Инструкция по работе с ViPNet PKI в ОС Альт Линукс

На 9 листах

2020 г.

Оглавление

1 РАЗВЕРТЫВАНИЕ VIPNET PKI В ОС АЛЬТ LINUX

Информация о ViPNet PKI Client расположена здесь https://infotecs.ru/product/vipnet-pki-client.html#soft.

Для установки ПК ViPNet PKI Client необходимо выполнить следующие действия:

- Распаковать дистрибутив в произвольный каталог с помощью команды:

  tar –xvf <путь к каталогу>/pki_client_linux-<разрядность операционной системы>-dist.tar.bz2

- Поместить файл лицензии в каталог с пакетами для установки ViPNet PKI Client.
- Перейти в папку с установочным файлом и пакетами ViPNet PKI Client с помощью команды:

  cd <путь к папке>

- Запустить скрипт install.sh с правами суперпользователя с помощью команды:

  sudo ./install.sh

  Будет запущена программа установки. Программа установки выполнит проверку наличия пакетов, необходимых для установки. Если какой-либо пакет не будет найден, программа установки завершит свою работу, и будет выдано соответствующее сообщение. В этом случае необходимо установить недостающие пакеты и снова запустить программу установки.

URL-адрес, по которому веб-страница будет обращаться к программе Web Unit:
http://127.0.0.1:61111/webhost — для подключения по протоколу HTTP;
https://127.0.0.1:61112/webhost — для подключения по протоколу HTTPS.

1.1 Установка сертификатов

1.1.1 Способ 1

Данный способ позволяет установить только личные сертификаты, запрос на которые был создан в ПК ViPNet PKI Client (см. Руководство пользователя ViPNet PKI Client File Unit Linux, стр 26).

Чтобы установить сертификаты и (или) CRL в хранилище сертификатов, необходимо выполнить следующие действия:

- Чтобы установить сертификаты издателей и CRL в хранилище локального компьютера, необходимо запустить настройки ViPNet PKI Client с правами суперпользователя.

  Внимание! При запуске настроек с правами суперпользователя нельзя устанавливать личные сертификаты и сертификаты получателей, поскольку они

будут установлены в хранилище сертификатов пользователя root и с ними невозможно будет работать после запуска настроек под своей учетной записью.

- Далее следует перейти в раздел «Сертификаты» и нажать кнопку «Добавить сертификат или CRL», затем указать путь к файлу сертификата или CRL.
- В окне «Добавление сертификатов и CRL» отображаются устанавливаемые сертификаты и (или) CRL. В окне «Добавление сертификатов» следует нажать кнопку «Добавить». В результате начнется установка сертификатов и (или) CRL в хранилище сертификатов.

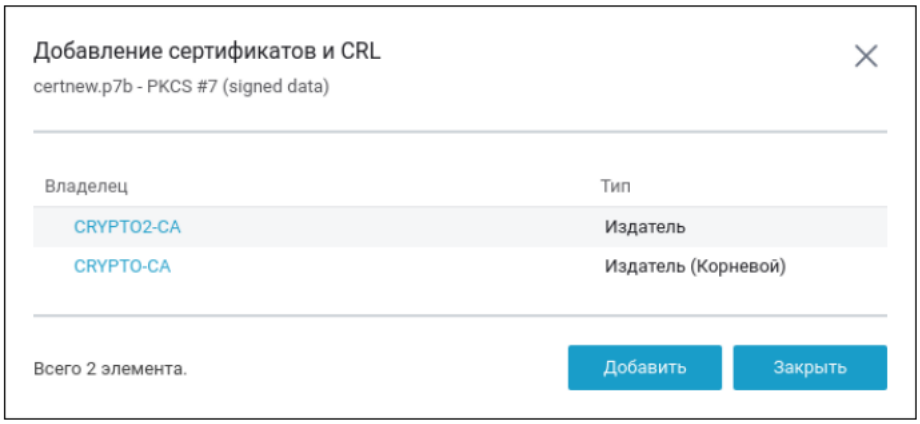


Рисунок 1.Добавление сертификата и CRL

- Далее следует нажать кнопку «Закрыть».

