, лит. А, стр.2, пом.7"/>

СРЕДСТВО ПОДПИСИ

Рутокен ЭЦП 2.0

СОЗДАТЬ ЗАПРОС ЗАПИСАТЬ СЕРТИФИКАТ

Сначала заполните данные формы

В полях отображаются примеры значений для каждого поля.

После этого вы можете работать с утилитой.

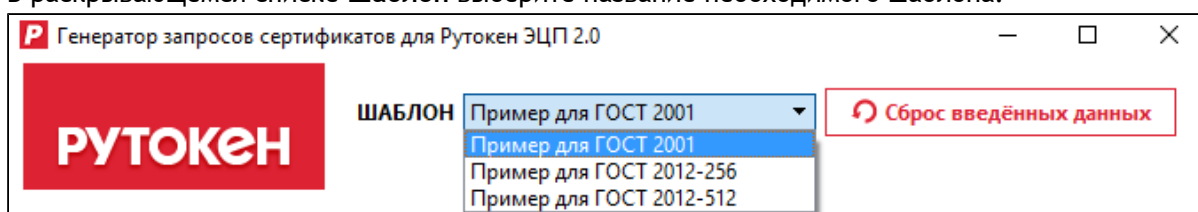
Краткое описание работы с утилитой

> Создание запроса на сертификат квалифицированной электронной подписи

Перед запуском утилиты отключите от компьютера все лишние устройства Рутокен. Оставьте только устройство, на которое необходимо записать сертификат квалифицированной электронной подписи.


Для создания запроса на сертификат квалифицированной электронной подписи:

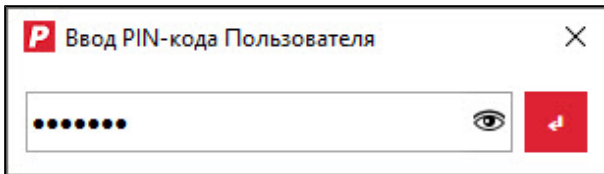
1. Запустите утилиту.
2. В раскрывающемся списке **Шаблон** выберите название необходимого шаблона.



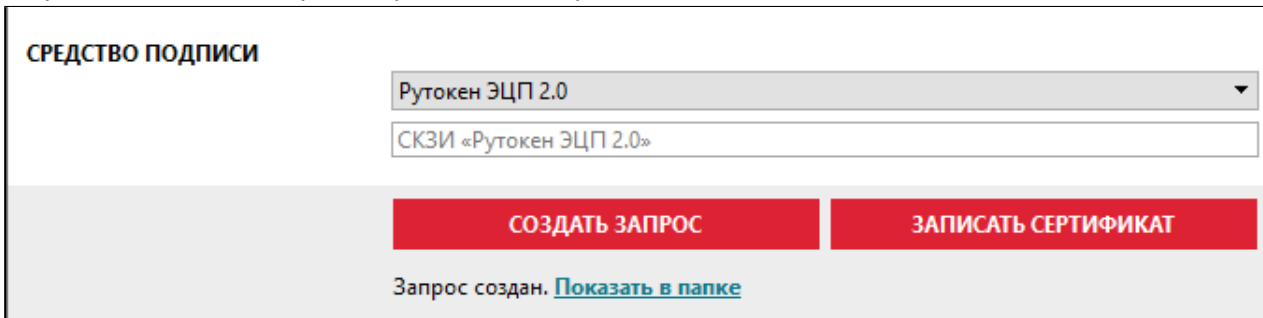
3. Введите необходимые значения полей запроса (все поля заполняются согласно Приказу ФСБ РФ от 27.12.2011 № 795 "Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи"). Требования к данным, указанным в запросе на сертификат квалифицированной электронной подписи смотрите в [таблице](#).

4. Нажмите на кнопку **[Создать запрос]**.
5. Выберите на компьютере папку для сохранения файла запроса и нажмите на кнопку **[Сохранить]**.
6. Укажите PIN-код Пользователя устройства Рутокен.

- Нажмите на кнопку . В результате на компьютере сохранится файл запроса, а на устройстве Рутокен сгенерируется ключевая пара.



