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.

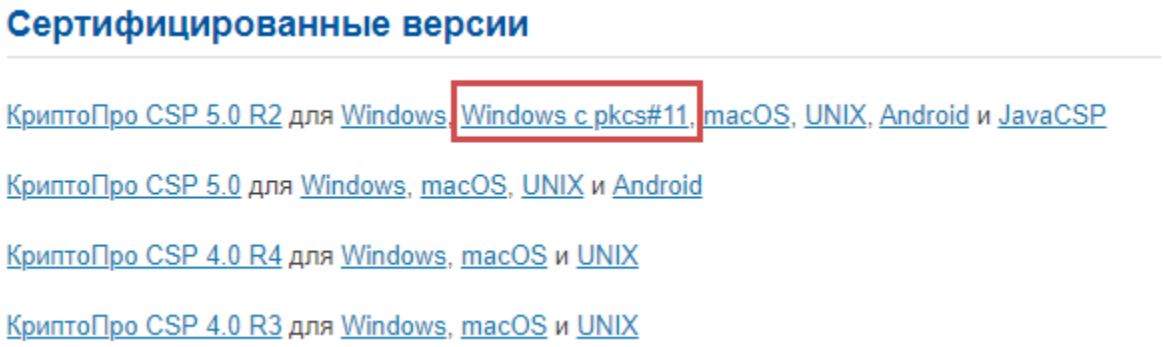
Преимущества использования

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.**



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».

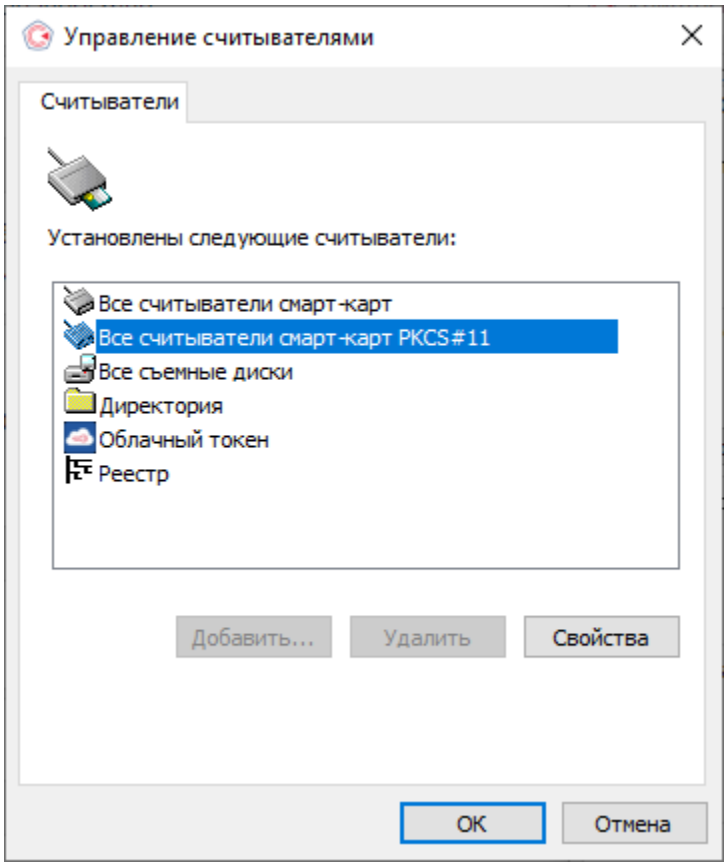
Установка в Linux

Перед установкой КриптоПро CSP необходимо установить библиотеку rtpkcs11ecp.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 cprocsp-rdr-cryptoki и cprocsp-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.

