



ViPNet PKI Client Linux

Руководство администратора

Версия продукта: 2.1.1

© АО «ИнфоТеКС», 2025

ФРКЕ.00175-03 32 05

Версия продукта 2.1.1

Этот документ входит в комплект поставки продукта ViPNet, и на него распространяются все условия лицензионного соглашения.

Ни одна из частей этого документа не может быть воспроизведена, опубликована, сохранена в электронной базе данных или передана в любой форме или любыми средствами, такими как электронные, механические, записывающие или иначе, для любой цели без предварительного письменного разрешения АО «ИнфоТеКС».

ViPNet® является зарегистрированным товарным знаком АО «ИнфоТеКС».

Все названия компаний и продуктов, которые являются товарными знаками или зарегистрированными товарными знаками, принадлежат соответствующим владельцам.

Все условия эксплуатации и ограничения на использование ViPNet PKI Client Linux приведены в Правилах пользования, Лицензионном соглашении с конечным пользователем либо в другой эксплуатационной документации, сопровождающей ViPNet PKI Client Linux.

АО «ИнфоТеКС»

125167, г. Москва, вн. тер. г. муниципальный округ Хорошевский, ул. Викторенко, д. 9, стр. 1, помещ. 47

Телефон: +7 (495) 737-6192, 8 (800) 250-0260 — бесплатный звонок из России (кроме Москвы)

Сайт: infotecs.ru

Служба поддержки: hotline@infotecs.ru

Содержание

Введение.....	5
О документе.....	6
Соглашения документа.....	6
Обратная связь.....	7
Что нового в версии 2.1.1	8
Лицензирование.....	9
 Глава 1. Начало работы	10
Установка и обновление	11
Установка и обновление на ОСноа в режиме замкнутой программной среды	11
Активация лицензии через ViPNet TLS Gateway.....	13
Импорт и экспорт настроек.....	15
Особенности импорта настроек	15
Экспорт настроек.....	16
Импорт настроек	16
Автоматическое распространение настроек из файла	16
 Глава 2. Настройка автоматического обновления CRL.....	18
Настройка подключения к прокси-серверам.....	19
Отслеживание событий при автообновлении CRL	21
 Глава 3. Настройка подключения к сайтам, использующим TLS ГОСТ	22
Требования к сертификатам для работы TLS Unit	23
Настройка подключения TLS Unit к прокси-серверам.....	25
Настройка совместной работы TLS Unit и браузера	27
Импорт сертификата ViPNet PKI Client Root в Firefox.....	27
Импорт сертификата ViPNet PKI Client Root в Chromium	27
Настройка прокси-сервера в Firefox.....	28
Настройка прокси-сервера в Chromium, Chromium ГОСТ, Opera, Яндекс.Браузер.....	28
 Глава 4. Подключение к туннелируемым ресурсам.....	29
Порядок настройки	30
Требования к сертификатам для работы Tunnel Unit	31
Добавление туннелируемого ресурса.....	32
Подключение к туннелируемому ресурсу	33

Приложение А. Возможные неполадки.....	34
Зависание при работе в Альт 8 СП Рабочая станция.....	34
Ошибки при обновлении CRL.....	34
Ошибка при установке ViPNet PKI Client	35
Ошибка при установке или запуске в Astra Linux Special Edition («Смоленск») 1.6.....	36
Ошибка при установке ViPNet PKI Client на Ubuntu	36
Ошибка при установке ViPNet PKI Client на ОСнова	37
Ошибка при установке сертификата на устройство Рутокен	37
Ошибка при запуске компонентов ViPNet PKI Client в РЕД ОС.....	38
После смены PIN-кода токена в ViPNet PKI Client не удастся ввести новый PIN-код.....	38
 Приложение В. История версий.....	 40
Что нового в версии 2.1.0.....	40
Что нового в версии 2.0.0.....	41
Что нового в версии 1.7.0.....	42
Что нового в версии 1.6.0.....	43
Что нового в версии 1.5.0.....	43
Что нового в версии 1.4.1.....	44
Что нового в версии 1.4.0.....	44
Что нового в версии 1.3.1.....	45
Что нового в версии 1.3	45
Что нового в версии 1.2	47
 Приложение С. Термины и сокращения.....	 48



Введение

О документе	6
Обратная связь	7
Что нового в версии 2.1.1	8
Лицензирование	9

О документе

Документ описывает установку и настройку программного комплекса ViPNet® PKI Client Linux (далее — ViPNet PKI Client).

Документ предназначен:

- для администраторов, которые устанавливают и настраивают ViPNet PKI Client на компьютерах пользователей;
- пользователей, которые самостоятельно устанавливают и настраивают ViPNet PKI Client на своих компьютерах.

Предполагается, что читатель имеет общее представление об инфраструктуре открытых ключей (PKI) и ознакомился с документом «ViPNet PKI Client Linux. Руководство пользователя».

Соглашения документа

Обозначение	Описание
Название	Название элемента интерфейса: окна, вкладки, поля, кнопки, ссылки
Клавиша+Клавиша	Сочетание клавиш: нажмите первую клавишу и, не отпуская её, нажмите вторую
Меню > Команда	Последовательность элементов или действий
Код	Имя файла, путь, фрагмент кода или команда в командной строке



Примечание. В документе могут присутствовать снимки интерфейса из предыдущих версий продукта. Поэтому некоторые элементы интерфейса, которые не влияют на понимание текста, могут выглядеть не так, как в продукте.

