Инструкция подачи запроса на сертификат с использованием электронной подписи (не требуется посещение территориального органа Федерального казначейства)

Важная информация! Для подачи запроса на сертификат посредством Портала заявителя без посещения ТОФК необходимо наличие выданного в УЦ ФК действующего сертификата ЭП и соответствующего ему действующего ключа ЭП (при условии, что ранее предоставленные в ТОФК сведения не изменились).

Перечень сокращений

Сокращение	Полное наименование
АРМ	Автоматизированное рабочее место
ВРС	Подсистема ведения реестра сертификатов, обеспечивающая ввод, проверку, централизованное хранение сведений, представленных заявителями, информирование владельцев сертификатов и публикацию списка аннулированных сертификатов
ИНН	Идентификационный номер налогоплательщика
ОГРН	Основной государственный регистрационный номер
ПО	Программное обеспечение
Портал заявителя	Онлайн сервис подачи документов для получения сертификатов (https://fzs.roskazna.ru/)
Сертификат	Квалифицированный сертификат ключа проверки электронной подписи
СМЭВ	Система межведомственного электронного взаимодействия
СКЗИ	Средство криптографической защиты информации
СНИЛС	Страховой номер индивидуального лицевого счета
ТОФК	Территориальный орган Федерального казначейства
УЦ ФК	Удостоверяющий центр Федерального казначейства

Системные требования к АРМ пользователя

Минимальные аппаратные требования	
Процессор	Тактовая частота не менее 2,3 ГГЦ
Оперативная память	Не менее 1 024 МБ
Пропускная способность канала	Не менее 1 024 Кбит/сек
Требования к ПО	
Операционная система	Microsoft Windows 7 и выше
Интернет-браузер	Яндекс.Браузер, Браузер «Спутник» с поддержкой отечественной криптографии, Браузер Chromium ГОСТ
Плагин (дополнение) к браузеру	КриптоПро ЭЦП Browser Plug-In версии 2.0 и выше
СКЗИ	СКЗИ «КриптоПро CSP 4.0» и выше

Рекомендуемая скорость подключения к информационно- телекоммуникационной сети «Интернет» от 256 Кбит/сек.

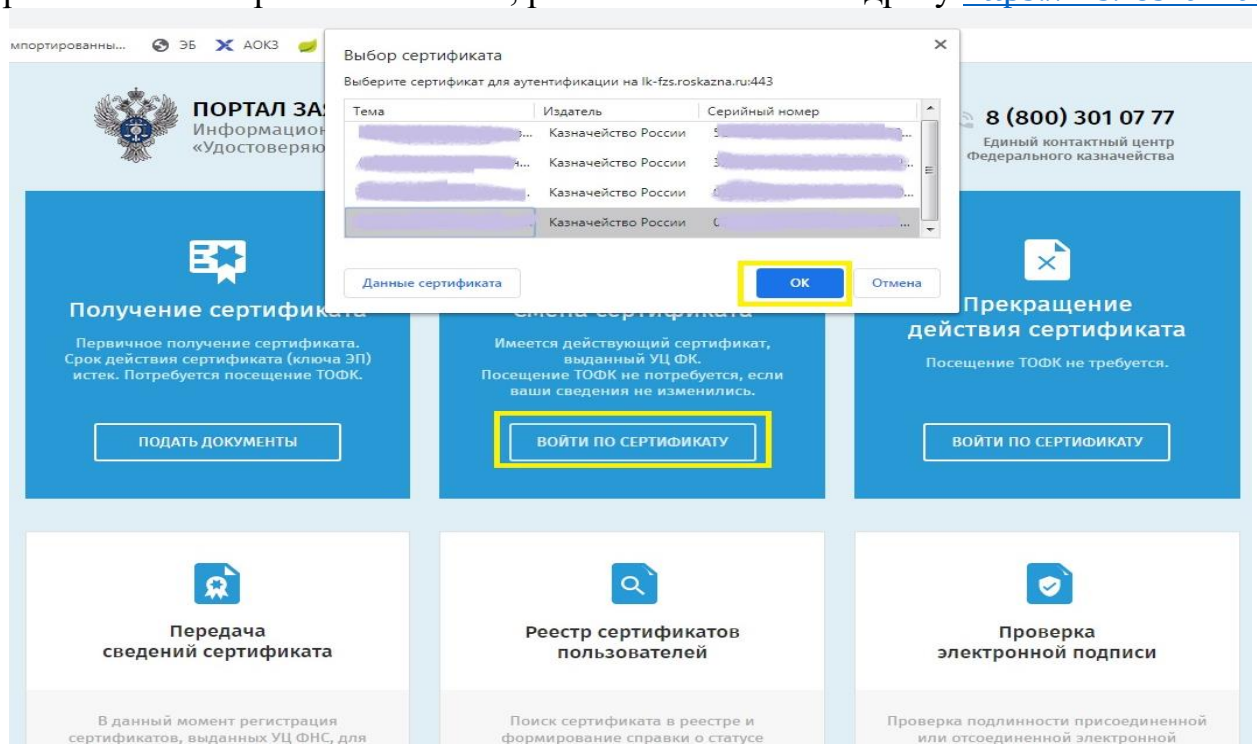
Подготовка к работе

- Обеспечить на АРМ наличие ОС Microsoft Windows 7 или выше.
- Обеспечить на АРМ наличие Интернет-браузера, поддерживающего TLS ГОСТ: Яндекс.Браузер, браузер «Спутник», браузер Chromium ГОСТ.
- Установить сертифицированную версию СКЗИ КриптоПро CSP 4.0 или выше.
- Установить «КриптоПро ЭЦП Browser Plugin» не ниже версии 2.0.
- Подключить ключевой носитель, например: USB-flash накопитель, Рутокен, e-Token.
- Установить сертификаты Минкомсвязи России (ГУЦ) и УЦ ФК ГОСТ Р 34.10-2012 согласно инструкции, размещенной на официальном сайте Федерального казначейства в сети «Интернет» roskazna.gov.ru в разделе «Деятельность» – «Государственные информационные системы» – «Удостоверяющий центр» – «Памятки, инструкции».

