КриптоПро CSP

Криптопровайдер КриптоПро CSP предназначен для:

- авторизации и обеспечения юридической значимости электронных документов при обмене ими между пользователями, посредством использования процедур формирования и проверки электронной подписи (ЭП) в соответствии с отечественными стандартами ГОСТ Р 34.10-2001 / ГОСТ Р 34.10-2012 (с использованием ГОСТ Р 34.11-94 / ГОСТ Р 34.11-2012);
- обеспечения конфиденциальности и контроля целостности информации посредством ее шифрования и имитозащиты, в соответствии с ГОСТ 28147-89;
- обеспечения аутентичности, конфиденциальности и имитозащиты соединений по протоколу TLS;
- контроля целостности системного и прикладного программного обеспечения для его защиты от несанкционированных изменений и нарушений правильности функционирования;
- управления ключевыми элементами системы в соответствии с регламентом средств защиты.

КриптоПро CSP

Сертифицированные версии

4.0 R3

- R3-4.0.9944 Debian amd64
- R3-4.0.9944 MS Windows

4.0 R4

- R4-4.0.9963 Debian amd64
- R4-4.0.9963 MS Windows

Установка

cryptoprocsp-install.sh

```
#!/bin/bash
tar -zxf linux-amd64_deb.tgz
cd /linux-amd64_deb
./install_gui.sh
```

Выбираем:

```
[*] KC1 Cryptographic Service Provider
[ ] KC2 Cryptographic Service Provider
[*] GUI for smart card and token support modules
[*] Smart Card and Token support modules
[*] OpenSSL library
[*] stunnel, SSL/TLS tunnel with GOST support
[*] PKCS #11 library
```

Лицензия

Файл:`/etc/opt/cprocsp/license.ini`

Посмотреть информацию о лицензии:

```
/opt/cprocsp/sbin/amd64/cpconfig -license -view
```

Ввод лицензии:

```
/opt/cprocsp/sbin/amd64/cpconfig -license -set НОМЕР
```

Как ввести серийный номер лицензии? Как посмотреть информацию о лицензии?

Считыватели

- FAT12 считыватели дискет
- FLASH считыватели флешек
- Registry (реестр в MS Windows)
- Считыватели смарт-карт
- HDimage — структура дискеты на жестком диске

Список подключённых считывателей

```
/opt/cprocsp/bin/amd64/list_pcsc
```

- Вывод:

  ```
  Aktiv Co. Rutoken S 00 00
  ```

- При отсутствии:

  ```
  ERROR: SCardListReaders(NULL)
  ```

КриптоПро | Что такое считыватели и носители? Чем они отличаются?

HDimage

Fix Me!

Структура дискеты на жестком диске

Смотри Ключи пользователей

Хранилища пользователей

Fix Me!

Папка: `/var/opt/cprocsp/users`

По умолчанию для каждого пользователя создаётся папка (имя пользователя)

```
/var/opt/cprocsp/users/user
stores
local.ini
```

```
/var/opt/cprocsp/users/user/stores
cache.sto
my.sto
request.sto
```

Ключи пользователей

Fix Me!

Папка: `/var/opt/cprocsp/keys`

По умолчанию для каждого пользователя создаётся папка (имя пользователя), внутри которой располагаются папки—контейнеры

Пример:

`/var/opt/cprocsp/keys/user/key0.000`

1. `header.key`
2. `masks.key`
3. `masks2.key`
4. `name.key`
5. `primary.key`
6. `primary2.key`

Права:

Владелец	`user`
Маска для папок	`0700/drwx`
Маска для файлов	`0600/drwx`

Работа с ключами и сертификатами

КриптоПро | Работа с ключами и сертификатами

Список всех ключевых носителей и контейнеров

Вывести список всех ключевых носителей и контейнеров

```
/opt/cprocsp/bin/amd64/csptest -keyset -enum_cont -verifyc -fqcn
```