Обозначения при описании команд в документе:

- Команды, которые могут быть выполнены только в режиме администратора, выделены красным цветом:

команда

- Параметры, которые должны быть заданы пользователем, заключены в угловые скобки:

команда <параметр>

- Необязательные параметры или ключевые слова заключены в квадратные скобки:

команда <обязательный параметр> [необязательный параметр]

- Если можно указать один из нескольких параметров, допустимые варианты заключены в фигурные скобки и разделены вертикальной чертой:

команда {вариант-1 | вариант-2}

Обратная связь

Контактная информация

- Единый многоканальный телефон:
+7 (495) 737-6192,
8 (800) 250-0-260 — бесплатный звонок из России (кроме Москвы).
- Служба поддержки: hotline@infotecs.ru.
Форма для обращения в службу поддержки через сайт.
Телеграм-канал поддержки: t.me/vhd21.
Телефон для клиентов с расширенной поддержкой: +7 (495) 737-6196.
- Отдел продаж: soft@infotecs.ru.

Дополнительная информация на сайте ИнфоТеКС

- [О продуктах ViPNet](#).
- [О решениях ViPNet](#).
- [Часто задаваемые вопросы](#).
- [Форум пользователей продуктов ViPNet](#).

Если вы обнаружили уязвимости в продуктах компании, сообщите о них по адресу security-notifications@infotecs.ru. Распространение информации об уязвимостях продуктов ИнфоТеКС регулируется [политикой ответственного разглашения](#).

Что нового в версии 2.1.1

- **Поддержка лицензий с относительным сроком действия**

Теперь в ViPNet PKI Client поддерживаются лицензии, срок действия которых начинается с момента их активации. Окончание срока действия лицензии отображается после активации.

- **Исправление ошибок**

Устранены дефекты, выявленные в ходе эксплуатации предыдущих версий ViPNet PKI Client, повышена стабильность работы.

Изменения в предыдущих версиях см. в приложении [История версий](#).

Лицензирование

При работе в ViPNet PKI Client без лицензии доступно только управление сертификатами и CRL.

Чтобы получить доступ ко всем функциям ViPNet PKI Client, активируйте лицензию с помощью файла лицензии или через ViPNet TLS Gateway.

Лицензирование с помощью файла

Получите файл лицензии в [ИнфоТеКс](#), загрузите его в ViPNet PKI Client и активируйте лицензию (см. «Руководство пользователя»).

Лицензия содержит:

- Разрешённые для использования компоненты и функции (все или некоторые из перечисленных):
 - компонент Cloud Unit для работы с облачным сервисом ЭП на базе ViPNet PKI Service;
 - компонент File Unit для подписи и зашифрования файлов;
 - компонент TLS Unit для установления TLS-соединений с односторонней аутентификацией (аутентификацией сервера);
 - функция установления TLS-соединений с двусторонней аутентификацией (взаимной аутентификацией сервера и пользователя) для компонента TLS Unit;
 - компонент Web Unit для использования криптографических функций в веб-приложениях.



Примечание. Для использования Tunnel Unit требуется лицензия, содержащая TLS Unit.

Для HTTPS-подключения к облачному сервису ЭП требуется лицензия, содержащая Cloud Unit и TLS Unit.

- Максимальную версию ViPNet PKI Client.
- Срок действия лицензии.

Лицензирование через ViPNet TLS Gateway

Можно [настроить активацию лицензии через ViPNet TLS Gateway](#). В этом случае активация лицензии будет проверяться автоматически при установлении соединения между ViPNet PKI Client и ViPNet TLS Gateway.



1

Начало работы

Установка и обновление	11
Активация лицензии через ViPNet TLS Gateway	13
Импорт и экспорт настроек	15

Установка и обновление



Примечание. Для установки ViPNet PKI Client подключите репозитории, используемые вашей операционной системой по умолчанию.

- 1 Если у вас ранее установлен ViPNet PKI Client версии 1.x, удалите устаревшую версию. В версии 2.x:
 - не будут доступны CRL;
 - будут доступны сертификаты и ключи ЭП при продолжении использования ViPNet CSP Linux.
- 2 Распакуйте архив с пакетами в произвольную папку.
- 3 Запустите скрипт `install.sh` с правами суперпользователя.
- 4 Ознакомьтесь с лицензионным соглашением.
- 5 Чтобы принять условия лицензионного соглашения, введите 1.
- 6 Запустится проверка пакетов. Если появится сообщение, что пакеты не найдены — установите недостающие пакеты и снова запустите скрипт `install.sh`.
- 7 Перезагрузите компьютер.



Совет. Если при установке ViPNet PKI Client произошла ошибка, см. раздел [Возможные неполадки](#).