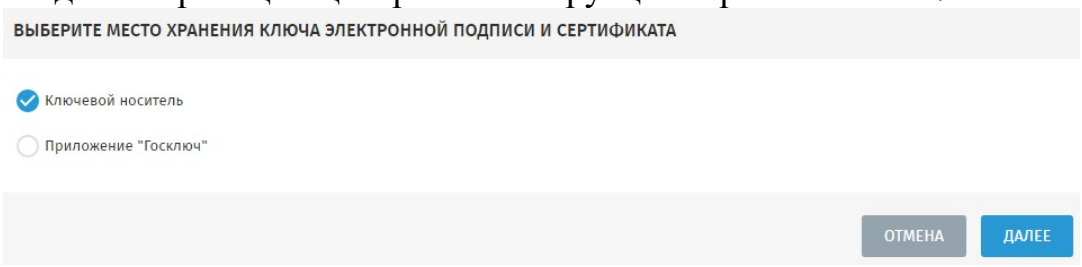
Формирование запроса для смены сертификата

- Для формирования запроса для смены сертификата необходимо выполнить следующие действия:
- Подключить к компьютеру ключевой носитель (Рутокен, eToken и др.).

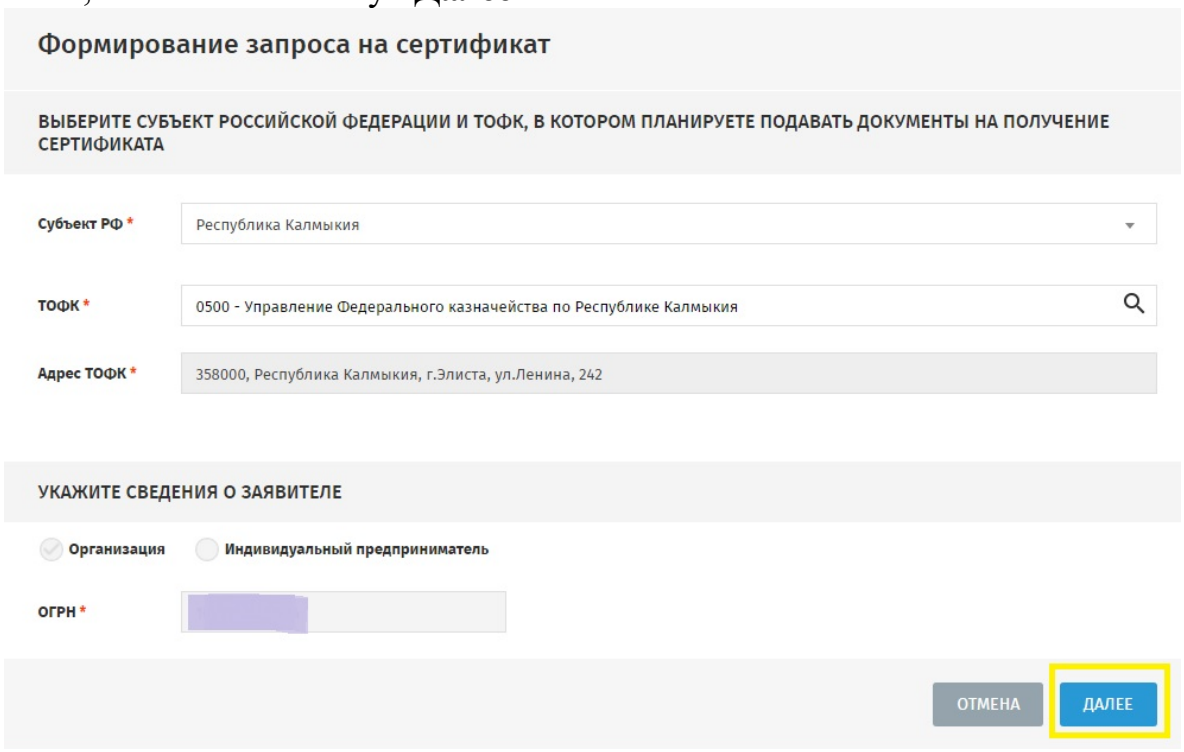
- Осуществить вход в личный кабинет авторизованного пользователя Портала Заявителя, нажав на кнопку **«Войти по сертификату»** в блоке «Смена сертификата» открытой части Портала Заявителя, расположенного по адресу https://fzs.roskazna.ru/