вывод:

```
CSP (Type:80) v4.0.9019 KC1 Release Ver:4.0.9963 OS:Linux CPU:AMD64 FastCode:READY:SSSE3.
AcquireContext: OK. HCRYPTPROV: 37226051
\\.\Aktiv Co. Rutoken S 00 00\95e7adc7-83aa-4508-be35-5e875cf36121
OK.
Total: SYS: 0,000 sec USR: 0,130 sec UTC: 1,030 sec
[ErrorCode: 0x00000000]
```

Копирование ключевого носителя из ключа в файлы

Копирование ключевого носителя из ключа в файлы, в данном случае в`/var/opt/cprocsp/keys/user/key0.000`

```
/opt/cprocsp/bin/amd64/csptest -keycopy -contsrc '\\.\Aktiv Co. Rutoken S 00 00\95e7adc7-83aa-4508-be35-5e875cf36121' -contdest '\\.\HDIMAGE\key0' -typesrc 75 -typedest 75 -pinsrc 12345678 -pindest 12345678
```

Загрузка личного сертификата в хранилище

Загрузка личного сертификата в хранилище в данном случае из локального считывателя

```
/opt/cprocsp/bin/amd64/csptestf -absorb -cert -pattern 'HDIMAGE'
```

Проверка работоспособности контейнера

```
/opt/cprocsp/bin/amd64/csptest -keyset -check -cont '\\.\HDIMAGE\key0'
```

КриптоПро | Как проверить, работоспособен ли контейнер с закрытыми ключами?

Просмотр установленных сертификатов

```
/opt/cprocsp/bin/amd64/certmgr -list
```

КриптоПро ЭЦП Browser plug-in

КриптоПро ЭЦП Browser plug-in предназначен для создания и проверки электронной подписи (ЭП) на веб-страницах с использованием СКЗИ «КриптоПро CSP».

версия 2.0 для пользователей (автоматическая загрузка версии плагина, соответствующей Вашей ОС)

- Актуальная, развивающаяся версия, находится в процессе сертификации.
- Поддерживает работу с алгоритмами ГОСТ Р 34.10/11-2012 (при использовании с КриптоПро CSP 4.0 и выше).
- Для Microsoft Windows совместима с КриптоПро CSP версии 3.6 R4 и выше, для других ОС – с КриптоПро CSP версии 4.0 и выше.
- Компоненты КриптоПро TSP Client 2.0 и КриптоПро OCSP Client 2.0, входящие в данную версию, не принимают лицензию от версий 1.x.
- Минимальная поддерживаемая версия Microsoft Windows — **Windows XP**.
- Для работы в Firefox версии 52 и выше требуется дополнительно установить расширение для браузера.

Порядок установки: 1. Установить пакет alien, необходимый для конвертации rpm-пакетов в deb-формат

```
apt install alien
```

2. Загрузить архив cades_linux_amd64.tar.gz https://www.cryptopro.ru/products/cades/plugin/get_2_0

3. Распаковать архив

```
tar -zxf cades_linux_amd64.tar.gz
```

4. Перейти в папку с распакованными файлами и выполнить преобразование пакетов:

```
alien *.rpm
```

5. Установить deb-пакеты:

```
dpkg -i lsb-cprocsp-devel_*.deb cprocsp-pki-*.deb
```

6. Установить расширение:

- Для FireFox https://www.cryptopro.ru/sites/default/files/products/cades/extensions/firefox_cryptopro_extension_latest.xpi
- Для Chromium CryptoPro Extension for CAdES Browser Plug-in

7. Создать символические ссылки на библиотеки:

```
ln -s /opt/cprocsp/lib/amd64/libnpcades.so /usr/lib/mozilla/plugins/lib/libnpcades.so
ln -s /opt/cprocsp/lib/amd64/libcppkcs11.so.4.0.4 /usr/lib/mozilla/plugins/lib/libcppkcs11.so
```