Установка и обновление на ОСноа в режиме замкнутой программной среды

- 1 Если у вас ранее установлен ViPNet PKI Client версии 1.x, удалите устаревшую версию. В версии 2.x:
 - не будут доступны CRL;
 - будут доступны сертификаты и ключи ЭП при продолжении использования ViPNet CSP Linux.
- 2 Распакуйте архив с пакетами в произвольную папку:

```
sudo tar --xattrs --xattrs-include='*' -jxvf pki_client_linux-x86_64-dist.tar.bz2
```
- 3 Установите сертификат `infotecs-osnova.der` из распакованного архива в системное хранилище:

```
sudo cp -f ./pki_client_linux/deb/signs/osnova/infotecs-osnova.der /etc/ima/certs/
```
- 4 Выполните команду:

```
sudo update-initramfs -u -k all
```

- 5 Перезагрузите компьютер.
- 6 Запустите скрипт `install.sh` с правами суперпользователя.
- 7 Ознакомьтесь с лицензионным соглашением.
- 8 Чтобы принять условия лицензионного соглашения, введите 1.
- 9 Запустится проверка пакетов. Если появится сообщение, что пакеты не найдены — установите недостающие пакеты и снова запустите скрипт `install.sh`.

Активация лицензии через ViPNet TLS Gateway



Примечание. Для приобретения ViPNet TLS Gateway [обратитесь в ИнфоТеКС](#).

Подробнее о настройке ViPNet TLS Gateway см. «ViPNet TLS Gateway. Руководство администратора».

Перед активацией лицензии:

1 Получите у администратора ViPNet TLS Gateway:

- Адрес и порт для лицензирования.
- Цепочку сертификатов транспортного сертификата ViPNet TLS Gateway, используемого для подключения к каналу лицензирования.

2 Установите в ViPNet PKI Client на компьютере пользователя:

- Личный сертификат с ключом ЭП для подключения к ViPNet TLS Gateway, доверие к которому установлено в ViPNet TLS Gateway. Сертификат должен соответствовать требованиям:
 - сертификат действителен;
 - ЭП сертификата действительна;
 - сертификат содержит расширения:
 - **Расширенное использование ключа** со значением **Проверка подлинности клиента**;
 - **Использование ключа** со значением **Цифровая подпись** и (или) **Согласование ключей**.



Примечание. Запрос на сертификат можно создать в ViPNet PKI Client. Подробнее см. «Руководство пользователя».

- Корневой сертификат УЦ, в котором издан сертификат пользователя для подключения к ViPNet TLS Gateway, а также все сертификаты цепочки и соответствующие CRL.
- Цепочку сертификатов транспортного сертификата ViPNet TLS Gateway, используемого для подключения к каналу лицензирования.

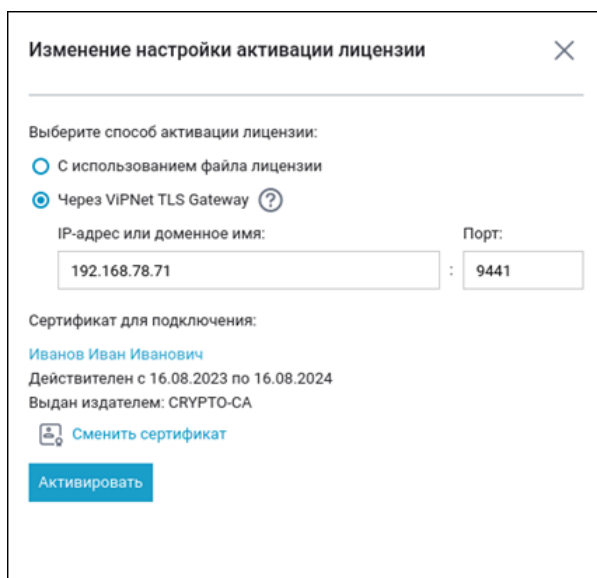
Для активации лицензии на компьютере пользователя:

1 Перейдите в настройки ViPNet PKI Client.

2 В разделе **Лицензия** нажмите **Выбрать способ > Через ViPNet TLS Gateway**.

3 Введите полученные адрес и порт.

4 Выберите установленный сертификат для подключения.



Изменение настройки активации лицензии

Выберите способ активации лицензии:

☐ С использованием файла лицензии

☒ Через ViPNet TLS Gateway ?

IP-адрес или доменное имя: 192.168.78.71 Порт: 9441

Сертификат для подключения:

Иванов Иван Иванович

Действителен с 16.08.2023 по 16.08.2024

Выдан издателем: CRYPTO-CA

 [Сменить сертификат](#)

[Активировать](#)

Рисунок 1. Активация через ViPNet TLS Gateway

5 Нажмите **Активировать**.

6 В зависимости от места хранения контейнера ключей:

- **Хранилище ViPNet PKI Client** — введите пароль хранилища ViPNet PKI Client и нажмите **Продолжить**.
- **Токен** — введите PIN-код.

7 ViPNet PKI Client отправит запрос на активацию на ViPNet TLS Gateway. После обработки запроса ViPNet PKI Client перейдёт в состояние **Лицензия активирована**.

Если активация завершится ошибкой, ознакомьтесь с причиной и следуйте указаниям.

Аннулирование активации лицензии через ViPNet TLS Gateway

Чтобы освободить лицензию, например, в случае увольнения сотрудника:

1 Перейдите в настройки ViPNet PKI Client.

2 В разделе  **Лицензия** нажмите **Аннулировать активацию** и подтвердите действие.

