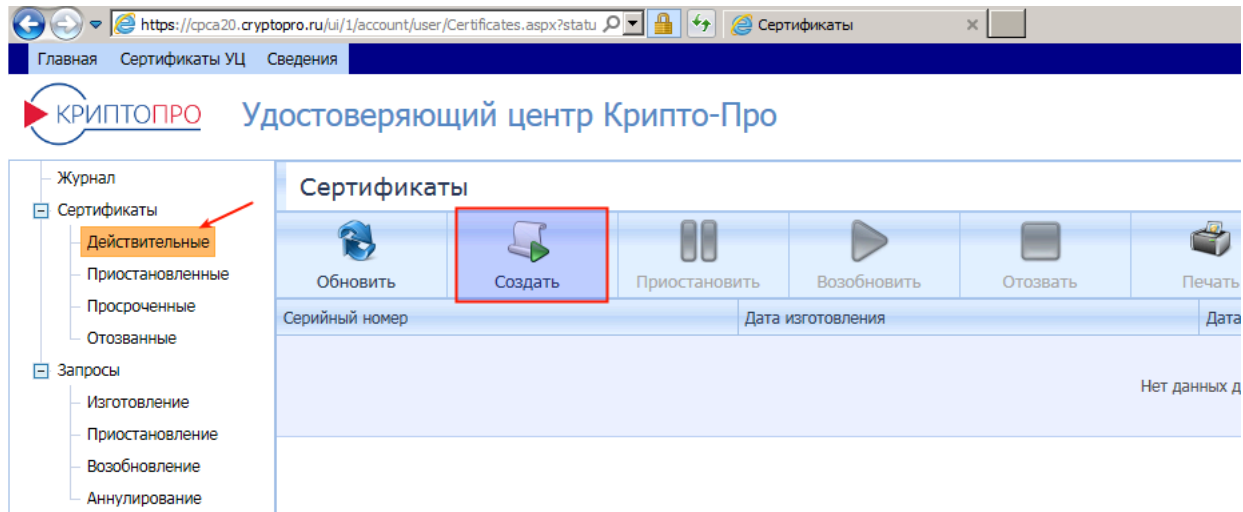


Как получить рабочий сертификат КриптоПро и установить на Linux

Создание запроса на сертификат

Идем на <https://cpca20.cryptopro.ru/ui/> [<https://cpca20.cryptopro.ru/ui/>] и входим как зарегистрированный пользователь (или регистрируемся).

Создаем запрос



Необходимо выбрать 2012 год:

Запрос на сертификат

Шаблон сертификата
Сертификат пользователя УЦ ГОСТ 2012 [УЦ КРИПТО-ПРО]

Криптопровайдер
Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider

Ключ будет использоваться для
☒ Подписи и шифрования
☐ Подписи
☐ Шифрования

Размер ключа
512

Алгоритм хеширования
ГОСТ Р 34.11-2012

Срок действия сертификата
5 лет

Срок действия ключа
1 лет

Комментарий

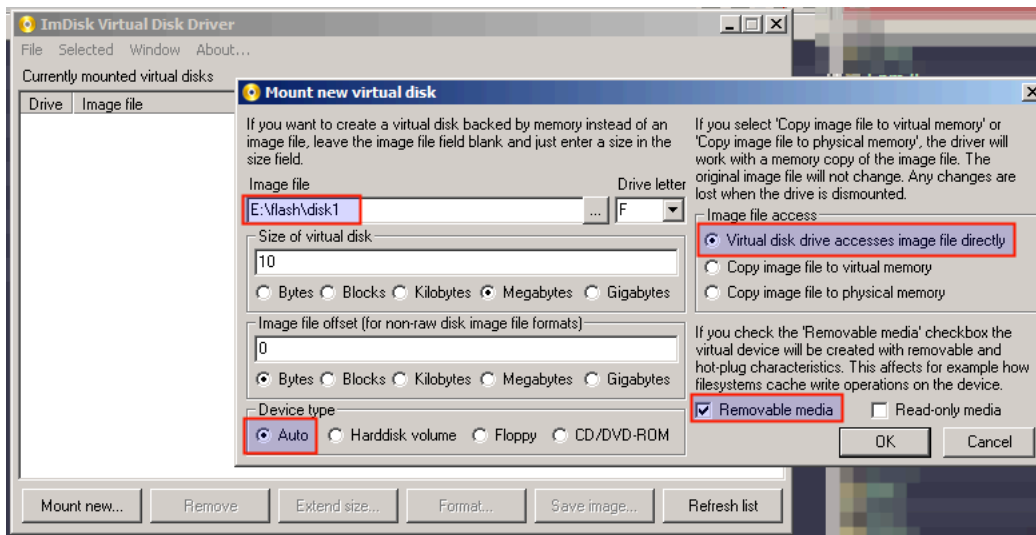
Создать

Полученный сертификат можно сохранить на флешке (рутокен) или в реестре системы.