Для проверки работы ПО и списка сертификатов удобно использовать:
Проверка работы КриптоПро ЭЦП Browser plug-in

PKCS11

Для корректной работы pkcs11, настройку слотов следует сделать явной, для этого в файл /etc/opt/cprocsp/config64.ini в разделе PKCS11 после

```
# [PKCS11\slot0]
# ProvGOST = "Crypto-Pro GOST R 34.10-2001 KC1 CSP"
# ProvRSA = "Microsoft Strong Cryptographic Provider"
# reader = hdimage
```

```
нужно добавить:
[PKCS11\slot17]
ProvGOST = "Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider"
Firefox = 1
Reader = ""
```

Linux

Fix Me!

Перечисление контейнеров

- Пользователя

```
/opt/cprocsp/bin/amd64/csptest -keyset -enum_cont -verifycontext -fqcn
```

- Компьютера

```
/opt/cprocsp/bin/amd64/csptest -keyset -enum_cont -verifycontext -fqcn -machinekeys
```

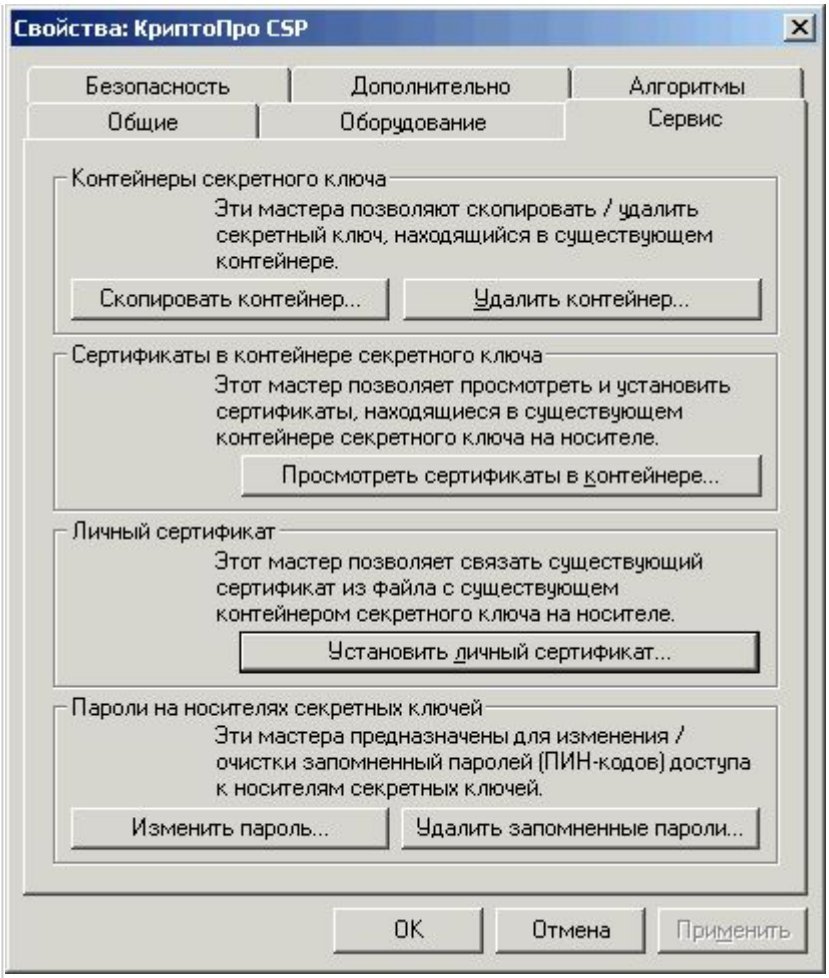
Как посмотреть список закрытых ключей?

