

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 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.

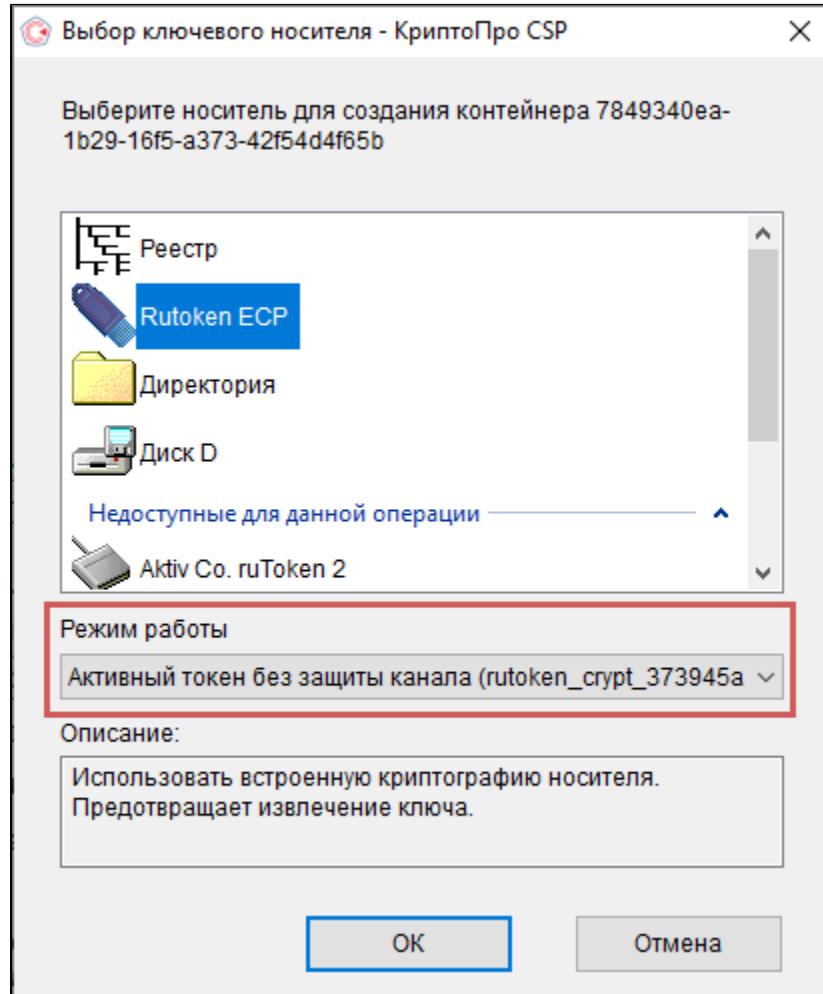
Можно использовать в системах: ЕГАИС, «Честный знак», Портал Госуслуг, palog.ru, на торговых площадках и т.д. А это значит, один ключ может быть использован в большинстве систем.

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

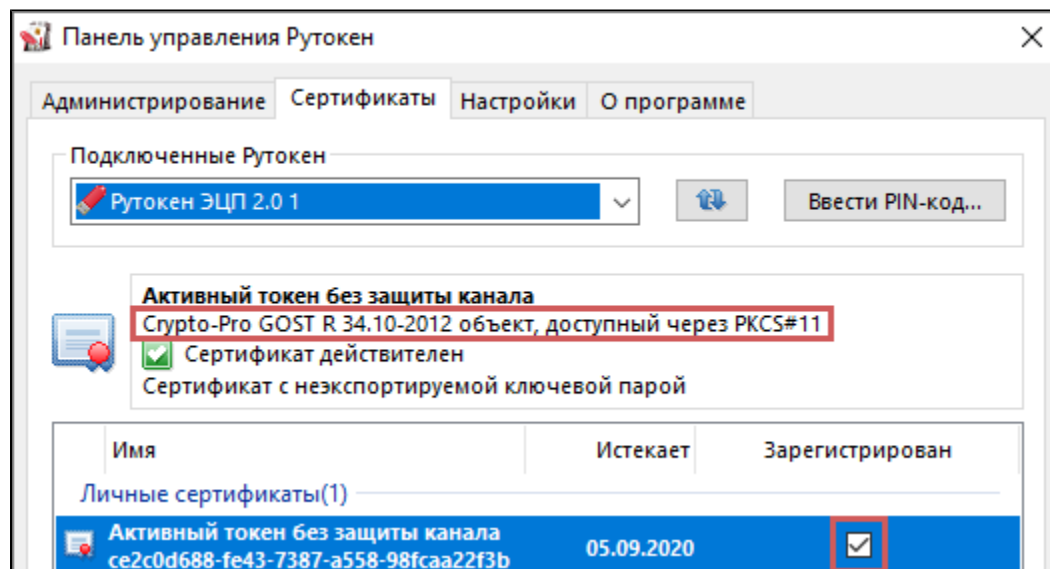
Способы генерации

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 или используя интерфейс javascript «Рутокен Плагин».