Импорт и экспорт настроек

Вы можете выгрузить часть настроек программы в файл *.json и использовать:

- чтобы перенести ViPNet PKI Client на другой компьютер;
- создать резервную копию настроек на случай сбоя в работе;
- применить одинаковые настройки для нескольких пользователей.

Ручной перенос настроек между компьютерами

- 1 [Ознакомьтесь с особенностями импорта настроек.](#)
- 2 На первом компьютере [экспортируйте настройки.](#)
- 3 На втором компьютере:
 - 3.1 [Установите ViPNet PKI Client.](#)
 - 3.2 [Импортируйте настройки.](#)

Автоматическое распространение настроек между несколькими пользователями

- 1 [Ознакомьтесь с особенностями импорта настроек.](#)
- 2 На одном из компьютеров сети [экспортируйте настройки.](#)
- 3 [Настройте автоматическое распространение настроек из файла.](#)

Особенности импорта настроек

Шифрование

Вместе с настройками шифрования импортируется список получателей, если их сертификаты:

- экспортированы в файл настроек;
- либо установлены в категорию **Сертификаты других пользователей**.

Сертификаты и CRL

Личные сертификаты не импортируются.

Сертификаты получателей будут установлены в хранилище текущего пользователя.

Точки распространения CRL

Для автоматического обновления CRL сертификат УЦ должен быть установлен в хранилище локального компьютера.

TLS и туннели

Для применения настройки **Разрешать соединения при неполном доверии к сертификату сервера** после импорта перезапустите TLS Unit.

Экспорт настроек

- 1 Перейдите в настройки ViPNet PKI Client.
- 2 В разделе  **Импорт и экспорт** нажмите **Сохранить настройки в файл**.
- 3 Выберите и включите  настройки для экспорта.
- 4 Вы можете добавить описание файла настроек в соответствующем поле.
- 5 Нажмите **Экспортировать** и укажите папку для сохранения файла настроек.

Импорт настроек

- 1 Перейдите в настройки ViPNet PKI Client.
- 2 В разделе  **Импорт и экспорт** нажмите **Загрузить настройки из файла**.
- 3 Укажите путь к файлу *.json.
- 4 Выберите настройки для импорта и нажмите **Импортировать**.
- 5 Подтвердите выполнение операции.

Автоматическое распространение настроек из файла

В ViPNet PKI Client есть настройки, которые могут быть одинаковыми для разных пользователей. Например, параметры подписи и шифрования, точки распространения CRL, настройки TLS и облачных сервисов. Чтобы не указывать настройки вручную на каждом компьютере, вы можете настроить их автоматическое распространение.

Общий порядок настройки

- 1 Настройте ViPNet PKI Client на одном компьютере (Windows или Linux).
- 2 Экспортируйте настройки (см. ниже).
- 3 Поместите файл настроек:
 - в сетевую папку, доступную для всех пользователей ViPNet PKI Client;

- в папку на компьютере каждого пользователя.
- 4 Поручите пользователям указать в ViPNet PKI Client путь к файлу с настройками (см. «Руководство пользователя»).

Экспортировать настройки для автоматического распространения

- 1 Ознакомьтесь с [особенностями импорта настроек](#).
- 2 Запустите **Настройки PKI Client > Импорт и экспорт**.
- 3 Нажмите **Сохранить настройки в файл**.
- 4 Выберите **Файл будет использоваться для автоматического распространения настроек**.
- 5 Включите  экспортируемые настройки, которые нужно установить на компьютерах других пользователей.
- 6 Выберите настройки, которые будут перезаписываться при автоматическом распространении.
- 7 Нажмите **Экспортировать** и сохраните файл с именем `pki_client_settings.json` (имя должно быть только таким).

Этот файл можно применить как на компьютере с Windows, так и с Linux.



Примечание. Если вы обновите файл настроек в общей папке, у пользователя появится окно о получении новых настроек. Чтобы их применить, пользователю потребуется перезапустить все компоненты ViPNet PKI Client.

Отключить автоматическое получение настроек

Поручите пользователям:

- 1 Сменить папку для файла с настройками: **Настройки PKI Client > Импорт и экспорт > Настройки > Папка пользователя**.
- 2 Убедиться, что в выбранной папке нет файла `pki_client_settings.json`.



2

Настройка автоматического обновления CRL

Настройка подключения к прокси-серверам	19
Отслеживание событий при автообновлении CRL	21

Настройка подключения к прокси-серверам

Если в вашей организации доступ в интернет осуществляется через один или несколько прокси-серверов, задайте параметры подключения к ним:

- 1 Откройте файл `/opt/itcs/share/pki-client/pki-client-crl-unit/crlunit.cfg` для редактирования.
- 2 Выполните одно из действий:
 - Замените секцию `<proxy-info>` на секцию `<proxy-settings>`.
 - Если секция `<proxy-info>` отсутствует, добавьте секцию `<proxy-settings>`.
- 3 Раскомментируйте строку `<!--proxy addr="msk-tmg-04.Sample-nt:3128" protocol="http" authtype="negotiate" /-->` и укажите параметры прокси-сервера для HTTP-соединений:
 - `proxy addr` — IP-адрес или доменное имя прокси-сервера и номер порта для подключения к нему;
 - `protocol` — протокол, по которому компьютер с ViPNet PKI Client соединяется с прокси-сервером (HTTP, FTP);
 - `authtype` — способ аутентификации на сервере (`any`, `ntlm`, `negotiate`).



