

Генерация неизвлекаемых ключей по стандарту PKCS#11 для ЕГАИС (Росалкогольрегулирование)

Модели Рутокен с аппаратной криптографией, которые подойдут для генерации ключей для ЕГАИС

- Рутокен ЭЦП 3.0 3220, серт. ФСБ
- Рутокен ЭЦП 2.0 2100, серт. ФСБ (USB/micro/Type-C)
- Рутокен ЭЦП 2.0 3000, серт. ФСБ (USB/micro/Type-C)
- Рутокен ЭЦП 2.0 Flash, серт. ФСБ
- Смарт-карта Рутокен ЭЦП 2.0 2100, серт. ФСБ
- Рутокен ЭЦП 2.0 (2000), серт. ФСБ (USB/micro)

Неизвлекаемые ключи изначально генерируются внутри устройства, подписание происходит «на борту» с использованием аппаратной криптографии токена. Какая-либо возможность извлечения или копирования закрытого ключа отсутствует.

ВАЖНО! При генерации ключевой пары по алгоритму ГОСТ Р 34.10 - 2012 следует выбирать короткий ключ 256 бит.

С ключами длиной 512 бит УТМ не работает. При подключении к УТМ ключа с длиной закрытой части 512 бит в логах УТМ будет **ошибка**

Способы генерации неизвлекаемых ключей по стандарту PKCS#11 для ЕГАИС:

- Модели Рутокен с аппаратной криптографией, которые подойдут для генерации ключей для ЕГАИС
- Способы генерации неизвлекаемых ключей по стандарту PKCS#11 для ЕГАИС:
 - Способ 1. С использованием «КриптоПро CSP» версии 5.0 R2 и новее
 - Способ 2. С использованием «Генератора запросов сертификатов для Рутокен ЭЦП 2.0 и 3.0»
 - Способ 3. С использованием программы «КриптоАРМ» 5 версии

Способ 1. С использованием «КриптоПро CSP» версии 5.0 R2 и новее

Для Windows советуем скачать **сертифицированную версию «КриптоПро CSP» со встроенными модулями pkcs#11** с официального сайта компании «КриптоПро» (для скачивания требуется предварительная регистрация). **В случае установки этой версии «КриптоПро CSP», установка Драйверов Рутокен не обязательна.**

Сертифицированные версии

- КриптоПро CSP 5.0 R2 для Windows, **Windows с pkcs#11**, macOS, UNIX, Android и JavaCSP
- КриптоПро CSP 5.0 для Windows, macOS, UNIX и Android
- КриптоПро CSP 4.0 R4 для Windows, macOS и UNIX
- КриптоПро CSP 4.0 R3 для Windows, macOS и UNIX

Корректное заполнение расширения 1.2.643.100.111

Модель	значение
Рутокен ЭЦП 3.0 3220	СКЗИ "Рутокен ЭЦП 3.0"
Рутокен ЭЦП 2.0 2100	СКЗИ "Рутокен ЭЦП 2.0 2100"
Рутокен ЭЦП 2.0 (2000)	СКЗИ "Рутокен ЭЦП 2.0"
Рутокен ЭЦП 2.0 micro	СКЗИ "Рутокен ЭЦП 2.0 micro"
Рутокен ЭЦП 2.0 3000	СКЗИ "Рутокен ЭЦП 2.0 3000"
Рутокен ЭЦП 2.0 3000 micro	СКЗИ "Рутокен ЭЦП 2.0 3000 micro"
Рутокен ЭЦП 2.0 3000 Type-C	СКЗИ "Рутокен ЭЦП 2.0 3000 Type-C"
Рутокен ЭЦП 2.0 Flash	СКЗИ "Рутокен ЭЦП 2.0 Flash"
Смарт-карта Рутокен ЭЦП 2.0 2100	СКЗИ "Смарт-карта Рутокен ЭЦП 2.0"

Может быть полезно

Инструкция: [Переход на УТМ ЕГАИС 4](#)

Установка в Windows

- Если на компьютере с ОС Windows установлены Драйверы Рутокен, и производится **первичная установка** КриптоПро CSP 5.0 R2, то **настройка системы будет выполнена автоматически**.
- При **обновлении** программы с **предыдущих версий КриптоПро CSP**, необходимо:

- 1) Установить актуальную версию «Драйверов Рутокен».
- 2) Запустить «КриптоПро CSP» с правами Администратора.
- 3) Выбрать «Оборудование» — «Настроить считыватели» — «Считыватель смарт-карт PKCS#11».