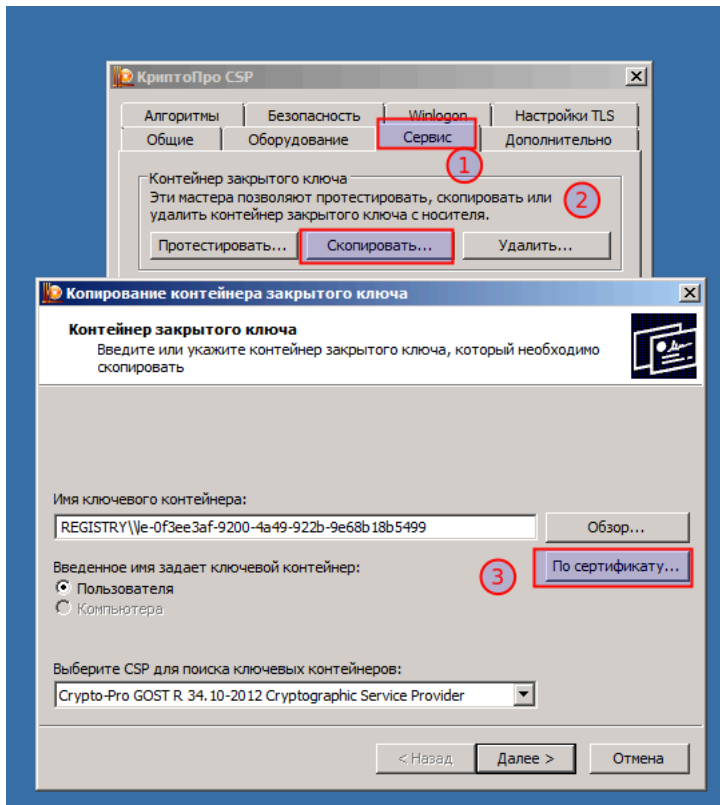
На флешку удобно сохранять для переноса на Linux-сервер, иначе придется идти более трудным путем.

Извлечение закрытого ключа из реестра

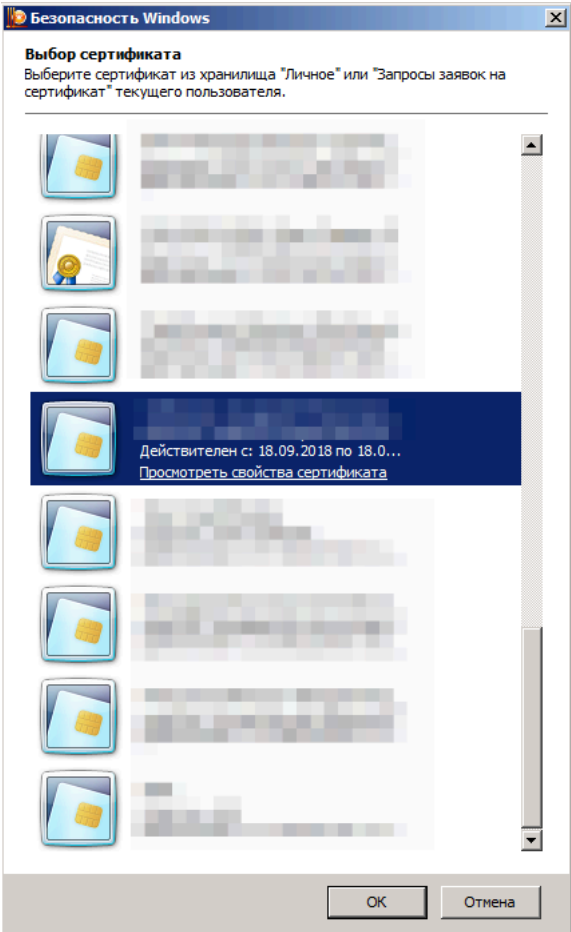
Так как разработчики заморочились с безопасностью, извлечь приватный сертификат средствами операционной системы или КриптоПро на жесткий диск невозможно. Но можно на флешку. Поэтому ставим ImDisk Virtual Disk Driver. Такие настройки позволяют сохранить сертификат:



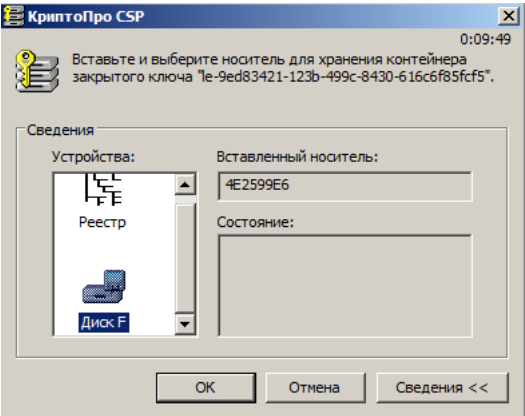
Запустить КриптоПро CSP, выбрать Сервис, Скопировать, По сертификату.