Примечание. Если на вашем прокси-сервере используется авторизация по имени учётной записи и паролю, укажите их в `proxy addr`:

```
</proxy addr="http://<имя учётной записи>:<пароль>@<адрес прокси-сервера>:<номер порта>" authtype="any"/>
```

-
- 4 Раскомментируйте строку `<!--proxy addr="msk-tmg-04.Sample-nt:3128" protocol="ftp" authtype="negotiate" /-->` и укажите параметры прокси-сервера для FTP-соединений:
 - `proxy addr` — IP-адрес или доменное имя прокси-сервера и порт для подключения к нему;
 - `protocol` — протокол, по которому происходит соединение с прокси-сервером (HTTP, FTP);
 - `authtype` — способ аутентификации на сервере (`any`, `ntlm`, `negotiate`).
 - 5 Сохраните изменения.
 - 6 Перезапустите программу CRL Unit.

Внимание!



- В значении параметра `proxy addr` запрещено использовать адреса со схемой `socks5h`.
 - Если на компьютере создана замкнутая программная среда в соответствии с требованиями ФСБ России к средствам криптографической защиты информации класса КСЗ, чтобы запретить непривилегированным пользователям изменять и удалять файл `/opt/itcs/share/pki-client/pki-client-crl-unit/crlunit.cfg`, настройте средства контроля среды функционирования.
-

Пример настройки прокси-сервера без авторизации

```
<?xml version="1.0" encoding="utf-8"?>

<certagent>
  <proxy-settings>
    <proxy addr="msk.proxy-server:3128" protocol="http" authtype="negotiate"/>
    <proxy addr="msk.proxy-server:3128" protocol="ftp" authtype="negotiate"/>
  </proxy-settings>
</certagent>
```

Пример настройки прокси-сервера с авторизацией по логину и паролю

```
<?xml version="1.0" encoding="utf-8"?>

<certagent>
  <proxy-settings>
    </proxy addr="http://user:password@msk.proxy-server:3128" authtype="ntlm"/>
  </proxy-settings>
</certagent>
```

Отслеживание событий при автообновлении CRL

В большинстве дистрибутивов Linux по умолчанию события записываются в журнал. Его расположение задаётся в конфигурации установленной системы логирования (обычно — `/var/log/messages` или `/var/log/syslog`).

Для просмотра журнала событий выполните с правами суперпользователя:

- В Astra Linux, Debian или Ubuntu:

```
cat /var/log/syslog | grep pki-client-crl-unit
```

- В Альт:

```
less /var/log/messages | grep pki-client-crl-unit
```

3

Настройка подключения к сайтам, использующим TLS ГОСТ

Требования к сертификатам для работы TLS Unit	23
Настройка подключения TLS Unit к прокси-серверам	25
Настройка совместной работы TLS Unit и браузера	27

Требования к сертификатам для работы TLS Unit

Сертификат сервера

При подключении к сайту проверяется:

- что сертификат действителен;
- ЭП сертификата действительна;
- адрес сайта соответствует адресу в сертификате;
- сертификат содержит расширения:
 - **Расширенное использование ключа** со значением **Проверка подлинности сервера**;
 - **Использование ключа** с одним или несколькими значениями:
 - **Шифрование ключей**;
 - **Согласование ключей**;
 - **Цифровая подпись**.



Внимание! Если не выполняется хотя бы одно из условий, соединение не будет установлено.

Вы можете разрешить установку соединений, если некоторые проверки не выполнены:

- срок действия сертификата истёк или не наступил;
- не удастся выяснить, аннулирован ли сертификат;
- цепочка сертификатов неполная или ее невозможно проверить.

Для этого:

- 1 Перейдите в настройки ViPNet PKI Client.
- 2 Выберите раздел  **TLS**.
- 3 Выберите **Разрешать соединение при неполном доверии к сертификату сервера**.
- 4 Нажмите **Сохранить**.

Сертификат пользователя

- Сертификат действителен;
- ЭП сертификата действительна;
- сертификат содержит расширения:

- **Расширенное использование ключа** со значением **Проверка подлинности клиента**;
- **Использование ключа** со значением **Цифровая подпись** и (или) **Согласование ключей**.

Примечание. Для подключения к некоторым сайтам сертификат пользователя должен быть издан в определённых УЦ. В этом случае:



- 1 У технической поддержки или на сайте получите информацию об УЦ.
 - 2 Посмотрите издателя в сертификате пользователя. Если его нет в списке УЦ, пользователю необходимо создать запрос на сертификат, передать его в нужный УЦ и получить сертификат.
-

Настройка подключения TLS Unit к прокси-серверам

Если в вашей организации доступ в интернет осуществляется через один или несколько прокси-серверов, настройте подключение TLS Unit к прокси-серверам:

- 1 Откройте файл `/opt/itcs/share/pki-client/pki-client-tls-unit/tlsunit.cfg` для редактирования.
- 2 В секции `#Here you can specify parent proxy bypass list` укажите адреса ресурсов, при подключении к которым не используется прокси-сервер, через запятую без пробелов:
`allow * * <IP-адрес ресурса, IP-адрес ресурса, ...>`
- 3 В секции `#Here you can specify parent HTTPS proxy` настройте подключение к прокси-серверу для HTTPS-соединений:
 - Вручную — раскомментируйте строку `#parent 1000 connect 10.0.4.245 3128` и введите IP-адрес прокси-сервера.
 - С использованием системного прокси-сервера — раскомментируйте строку `parent 1000 connect %SYSTEM_PROXY%`.
- 4 В секции `#Here you can specify parent HTTP proxy` настройте подключение к прокси-серверу для HTTP-соединений:
 - Вручную — раскомментируйте строку `#parent 1000 http 10.0.4.245 3128` и введите IP-адрес прокси-сервера.
 - С использованием системного прокси-сервера — раскомментируйте строку `parent 1000 http %SYSTEM_PROXY%`.
- 5 Сохраните изменения.
- 6 Перезапустите TLS Unit.



Примечание. Если для подключения к корпоративному прокси-серверу требуется аутентификация по протоколу HTTPS, используйте промежуточный прокси-сервер, например, CNTLM, на котором настроены параметры аутентификации.

Пример настройки подключения TLS Unit к прокси-серверам

```
#!/opt/itcs/bin/pki-client-tls-unit
log INFO
rotate 30
internal 127.0.0.1
#Here you can specify parent proxy bypass list
```

```
allow * * 127.0.0.1,10.0.0.0/8,11.0.0.0/8,192.168.0.0/16
#Here you can specify parent HTTPS proxy
allow * * * * HTTP_CONNECT
#parent 1000 connect 10.0.4.245 3128
parent 1000 connect %SYSTEM_PROXY%
#Here you can specify parent HTTP proxy
allow * * * * HTTP
#parent 1000 http 10.0.4.245 3128
parent 1000 http %SYSTEM_PROXY%
proxy -p9998 -T -n -a
```

Настройка совместной работы TLS Unit и браузера

- 1 Импортируйте корневой сертификат ViPNet PKI Client Root в браузер.

Процесс импорта корневого сертификата ViPNet PKI Client Root схож для разных браузеров. Для примера представлены инструкции для браузеров Firefox и Chromium:

- [Импорт сертификата ViPNet PKI Client Root в Firefox.](#)
- [Импорт сертификата ViPNet PKI Client Root в Chromium.](#)

- 2 Настройте браузер для использования TLS Unit в качестве прокси-сервера:

- [Настройка прокси-сервера в Firefox.](#)
- [Настройка прокси-сервера в Chromium, Chromium ГОСТ, Opera, Яндекс.Браузер.](#)

Импорт сертификата ViPNet PKI Client Root в Firefox

- 1 В Firefox перейдите в меню **Настройки**.
- 2 Слева выберите раздел **Приватность и Защита**.
- 3 В группе **Защита** нажмите **Просмотр сертификатов**.
- 4 В окне **Управление сертификатами** выберите вкладку **Центры сертификации** и нажмите **Импортировать**.
- 5 Выберите файл сертификата `/opt/itcs/share/pki-client/certs/root.pem` и нажмите **Выбрать**.
- 6 В окне **Загрузка сертификата** выберите **Доверять при идентификации веб-сайтов** и нажмите **ОК**.
- 7 Перезапустите Firefox.

Импорт сертификата ViPNet PKI Client Root в Chromium

- 1 В Chromium перейдите в меню **Настройки**.
- 2 В разделе **Конфиденциальность и безопасность** нажмите **Безопасность > Настроить сертификаты**.
- 3 Выберите вкладку **Центры сертификации** и нажмите **Импорт**.

- 4 Выберите файл сертификата `/opt/itcs/share/pki-client/certs/root.pem` и нажмите **Выбрать**.
- 5 В окне **Центр сертификации** выберите **Доверять этому сертификату при идентификации сайтов** и нажмите **ОК**.
- 6 Перезапустите Chromium.

Настройка прокси-сервера в Firefox

- 1 В Firefox перейдите в меню **Настройки**.
- 2 Слева выберите раздел **Основные**.
- 3 В группе **Настройки сети** нажмите **Настроить**.
- 4 В окне **Параметры соединения**:
 - 4.1 Выберите **Ручная настройка прокси**.
 - 4.2 В поле **HTTP прокси** укажите IP-адрес прокси-сервера — `127.0.0.1`.
 - 4.3 В поле **Порт** укажите порт для подключения к прокси-серверу — `9998`.
 - 4.4 Выберите **Также использовать этот прокси для HTTPS**.
- 5 В поле **Не использовать прокси для** укажите адреса ресурсов, при подключении к которым прокси-сервер не используется.
- 6 Нажмите **ОК**.

Настройка прокси-сервера в Chromium, Chromium ГОСТ, Opera, Яндекс.Браузер

В зависимости от браузера выполните команду:

- Chromium:

```
chromium --proxy-server="127.0.0.1:9998"
```
- Chromium ГОСТ:

```
chromium-gost --proxy-server="127.0.0.1:9998"
```
- Opera:

```
opera --proxy-server="127.0.0.1:9998"
```
- Яндекс.Браузер:

```
yandex-browser --proxy-server="127.0.0.1:9998"
```



Внимание! Если у вас уже открыто окно браузера без настроек прокси и вы запускаете ещё одно окно в командной строке с настройками прокси, то новое окно не будет использовать эти настройки. Чтобы настройки применились, закройте все окна и выполните команду.