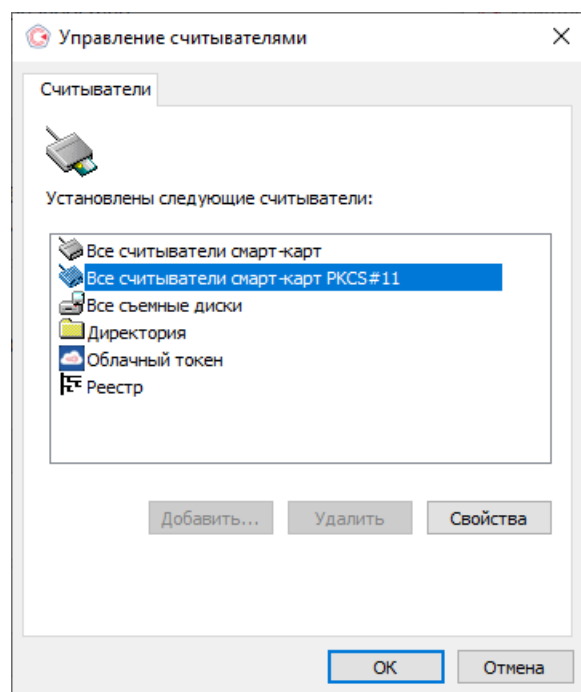
Установка в Linux

Перед установкой КриптоПро CSP необходимо установить библиотеку rtpkcs11esp.so, она доступна <https://www.rutoken.ru/support/download/pkcs/>.

- Если установка КриптоПро происходит скриптом install_gui.sh, то необходимо отметить пункт "Поддержка токенов и смарт-карт".
- Если установка КриптоПро происходит скриптом install.sh, то после установки основных пакетов необходимо установить пакеты cproscsp-rdr-cryptoki и cproscsp-rdr-rutoken.

В «КриптоПро CSP» версии 5.0 R2 и выше в разделе «Оборудование» — «Настроить считыватели» должен быть добавлен пункт «Все считыватели смарт-карт PKCS#11».

Если такого пункта нет, **запустите «КриптоПро CSP» с правами Администратора** и в этом окне добавьте считыватели, нажав на кнопку «Добавить...»



