

# Неизвлекаемые ключи на Рутокенах в КриптоПро CSP 5.0

«КриптоПро» CSP 5.0 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
- «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 совместимы с большинством криптографических плагинов: КриптоПро Browser Plug-In, Рутокен Плагин, IFCPlugin.

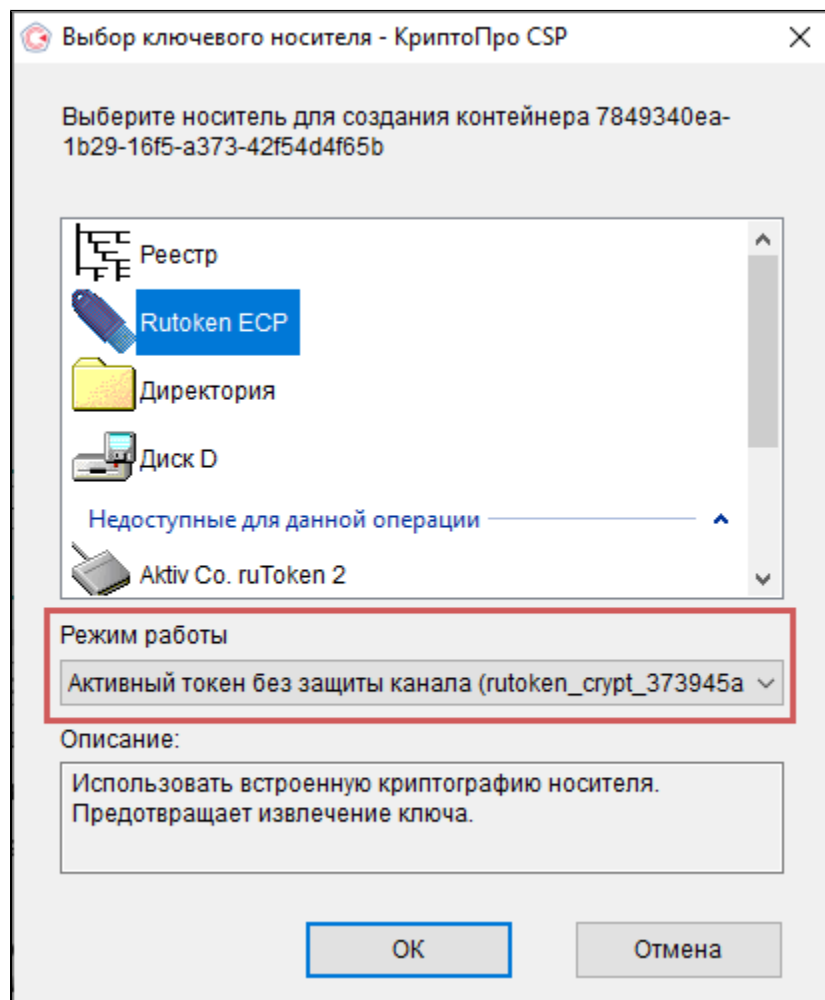
Можно использовать в системах: ЕГАИС, «Честный знак», Портал Госуслуг, palog.ru, на торговых площадках и т.д. А это значит, один ключ может быть использован в большинстве систем.

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

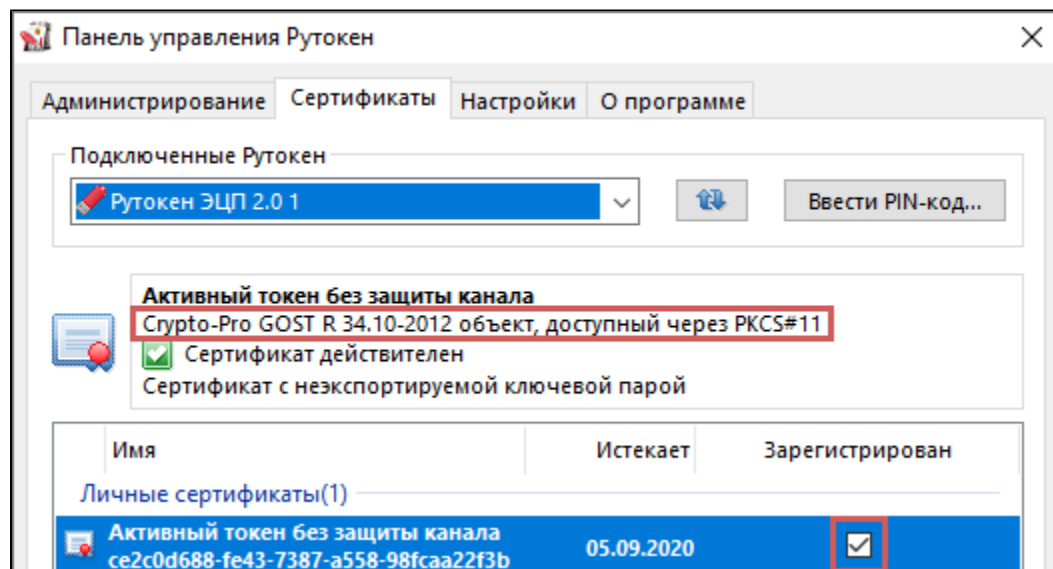
## Способы генерации

## Генерация в КриптоПро УЦ 2.0 с использованием «КриптоПро CSP» версии 5.0

Неизвлекаемые ключи генерируются в режиме «Активный токен без защиты канала»



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](http://ra.rutoken.ru) или используя интерфейс javascript «Рутокен Плагин».