Установка ЭЦП в MS Windows

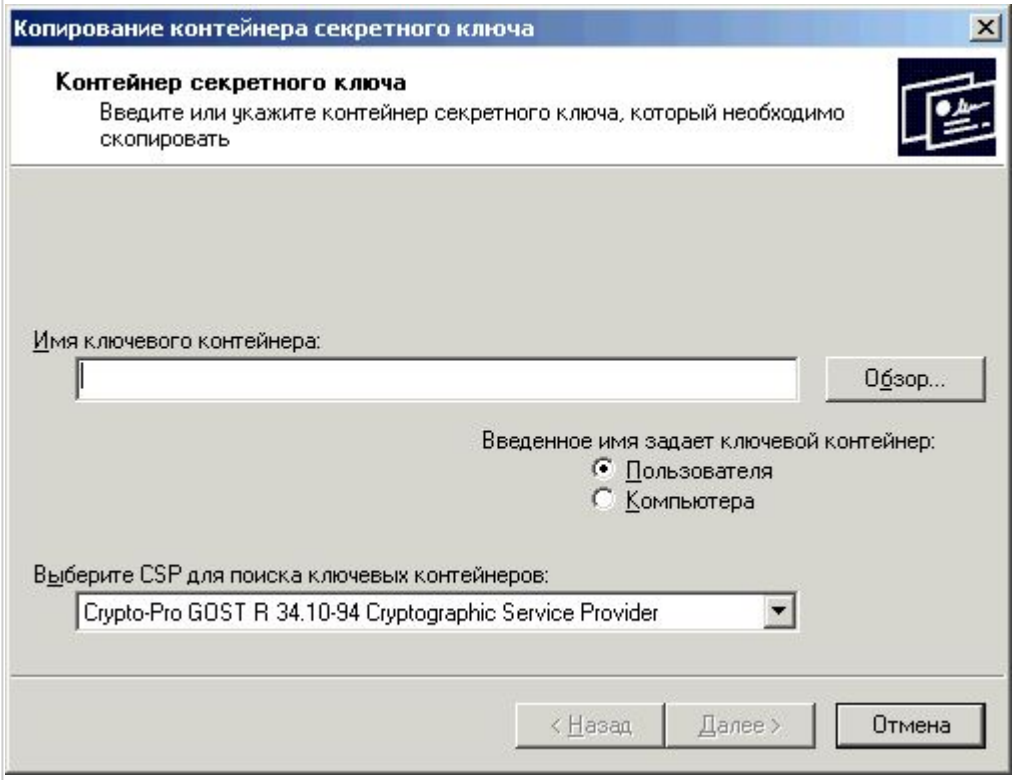
Создание рабочей копии

1. Вставьте ОРИГИНАЛ дискеты с ЭЦП Директора в дисковод.

2. Зайдите «Пуск» - «Панель управления» - «КриптоПро CSP», вкладка «Сервис» (см.рис.)



3. Нажмите кнопку Скопировать контейнер. Откроется окно «Копирование контейнера секретного ключа» (см.рис.).