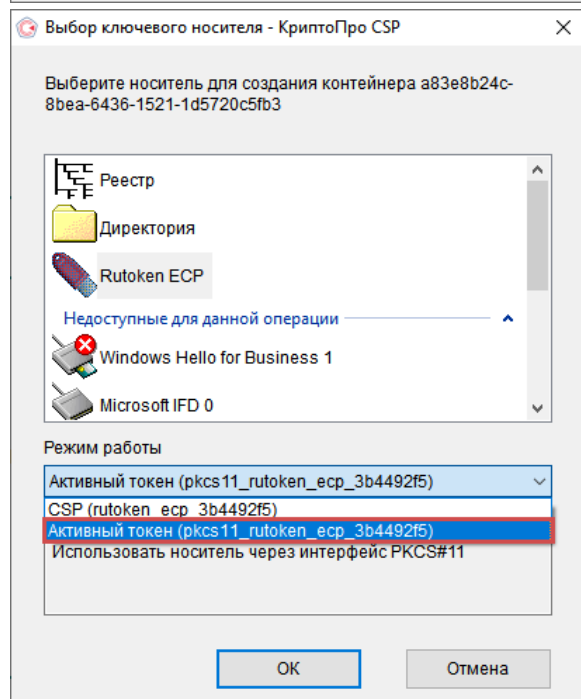
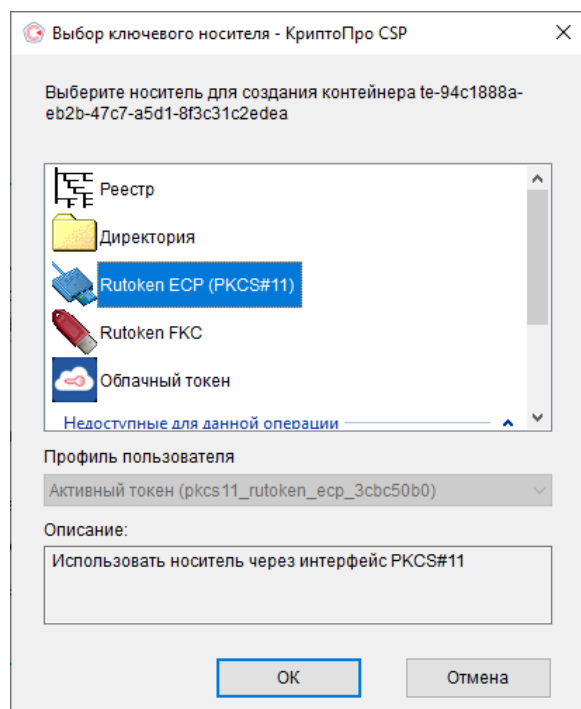
Если такой вариант считывателя отсутствует, удалите «КриптоПро CSP» и, убедившись, что вы устанавливаете версию 5.0 R2 или выше, еще раз ее установите.

- 1) Установите актуальную версию [Драйверов Рутокен](#).
- 2) Подключите устройство из семейства Рутокен ЭЦП 2.0/3.0 к компьютеру.
- 3) При генерации ключей нужно использовать версию «КриптоПро CSP» **версии 5.0 R2 или новее**.

4) В окне выбора ключевого носителя выберите режим, который позволяет работать с внутренним криптоядром Рутокена через библиотеку PKCS#11.

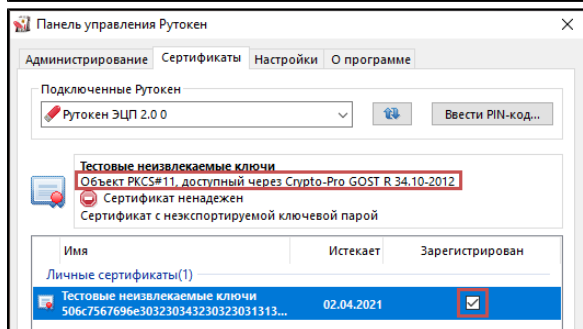
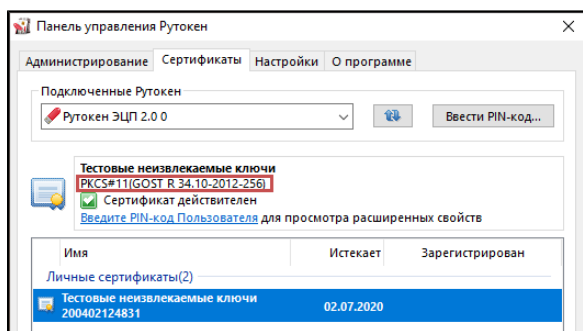
У вас может быть один из двух вариантов (зависит от версии КриптоПро CSP):

- Вариант 1. Выберите в списке носителей «**Rutoken ECP (PKCS#11)**».
- Вариант 2. Выберите в списке носителей «**Rutoken ECP**», а в выпадающем списке "**Активный токен (pkcs11_rutoken_ecp_XXXXX)**".

