

Неизвлекаемые ключи на Рутокенах в КриптоПро CSP 5.0 R2

«КриптоПро» CSP 5.0 R2 это новое поколение криптопровайдера, с добавлением поддержки неизвлекаемых ключей. Работа производится с внутренним криптоядром Рутокена.

Ключи создаются сразу в защищенной памяти устройства с помощью:

- «КриптоПро CSP» версии 5.0 R2
- «Рутокен Плагин»
- «Генератор запросов сертификатов для Рутокен ЭЦП 2.0»

или других приложений.

Использование такого типа ключей предотвращает извлечение ключа в память компьютера в момент подписания.

Поддержка новых форматов неизвлекаемых ключей добавлена в комплект «Драйверов Рутокен» начиная с версии 4.8.5. Обязательно их обновите.

- Рутокен ЭЦП 3.0 3100
- Рутокен ЭЦП 3.0 3100 NFC
- Рутокен ЭЦП 2.0 2100;
- Рутокен ЭЦП 2.0 (micro);
- Рутокен ЭЦП 2.0 3000 (Type-C/micro);
- Рутокен ЭЦП 2.0 Flash/Touch;
- Рутокен ЭЦП Bluetooth;
- Рутокен ЭЦП PKI;
- Рутокен 2151
- Смарт-карты Рутокен ЭЦП 2.0 2100;
- Смарт-карты Рутокен ЭЦП SC.

Преимущества использования

Универсальность — неизвлекаемые ключи в связке с «КриптоПро CSP» версии 5.0 R2 совместимы с большинством криптографических плагинов: КриптоПро Browser Plug-In, Рутокен Плагин, IFCPlugin.

Можно использовать в системах: ЕГАИС, «Честный знак», Портал Госуслуг, nalog.ru, на торговых площадках и т.д. А это значит, один ключ может быть использован в большинстве систем.

Безопасность — ключи неизвлекаемые, а значит надежно защищены от экспорта или копирования.

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](#)

Установка в Windows

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

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

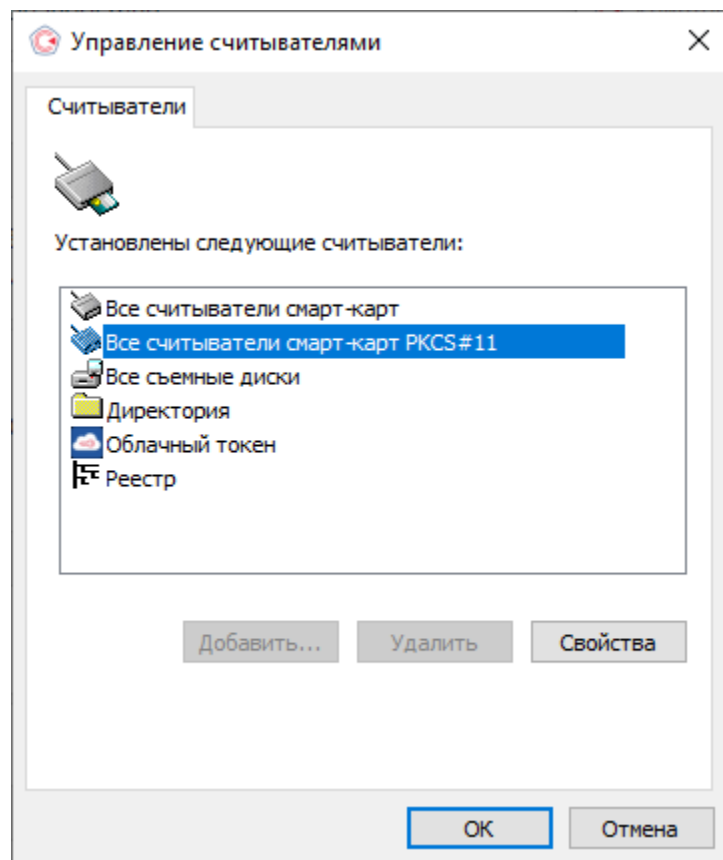
Установка в Linux

Перед установкой КристоПро CSP необходимо установить библиотеку [rtpkcs11ecp.so](https://www.rutoken.ru/support/download/pkcs/), она доступна <https://www.rutoken.ru/support/download/pkcs/>.

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

В «КристоПро 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 «КристоПро CSP» с правами Администратора](#) и в этом окне добавьте считыватели, нажав на кнопку «Добавить...»



Если такой вариант считывателя отсутствует, удалите «КристоПро 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.