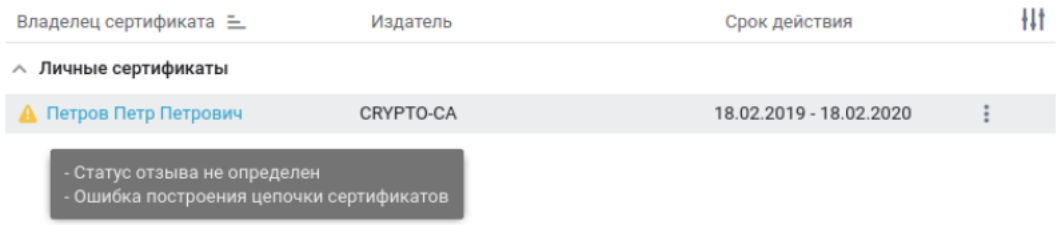


Рисунок 2. Просмотр предупреждающих сообщений

Предупреждающие сообщения описаны в Руководстве пользователя ViPNet PKI Client File Unit Linux, стр 28.

1.1.2 Способ 2

Данный способ позволяет установить сертификат в системное хранилище с помощью утилиты для работы с системным хранилищем, имеющей графический интерфейс (см. Руководство пользователя ViPNet CSP Linux User Guide Ru, стр. 47).

Чтобы установить сертификат в хранилище сертификатов, необходимо выполнить следующие действия:

- Перейти в каталог /opt/itcs/bin и запустить утилиту certmgr-gui.
- В окне «Хранилище сертификатов» на панели инструментов необходимо выбрать в какое хранилище сертификатов следует установить сертификат:

– Текущий пользователь – если требуется установить сертификат в хранилище сертификатов пользователя.
– Локальный компьютер – если требуется установить сертификат в хранилище сертификатов компьютера.

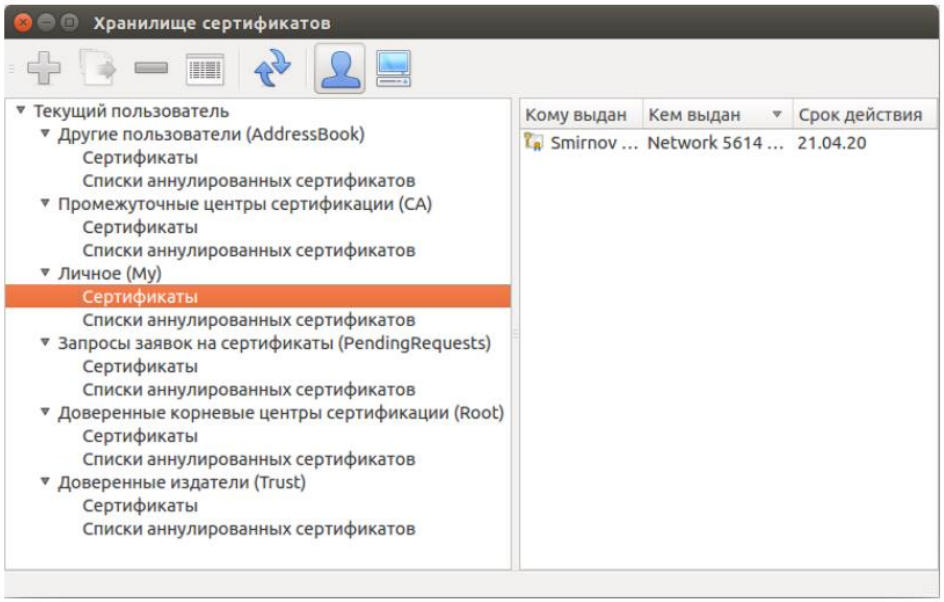


Рисунок 3. Работа с системным хранилищем сертификатов с помощью утилиты certmgr-gui

- Далее следует выбрать на левой панели раздел Личное (My).
- Затем, на панели инструментов следует нажать кнопку «Импорт». В результате откроется мастер импорта элемента.

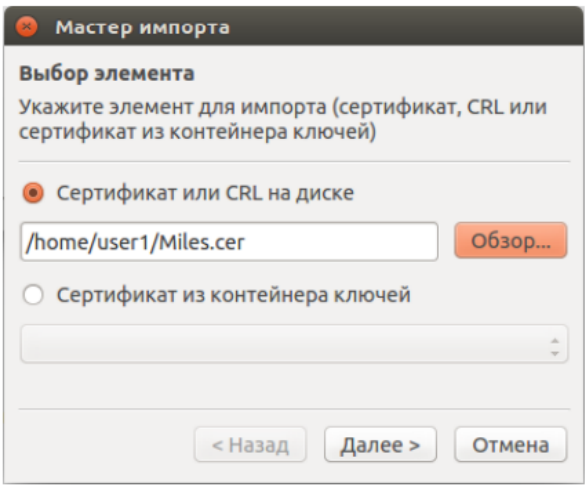


Рисунок 4. Выбор сертификата или списка CRL для установки в хранилище

- В окне мастера на странице «Выбор элемента» следует выполнить следующие действия:
  – Если устанавливается отдельный сертификат, не находящийся в контейнере ключей, то следует установить переключатель в положение «Сертификат или

CRL на диске», затем выбрать сертификат, который необходимо установить в системное хранилище.

