Работа с VipNet CSP

О программе

Программное обеспечение ViPNet CSP Linux позволяет организовать выполнение криптографических операций на компьютерах, работающих под управлением операционных систем семейства Linux, и обеспечить защищенный обмен данных на основе инфраструктуры открытых ключей (PKI)

Состав программного обеспечения

Программное обеспечение ViPNet CSP Linux состоит из нескольких пакетов. В зависимости от ваших задач вы можете установить лишь некоторые из них.

Основные пакеты, входящие в ПО ViPNet CSP Linux. Полный перечень всех пакетов можно найти в Руководстве пользователя Vipnet CSP.

Название пакета	Основные файлы	Назначение
itcs-licensing	license	Утилита для регистрации ViPNet CSP Linux.
itcs-winapi	certmgr	Утилита с командным интерфейсом для работы с хранилищем сертификатов.
	certreq	Утилита с командным интерфейсом для создания контейнера ключей и запроса на сертификат.
itcs-winapi-gui	certmgr-gui	Утилита с графическим пользовательским интерфейсом для работы с хранилищем сертификатов.

itcs-entropy-gost	rngcmgr rngpkcs11host	Утилита с командным интерфейсом для работы с датчиками случайных чисел. Утилита, вызов которой используется при использовании датчика случайных чисел, реализованного на поддерживаемом внешнем устройстве
itcs-entropy-gost-gui	rngqtmgr	Утилита с графическим пользовательским интерфейсом для работы с датчиками случайных чисел.
itcs-csp-gost	csp-integral-test csp-gost	Утилита для проверки функциональности криптопровайдера. Утилита с командным интерфейсом для настройки криптопровайдера ViPNet CSP Linux. Позволяет выполнять следующие действия: • Просмотр и удаление контейнеровключей. • Просмотр и настройка списка опрашиваемых внешних устройств. • Регламентный контроль датчика случайных чисел.
itcs-csp-gost-gui	Библиотека графических элементов	Содержит элементы, реализующие графический пользовательский интерфейс криптопровайдера. К таким элементам относятся, например, окна для работы с контейнерами ключей.
itcs-integrity-check	check_prg make_ext_crg	Служебная утилита для проверки контроля целостности файлов программного обеспечения вручную. Служебная утилита для создания списка системных файлов ОС Linux, подлежащих контролю целостности.
itcs-cryptofile	cryptofile	Утилита, которая позволяет выполнять следующие операции с файлами: • формирование и проверка электронной подписи; • шифрование и расшифрование файлов; • кодирование данных в формат Base64.
itcs_wiper	wipe	Утилита для надежного удаления файлов.
itcs-softtoken	token_manager	Утилита для работы с программными токенами
itcs-openssl	key_manager	Служебная утилита для выполнения криптографических операций при работе с пакетом itcs-openssl.

Установка

Вы можете либо установить все пакеты, входящие в комплект поставки ПО ViPNet CSP Linux, либо выбрать только пакеты, необходимые для выполнения вашей конкретной задачи.

Расположение файлов после установки пакета будет следующим:
Библиотеки и утилиты, входящие во все пакеты:

- Примеры использования — /opt/itcs/share/samples .
- Заголовочные файлы — /opt/itcs/include .
- Исполняемые файлы — /opt/itcs/bin .

Кроме того, будут созданы необходимые служебные каталоги:

- Каталог для файлов настроек: /etc/opt/itcs .
- Каталог для хранения данных приложений: /var/opt/itcs/vipnet-csp .

Каталог для хранения пользовательских данных (например, контейнеров ключей): /home/<username>/.itcs/vipnet-csp .

Ручная установка

Для установки следует воспользоваться командой:

```
sudo dpkg -i /  /__>.deb
```

Пакеты из состава ПО ViPNet CSP Linux следует последовательно устанавливать в следующем порядке:

1. itcs-licensing
2. itcs-known-path
3. itcs-entropy-gost
4. itcs-winapi
5. itcs-csp-gost

Чтобы добавить библиотеки и утилиты с реализацией графического интерфейса криптопровайдера, установите пакеты:

- itcs-winapi-gui.
- itcs-entropy-gost-gui.
- itcs-csp-gost-gui.