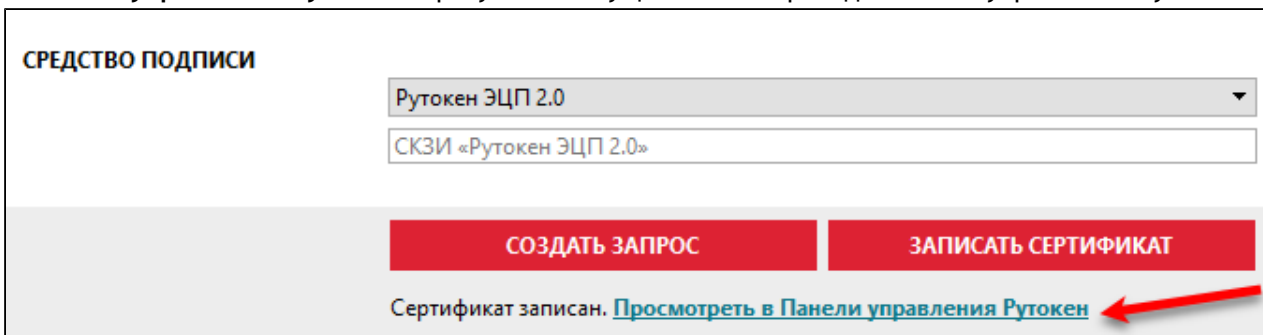
- Чтобы убедиться в том, что запрос создан, щелкните по ссылке **Показать в папке**. В результате откроется папка, в которой сохранен этот запрос.



> Запись сертификата квалифицированной электронной подписи на устройство Рутокен

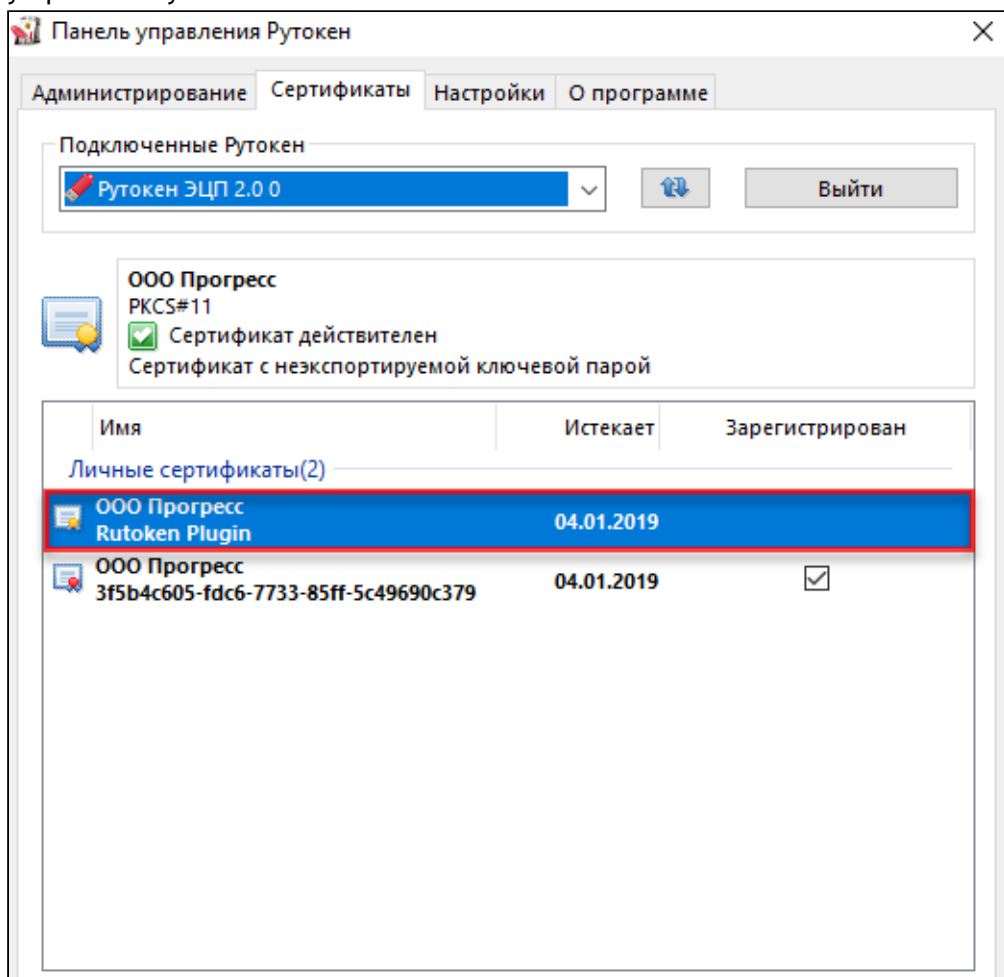
Для записи сертификата квалифицированной электронной подписи на устройство Рутокен ЭЦП 2.0:

- Нажмите на кнопку [Запись сертификата].
- Выберите на компьютере файл с сертификатом и нажмите на кнопку [Открыть]. В результате сертификат запишется на устройство Рутокен.
- Для просмотра сертификата, записанного на устройство Рутокен, щелкните по ссылке **Просмотреть в Панели управления Рутокен**. В результате осуществится переход в Панель управления Рутокен.



- Перейдите на вкладку **Сертификаты** и нажмите на кнопку .

- Найдите созданный сертификат квалифицированной электронной подписи. Сертификат записан на устройство Рутокен.



Дополнительные возможности утилиты

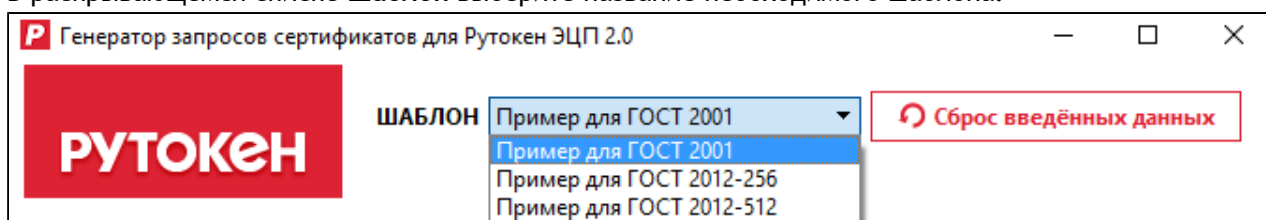
Пользователям утилиты доступны следующие возможности для работы с шаблонами:

- изменение параметров шаблона;
- сохранение нового шаблона на компьютере;
- использование существующего или нового шаблона.

