RU1081

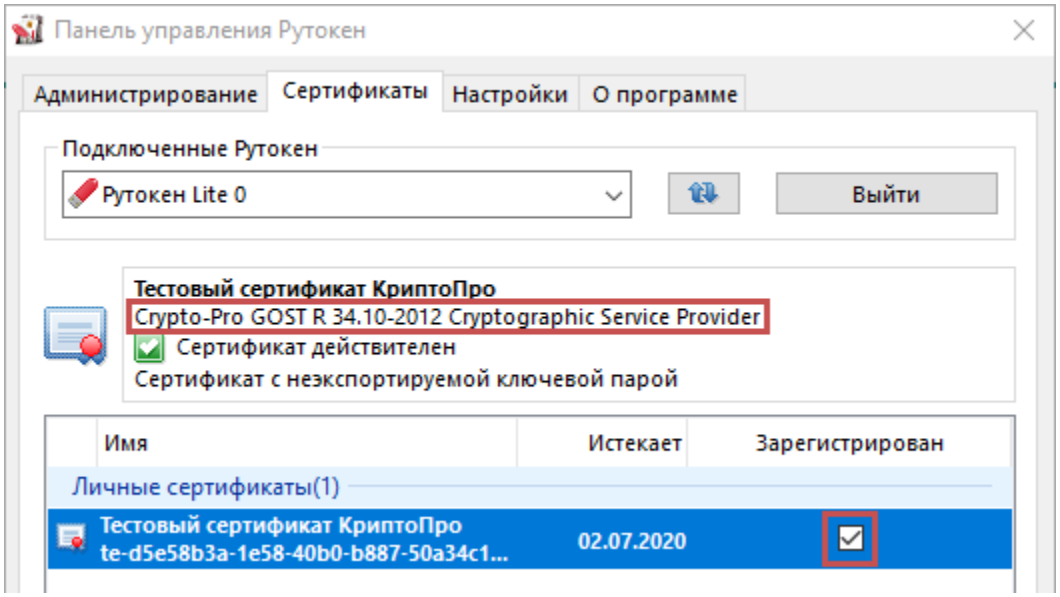
Форматы ключей электронной подписи

Формат уже имеющихся ключей электронной подписи можно посмотреть через “Панель управления Рутокен”, которая появляется после установки “Драйверов Рутокен”.

Увидеть формат ключей можно на вкладке “Сертификаты”, после того, как сертификат будет установлен в хранилище “Личное” на текущий компьютер.

Чаще всего, сертификат устанавливается автоматически, но если служба установки сертификатов отключена, установить его можно вручную, поставив флаг “Зарегистрирован”. После этого над таблицей мы увидим формат сертификата.
Так как мы постоянно работаем над улучшением своих программ, а форматы ключей могут меняться со временем, обязательно проверьте, что у вас установлена актуальная версия “Драйверов Рутокен”.

Контейнер с сертификатом "КриптоПро CSP" или "VipNet CSP"