Установка с помощью скрипта

В ViPNet CSP Linux версии 4.4 и выше, Вы можете установить необходимые пакеты с помощью специального скрипта **vipnetcsp_pkg_manager.sh**. При этом зависимости между пакетами будут учтены автоматически.

Для ОС Astra Linux Special Edition (Smolensk 1.5, 1.6) и Astra Linux Common Edition (Orel 2.12) :

```
./vipnetcsp_pkg_manager.sh install --package deb --platform x86_64 --dist ../deb/
```

⚠ Наборы пакетов, подлежащие установке. Возможные значения:

- all — все подходящие пакеты, находящиеся в каталоге.
- vipnet_csp — все подходящие пакеты ViPNet CSP Linux без пакетов, отвечающих за работу утилит с графическим интерфейсом.
- vipnet_csp_gui — все подходящие пакеты ViPNet CSP Linux.

Регистрация ViPNet CSP Linux

После установки на компьютер программное обеспечение ViPNet CSP Linux работает в демо-режиме (срок его использования ограничен двумя неделями).

Чтобы зарегистрировать ViPNet CSP Linux с помощью полученного кода регистрации, в командной строке перейдите в каталог /opt/itcs/bin и запустите утилиту license со следующими параметрами:

```
sudo ./license register --product=<> --serial=< > --code=< >
```

где:

- <идентификатор> — идентификатор продукта (csp_linux).
- <серийный номер> — Ваш серийный номер.
- <регистрационный код> — Ваш регистрационный код.

Чтобы убедиться, что программное обеспечения ViPNet CSP Linux зарегистрировано, запустите утилиту license со следующим параметром:
./license list
В результате будет выведена информация об установленной лицензии.

Носители и контейнеры

Просмотр доступных контейнеров ключей:

```
$ ./csp-gost print_containers

Printing available containers (for user):

 0. SafeNet eToken (eToken Aladdin)(Makhmadiev): abn_0199.key
 1. /home/astrauser/.itcs/vipnet-csp/containers/test1234

SUCCESSED
```

Свойства контейнера:

```
$ ./csp-gost container_content --container abn_0199.key

Container
 Name: abn_0199.key
 Type: Device
 Location: SafeNet eToken (eToken Aladdin)(Makhmadiev)

Certificate
 Issuer:
 Subject: "-     "
 Serial: 01 d4 71 12 b2 ad 03 20 00 00 0a 57 06 ba 00 05
 Subject key identifier: e4 09 ca 71 42 ef 6a 5d 8a ec 70 8c 9d dd dd dd dd 74 e4 78
 Not before: 31-10-2018 17:10:00
 Not after: 31-10-2019 17:10:00
 Fingerprint (SHA1 hash): aa bb cc dd 0e 8e e0 84 e3 8f 48 85 4f 40 80 ef 1a c6 31 04

SUCCESSED
```