Способы генерации

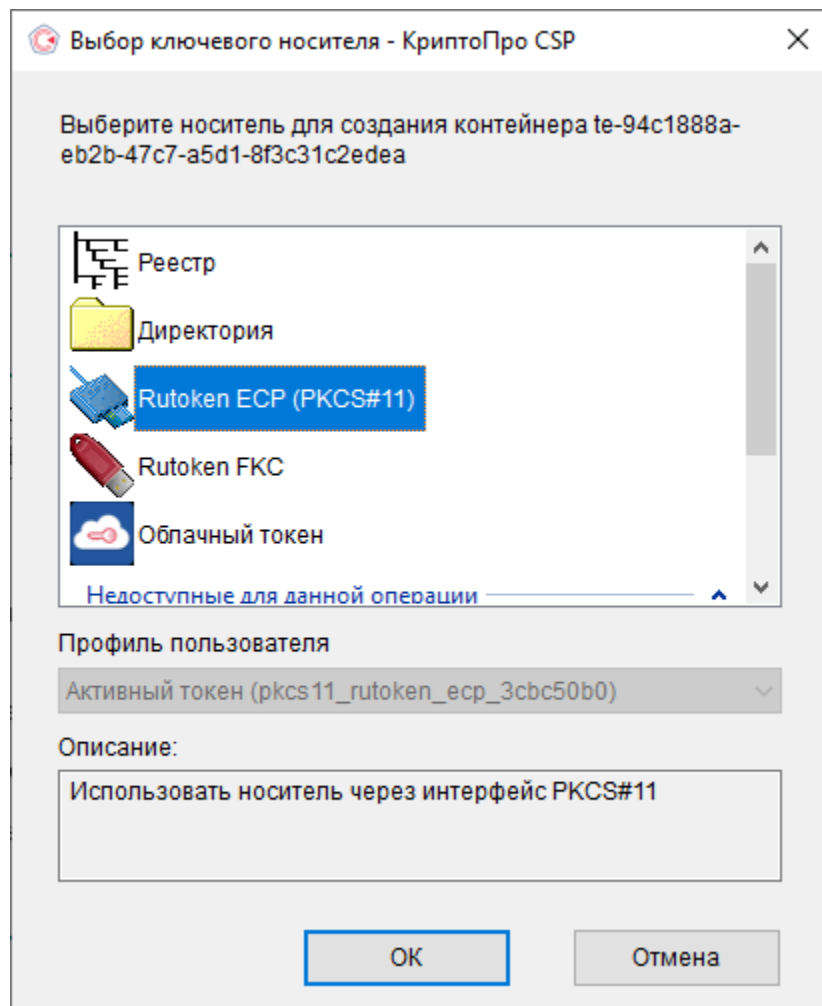
Генерация с использованием «КриптоПро CSP» версии 5.0 R2

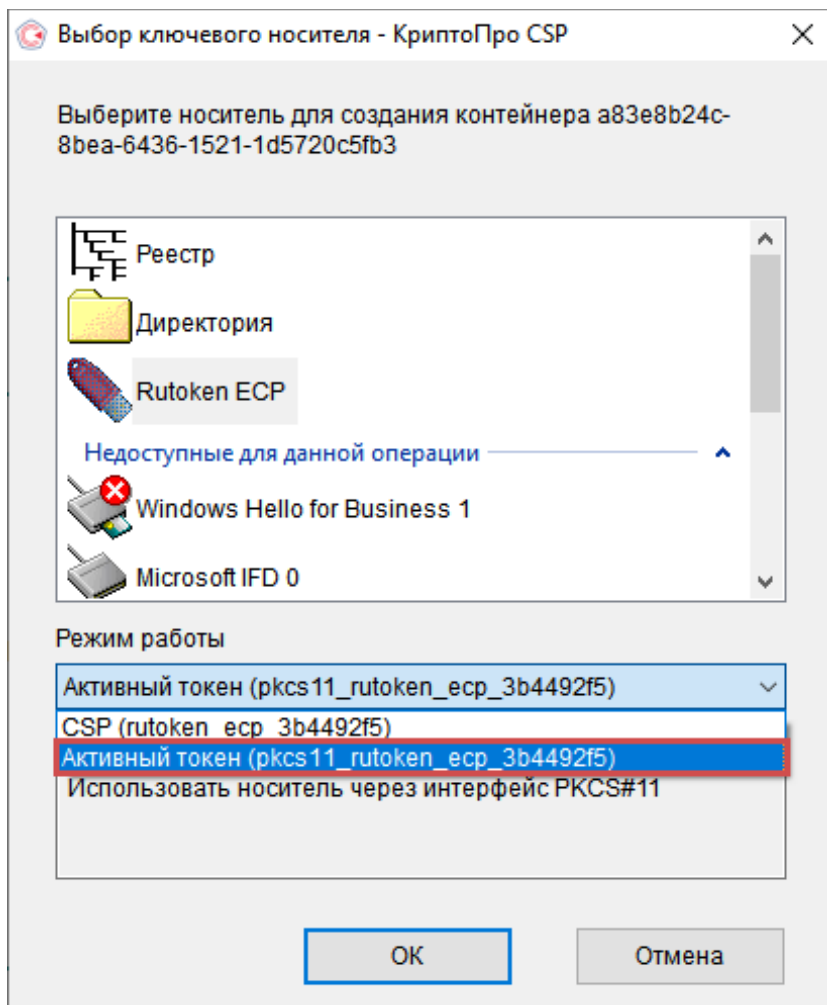
При генерации ключей нужно использовать версию «КриптоПро CSP» версии 5.0 R2 или новее.