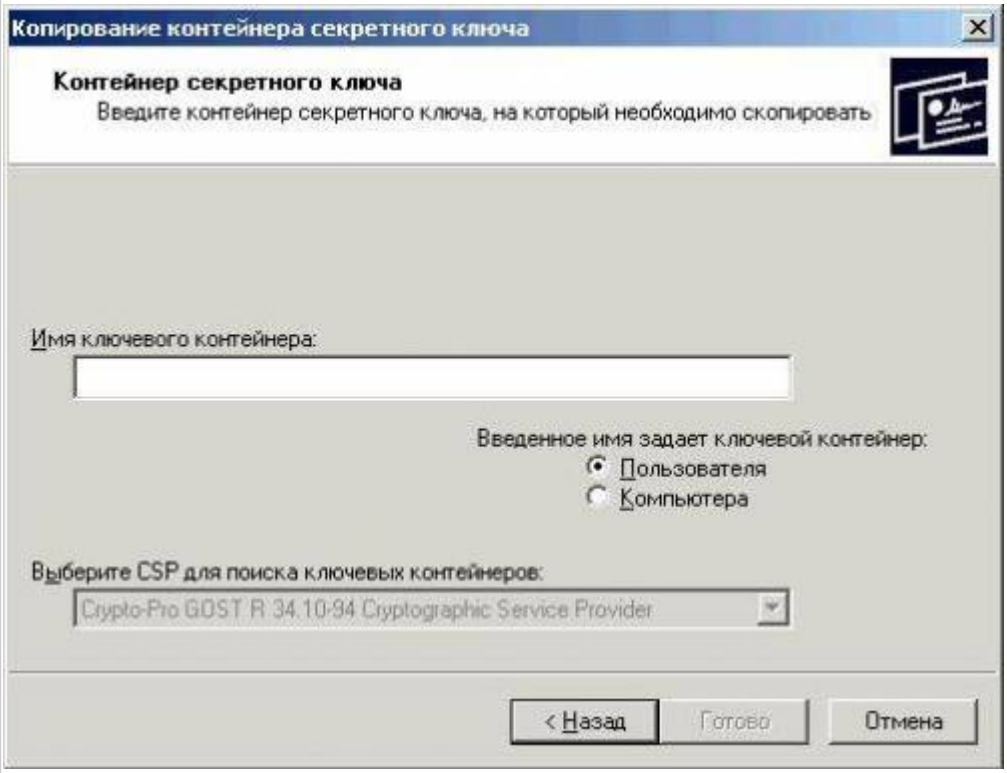


4. Нажмите кнопку Обзор и выберите ключевой контейнер с дискеты.

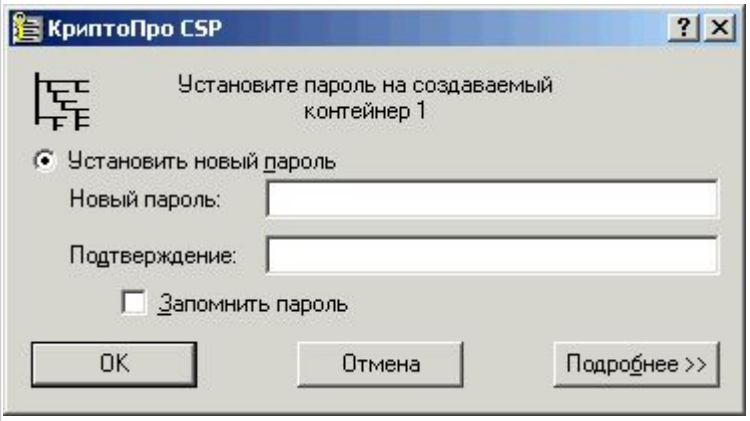
5. Нажмите кнопку Далее.

6. Извлеките ОРИГИНАЛ дискеты из дисковода и вставьте ЧИСТУЮ дискету.

7. В поле «Имя ключевого контейнера» (см.рис.) введите ТОЛЬКО фамилию директора.



8. Нажмите кнопку Готово. Откроется окно «КриптоПро CSP» с просьбой установить пароль на создаваемый контейнер (см.рис.), ничего не вводите и нажмите «ОК»