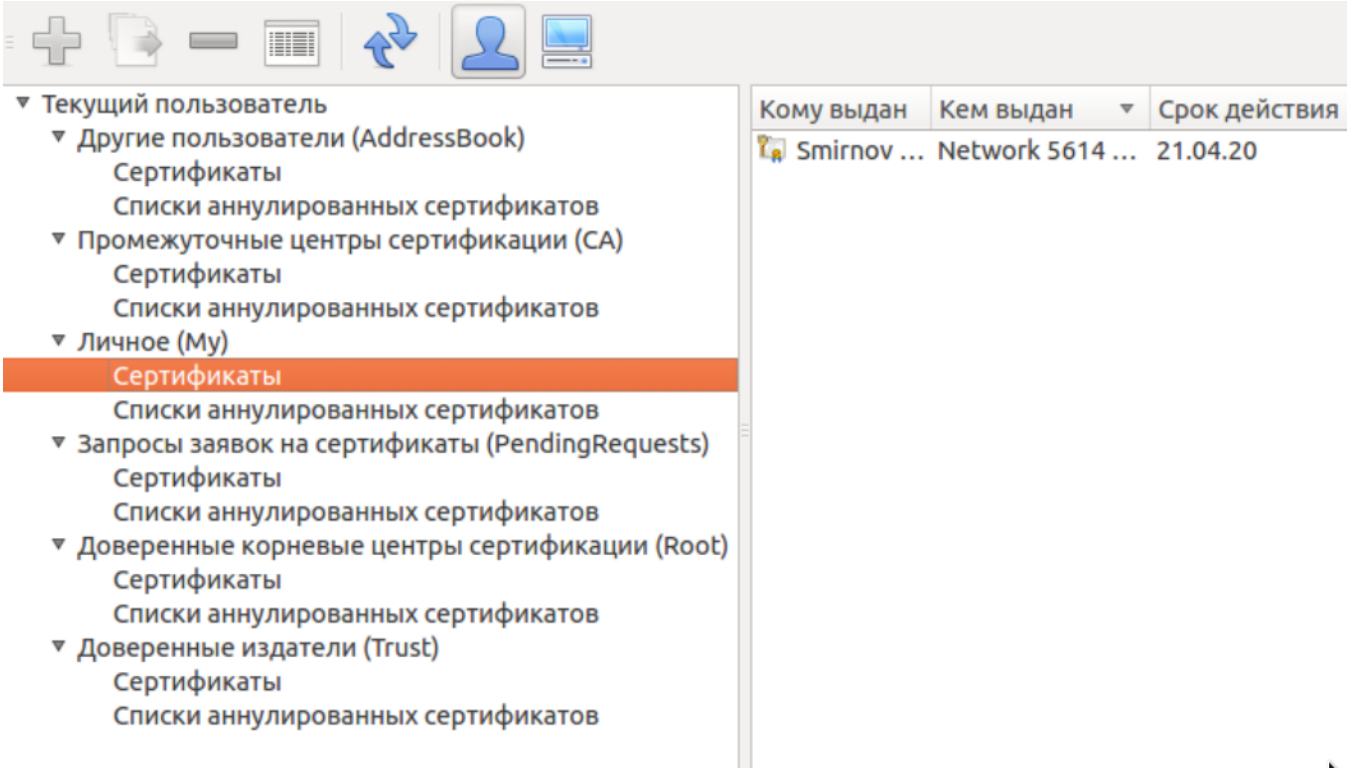
В результате на экран будет выведен список свойств контейнера ключей, а также соответствующего сертификата, если таковой имеется.

Менеджер сертификатов Vipnet CSP Linux

Установка и сертификата в системное хранилище с помощью утилиты, имеющей графический интерфейс (gui)

Чтобы установить сертификат в системное хранилище с помощью утилиты с графическим интерфейсом пользователя, выполните следующие действия:

- Перейдите в каталог /opt/itcs/bin и запустите утилиту certmgr-gui



В окне Хранилище сертификатов на панели инструментов, выберите в какое хранилище сертификатов вы хотите установить сертификат (My, Root, CA, AddressBook).

Текущий пользователь - Личное - если вы хотите установить сертификат в хранилище сертификатов пользователя.

Локальный компьютер - если вы хотите установить сертификат в хранилище сертификатов компьютера.

Установка сертификата в системное хранилище с помощью утилиты, имеющей командный интерфейс (cli)

Установка

Чтобы установить сертификат в системное хранилище с помощью утилиты с командным интерфейсом, в командной строке перейдите в каталог /opt/itcs/bin и запустите утилиту certmgr со следующими параметрами:

```
./certmgr add_certificate --location=<> --store=My --file=< > --container=<  >
```

где:

<хранилище> — хранилище сертификатов, задайте одно из следующих значений:

CurrentUser — если вы хотите установить сертификат в хранилище сертификатов пользователя (является значением по умолчанию);

LocalMachine — если вы хотите установить сертификат в хранилище сертификатов компьютера .

Пример запуска утилиты certmgr с параметрами:

```
./certmgr add_certificate --location=CurrentUser --store=My --file=/home/astrauser/cert1 --container=/home
/astrauser/.itcs/vipnet-csp/containers/cont1
```

В результате сертификат будет установлен в выбранное хранилище. Если вы указали путь к соответствующему контейнеру ключей, между сертификатом и контейнером ключей будет установлена связь. Это позволит внешним приложениям, работающим с сертификатом, обращаться к соответствующему контейнеру ключей и выполнять с помощью него криптографические операции.

