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.

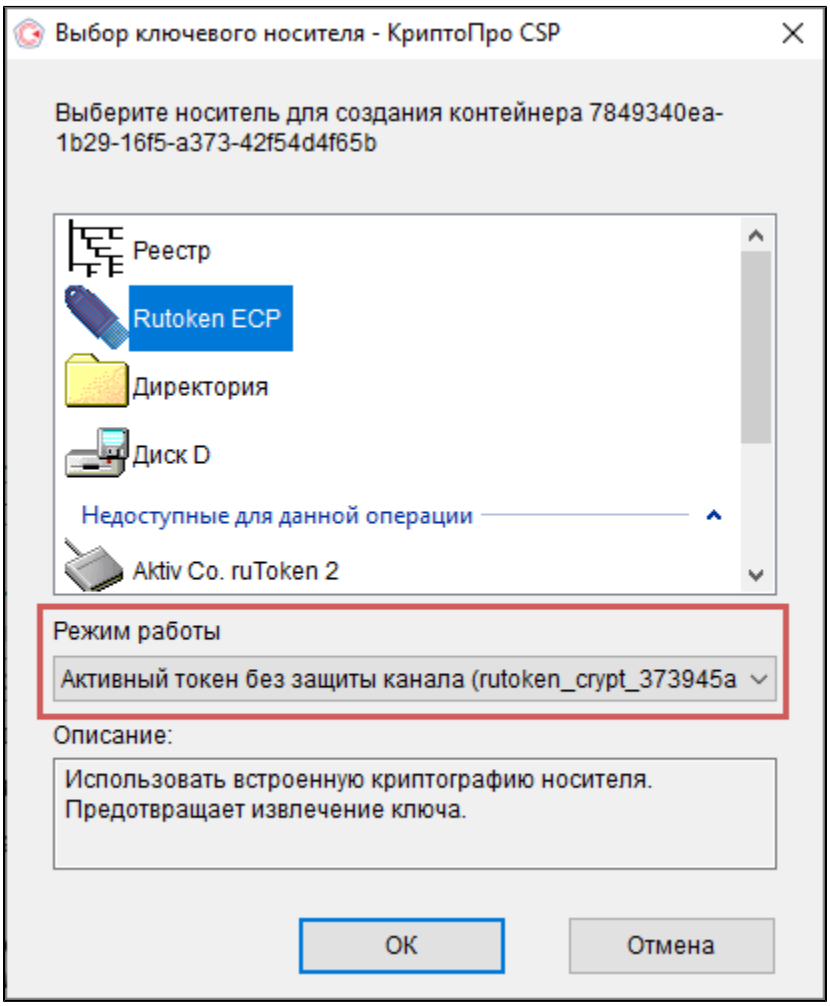
Можно использовать в системах: ЕГАИС, «Честный знак», Портал Госуслуг, nalog.ru, на торговых площадках и т.д. А это значит, один ключ может быть использован в большинстве систем.