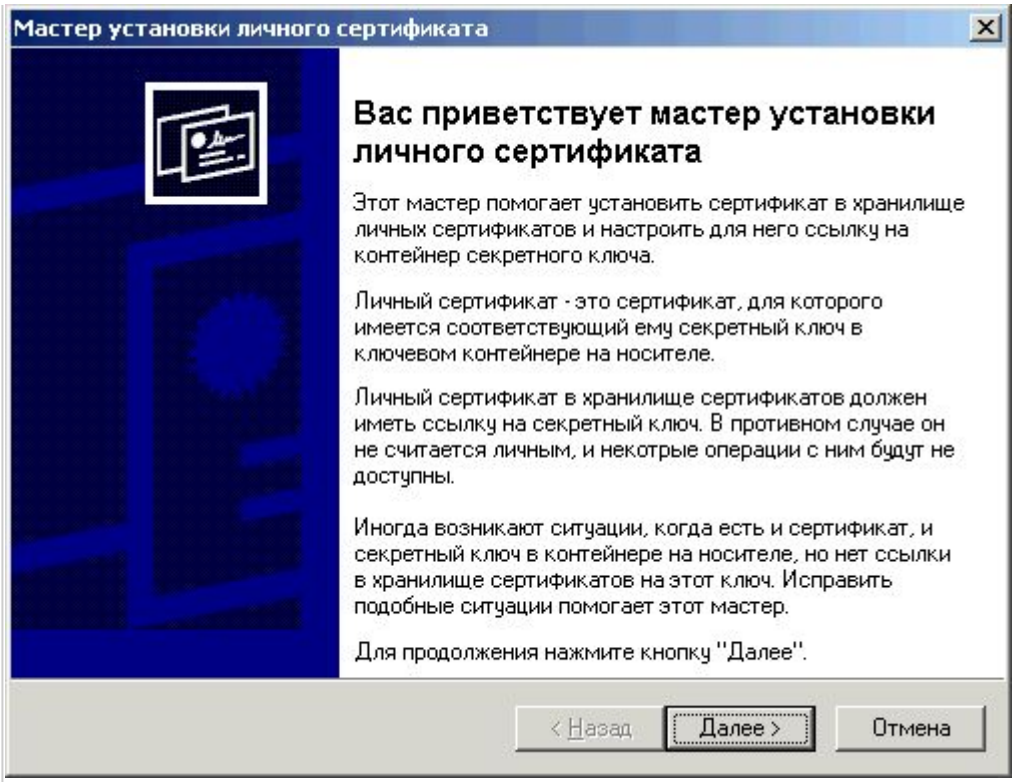
9. Скопируйте личный сертификат с ОРИГИНАЛА дискеты («зеленый» файл с расширением .cer) на КОПИЮ (Посредством копирования на «Рабочий стол»).

10. Если у Вас есть ЭЦП на Главного бухгалтера, то повторите пункты с 1 по 9 для ЭЦП Главного бухгалтера (в п. 6. Извлеките ОРИГИНАЛ дискеты из дисковода и вставьте КОПИЮ дискеты с подписью Директора.).

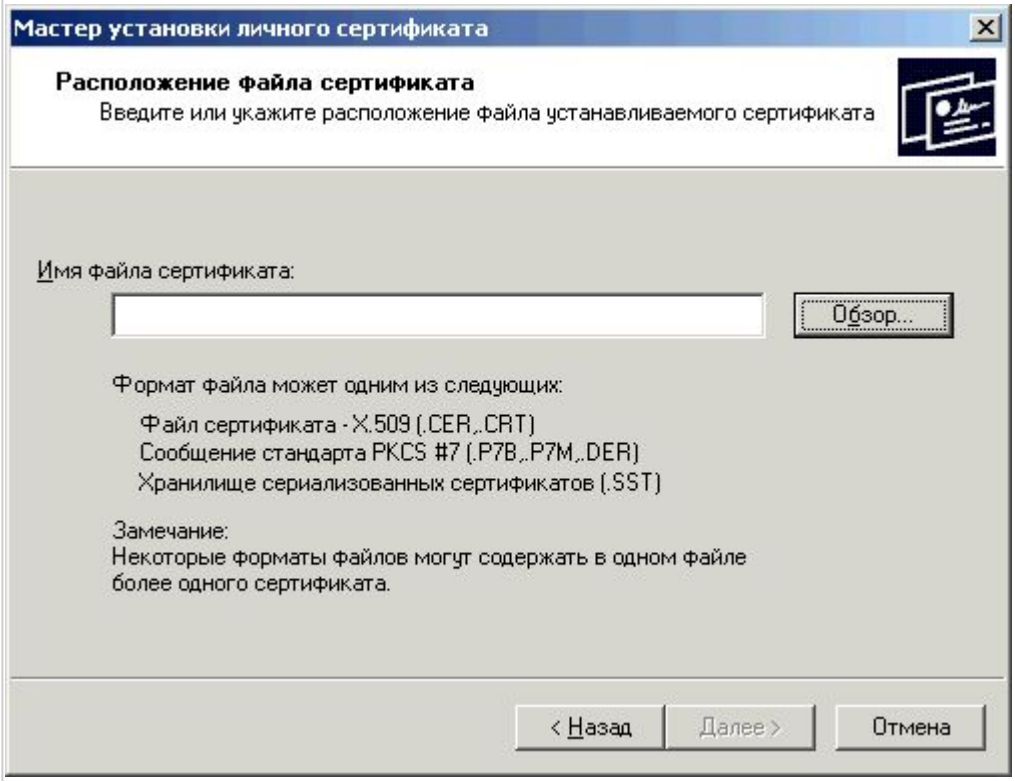
1. Вставьте КОПИЮ дискеты с ЭЦП Директора в дисковод.