Выбрать необходимый сертификат из предложенных.



Ввести пароль и сохранить на созданный виртуальный диск:



Все, теперь файлы получены, остальное - дело техники:

Съемный диск (F:) - Ie-9ed83.000		
Имя	Тип	Размер
<DIR>		
header	key	116
masks	key	56
masks2	key	56
name	key	43
primary	key	36
primary2	key	36

Сохранение сертификата

Снова заходим в КриптоПро, и сохраняем изготовленный сертификат по кнопке «Установить».

Главная Сертификаты УЦ Сведения

КРИПТОПРО Удостоверяющий центр Крипто-Про

Журнал

- Сертификаты
 - Действительные
 - Приостановленные
 - Просроченные
 - Отозванные
- Запросы
 - Изготовление

Запросы

Обновить Печать

Дата создания	Статус	Дата одобрения	Сертификат
18.09.2018 14:46:19	Завершен	18.09.2018 15:00:56	014ABBC5005FA9A98F46

Я получит такое сообщение об ошибке:

CertEnroll::CX509Enrollment::InstallResponse: Цепочка сертификатов обработана, но обработка прервана на корневом сертификате, у которого отсутствует отношение доверия с поставщиком доверия. 0x800b0109

КРИПТОПРО Удостоверяющий центр Крипто-Про

Установка сертификата



Вы получили запрошенный сертификат.

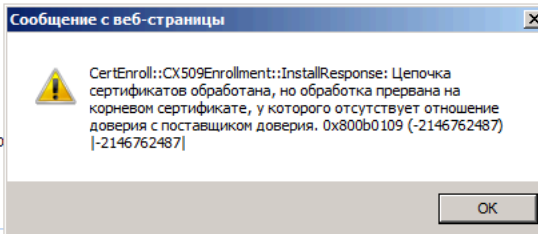
Нажмите кнопку "Установить сертификат", чтобы установить его для дальнейшего использования.

Установить сертификат

Вы должны подтвердить получение

Для этого нажмите кнопку "Подтвер

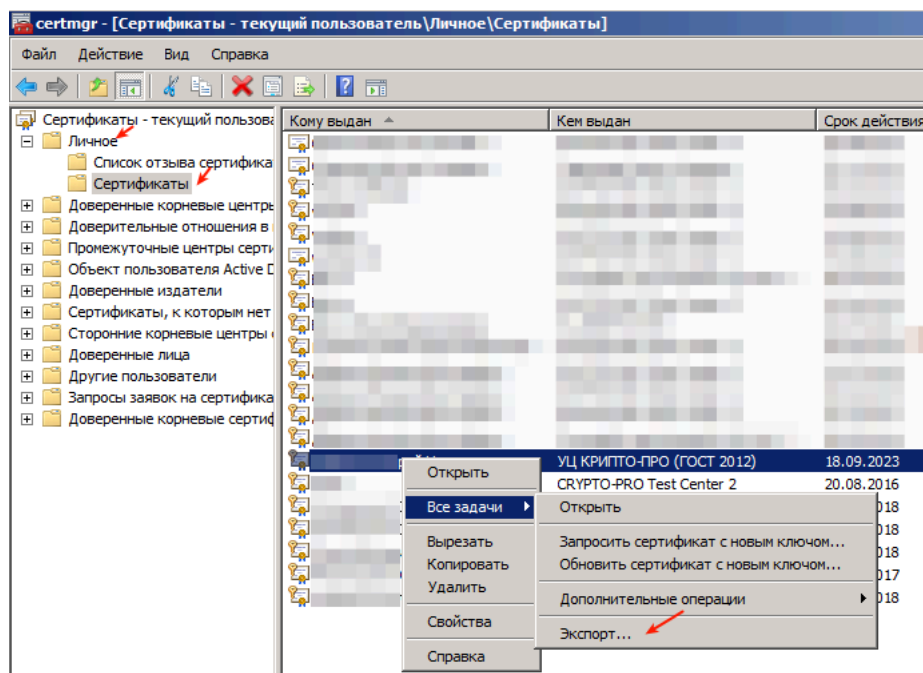
Подтвердить установку



Решается установкой корневого сертификата, периодически они добавляют в него новые, взять можно тут: <http://cpca20.cryptopro.ru/cacer.p7b> [<http://cpca20.cryptopro.ru/cacer.p7b>]

Далее запускаем certmgr.msc

Ищем в Личное, Сертификаты, и делаем Экспорт.



Теперь у нас есть закрытый ключ и сертификат, которые можно использовать для подписания на Linux-сервере

```
le-9ed83.000
├── header.key
├── masks2.key
├── masks.key
├── name.key
├── primary2.key
├── primary.key
└── public.cer
```