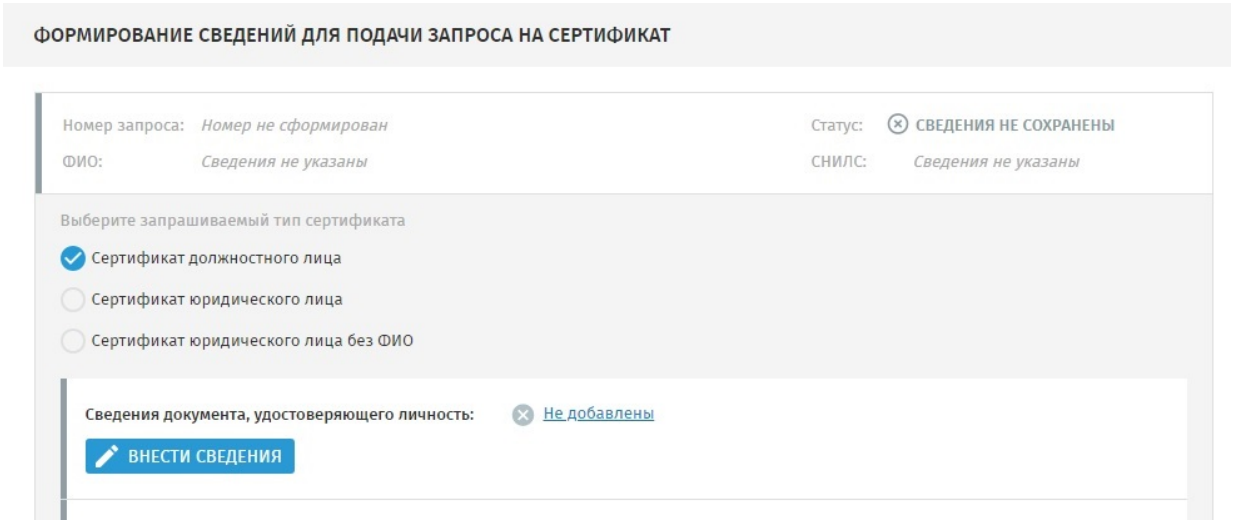
- Далее необходимо отметить галочкой **«Ключевой носитель»** нажать **«Далее»**. Если запрос на сертификат формируется с использованием мобильного приложения «Госключ», ставим галочку **«Приложение Госключ»** и руководствуемся **«Инструкцией подачи запроса на получение сертификата должностного лица с помощью мобильного приложения «Госключ»**, размещенной на официальном сайте Управления Федерального казначейства по Республике Калмыкия в разделе «ГИС» – «Удостоверяющий центр» – «Инструкции и разъяснения».



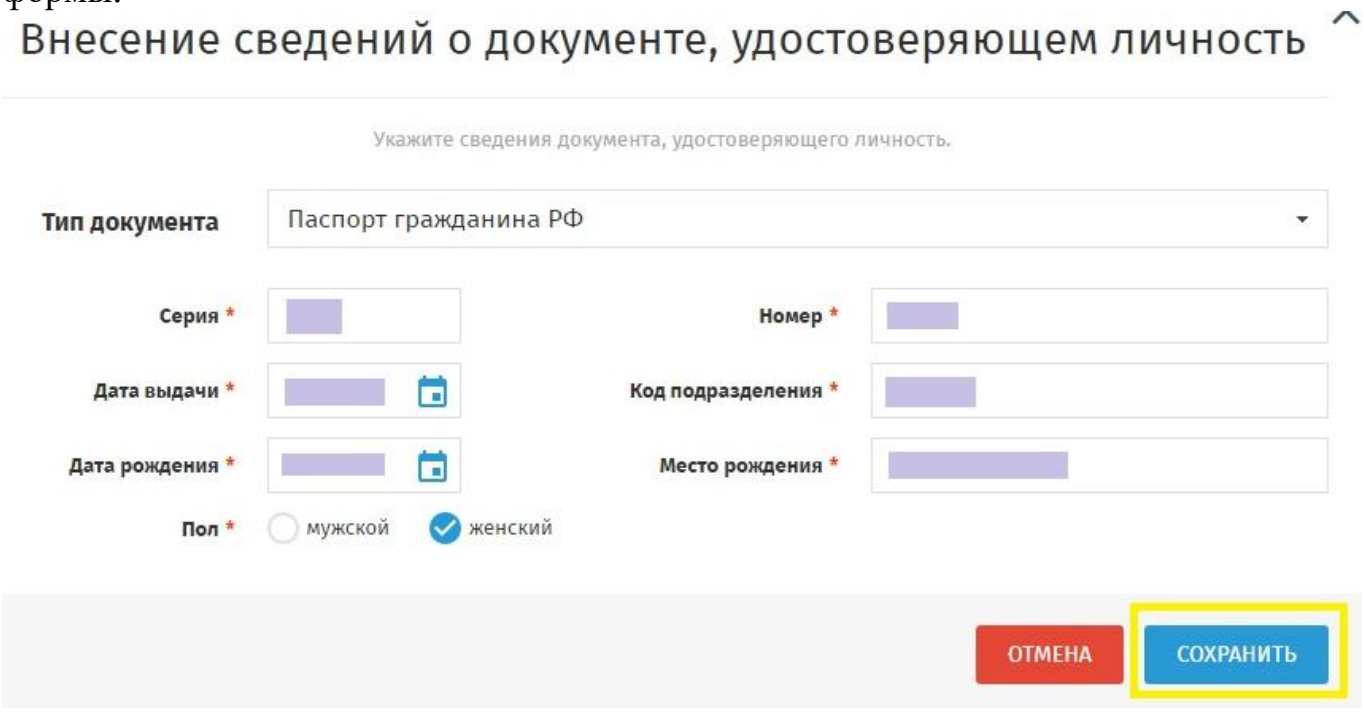
- В отобразившейся форме «Формирование запроса на сертификат» поля уже заполнены, нажимаем кнопку **«Далее»**