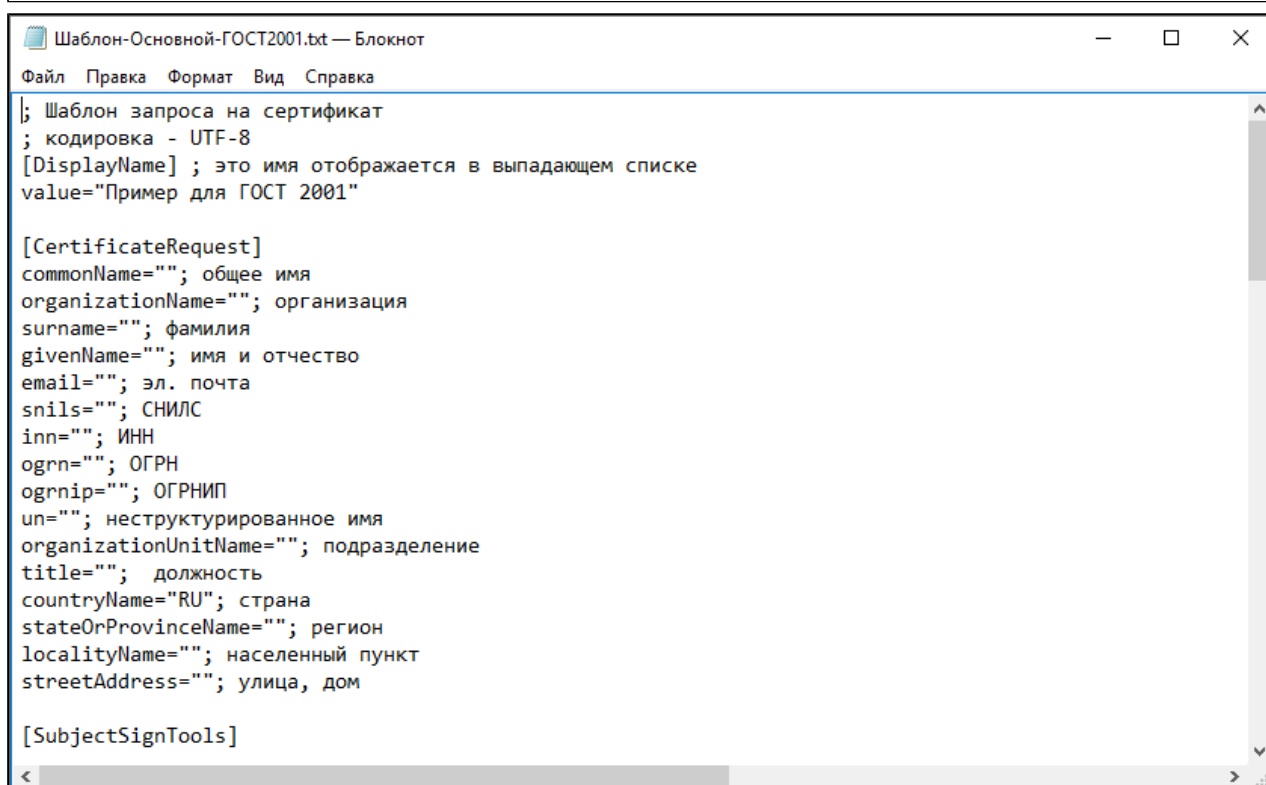
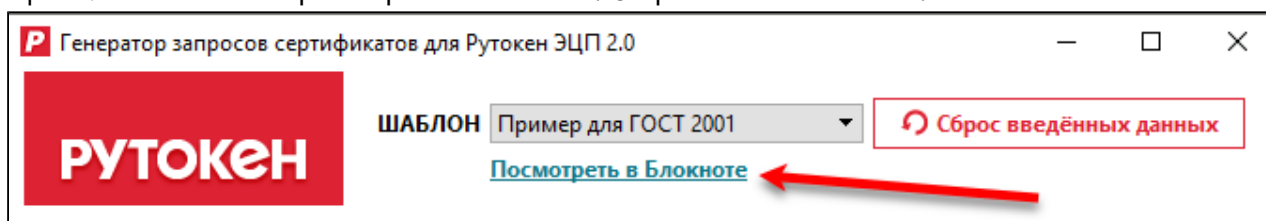
> Изменение параметров шаблона запроса на сертификат квалифицированной электронной подписи

Для изменения параметров шаблона:

1. Запустите Панель управления Рутокен.
2. Запустите утилиту.
3. В раскрывающемся списке **Шаблон** выберите название необходимого шаблона.



4. Щелкните по ссылке "Посмотреть в Блокноте". Откроется окно шаблона.



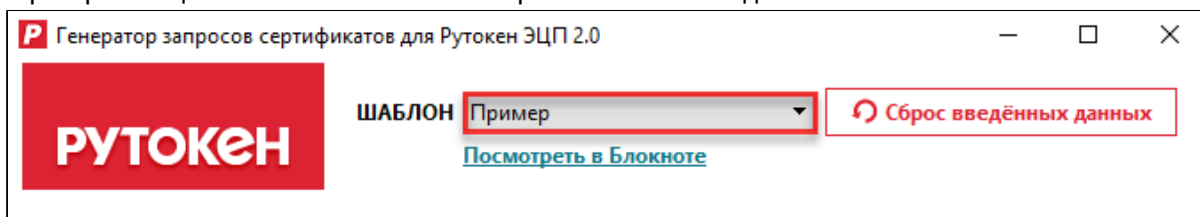
5. Измените необходимый параметр запроса.

6. В окне шаблона выберите пункт **Файл** и подпункт **Сохранить как**.
7. Выберите папку для сохранения шаблона на компьютере.
8. Укажите имя файла.
9. Нажмите на кнопку **[Сохранить]**.