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

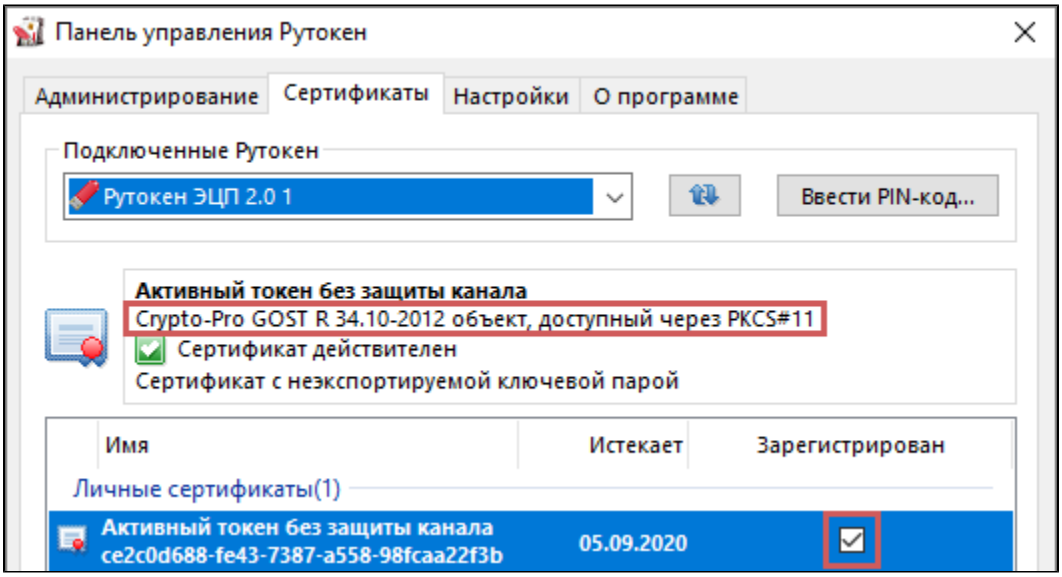
Способы генерации

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

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

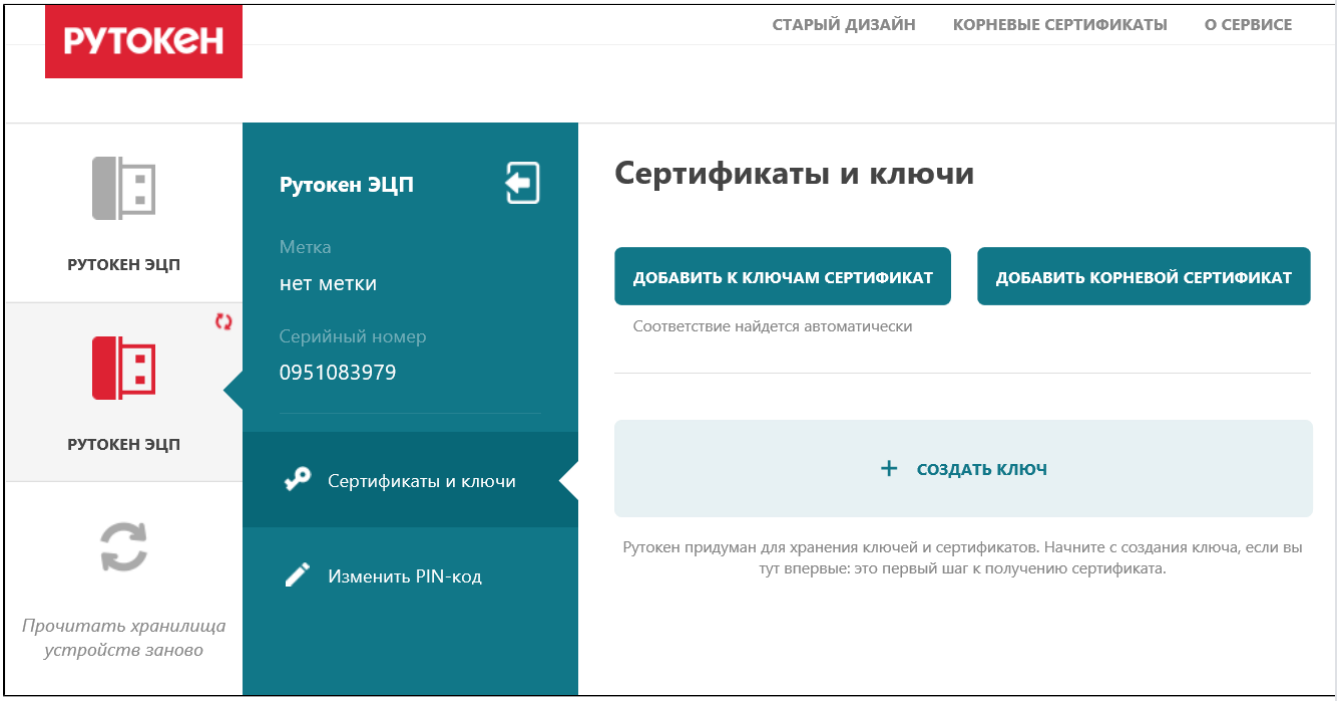


В «Панели управления Рутокен» такие ключи будут отображаться как **«Crypto-Pro GOST объект, доступный через PKCS#11»**