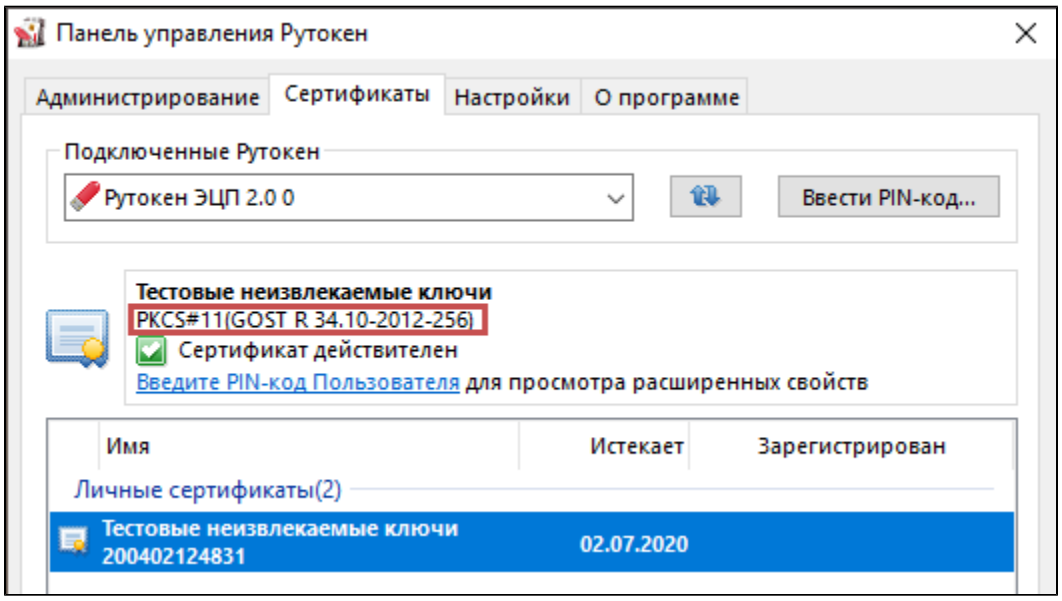


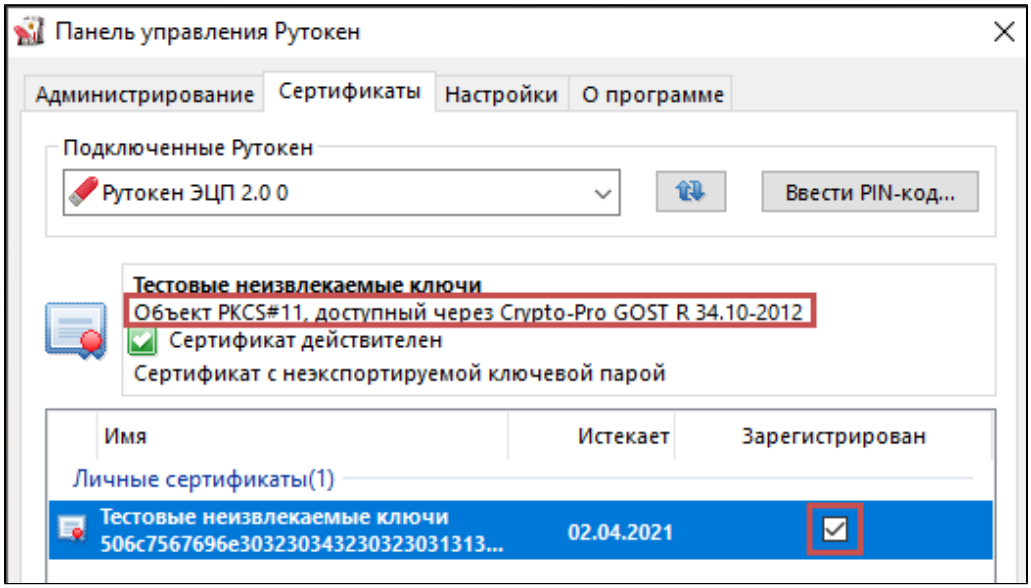
Первый тип - это сертификат, сгенерированный с помощью программных средств криптопровайдера “КриптоПро CSP”. Его можно записать на любую модель Рутокена, которая подходит для хранения электронной подписи. Ключи надежно хранятся в защищенной памяти Рутокена под PIN-кодом. Каждый раз для использования криптографической функции с ключом такого формата программный криптопровайдер передает ключи в оперативную память компьютера. Возможность экспорта (копирования) закрытого ключа формата "КриптоПро CSP" устанавливается в момент генерации ключевой пары в удостоверяющем центре и не зависит от модели Рутокена.

Также электронная подпись может быть выписана с помощью других программных криптопровайдеров:

- ViPNet CSP (если используется модель Рутокен, отличная от ЭЦП 2.0/3.0)
- Signal COM
- Aktiv Rutoken CSP

Сертификат с неизвлекаемым ключом ЭП на Рутокен ЭЦП 2.0 / 3.0





Второй тип - это электронная подпись формата ЕГАИС. Это неизвлекаемые ключи, которые генерируются по стандарту PKCS#11 и более правильно было бы называть их ключами, сгенерированными аппаратными средствами Рутокен.

Однако, уже несколько лет ключи такого формата наиболее активно используются в системе Росалкогольрегулирования и легче узнаваемы по названию сертификаты ЕГАИС.

Генерация такого типа сертификата возможна только при использовании возможностей интеллектуального ключевого носителя семейства Рутокен ЭЦП 2.0 / 3.0.

Все криптографические функции происходят аппаратного токена, закрытый ключ является неизвлекаемым и никогда не покидает Рутокен ЭЦП 2.0 / 3.0.

Способы генерации такого типа ключей описаны в этой статье.