> Использование нового шаблона запроса на сертификат квалифицированной электронной подписи

Для использования нового шаблона запроса на сертификат квалифицированной электронной подписи:

1. Запустите **Панель управления Рутокен**.
2. Запустите утилиту.
3. В раскрывающемся списке **Шаблон** выберите название созданного шаблона.



4. Следуйте [инструкции](#) по созданию запроса на сертификат квалифицированной электронной подписи.

Структура кода шаблона запроса на сертификат квалифицированной электронной подписи

Код шаблона запроса на сертификат квалифицированной электронной подписи состоит из блоков, у каждого из которых 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
<i>Общее имя</i> (commonName)	<ul style="list-style-type: none"> ■ для физического лица – имя, фамилия и отчество владельца сертификата ■ для юридического лица – наименование организации владельца сертификата
<i>Организация</i> (organizationName)	<ul style="list-style-type: none"> ■ наименование организации владельца сертификата
<i>Фамилия</i> (surname)	<ul style="list-style-type: none"> ■ фамилия владельца сертификата с большой буквы в одно слово (без пробелов)
<i>Имя и отчество</i> (givenName)	<ul style="list-style-type: none"> ■ имя и отчество владельца сертификата
<i>Эл. почта</i> (email)	<ul style="list-style-type: none"> ■ адрес электронной почты владельца сертификата (используются только латинские буквы и цифры)
<i>СНИЛС</i> (snils)	<ul style="list-style-type: none"> ■ строка, состоящая из 11 цифр ■ для физического лица – СНИЛС владельца сертификата ■ для юридического лица – СНИЛС организации владельца сертификата
<i>ИНН</i> (inn)	<ul style="list-style-type: none"> ■ 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)	<ul style="list-style-type: none"> ■ строка, состоящая из 13 цифр ■ ОГРН организации владельца сертификата
ОГРНИП (ogrnip)	<ul style="list-style-type: none"> ■ строка, состоящая из 15 цифр ■ ОГРНИП владельца сертификата
Неструктурир. имя (un)	<ul style="list-style-type: none"> ■ КПП организации владельца сертификата (для ЕГАИС)
Подразделение (organizationUnitName)	<ul style="list-style-type: none"> ■ подразделение или отдел, в котором работает владелец сертификата
Должность (title)	<ul style="list-style-type: none"> ■ должность владельца сертификата
Страна (countryName)	<ul style="list-style-type: none"> ■ 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)	<ul style="list-style-type: none"> ■ для физического лица – название региона, в котором проживает владелец сертификата ■ для юридического лица – название региона, в котором находится организация владельца сертификата
Населенный пункт (localityName)	<ul style="list-style-type: none"> ■ 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)	<ul style="list-style-type: none"> ■ для физического лица – адрес, по которому проживает владелец сертификата ■ для юридического лица – юридический адрес организации владельца сертификата

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 операций, классов пользователей и устройств. Примеры значений смотрите в **Таблице 3**. В данном блоке вы можете задавать и свои значения.

Таблица 3

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 значения поля запроса на сертификат квалифицированной электронной подписи

Для изменения параметра запроса на сертификат квалифицированной электронной подписи необходимо выполнить следующие действия:

1. Запустите **Панель управления Рутокен**.
2. Запустите утилиту.
3. Выберите название шаблона.
4. Щелкните по ссылке "Просмотреть в блокноте". Откроется окно **Шаблон-Основной**.
5. Поставьте курсор мыши в необходимой строке между кавычками и укажите значение параметра.
6. В окне шаблона выберите пункт **Файл** и подпункт **Сохранить как**.
7. Выберите папку для сохранения шаблона на компьютере.
8. Укажите имя файла.
9. Нажмите на кнопку **[Сохранить]**.