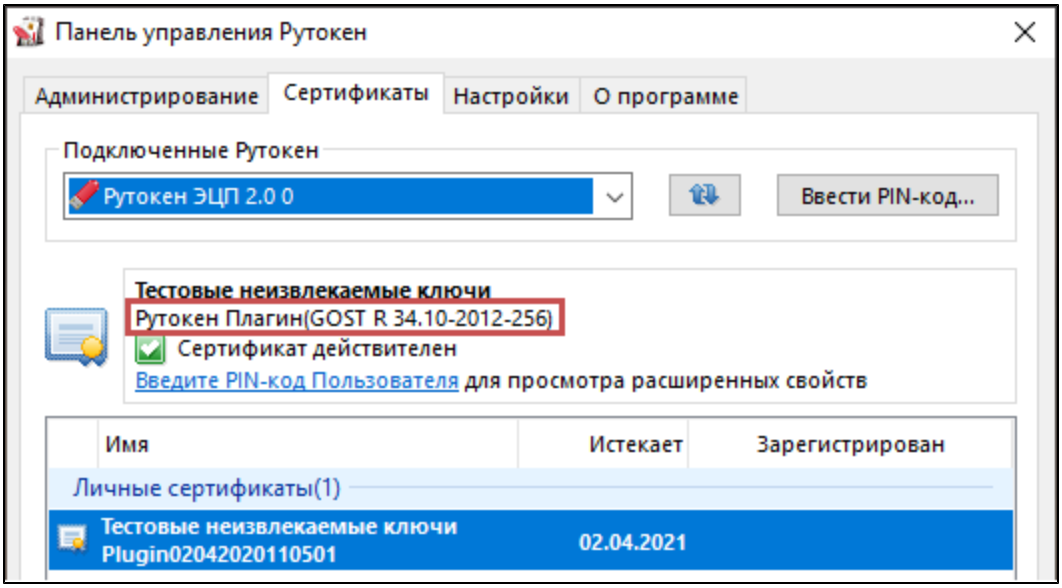


Генерация с помощью Рутокен Плагина

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

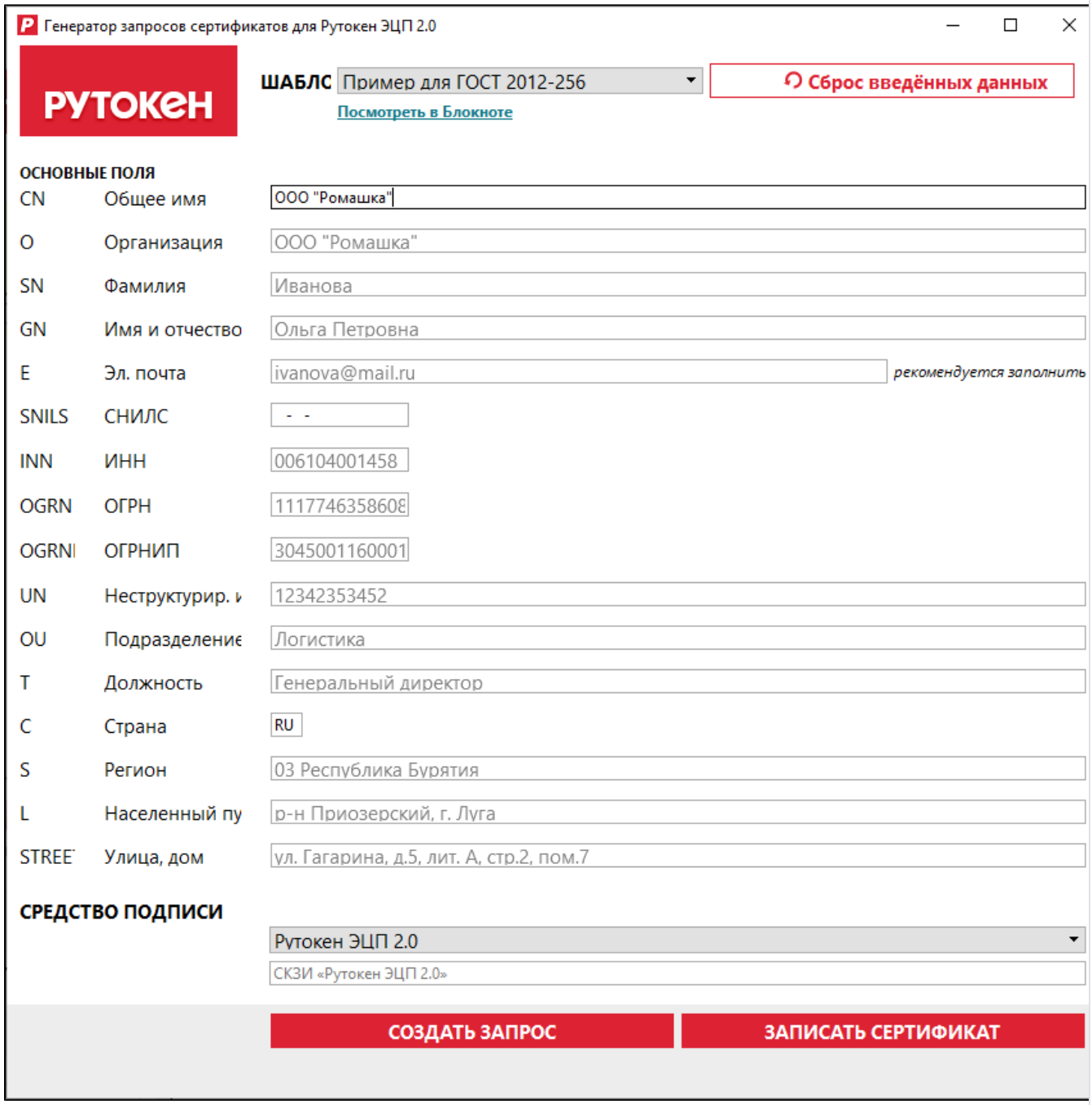


В «Панели управления Рутокен» такие ключи будут