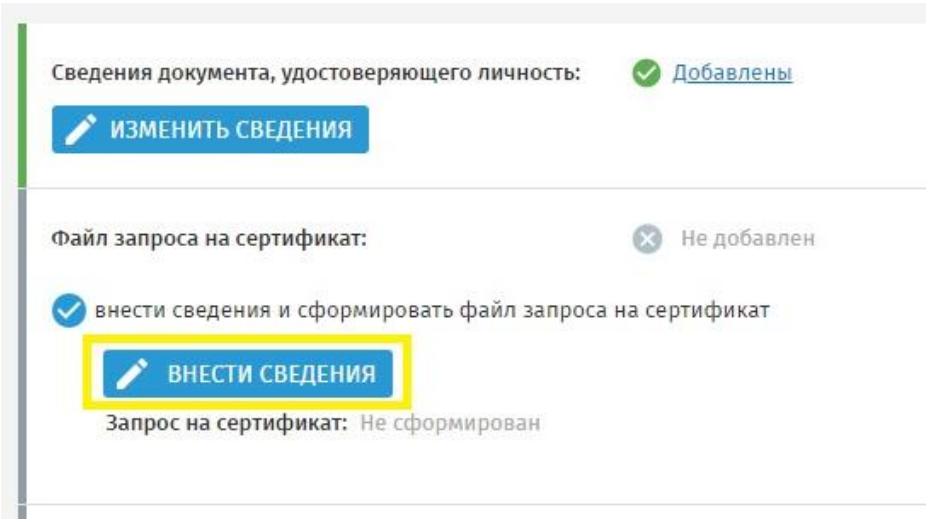
- В следующем блоке необходимо **выбрать запрашиваемый тип сертификата** и в поле «Сведения документа, удостоверяющего личность» нажать **«внести сведения»**.



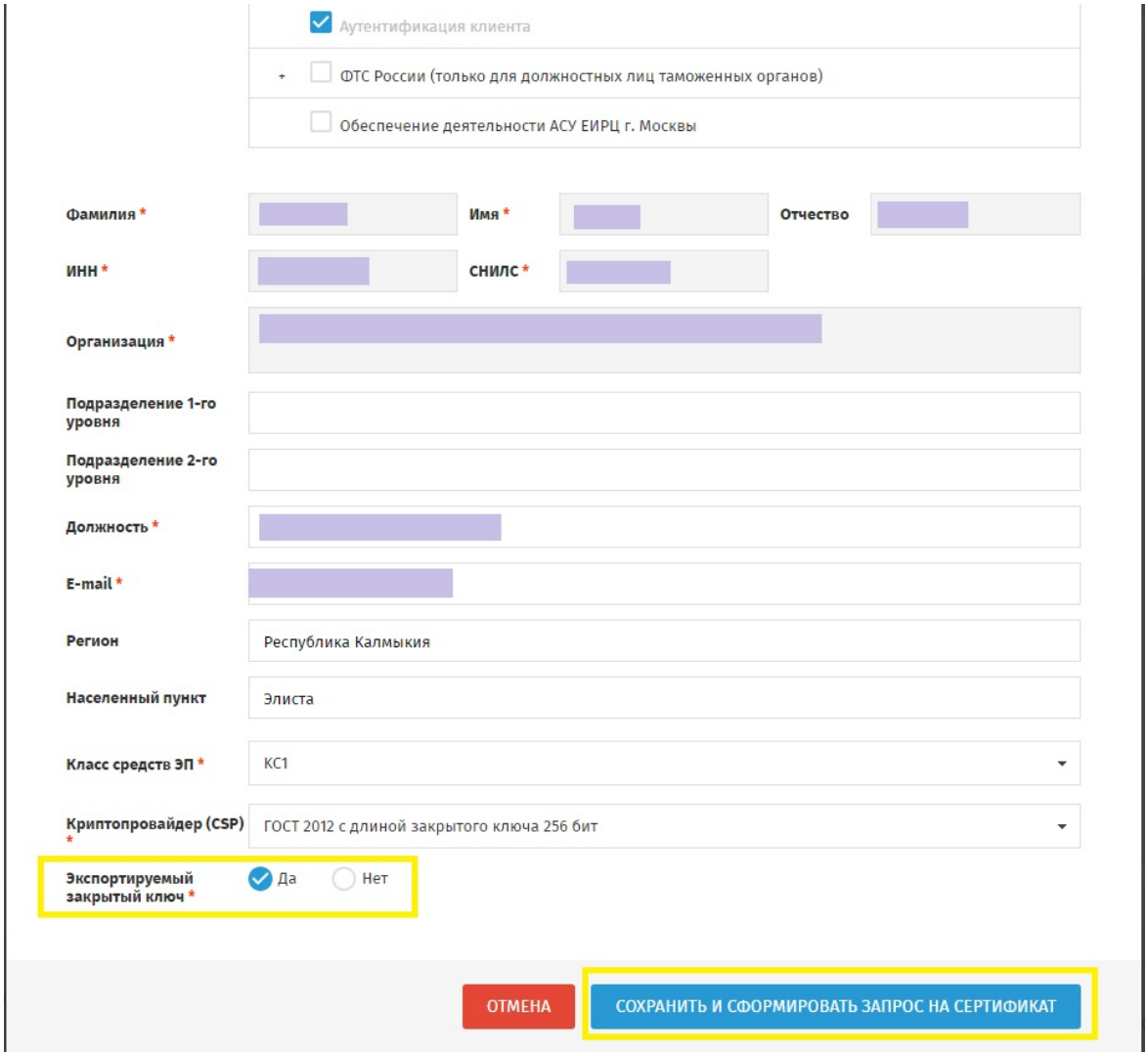
- В отобразившейся форме «Внесение сведений о документе, удостоверяющем личность» поля уже заполнены, нажимаем кнопку **«Сохранить»**. В случае изменения паспортных данных необходимо отредактировать поля формы.



- В следующем поле «Файл запроса на сертификат» нажмите кнопку **«Внести сведения»**.



- В отобразившейся форме «Формирование запроса на сертификат» укажите полномочия, необходимые для работы в информационных системах.



Примечание: **при формировании запроса на основании существующего сертификата нажмите на кнопку «Обзор» и выберите необходимый файл. Поля формы в этом случае заполнятся сведениями, указанными в выбранном сертификате.**

В поле **«Должность»** укажите должность, в соответствии с приказом о назначении на должность.