Просмотр свойств сертификатов

Если вы хотите просмотреть свойства сертификата, следует воспользоваться командой:

```
./certmgr print_certificates --location =<> --store=< >
```

Отобразится список сертификатов, установленных в заданном разделе хранилища. Каждому сертификату присваивается порядковый номер (параметр Index). Используйте его при следующем запуске утилиты с новыми параметрами:

```
./certmgr print_certificate --location =<> --store=< > --index=<  >
```

Пример запуска утилиты для просмотра свойств сертификата:

```
./certmgr print_certificates --location=CurrentUser --store=My
./certmgr print_certificate --location=CurrentUser --store=My --index=4
```

Пример запуска утилиты для просмотра свойств списка CRL:

```
./certmgr print_crls --location=CurrentUser --store=My
./certmgr print_crl --location=CurrentUser --store=My --index=2
```

Выполнение криптографических операций с файлами

С помощью тестовой утилиты cryptofile вы можете зашифровывать и расшифровывать файлы,подписывать файлы электронной подписью и проверять электронную подпись.

Примеры команд для выполнения таких операций приведены ниже.

Пример подписания файла test.doc (для задания закрытого ключа используется имя издателя и серийный номер соответствующего ему сертификата):

```
/opt/itcs/bin/cryptofile sign --in=/home/user1/test.doc --out=/home/user1/test.doc.sig --nodetach --DER --
issuer_serial="CRYPTO-CA|4ee987f40000000009fd"
```

Пример зашифрования файла test.doc:

```
/opt/itcs/bin/cryptofile encrypt --in=/home/user1/test.doc --out=/home/user1/test.doc.enc --issuer_serial="
CRYPTO-CA|4ee987f40000000009fd"
```

Пример проверки электронной подписи файла test.doc.sig:

```
/opt/itcs/bin/cryptofile verify --in=/home/user1/test.doc.sig --out=/home/user1/test.doc
```

Пример расшифрования файла test.doc.enc:

```
/opt/itcs/bin/cryptofile decrypt --in=/home/user1/test.doc.enc --out=/home/user1/test.doc
```

Работа ViPNet CSP Linux в режиме замкнутой программной среды

Под управлением ОС Astra Linux SE 1.5

Если вы устанавливаете ПО ViPNet CSP Linux на компьютер под управлением ОС Astra Linux Special Edition («Смоленск») 1.5 и планируете работать с данным ПО в режиме замкнутой программной среды, используйте открытый ключ infotecs_pub_key.gpg, входящий в комплект поставки ViPNet CSP Linux, и следуйте инструкциям из справочного центра Astra Linux: https://wiki.astralinux.ru/pages/viewpage.action?pageId=1212431

Под управлением ОС Astra Linux SE 1.6

Если вы устанавливаете ПО ViPNet CSP Linux на компьютер под управлением ОС Astra Linux Special Edition («Смоленск») 1.6 и планируете использовать данное ПО в режиме замкнутой программной среды, выполните следующие действия:

1) Установите пакет из состава Astra Linux astra-digsig-oldkeys.
2) Поместите открытый ключ infotecs_pub_key.gpg, входящий в комплект поставки ViPNet CSP Linux, в следующий каталог:
/etc/digsig/keys/legacy/keys/
3) Следуйте инструкциям из справочного центра Astra Linux: https://wiki.astralinux.ru/pages/viewpage.action?pageId=1212431

Полезные ссылки

Сведения о продуктах и решениях ViPNet, распространенные вопросы и другая полезная информация собраны на сайте «ИнфоТеКС»:

- Веб-портал документации ViPNet http://docs.infotecs.ru.
- Описание продуктов ViPNet http://www.infotecs.ru/products/line/
- Информация о решениях ViPNet http://www.infotecs.ru/solutions/
- Сборник часто задаваемых вопросов (FAQ) http://www.infotecs.ru/support/faq/
- Форум пользователей продуктов ViPNet http://www.infotecs.ru/forum/.