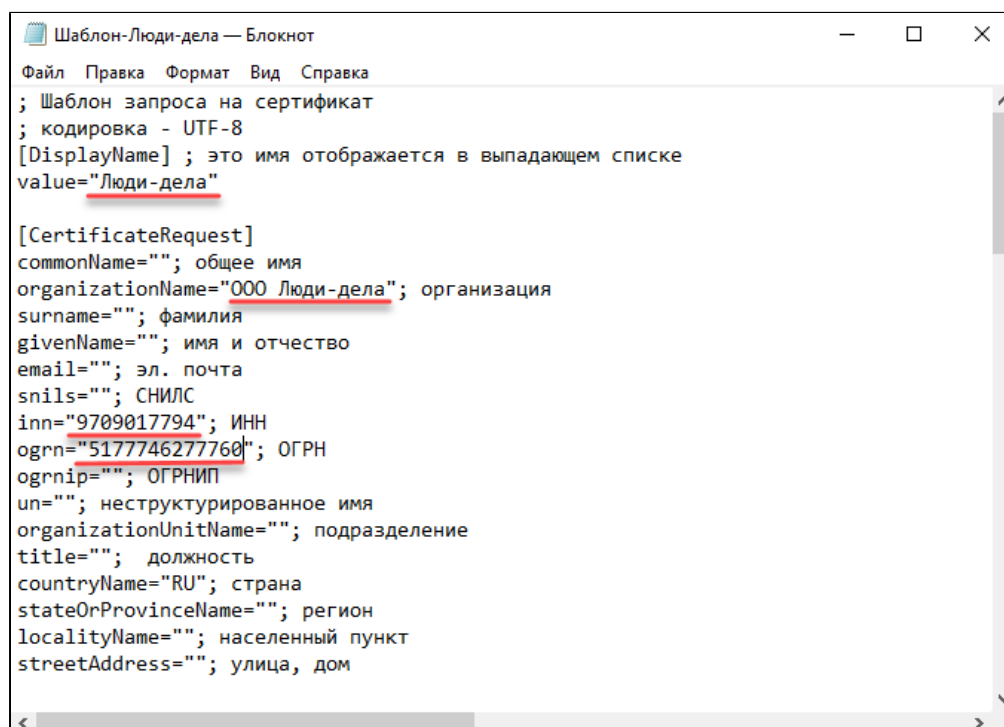
Примеры работы с шаблонами запросов

Пример 1:

Изменения в блоке `[CertificateRequest]`.

1) Изменим следующие параметры запроса на сертификат квалифицированной электронной подписи:

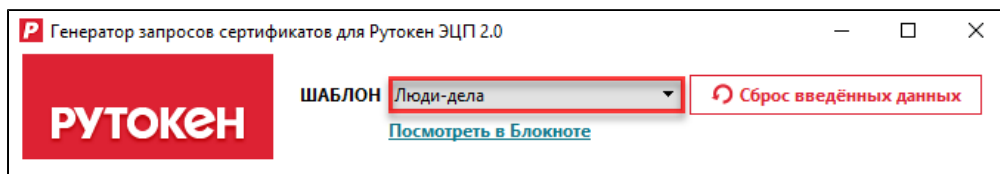
- value;
- organizationName;
- inn;
- ogrn.