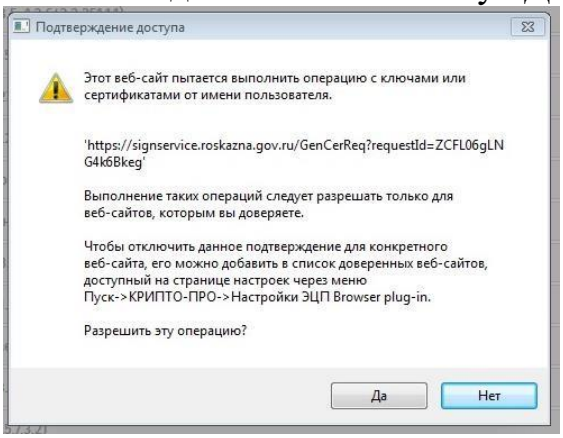
На указанный, в поле **«E-mail»** электронный адрес, будут приходить сообщения о смене статуса запроса на сертификат, и изготовленный сертификат **(указывайте актуальную почту, к которой у вас есть непосредственный доступ).**

Поля «Класс средств ЭП» и «Криптопровайдер (CSP)» оставляем без изменений. **Поле «Экспортируемый закрытый ключ»: галочка «нет» – копирование закрытого ключа будет не возможно; галочка «да» – закрытый ключ можно будет копировать.**

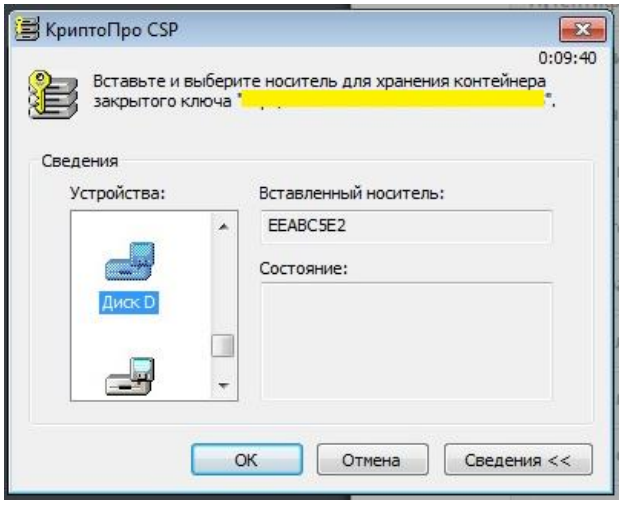
- После внесения сведений нажмите на кнопку **«Сохранить и сформировать запрос на сертификат»**. На форме «Создание запроса на сертификат» нажать **«Сформировать»**.

Важно! Формирование запроса осуществляется с использованием СКЗИ «КриптоПро CSP 4.0» и выше. Для формирования запроса необходимо подключить ключевой носитель (Рутокен, флеш-накопитель и т.п.) к АРМ.

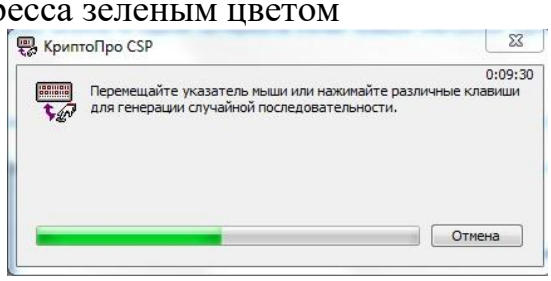
- Далее в появившемся окне необходимо нажать кнопку **«Да»**



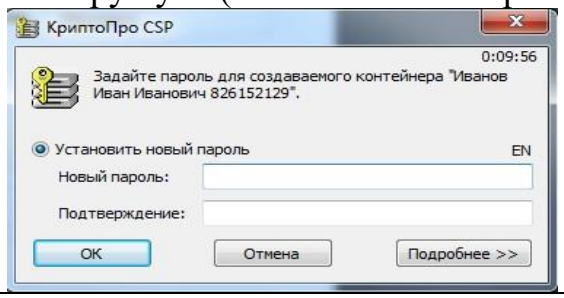
Откроется окно выбора носителя информации для хранения контейнера закрытого ключа. Выберите подключенный ключевой носитель и нажмите **«Ок»**



Далее выполняйте требования появившегося окна, «Перемещайте указатель мыши или нажимайте различные клавиши для генерации последовательности» до полного заполнения полосы прогресса зеленым цветом



В появившемся окне необходимо задать пароль для подписи, будьте внимательны к языковой раскладке и к регистру букв (заглавные или строчные)



РЕКОМЕНДУЕМ устанавливать стойкие пароли не менее 6 символов с использование букв различного регистра (заглавные или строчные), цифры и спецсимволы.

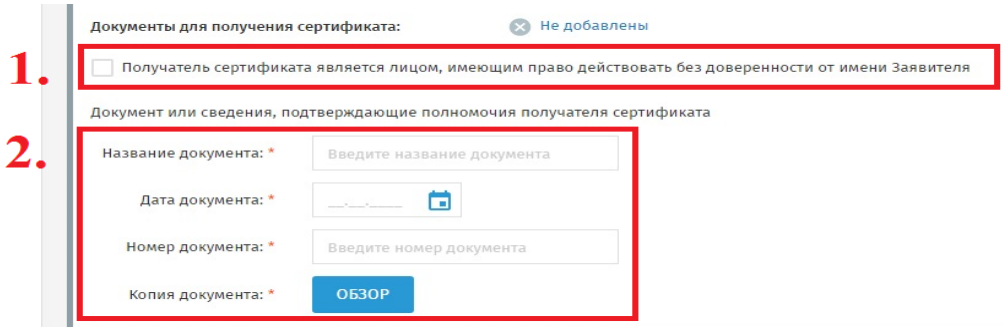
!!! ВНИМАНИЕ !!!

Если пользователь забудет пароль, электронную подпись необходимо формировать заново! Сотрудники отдела РСиБИ не знают установленного Вами пароля, восстановить или сбросить пароль без знания старого невозможно!