4

Подключение к туннелируемым ресурсам

Порядок настройки	30
Требования к сертификатам для работы Tunnel Unit	31
Добавление туннелируемого ресурса	32
Подключение к туннелируемому ресурсу	33

Порядок настройки

- 1 У администратора ViPNet TLS Gateway получите:
 - сертификат УЦ, в котором изданы транспортные сертификаты ViPNet TLS Gateway, а также при наличии сертификаты всех УЦ из цепочки и соответствующие CRL;
 - адрес и порт ViPNet TLS Gateway для подключения к туннелируемому ресурсу.
- 2 Установите полученные сертификаты и CRL.
- 3 Чтобы подключаться к туннелируемым ресурсам с аутентификацией пользователя, убедитесь, что личный сертификат, который будет использоваться для подключения, соответствует [требованиям](#).
- 4 [Добавьте туннелируемый ресурс в ViPNet PKI Client](#).
- 5 [Подключитесь к туннелируемому ресурсу](#).

Требования к сертификатам для работы Tunnel Unit

Сертификат сервера (транспортный сертификат ViPNet TLS Gateway)

- Сертификат действителен;
- ЭП сертификата действительна;
- адрес ViPNet TLS Gateway соответствует адресу в сертификате;
- сертификат содержит расширения:
 - **Расширенное использование ключа** со значением **Проверка подлинности сервера**.
 - **Использование ключа** с одним или несколькими значениями:
 - **Шифрование ключей**;
 - **Согласование ключей**;
 - **Цифровая подпись**.



Внимание! Если не выполняется хотя бы одно из условий, соединение не будет установлено.

Сертификат пользователя

- Сертификат действителен;
- ЭП сертификата действительна;
- сертификат добавлен в ViPNet TLS Gateway в список **Сертификаты пользователей > Разрешенные**, и разрешён доступ к туннелируемому ресурсу (см. «ViPNet TLS Gateway. Руководство администратора»);
- сертификат содержит расширения:
 - **Расширенное использование ключа** со значением **Проверка подлинности клиента**;
 - **Использование ключа** со значением **Цифровая подпись** и (или) **Согласование ключей**.

Добавление туннелируемого ресурса

- 1 Перейдите в настройки ViPNet PKI Client.
- 2 Выберите раздел  **Туннели**.
- 3 Нажмите  **Добавить туннель**.
- 4 В поле **Туннель** введите произвольное имя туннелируемого ресурса.
- 5 В поле **Порт** введите номер порта локального сетевого интерфейса для обмена данными с туннелируемым ресурсом. Этот же номер порта укажите в настройках приложения для подключения к туннелируемому ресурсу.



Примечание. Порт не должен быть занят другим приложением. Доступность порта можно проверить с помощью консольной утилиты `netstat`.

- 6 В списке  **Аутентификация клиента** выберите тип подключения к туннелируемому ресурсу:
 -  — для подключения к туннелируемому ресурсу без аутентификации пользователя;
 -  — для подключения к туннелируемому ресурсу с аутентификацией пользователя. В этом случае в окне **Выбор сертификата** выберите сертификат и в зависимости от места его хранения введите пароль хранилища ViPNet PKI Client или PIN-код токена.
- 7 В поле **Адрес и порт удаленного узла** укажите адрес и порт ViPNet TLS Gateway для подключения к туннелируемому ресурсу.
- 8 Чтобы подключение к туннелируемому ресурсу выполнялось автоматически после запуска Tunnel Unit, установите флажок в столбце **Авто**.
- 9 Нажмите .

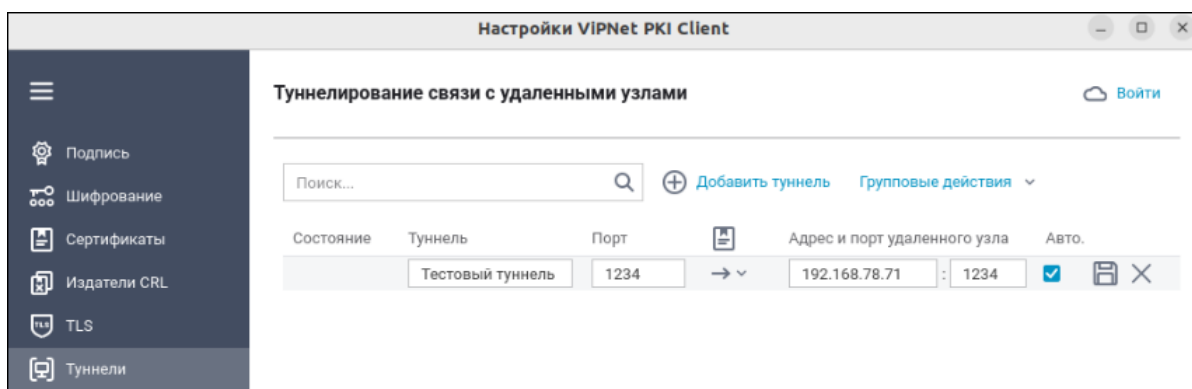


Рисунок 2. Добавление туннелируемого ресурса



Примечание. Чтобы отредактировать или удалить туннелируемый ресурс, выберите его и нажмите  или  соответственно.