- Если устанавливается сертификат, находящийся в контейнере ключей, то следует установить переключатель в положение «Сертификат из контейнера ключей», затем выбрать необходимый сертификат из списка.

  Примечание. Контейнер ключей, из которого устанавливается сертификат в хранилище сертификатов, должен находиться в каталоге хранения контейнеров ключей.

- Если необходимо установить отдельный сертификат, не находящийся в контейнере ключей, на странице «Выбор контейнера ключей» необходимо выполнить следующие действия:
  - Если на жестком диске компьютера в каталоге хранения контейнеров ключей сохранен контейнер ключей с закрытым ключом, соответствующим устанавливаемому сертификату, то необходимо выбрать его из списка.
  - Если на жестком диске компьютера не сохранен контейнер ключей с закрытым ключом, соответствующим устанавливаемому сертификату, то следует пропустить эту страницу мастера и нажать кнопку «Далее».

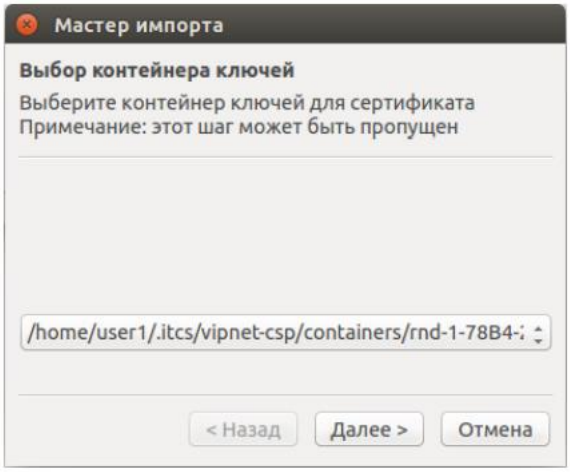


Рисунок 5. Выбор контейнера ключей, соответствующего устанавливаемому сертификату

- На последней странице мастера следует нажать кнопку «Завершить».

1.1.3 Способ 3

Данный способ позволяет установить сертификат в системное хранилище с помощью утилиты для работы с системным хранилищем, имеющей командный интерфейс (см. Руководство пользователя ViPNet CSP Linux User Guide Ru, стр. 49).

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

./certmgr add_certificate --location=<хранилище> --store=My --file=<путь к сертификату> --container=<путь к контейнеру>

где:

- <хранилище> – хранилище сертификатов, может принимать одно из следующих значений:
  - CurrentUser – если необходимо установить сертификат в хранилище сертификатов пользователя (является значением по умолчанию);
  - LocalMachine – если необходимо установить сертификат в хранилище сертификатов компьютера.
- <путь к сертификату> – путь к файлу с устанавливаемым сертификатом.
- <путь к контейнеру> – путь к контейнеру ключей, соответствующему устанавливаемому сертификату; параметр --container можно опустить, если на жестком диске компьютера не сохранен нужный контейнер.

Пример запуска утилиты certmgr с параметрами:

./certmgr add_certificate --location=CurrentUser --store=My -file=/home/user1/cert1 --container=/home/user1/.itcs/vipnet-csp/containers/cont1

В результате сертификат будет установлен в выбранное хранилище. Если был указан 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.

1.2 Возможные проблемы при развертывании

1.2.1 Проблема 1

```
installing itcs-entropy-gost-gui(4.4) itcs-entropy-gost-gui-4.4.0.1086-1 ...
ошибка: неудовлетворенные зависимости:
        qt >= 4.2 нужен для itcs-entropy-gost-gui-4.4.0.1086-1
 FAILED
```

Проблема: Используются обновления из кэша на диске.