После генерации запроса на сертификат владелец должен обеспечивать хранение носителя ключевой информации с ключом электронной подписи в соответствии с установленными требованиями (приказ ФАПСИ от 13.06.2001 № 152).

- На вновь отобразившемся блоке «Формирование сведений для подачи запроса на сертификат» в разделе «Документы для получения сертификата» необходимо заполнить:

1. В случае, если Получатель сертификата является лицом, имеющим право действовать без доверенности от имени Заявителя **(указан в ЕГРЮЛ)**, необходимо установить признак **«Получатель сертификата является лицом, имеющим право действовать без доверенности от имени Заявителя»**;
2. Если Получатель сертификата не является лицом, имеющим право действовать без доверенности от имени Заявителя, необходимо заполнить поля **«название документа, дата документа, номер документа»**, а также посредством нажатия кнопки **«Обзор»** прикрепить сканированный образ документа, подтверждающего замещение Заявителем соответствующей должности (заверенная копия приказа о назначении на должность или выписка из приказа о назначении на должность или заверенная копия трудовой книжки или справка о замещении должности за подписью руководителя). **Скан-копия документа должна быть цветной и читаемой!!!**



Заверение копии документа оформляется в соответствии с пунктом 5.26 **ГОСТ Р 7.0.97-2025** (утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 26 июня 2025 г. № 622-ст).

Образец заверения документов для представления в УЦ ФК

ТЕКСТ ДОКУМЕНТА

Подпись руководителя

Верно

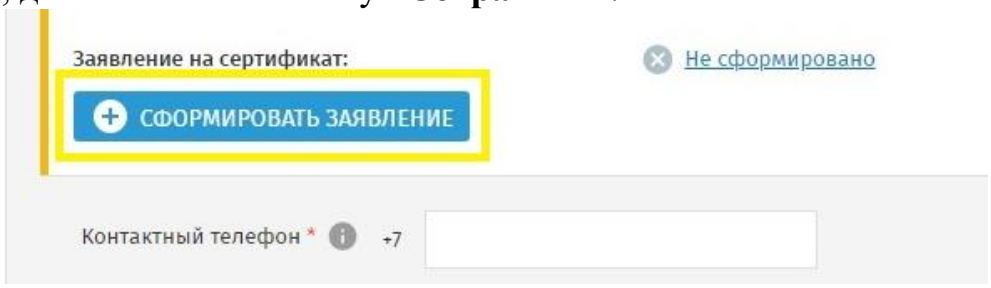
Должность лица, заверившего копию Подпись И.О. Фамилия (указывается без сокращений)

Дата заверения

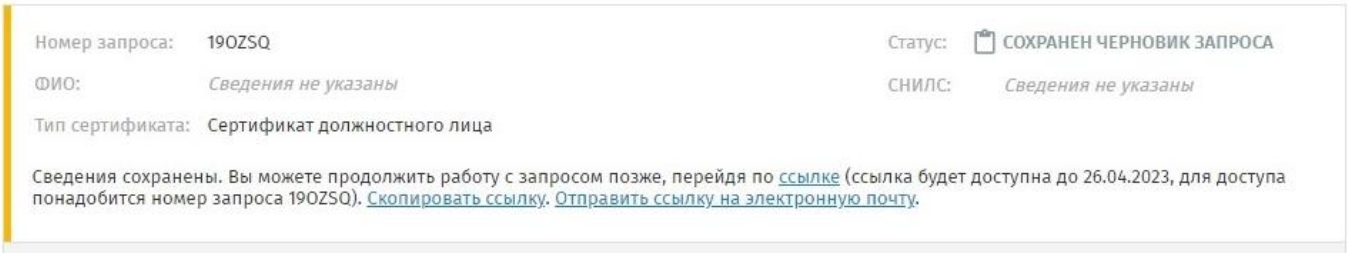
Подлинник документа находится в (наименование организации) в деле №…….... за ……..... год

Печать организации

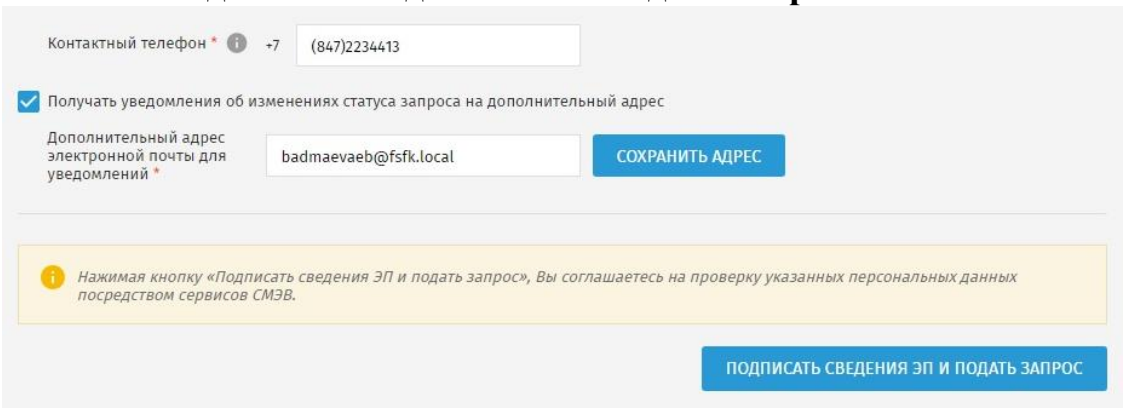
- В разделе «Заявление на сертификат» нажмите на кнопку **«Сформировать заявление»**, далее нажмите кнопку **«Сохранить»**.



Важно! Для доступа к карточке запроса необходимо предварительно сохранить ссылку на запрос и его номер.