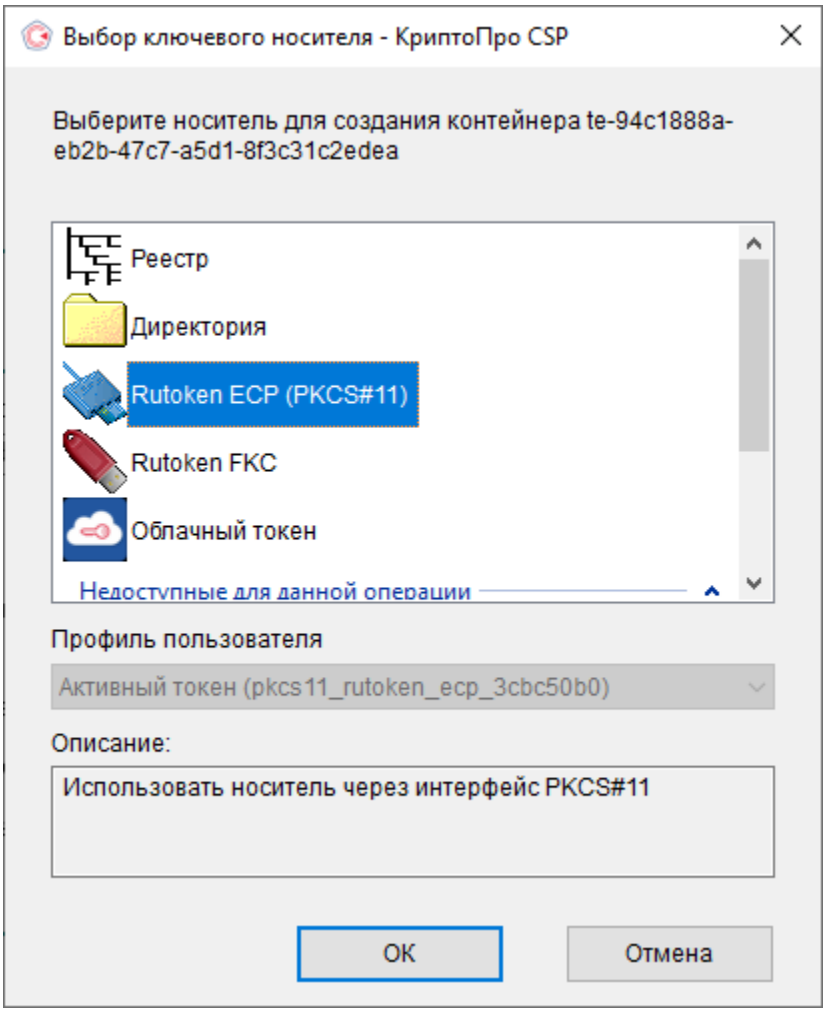
Способы генерации

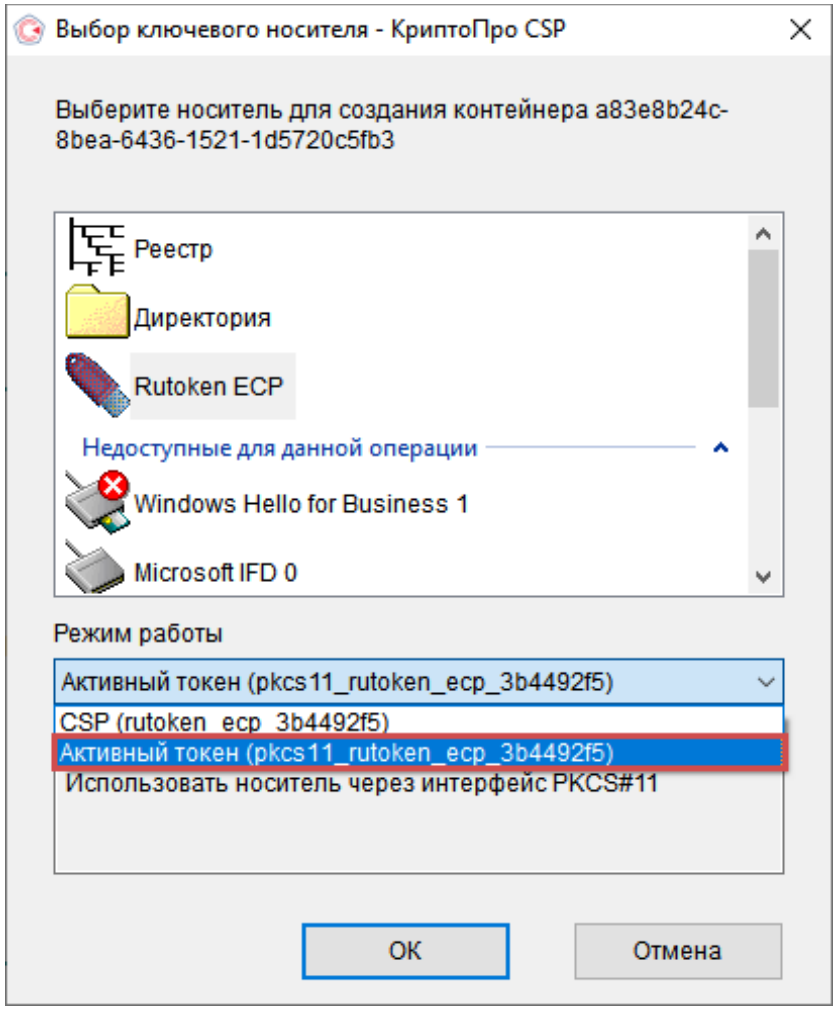
Генерация с использованием «КриптоПро CSP» версии 5.0 R2