Решение: Необходимо включить репозитории. Последовательность действий по устранению проблемы:

- Открыть терминал.
- Ввести команду: su.
- Ввести команду: mc.
- Перейти в каталог с файлом altsp.list. Открыть файл.

```
/etc/apt/sources.list.d/altsp.list
# update.altsp.su (IVK, Moscow)
# ALT Certified 8
# rpm [cert8] ftp://update.altsp.su/pub/distributions/ALTLinux/ c8/branch/x86_64 classic
# rpm [cert8] ftp://update.altsp.su/pub/distributions/ALTLinux/ c8/branch/x86_64-i586 classic
# rpm [cert8] ftp://update.altsp.su/pub/distributions/ALTLinux/ c8/branch/noarch classic
rpm [cert8] http://update.altsp.su/pub/distributions/ALTLinux/ c8/branch/x86_64 classic
rpm [cert8] http://update.altsp.su/pub/distributions/ALTLinux/ c8/branch/x86_64-i586 classic
rpm [cert8] http://update.altsp.su/pub/distributions/ALTLinux/ c8/branch/noarch classic
```

Рисунок 6. Файл altsp.list

- В файле altsp.list необходимо убрать комментарии у 3х нижних строчек.
- Сохранить и закрыть файл.
- Загрузить пакеты из репозитория и обновить установленные в системе пакеты с помощью команды:

apt-get update && apt-get dist-upgrade -y

1.2.2 Проблема 2

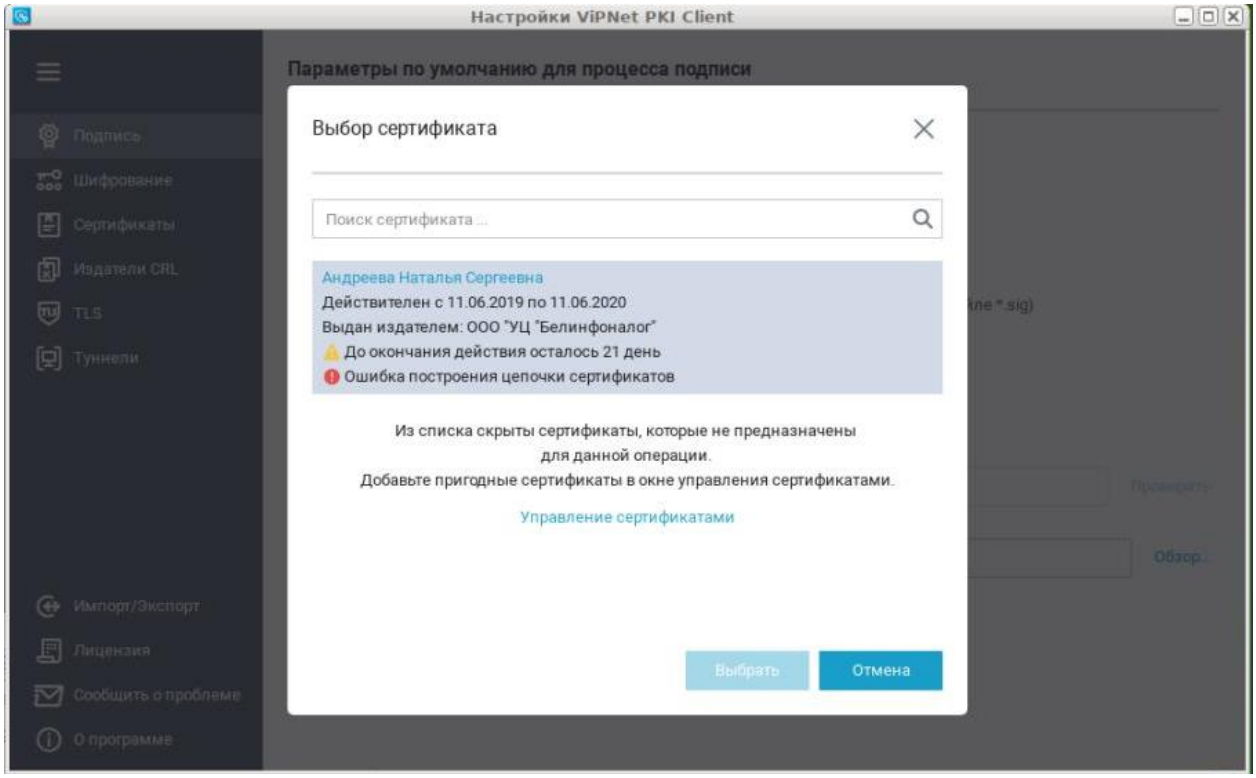
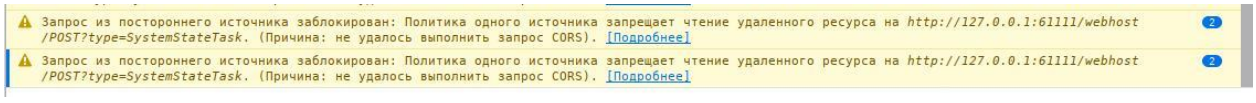


Рисунок 7. Ошибка построения цепочки

Решение: Просмотр цепочки сертификатов необходимо проверять в «Настройки VipNet PKI Client», т.к. в хранилище сертификатов может не отображаться пропущенный элемент цепочки.