2. Зайдите «Пуск» - «Панель управления» - «КриптоПро CSP», вкладка «Сервис».

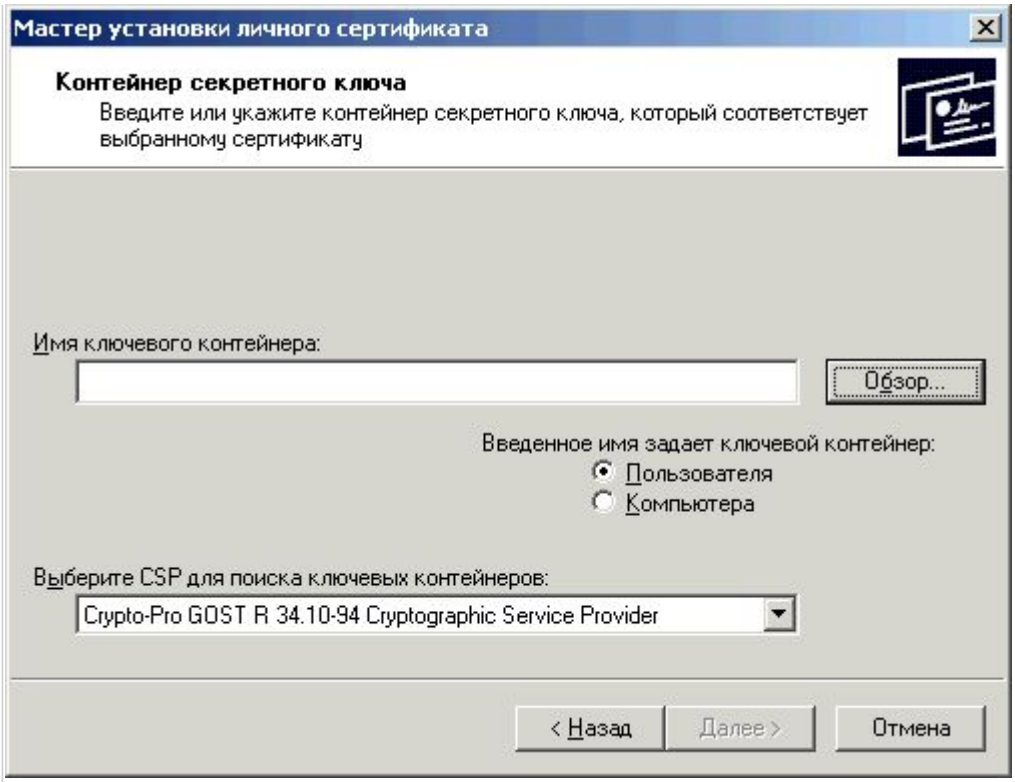
3. Нажмите кнопку Установить личный сертификат. Откроется мастер установки личного сертификата.