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

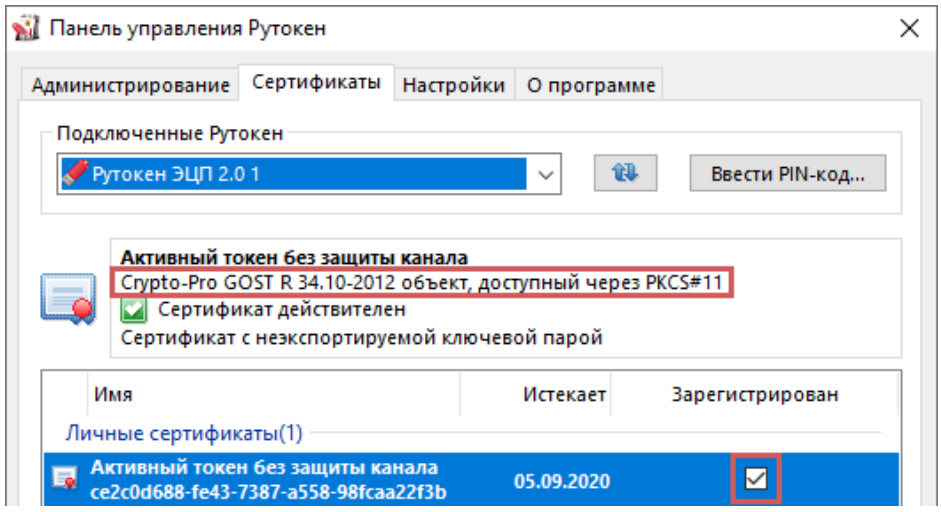
В окне выбора ключевого носителя выберите режим, который позволяет работать с внутренним криптоядром Рутокена через библиотеку PKCS#11.
У вас может быть один из двух вариантов (зависит от версии КриптоПро CSP):

- 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)**.



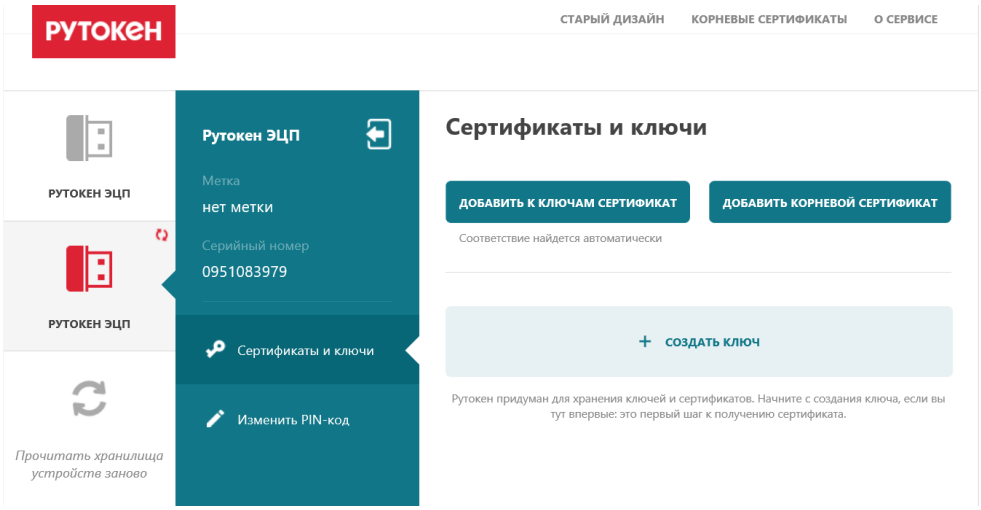


В «Панели управления Рутокен» такие ключи будут отображаться как **«Crypto-Pro GOST объект, доступный через PKCS#11»**