1.2.3 Проблема 3



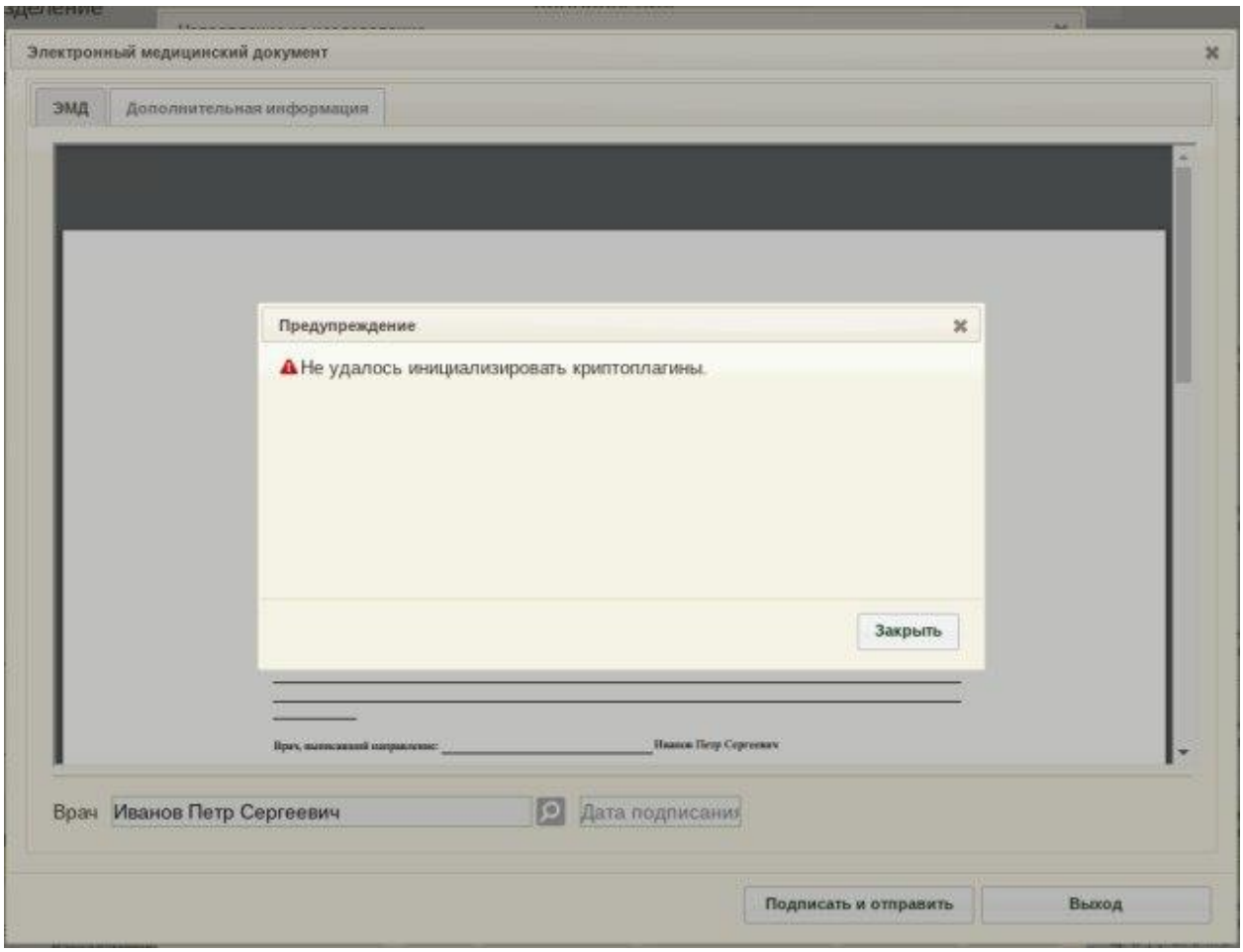


Рисунок 8. Ошибка инициализации

При пробросе через ssh окна браузера по какой-то причине тестовые методы ViPNet не отрабатываются ожидаемым образом. Может влиять различие идентификаторов x-сессии браузера и file-unit, который запускается при логине в сессии 0.

Решение: подключении по vnc.