CP1025

Новые функции КриптоПро CSP версии 5.0 R2

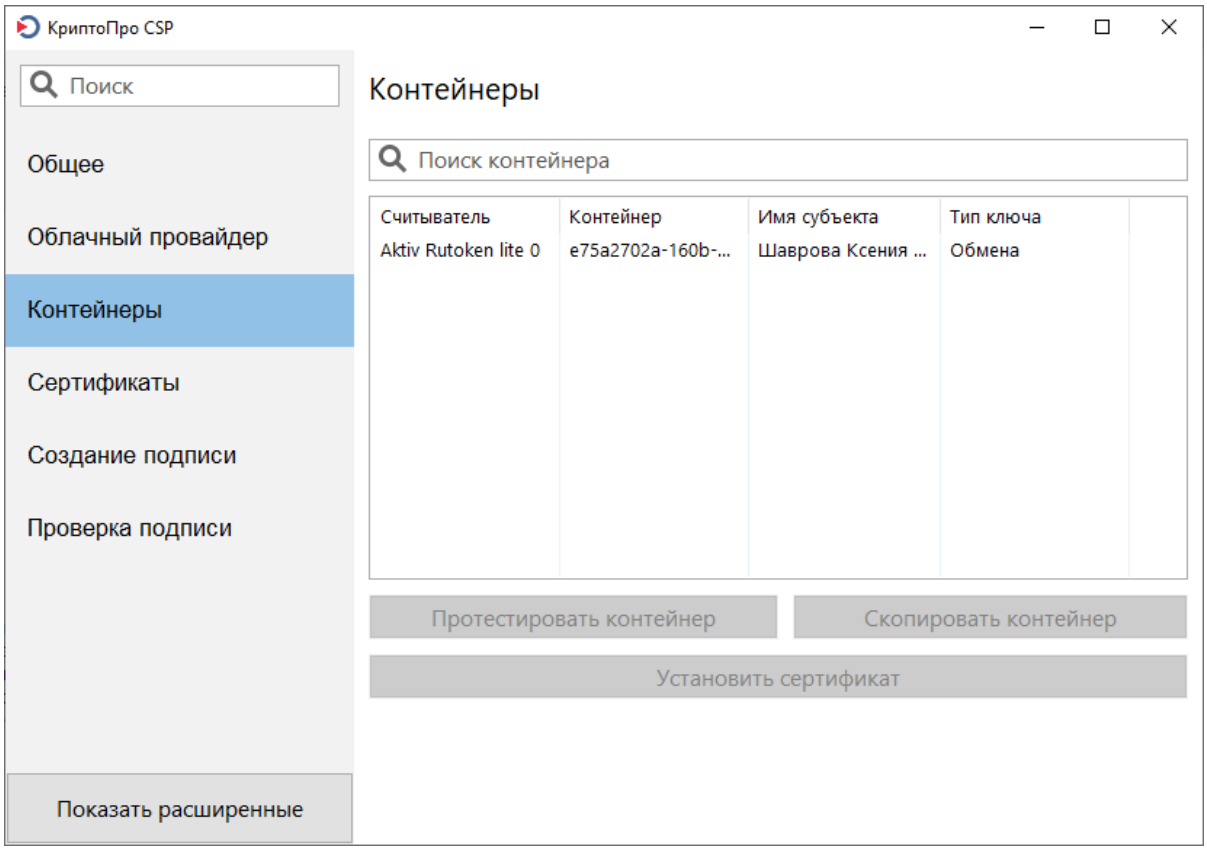
Интерфейс стал дружелюбнее и современнее.

В «КриптоПро CSP» 5.0 R2 реализована обёртка pkcs11-библиотеки для работы с носителями Рутокен ЭЦП 2.0/3.0. Это значит, что неизвлекаемые ключи, сгенерированные по стандарту PKCS#11 (как для ЕГАИС) на носителях Рутокен ЭЦП 2.0/3.0 могут работать через «КриптоПро CSP». При этом сертификат можно установить в хранилище Личные со ссылкой на закрытый ключ PKCS#11 контейнера и работать в сервисах, где можно использовать стандартные сертификаты, выданные на криптопровайдере «КриптоПро CSP». Для работы через «КриптоПро CSP» требуется лицензия.

«КриптоПро Browser Plug-In» также научился работать с неизвлекаемыми ключами PKCS#11.

Инструменты КриптоПро CSP

В составе «КриптоПро CSP 5.0 R2» появилось графическое приложение для Windows, Linux и macOS - «Инструменты КриптоПро» («CryptoPro Tools») или просто cptools.



Оно позволяет:

- управлять контейнерами и сертификатами
- создавать и проверять CMS-подписи под файлами
- выполнять сервисные операции с носителями
- отображать информацию о провайдере и лицензии и делать некоторые настройки

Полное описание функциональности «Инструментов КриптоПро CSP» есть на сайте разработчика.

Три режима работы с Рутокенами

Работа со внутренним криптоядром Рутокена

В режиме «активного вычислителя» ключи контейнера КриптоПро CSP создаются сразу в защищенной памяти устройства.

Подписание документов теперь возможно и на неизвлекаемых аппаратных ключах. Этот режим предотвращает извлечение ключа в память компьютера в момент подписания.

- Вся линейка Рутокен ЭЦП 3.0
- Рутокен ЭЦП 2.0 2100 (Type-C/micro);
- Рутокен ЭЦП 2.0 (micro);
- Рутокен ЭЦП 2.0 2151;
- Рутокен ЭЦП 2.0 Flash/Touch;
- Рутокен ЭЦП Bluetooth;
- Смарт-карты Рутокен ЭЦП 2.0 2100;

Поддержка протокола SESPAKE (ФКН)

В «КриптоПро CSP» версии 5.0 R2 реализован криптографический протокол SESPAKE, который так же поддерживается в моделях Рутокен ЭЦП 2.0 3000 (Type-C/micro) и во всей линейке Рутокен ЭЦП 3.0.

Данный протокол позволяет провести аутентификацию, не передавая в открытом виде PIN-код пользователя, и установить шифрованный канал для обмена сообщений между криптопровайдером и носителем

Хранение в защищенной файловой системе Рутокен

Как и в «КриптоПро CSP» версии 4.0, использование Рутокена в этом режиме позволяет обезопасить ключевую информацию от несанкционированного использования. Ключи и сертификаты надёжно хранятся в защищенной файловой системе Рутокен.

- Рутокен S (micro)
- Рутокен Lite (micro)
- Рутокен ЭЦП PKI (Type-C/micro)
- Рутокен ЭЦП 2.0 2100 (Type-C/micro);
- Рутокен ЭЦП 2.0 (micro);
- Рутокен ЭЦП 2.0 2151;
- Рутокен ЭЦП 2.0 Flash/Touch;
- Рутокен ЭЦП Bluetooth;
- Смарт-карты Рутокен ЭЦП 2.0 2100;
- Вся линейка Рутокен ЭЦП 3.0