- Далее необходимо заполнить поле **«Контактный телефон»** в формате «(XXX)XXXXXXX», указать (если нужно) дополнительный адрес электронной почты и нажать **«Подписать сведения ЭП и подать запрос»**.



- На вопрос «Подписать сведения электронной подписью?» нажмите «Да», далее нажмите «Подписать ЭП», на вопрос «Разрешить эту операцию?» нажимаем «Да». Выбираем сертификат нажимаем «Подписать», далее нажимаем «Ок».

Запрос сформирован и отправлен на проверку в «Сервис Межведомственного Электронного Взаимодействия». На этом процесс формирования электронного запроса завершен.

ВНИМАНИЕ! После направления запроса в СМЭВ срок подготовки ответа может составлять до 5 рабочих дней.

При получении извещения об отказе, расхождении внесенных данных с СМЭВ необходимо пройти по ссылке в сообщении и ознакомится с причиной отказа. При выявлении расхождений предоставленных сведений с данными, содержащимися в информационных базах МВД России, ФНС России и СФР необходимо руководствоваться **разделом II «Типовые рекомендации для получателей квалифицированных сертификатов ключей проверки электронных подписей (далее - сертификат) в территориальных органах Федерального казначейства»** размещенные на официальном сайте Федерального казначейства в сети «Интернет» roskazna.gov.ru в разделе «Деятельность» – «Государственные информационные системы» – «Удостоверяющий центр» – «Памятки, инструкции»

!!! ВНИМАНИЕ !!!

Специалисты казначейства не имеют возможности вносить изменения в информационные базы МВД России, ФНС России и СФР

В случае успешных проверок запроса в СМЭВ, запрос передается на обработку в УЦ ФК

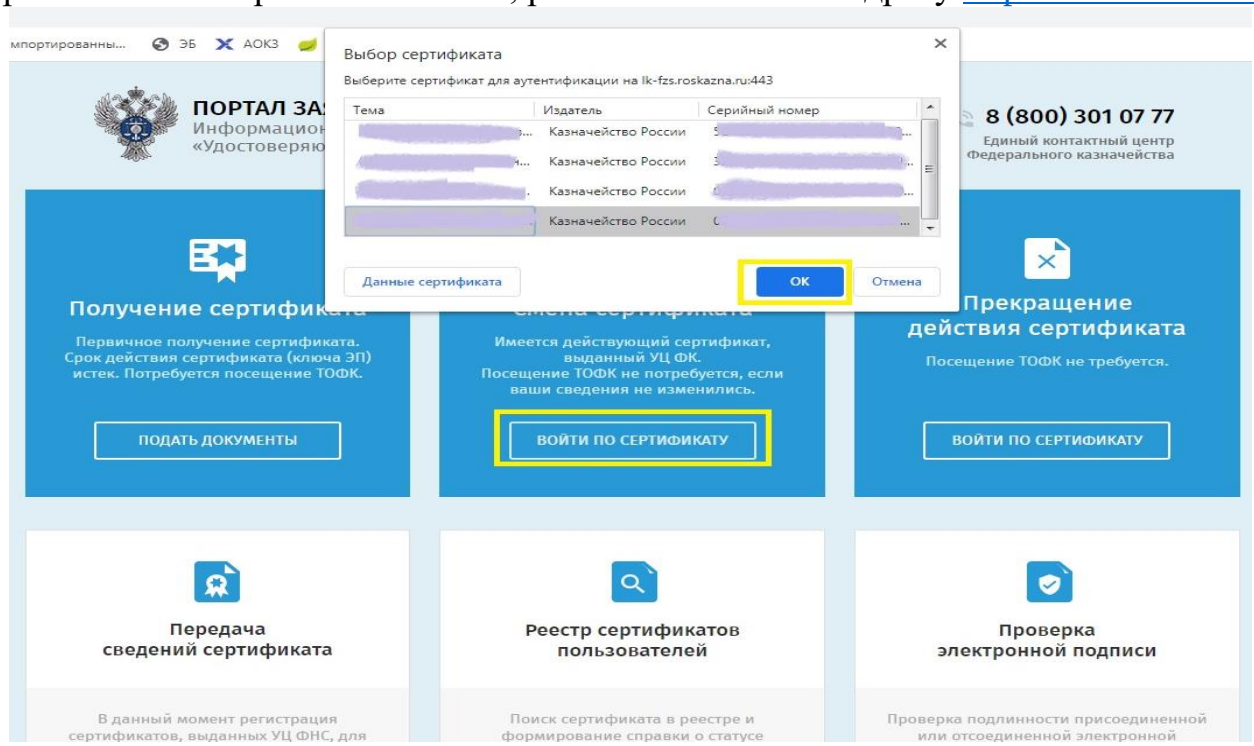
Оператор УЦ ФК осуществляет проверку комплекта электронных документов на создание сертификата. В случае положительного результата проверки, Оператор УЦ согласовывает запрос на сертификат, и осуществляет создание сертификата. Получателю сертификата направляется соответствующее уведомление на адрес электронной почты и появляется возможность получить сертификат в личном кабинете Портала заявителя.

Если Оператор УЦФК отклоняет запрос, запрос переходит в статус «Отклонен», о чем Получателю сертификата направляется соответствующее уведомление на адрес электронной почты.