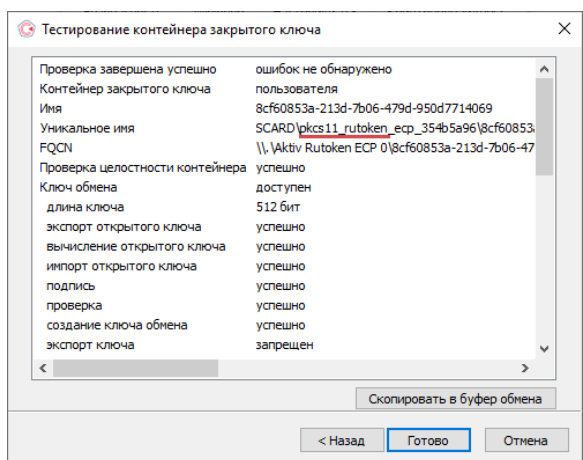


5) После генерации ключей и записи сертификата на Рутокен, проверьте формат ключей одним из двух способов:

- Способ 1. Через «Панель управления Рутокен»: вкладка "Сертификаты".



- Способ 2. Через «КриптоПро CSP»: вкладка «Сервис» — «Протестировать...» .



Способ 2. С использованием «Генератора запросов сертификатов для Рутокен ЭЦП 2.0 и 3.0»

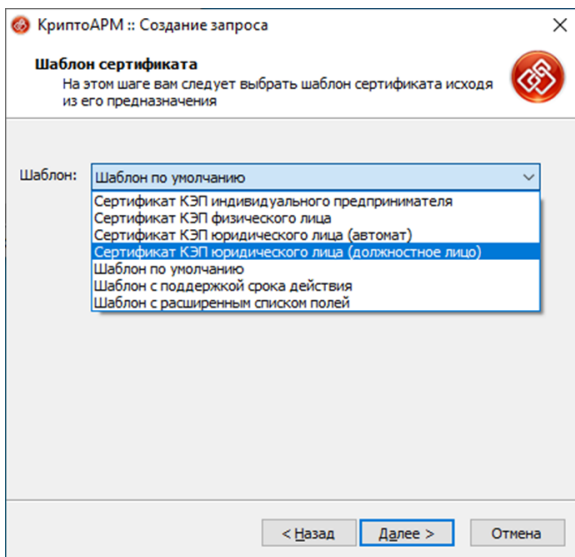
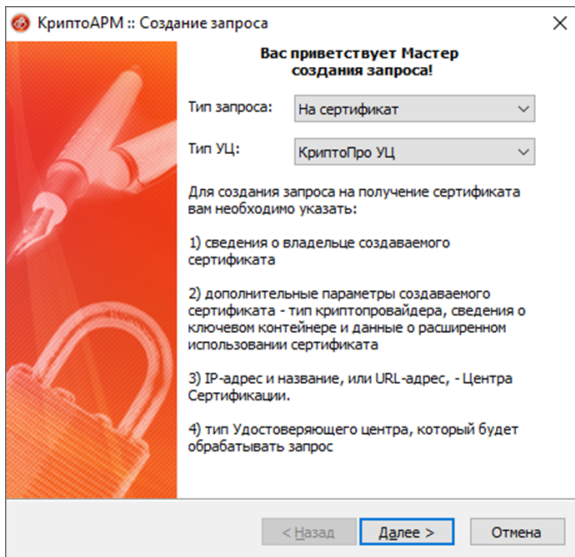
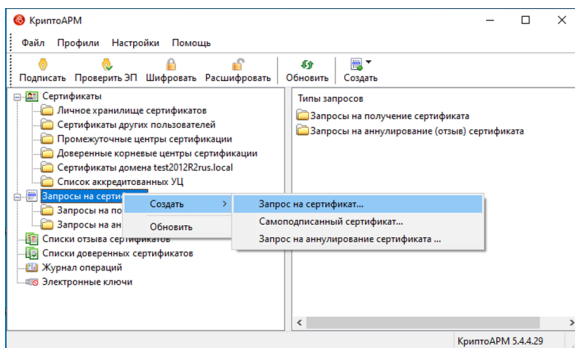
«Генератор запросов сертификатов для Рутокен ЭЦП 2.0 и 3.0» входит в состав Драйверов Рутокен.