**РУТОКЕН**

СТАРЫЙ ДИЗАЙН    КОРНЕВЫЕ СЕРТИФИКАТЫ    О СЕРВИСЕ

РУТОКЕН ЭЦП

РУТОКЕН ЭЦП

Прочитать хранилища устройств заново

Рутокен ЭЦП

Метка  
нет метки

Серийный номер  
0951083979

Сертификаты и ключи

Изменить PIN-код

### Сертификаты и ключи

ДОБАВИТЬ К КЛЮЧАМ СЕРТИФИКАТ    ДОБАВИТЬ КОРНЕВОЙ СЕРТИФИКАТ

Соответствие найдется автоматически

+ СОЗДАТЬ КЛЮЧ

Рутокен придуман для хранения ключей и сертификатов. Начните с создания ключа, если вы тут впервые: это первый шаг к получению сертификата.

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

Панель управления Рутокен

Администрирование   Сертификаты   Настройки   О программе

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

Тестовые неизвлекаемые ключи  
Рутокен Плагин(GOST R 34.10-2012-256)

Сертификат действителен  
Введите PIN-код Пользователя для просмотра расширенных свойств

| Имя                                                  | Истекает   | Зарегистрирован |
|------------------------------------------------------|------------|-----------------|
| Личные сертификаты(1)                                |            |                 |
| Тестовые неизвлекаемые ключи<br>Plugin02042020110501 | 02.04.2021 |                 |

## 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](#).

**РУТОКЕН**

ШАБЛОН Пример для ГОСТ 2012-256

[Посмотреть в Блокноте](#) Сброс введенных данных

## 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 <small>рекомендуется заполнить</small> |
| SNILS  | СНИЛС            | - -                                                    |
| INN    | ИНН              | 006104001458                                           |
| OGRN   | ОГРН             | 1117746358608                                          |
| OGRNIP | ОГРНИП           | 3045001160001                                          |
| UN     | Неструктурир. и  | 12342353452                                            |
| OU     | Подразделение    | Логистика                                              |
| T      | Должность        | Генеральный директор                                   |
| C      | Страна           | RU                                                     |
| S      | Регион           | 03 Республика Бурятия                                  |
| L      | Населенный пункт | р-н Приозерский, г. Луга                               |
| STREET | Улица, дом       | ул. Гагарина, д.5, лит. А, стр.2, пом.7                |

## СРЕДСТВО ПОДПИСИ

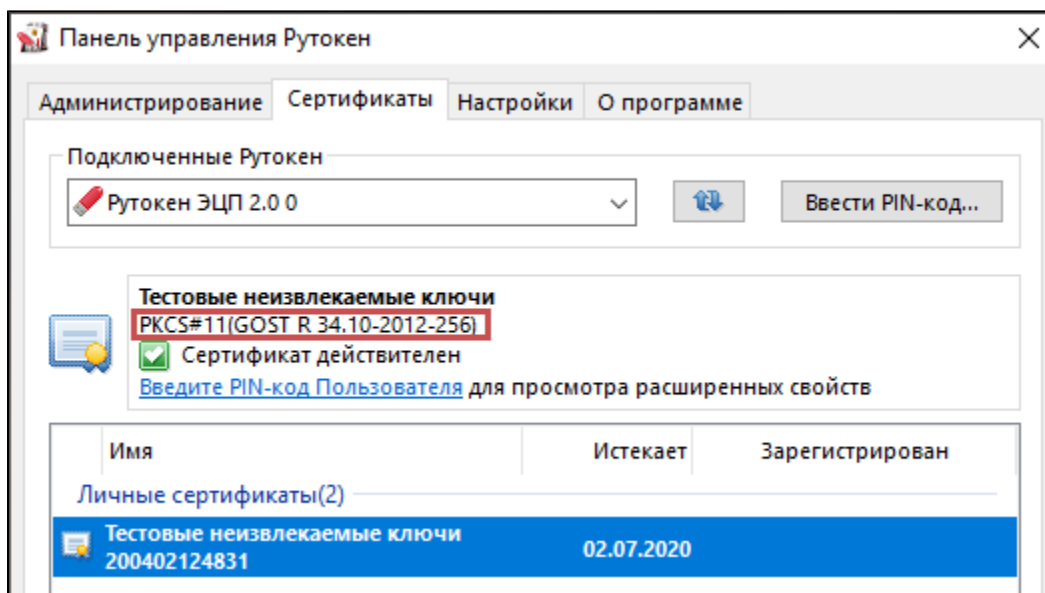
Рутокен ЭЦП 2.0

СКЗИ «Рутокен ЭЦП 2.0»

СОЗДАТЬ ЗАПРОС

ЗАПИСАТЬ СЕРТИФИКАТ

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».