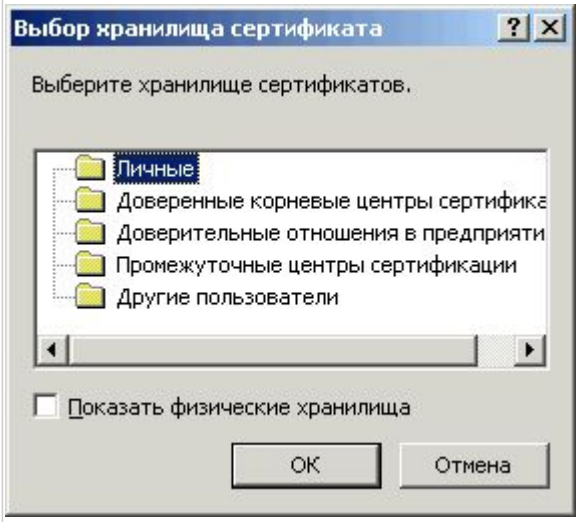
4. Нажмите кнопку Далее, на следующей вкладке (см.рис.) нажмите кнопку Обзор и выберите личный сертификат с дискеты («зеленый» файл с расширением .cer).



5. Нажмите два раза кнопку Далее, затем кнопку Обзор (см.рис.) и выберите ключевой контейнер с дискеты.



6. Нажмите кнопку «Далее», затем кнопку Обзор и выберите хранилище «Личные» (см.рис.).



7. Нажмите кнопку Далее, Готово.

8. Если у Вас есть ЭЦП на Главного бухгалтера, то повторите пункты с 1 по 7 для ЭЦП Главного бухгалтера.

9. После установки сертификата закройте КриптоПро CSP, нажав на кнопку OK.

ГОСТ Р 34.10-2012

В соответствии с принятым в 2014 году порядком перехода на ГОСТ Р 34.10-2012 с 1 января 2019 года приведет к ошибке/предупреждению (в зависимости от продукта и режима работы), которые могут привести к неработоспособности автоматических/автоматизированных систем при использовании ими ключей ГОСТ Р 34.10-2001.

ГОСТ 2012. Сообщение КриптоПро о переходе на новый ГОСТ — Контур.Экстерн

О работе с ГОСТ Р 34.10-2001 в КриптоПро CSP 3.9,4.0 и КриптоПро JCP 2.0 в 2019 году

КриптоПро | Согласовано использование ГОСТ Р 34.10-2001 в 2019 году для ряда существующих продуктов КриптоПро

КриптоПро CSP в 2019 году (инструмент для MS Windows, позволяющий за один вызов снять технические запреты)

Отключение окон о необходимости перехода на ГОСТ Р 34.10-2012

Для отключения данных предупреждений в КриптоПро CSP, нужно добавить два ключа в конфигурационный файл `/etc/opt/cprocsp/config64.ini` в существующую секцию `Parameters`:

```
[Parameters]
#Параметрыпровайдера
warning_time_gen_2001=ll:9223372036854775807
warning_time_sign_2001=ll:9223372036854775807
```

Отключение окон о необходимости перехода на ГОСТ Р 34.10-2012

Ссылки

Логотип

FAQ - Использование КриптоПро CSP под управлением ОС семейства Unix/Linux.

Работа с КриптоПро на linux сервере

Установка сертификатов используя КриптоПРО в Linux

КриптоПро — ALT Linux Wiki

Инструкция по установке КриптоПро

Установка и настройка КриптоПро CSP в Porteus Linux - Porteus

Работа с КриптоПро CSP - Справочный центр - Справочный центр Astra Linux

Установка и настройка КриптоПРО на Linux

http://sysadminmosaic.ru/crypto_pro_csp/crypto_pro_csp

2024-01-16 13:48