The screenshot shows the RuToken website interface. At the top left is the RuToken logo. On the right, there are navigation links: 'СТАРЫЙ ДИЗАЙН', 'КОРНЕВЫЕ СЕРТИФИКАТЫ', and 'О СЕРВИСЕ'. The main content area is titled 'Сертификаты и ключи'. On the left, there is a sidebar with three items: 'РУТОКЕН ЭЦП' (with a device icon), 'РУТОКЕН ЭЦП' (with a device icon and a refresh symbol), and 'Прочитать хранилища устройств заново' (with a refresh icon). The central area shows a teal card for 'Рутокен ЭЦП' with a back arrow icon. It displays 'Метка: нет метки' and 'Серийный номер: 0951083979'. Below this are two icons: a key icon for 'Сертификаты и ключи' and a pencil icon for 'Изменить PIN-код'. On the right, there are two buttons: 'ДОБАВИТЬ К КЛЮЧАМ СЕРТИФИКАТ' and 'ДОБАВИТЬ КОРНЕВОЙ СЕРТИФИКАТ'. Below these buttons, it says 'Соответствие найдется автоматически'. At the bottom right, there is a large light blue button with a plus sign and the text 'СОЗДАТЬ КЛЮЧ'. Below this button, there is a note: '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».

The screenshot shows the 'Панель управления Рутокен' (RuToken Management Panel) window. It has a title bar with a close button. Below the title bar are four tabs: 'Администрирование', 'Сертификаты', 'Настройки', and 'О программе'. The 'Сертификаты' tab is active. Under the 'Подключенные Рутокен' section, there is a dropdown menu showing 'Рутокен ЭЦП 2.0 0' and a 'Ввести PIN-код...' button. Below this, there is a section for 'Тестовые неизвлекаемые ключи' with a red box around the text 'Рутокен Плагин(GOST R 34.10-2012-256)'. There is a green checkmark icon and the text 'Сертификат действителен'. Below this, there is a link: 'Введите PIN-код Пользователя для просмотра расширенных свойств'. At the bottom, there is a table with columns 'Имя', 'Истекает', and 'Зарегистрирован'. The table has one row with the following data:

Имя	Истекает	Зарегистрирован
Личные сертификаты(1)		
Тестовые неизвлекаемые ключи 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

[Сброс введенных данных](#)

[Посмотреть в Блокноте](#)

ОСНОВНЫЕ ПОЛЯ

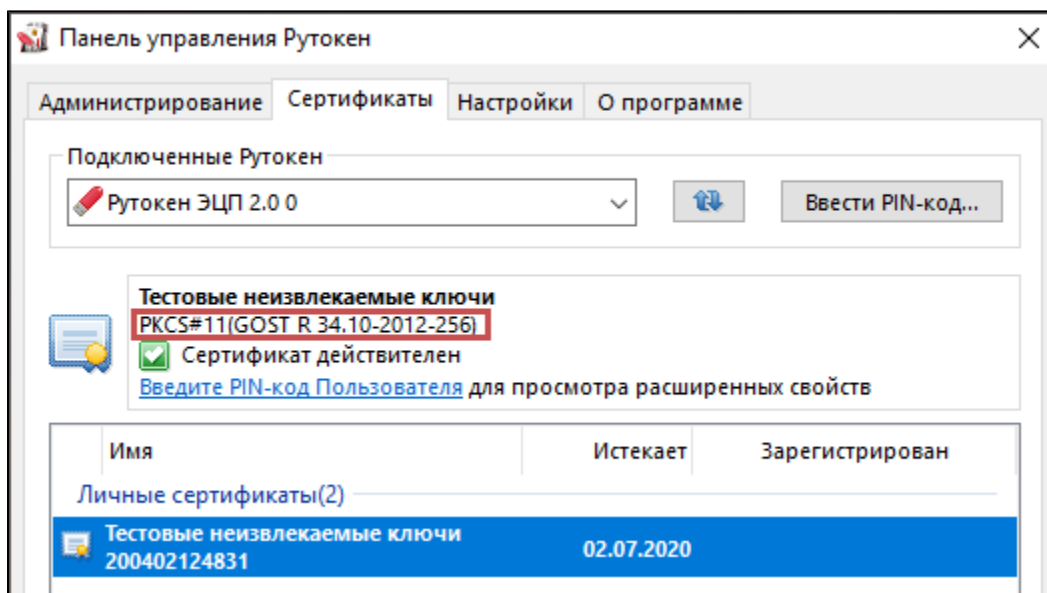
CN	Общее имя	<input type="text" value="ООО " ромашка"=""/>
O	Организация	<input type="text" value="ООО " ромашка"=""/>
SN	Фамилия	<input type="text" value="Иванова"/>
GN	Имя и отчество	<input type="text" value="Ольга Петровна"/>
E	Эл. почта	<input type="text" value="ivanova@mail.ru"/> <small>рекомендуется заполнить</small>
SNILS	СНИЛС	<input type="text" value="- -"/>
INN	ИНН	<input type="text" value="006104001458"/>
OGRN	ОГРН	<input type="text" value="1117746358608"/>
OGRNIP	ОГРНИП	<input type="text" value="3045001160001"/>
UN	Неструктурир. и	<input type="text" value="12342353452"/>
OU	Подразделение	<input type="text" value="Логистика"/>
T	Должность	<input type="text" value="Генеральный директор"/>
C	Страна	<input type="text" value="RU"/>
S	Регион	<input type="text" value="03 Республика Бурятия"/>
L	Населенный пу	<input type="text" value="р-н Приозерский, г. Луга"/>
STREET	Улица, дом	<input type="text" value="ул. Гагарина, д.5, лит. А, стр.2, пом.7"/>

СРЕДСТВО ПОДПИСИ

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».