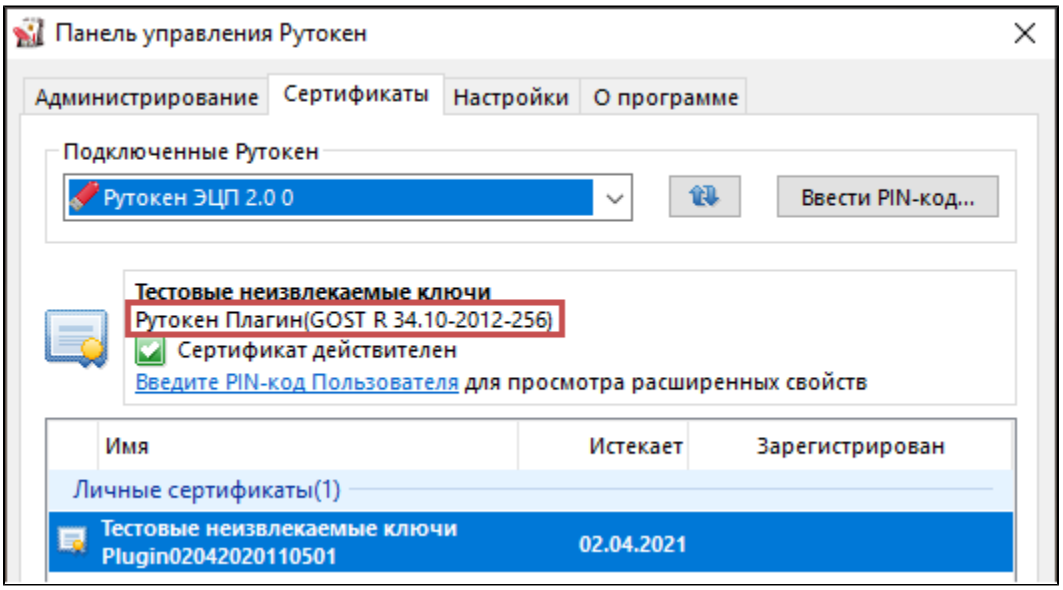


Генерация с помощью Рутокен Плагина

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

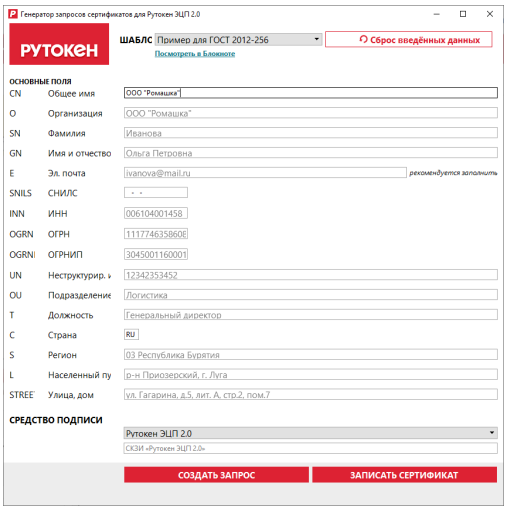


В «Панели управления Рутокен» такие ключи будут отображаться как **«Рутокен Плагин».**

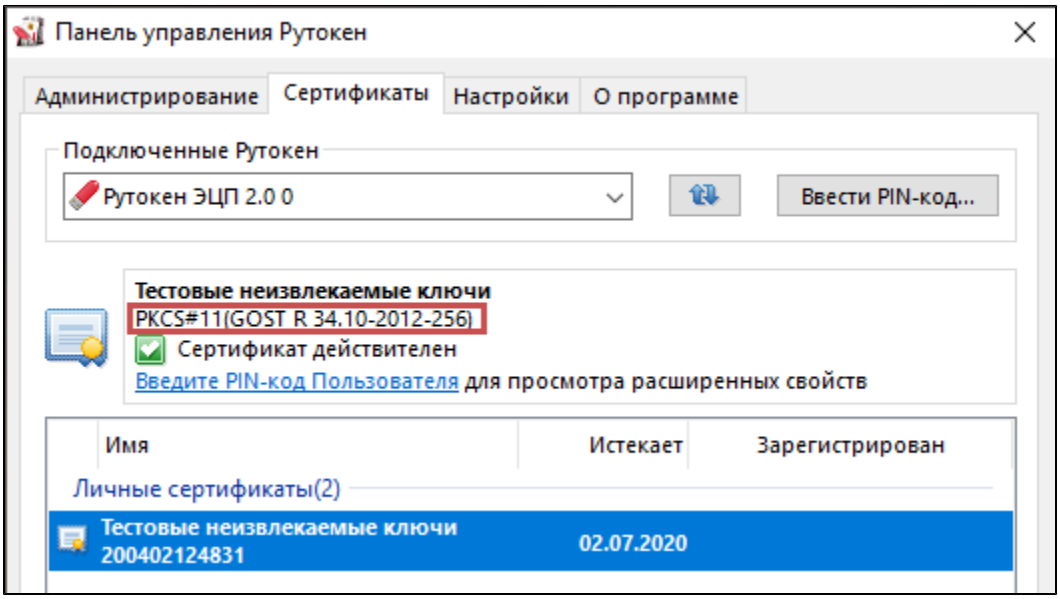


Генерация с помощью утилиты «Генератор запросов сертификатов для Рутокен ЭЦП 2.0»

Воспользоваться утилитой «Генератор запросов», которая входит в состав Драйверов Рутокен и доступна на нашем сайте в разделе: Цент р загрузки — Драйверы для Windows — Утилиты.



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



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