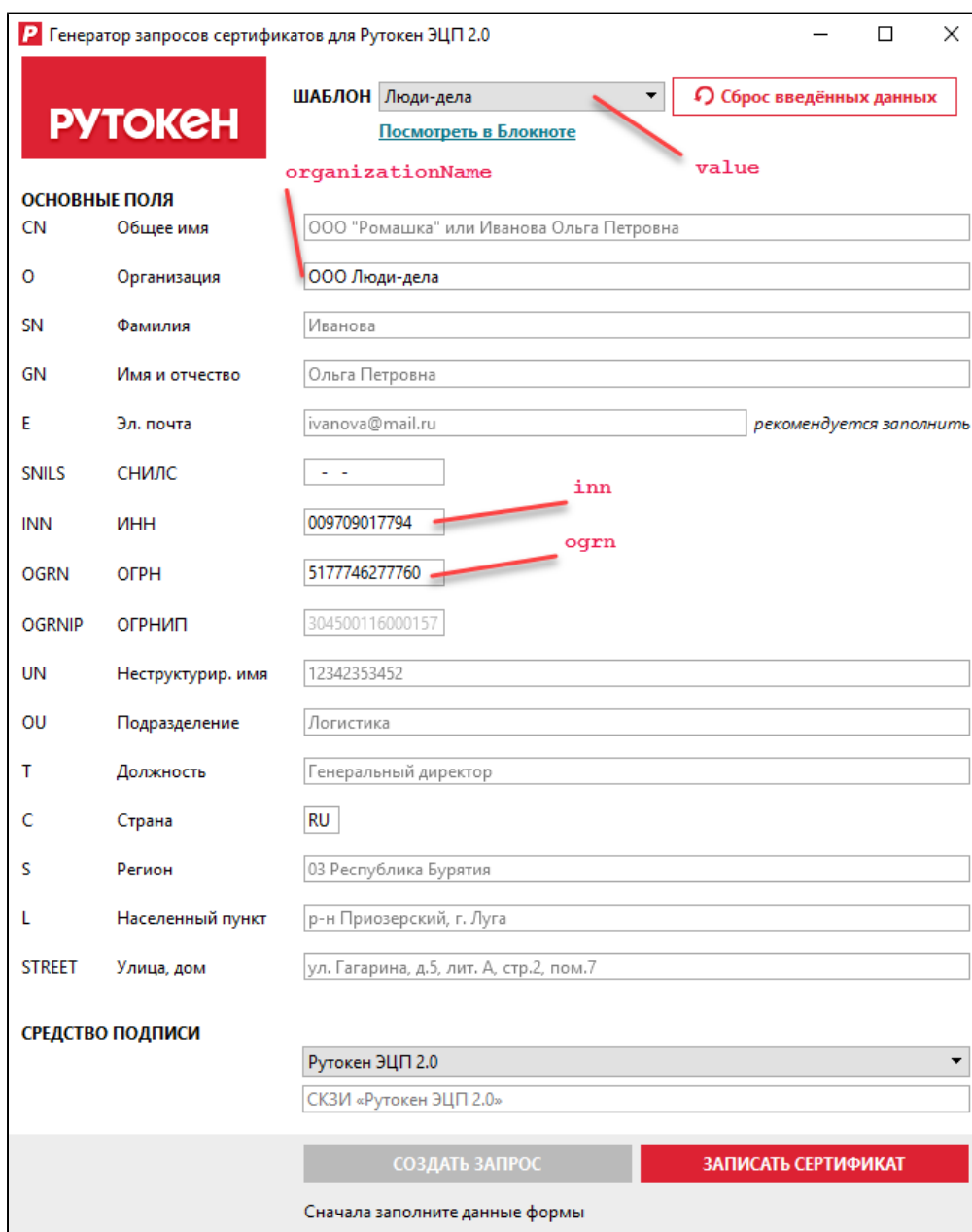
```
Шаблон-Люди-дела — Блокнот
Файл  Правка  Формат  Вид  Справка
; Шаблон запроса на сертификат
; кодировка - UTF-8
[DisplayName] ; это имя отображается в выпадающем списке
value="Люди-дела"

[CertificateRequest]
commonName=""; общее имя
organizationName="ООО Люди-дела"; организация
surname=""; фамилия
givenName=""; имя и отчество
email=""; эл. почта
snils=""; СНИЛС
inn="9709017794"; ИНН
ogrn="5177746277760"; ОГРН
ogrnip=""; ОГРНИП
ip=""; неструктурированное имя
organizationUnitName=""; подразделение
title=""; должность
countryName="RU"; страна
stateOrProvinceName=""; регион
localityName=""; населенный пункт
streetAddress=""; улица, дом
```

- 2) Сохраним новый шаблон на компьютере и назовем его **Люди-дела**.
- 3) Запустим **Панель управления Рутокен**.
- 4) Откроем утилиту.
- 5) 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 criticality= 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>
Веб-сайт содержит большой объем справочной информации об устройствах Рутокен.
WWW: <https://dev.rutoken.ru>
- Портал разработчиков содержит техническую информацию об устройствах Рутокен и руководства по их интеграции.
- База знаний: <https://kb.rutoken.ru/display/kb>
База знаний содержит инструкции по решению большинства ошибок, полезные статьи и ответы на часто задаваемые вопросы. Здесь вы можете найти нужную информацию по ключевым словам.
- Форум: <https://forum.rutoken.ru>
Форум содержит ответы на вопросы пользователей. 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