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

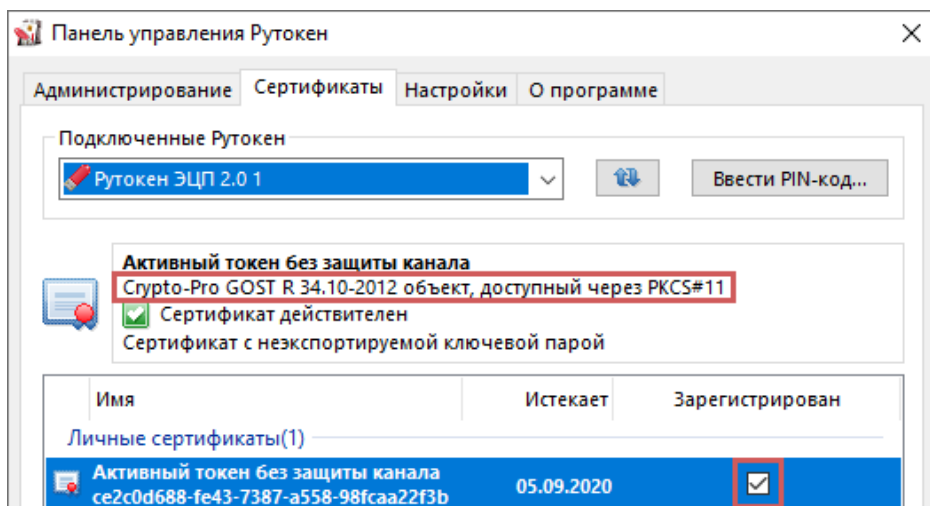
У вас может быть один из двух вариантов (зависит от версии КриптоПро CSP):

- 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)".



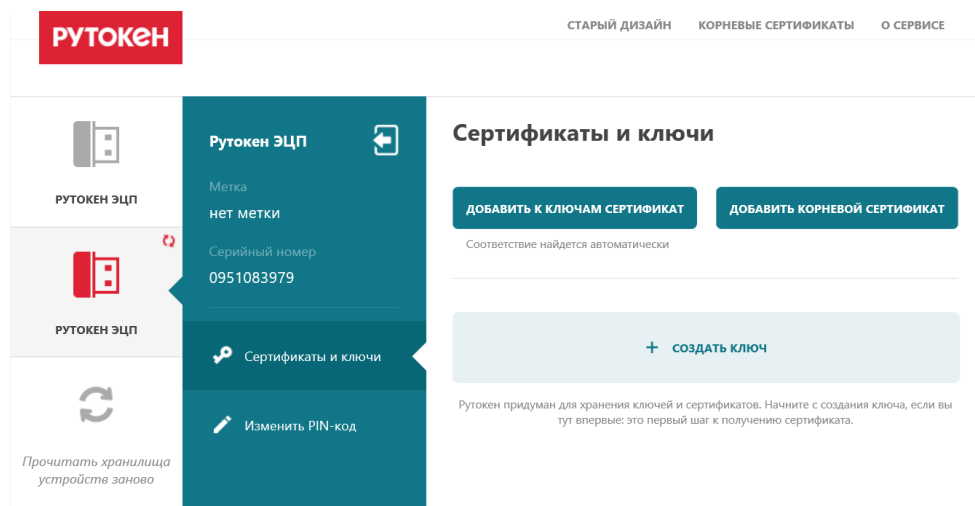


В «Панели управления Рутокен» такие ключи будут отображаться как «Crypto-Pro GOST объект, доступный через PKCS#11»