отображаться как **«Рутокен Плагин».**

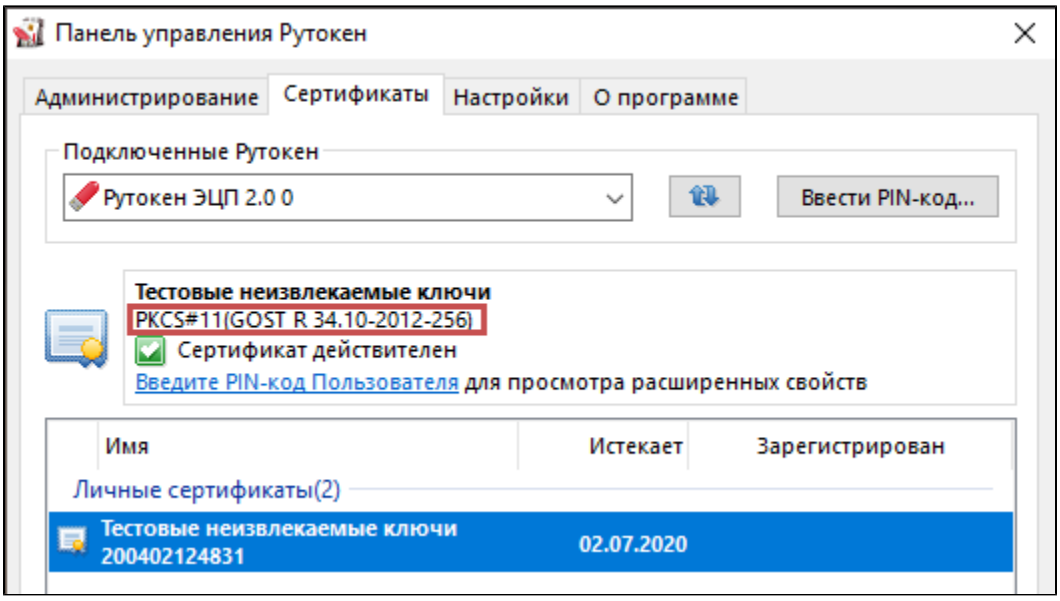


Генерация с помощью утилиты «Генератор запросов сертификатов для Рутокен ЭЦП 2.0»

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».**