- 1) Установите актуальную версию [Драйверов Рутокен](#).
- 2) Подключите устройство из семейства Рутокен ЭЦП 2.0/3.0 к компьютеру.
- 3) Запустите «Панель управления Рутокен».
- 4) Перейдите на вкладку «Сертификаты».
- 5) Нажмите кнопку «Ввести PIN-код» и введите PIN-код Администратора.
- 6) Нажмите на кнопку «Выписать сертификат», откроется приложение:

Далее используйте [Инструкцию по работе с Генератором запросов](#).

Способ 3. С использованием программы «КриптоАРМ» 5 версии

Для генерации неизвлекаемых ключей можно использовать программу [КриптоАРМ 5](#).



КриптоАРМ :: Создание запроса

Основная информация

Указанные на этом шаге параметры будут храниться в поле "Subject" созданного сертификата

Идентификационная информация

Общее имя (CN)*:

Страна*:

Регион*:

Населенный пункт*:

Адрес:

ОГРНИП*:

СНИЛС*:

ИНН*:

< Назад

Далее >

Отмена

КриптоАРМ :: Создание запроса

Параметры ключа

На этом шаге вам следует указать параметры ключа, связанного с сертификатом

Используемый криптопровайдер:

РутOKEN ЭЦП 2.0

☒ Создать новый ключевой набор

☐ Использовать существующий ключевой набор

Имя ключевого набора:

e91404c2-3a69-4fdc-9ebd-38a5d92380e4

Выбрать...

Назначение ключа

☐ Создание ЭП

Длина ключа: Нет

☐ Шифрование

Дополнительно...

☒ Шифрование и создание ЭП

Дополнительно...

☐ Пометить ключи как экспортируемые

< Назад

Далее >

Отмена

КриптоАРМ :: Создание запроса

Выбор дополнительных параметров

Выберите дополнительные параметры

☒ Сохранить запрос в файл

Имя:

C:\Users\user1\Desktop\тест.pem

Выбрать

☐ Отправить запрос по электронной почте

☐ Отправить запрос по сети

☐ Напечатать свойства сформированного запроса

< Назад

Далее >

Отмена

КриптоАРМ :: Создание запроса

Статус
Данные для создания запроса на получение сертификата собраны.

Параметры

Данные владельца:

Общее имя (CN)	test
Страна	RU
Регион	MSK
Населенный пункт	Москва
ОГРНИП	308655158917
СНИЛС	72892898072
Криптопровайдер	Рутокен ЭЦП

Параметры ключа

Ключевой контейнер	e91404c2-3a69-4fdc-9ebd-38a5d92380e4
Назначение ключа	Шифрование и
Использование ключа	Подпись данн
Назначение сертификата	1.3.6.1.5.5.7.1
Имя файла запроса	C:\Users\user1

< Назад Готово Отмена

Введите PIN-код (пароль)

Ключ: e91404c2-3a69-4fdc-9ebd-38a5d92380e4

Осталось попыток: 1

Токен: Rutoken ECP <no label> (3dbc50b) ▾

PIN-код: ●●●●●●●●

OK Отмена Детали

КриптоАРМ

Файл Профили Настройки Помощь

Подписать Проверить ЭП Шифровать Расшифровать Обновить Фильтр Создать

Сертификаты

- Личное хранилище сертификатов
- Сертификаты других пользователей
- Промежуточные центры сертификации
- Доверенные корневые центры сертификации
- Сертификаты домена test2012R2rus.local
- Список аккредитованных УЦ

Запросы на сертификат

- Запросы на получение сертификата
- Запросы на аннулирование (отзыв) сертификата

Списки отзыва сертификатов

Списки доверенных сертификатов

Журнал операций

Электронные ключи

Владелец: test Дата: 10.12.2021

КриптоАРМ 5.4.4.29