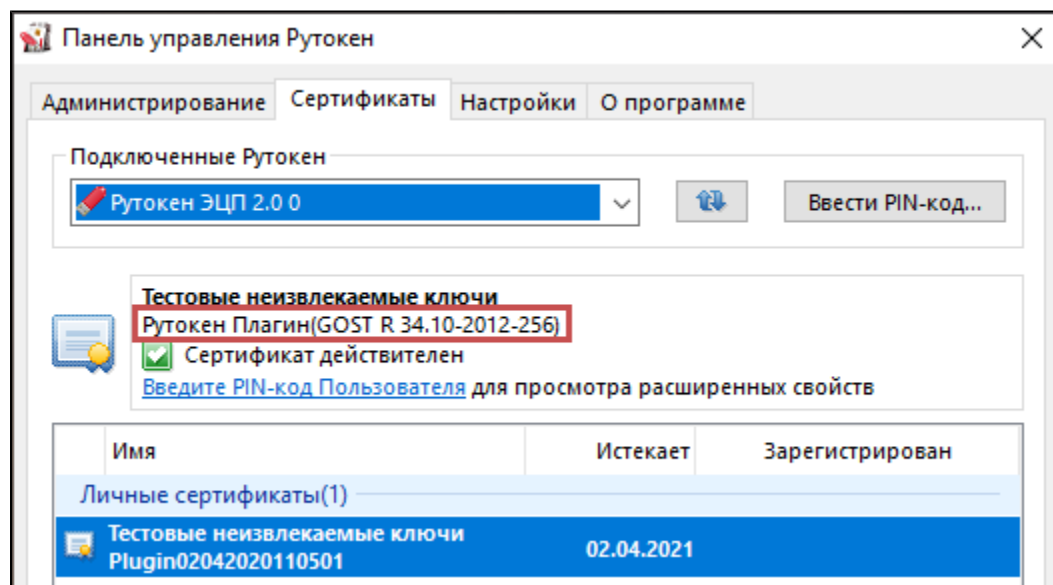


Генерация с помощью Рутокен Плагина

Сгенерировать такие ключи можно с помощью портала ra.rutoken.ru или используя интерфейс javascript «Рутокен Плагин».



В «Панели управления Рутокен» такие ключи будут отображаться как «Рутокен Плагин».



Генерация с помощью утилиты «Генератор запросов сертификатов для Рутокен ЭЦП 2.0»

Воспользоваться утилитой «Генератор запросов», которая входит в состав [Драйверов Рутокен](#) и доступна на нашем сайте в разделе: [Центр загрузки](#) — [Драйверы для Windows](#) — [Утилиты](#).

Генератор запросов сертификатов для Рутокен ЭЦП 2.0

РУТОКЕН ШАБЛОН Пример для ГОСТ 2012-256 [Сброс введенных данных](#)

[Посмотреть в Блокноте](#)

ОСНОВНЫЕ ПОЛЯ

CN Общее имя ООО "Ромашка"

O Организация ООО "Ромашка"

SN Фамилия Иванова

GN Имя и отчество Ольга Петровна

E Эл. почта ivanova@mail.ru рекомендуется записать

SNILS СНИЛС - -

INN ИНН 006104001458

OGRN ОГРН 1117746358608

OGRNI ОГРНИП 3045001160003

UN Неструктурир. 12342353452

OU Подразделение Логистика

T Должность Генеральный директор

C Страна RU

S Регион 03 Республика Бурятия

L Населенный пу г-н Полюховский, г. Луга

STREET Улица, дом ул. Гагарина, д.5, лит. А, стр.2, пом.7

СРЕДСТВО ПОДПИСИ Рутокен ЭЦП 2.0
СММ Рутокен ЭЦП 2.0

СОЗДАТЬ ЗАПРОС **ЗАПИСАТЬ СЕРТИФИКАТ**

В «Панели управления Рутокен» такой сертификат будет отображаться как **«PKCS#11 GOST»**.

Панель управления Рутокен

Администрирование Сертификаты Настройки О программе

Подключенные Рутокен

Рутокен ЭЦП 2.0 0 **Ввести PIN-код...**

Тестовые неизвлекаемые ключи
PKCS#11(GOST R 34.10-2012-256)
Сертификат действителен
[Введите PIN-код Пользователя](#) для просмотра расширенных свойств

Имя	Истекает	Зарегистрирован
Личные сертификаты(2)		
Тестовые неизвлекаемые ключи 200402124831	02.07.2020	

Или, при наличии на компьютере программы КриптоПро CSP версии 5.0, такие ключи будут называться **«Объект PKCS#11, доступный через CryptoPro GOST»**.

Панель управления Рутокен

Администрирование Сертификаты Настройки О программе

Подключенные Рутокен

Рутокен ЭЦП 2.0 1 **Ввести PIN-код...**

Объект PKCS#11, доступный через Crypto-Pro GOST R 34.10-2012
Сертификат действителен
Сертификат с неэкспортируемой ключевой парой

Имя	Истекает	Зарегистрирован
Личные сертификаты(1)		
19080101	01.11.2020	☒