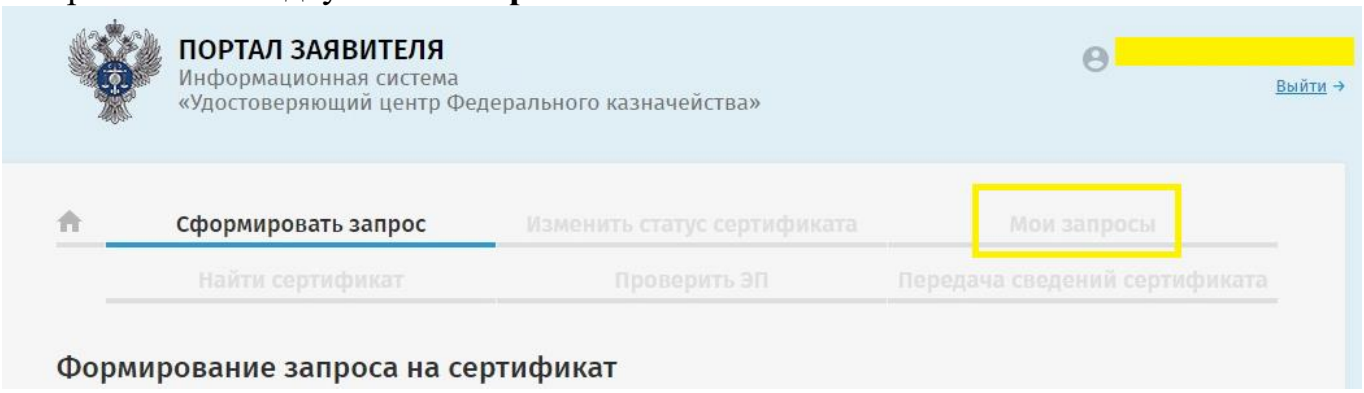
Скачивание готового сертификата Получателем сертификата

- Для скачивания готового сертификата Получателю сертификата необходимо выполнить следующие действия:

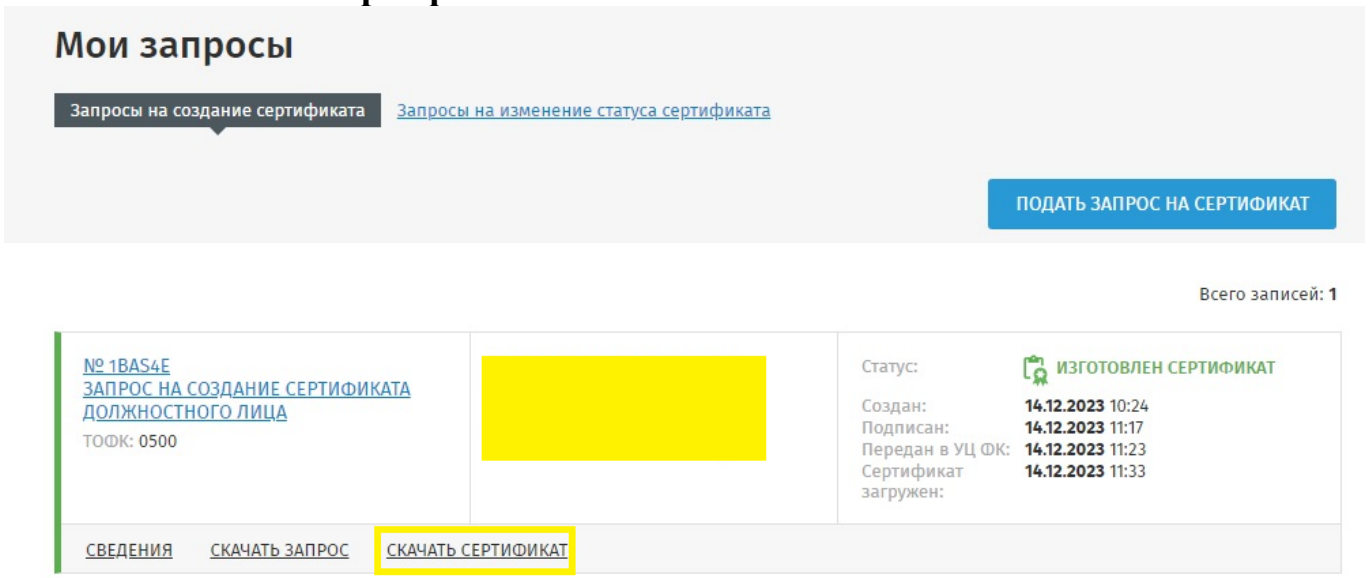
- Осуществить вход в личный кабинет авторизованного пользователя Портала Заявителя, нажав на кнопку **«Войти по сертификату»** в блоке «Смена сертификата» открытой части Портала Заявителя, расположенного по адресу https://fzs.roskazna.ru/



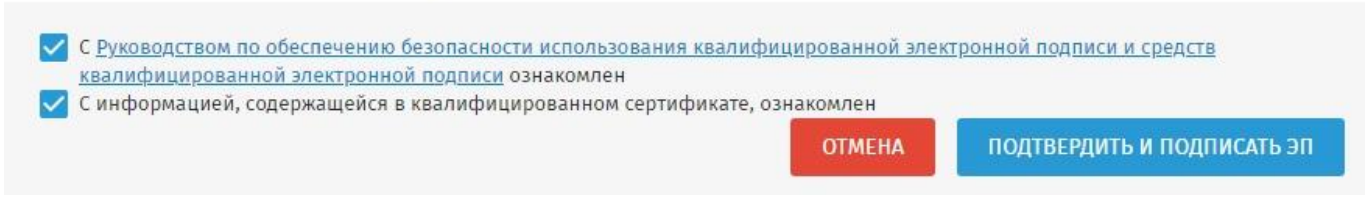
- Перейти на вкладку **«Мои запросы»**.



- Нажать **«Скачать сертификат»**.



- Отметить **чек-боксы** и нажать **«Подтвердить и подписать ЭП»**.



- На вопрос «Подписать сведения электронной подписью?» нажмите «Да», далее нажмите «Подписать ЭП», на вопрос «Разрешить эту операцию?» нажимаем «Да». Выбираем сертификат нажимаем «Подписать», начнется скачивание сертификата.