

iliakan сегодня в 10:52

Экспорт ключа ФНС

Информационная безопасность *Криптография *Системное программирование *

Tutorial

Всем привет,

Пишу этот пост как инструкцию для себя и других, кто получил ключ "на флешке" в Российской налоговой и хочет скопировать его на компьютер, чтобы пользоваться без флешки.

Также далее пишу, как преобразовать его в openssl-формат, пригодный для Diadoc API и других.

Предполагается, что обычный доступ по токену у вас и так работает, в интернет куча инструкций на эту тему.

Проблема в том, что ФНС ставит на токене флаг "экспорт запрещён". Большинство стандартных средств экспорта перестают работать.

Предупреждение! Флаг стоит не просто так. Ключ, полученный в ФНС, имеет очень много полномочий. Пока ключ на флешке, он защищён гораздо лучше, чем в вашей файловой системе.

С другой стороны, в некоторых ситуациях копирование ключа уместно. Например, можно сделать зашифрованный архив на случай, если токен сломается.

ФНС использует два типа токенов. Первый, вроде бы, дают, если идет работа с алкоголем (ЕГАИС), и там шифрование аппаратное, ключ не покидает токен, в этом случае, насколько я слышал, чисто программно сделать ничего нельзя.

Если же вы алкоголь не продаете, то можно использовать обычный токен (у меня рутокен). И там все проще, запрет экспорта - чисто программный флажок, который можно снять, детали далее.

Копирование на файловую систему

Вначале создадим копию контейнера с токена на файловую систему.

Для этого понадобится утилита <https://www.kontur-extern.ru/Files/Modules/CmsFile/Tokens.zip> (под Windows).

Качаем, запускаем, она выдает ошибку и просит поставить компоненты дополнительно по ссылкам - ставим их. После этого втыкаем токен и перезапускаем утилиту.

Токен появляется в списке, экспортируем его. Можно выбрать имя директории, я назвал FNS.000 (расширение 000 использует Crypto Pro).

В итоге у вас появляется директория с файлами: header.key и другими. Это сертификат вместе с закрытым ключом в формате Crypto Pro.

Фактически этим уже можно пользоваться. У меня основная система Mac, уже было настроено Crypto Pro, я просто скопировал его в директорию /var/opt/cprosp/keys/iliakan, далее запустил CryptoPro Tools и там Containers - выбираю нужный контейнер - Install certificate.

Затем браузер <https://www.cryptopro.ru/products/chromium-gost> (там ГОСТ-шифрование, обычный Chrome не подойдет) с установленным расширением КриптоПро автоматически видит этот сертификат - и доступ на сайт налоговой работает, прямая ссылка: <https://lkipgost2.nalog.ru/lk>.

Под Windows нужно, видимо, в аналогичную директорию скопировать, кто знает - дополните в комментариях?

Если ваша задача была сделать архив токена или отвязать его от флешки - она выполнена. Дальше можно не читать ;)

Снятие запрета на экспорт

В скопированном с токена контейнере все еще стоит флаг "экспорт запрещён". Это естественно, ведь по сути директория-контейнер - это копия токена, с соответствующими флагами.

Снять его может другая утилита: CertFix, но не последней версии, а более старая, доступная по ссылке <https://api.kontur.ru/drive/v1/public/diag/files/certfix.000032.exe>.

Это может быть нужно, чтобы подготовить сертификат для конвертации в формат openssl (для API). Просто чтобы пользоваться для взаимодействия через браузер с госслужбами - снимать флаг не обязательно.

Для этого копируем директорию с файлами на флешку (важно именно на флешку), в корень, и, выключив интернет (!) запускаем certfix.000032.exe. Если не выключить, то эта утилита обновится, а в последней версии опция, о которой идет речь ниже, отключена.

В списке находим свой сертификат - справа в колонке экспорта будет стоять DENIED, ждем Shift и правый(!) клик мышкой, появится меню с опцией "сделать экспортируемым (файловая система)".

Клик на эту опцию и задаём пароль (обязательно).

Готово, файлы на флешке обновлены, появилась поддиректория с бэкапом - можно ее удалить.

Это всё ещё сертификат в формате Крипто Про, только с разрешённым экспортом. Пользоваться так же, как и ранее.

Конвертация в формат для OpenSSL

Для API обычно использую openssl.

К сожалению, в сертификатах РФ используется свой стандарт шифрования: ГОСТ, поэтому обычный openssl не подходит, нужен патченный.

Если вас занесла нелёгкая в эти дебри, то наверно вы уже это знаете про патч <https://github.com/gost-engine/engine>. Его можно собрать самостоятельно, но гораздо проще - поставить docker-контейнер, в котором оно уже готовое.

Вот нужный образ: <https://hub.docker.com/r/mix/openssl-gost/>. Если вы не знаете, что такое docker - отличный повод изучить, это очень просто. Во всяком случае, прочитать с нуля про основы и поставить/запустить, расшарить каталог с сертификатом - займёт в пределах 1-3 часов.

Далее, чтобы сертификат дружил с этим openssl, его нужно преобразовать в "нормальный" формат из openssl. Это делает утилита <https://github.com/kov-serg/get-cpcert>.

При сборке она меняет системный openssl, так что имеет смысл собирать её в отдельном docker-контейнере, ну или просто где не жалко.

Затем запускаем, как там в readme указано: `get-cpcert FNS.000 "пароль, выбранный при экспорте" > certificate.pem`.

В результате из Crypto Pro формата появляется аккуратный файл с сертификатом и приватным ключом.

Всё, можно с этим уже делать что угодно, отсылать через openssl запросы к любым API.

Будут нужны какие-то уточнения - задавайте вопросы в комментариях.

Илья Кантор @iliakan