Подключение к туннелируемому ресурсу

Если при [добавлении туннелируемого ресурса](#) вы установили флажок в столбце **Авто**, связь с этим ресурсом будет установлена автоматически при запуске программы Tunnel Unit.

Чтобы подключиться к удалённому рабочему столу по RDP:



Примечание. Подключение к туннелируемым ресурсам с помощью других приложений и по другим протоколам выполняется аналогично.

- 1 Запустите Tunnel Unit.
- 2 Перейдите в настройки ViPNet PKI Client.
- 3 Выберите раздел  **Туннели**.
- 4 В списке выберите туннелируемый ресурс и с помощью переключателя в столбце **Состояние** установите соединение с ним.

Примечание. Для работы сразу со всеми туннелируемыми ресурсами нажмите **Групповые действия** и выберите:



- **Включить все туннели** — установить соединение со всеми туннелируемыми ресурсами.
 - **Включить автозапускаемые** — установить соединение с туннелируемыми ресурсами, для которых включено автоматическое установление соединения при запуске Tunnel Unit, если соединение было прервано вручную.
 - **Выключить все туннели** — разорвать соединение со всеми туннелируемыми ресурсами.
 - **Удалить все туннели** — удалить все туннелируемые ресурсы.
-

- 5 Запустите клиент удалённого рабочего стола, например, Remmina.
- 6 В списке протоколов выберите **RDP** и в поле рядом введите адрес подключения 127.0.0.1:<порт>, где <порт> — номер порта локального сетевого интерфейса, заданный при [добавлении туннелируемого ресурса](#).
- 7 Нажмите **Подключить**.



Возможные неполадки

Зависание при работе в Альт 8 СП Рабочая станция

ViPNet PKI Client может зависать из-за системного ограничения количества пользовательских процессов:

- 1 Откройте файл `/etc/security/limits.d/50-defaults.conf` для редактирования.
- 2 Измените значение параметра `nproc` в строке «`*soft nproc 512`» на 1024. При повторном зависании используйте большее значение.
- 3 Сохраните изменения.

Ошибки при обновлении CRL

Для определения причины сбоя:

- 1 [Откройте журнал](#), в который записываются события.
- 2 В строке события посмотрите значение `Error code`.

Ошибка данных (ErrorCode: -4)

Выполните одно из действий:

- Проверьте доступность точки распространения CRL. Для этого загрузите список CRL вручную: скопируйте URL точки распространения CRL в адресную строку браузера и перейдите по нему. Если на ваш компьютер загрузился файл `*.crl`, значит, точка распространения доступна.

- Если в вашей организации доступ в интернет осуществляется через прокси-сервер, в файле конфигурации `crlunit.cfg` укажите настройки прокси-сервера.

Ошибка загрузки (ErrorCode: -5)

Возможно, нет доступа в интернет или к точке распространения CRL.

Для устранения ошибки:

- Проверьте доступ в интернет.
- Проверьте доступ к точке распространения CRL. Для этого загрузите CRL вручную: скопируйте URL точки распространения CRL в адресную строку браузера и перейдите по нему. Если на ваш компьютер загрузился файл `*.crl`, значит, точка распространения доступна.

Сертификат не найден (ErrorCode: -7)

Получите сертификат издателя выбранной точки распространения CRL и установите его в локальное хранилище компьютера.

CRL просрочен (ErrorCode: -8)

Срок действия CRL, загруженного из указанной точки распространения, истёк. Обратитесь к администратору УЦ.

CRL уже установлен (ErrorCode: -11)

Попытка установить CRL, который уже есть в хранилище сертификатов.

Ошибка при установке ViPNet PKI Client

Во время установки ViPNet PKI Client может возникнуть ошибка:

```
/var/lib/dpkg/info/pki-client-common.postinst: line 82: /opt/itcs/bin/oss1_manager-1.1: No such file or directory
Failed to copy certificate to storage...
```

Ошибка возникает, если в системе установлен ViPNet OSSL версии 5.6 или выше.

Для устранения ошибки выполните команду:

```
sudo ln -s /opt/itcs/bin/oss1_manager /opt/itcs/bin/oss1_manager-1.1
```

Ошибка при установке или запуске в Astra Linux Special Edition («Смоленск») 1.6

При установке или запуске ViPNet PKI Client на компьютерах с Astra Linux Special Edition («Смоленск») 1.6 с включённым режимом замкнутой программной среды может появиться сообщение о блокировке загрузки пакетов.

Причиной может быть отсутствие пакета `astra-digsig-oldkeys`:

- 1 Проверьте, что пакет установлен:

```
dpkg -s astra-digsig-oldkeys
```

- 2 Если пакет не установлен, установите его:

```
sudo apt-get install astra-digsig-oldkeys
```

Ошибка при установке ViPNet PKI Client на Ubuntu

При установке ViPNet PKI Client на компьютеры под управлением Ubuntu может появиться сообщение об отсутствии пакета `libgconf-2-4`.

Если используется Ubuntu версии 24.04

- 1 Скачайте пакеты `libgconf-2-4` и `gconf2-common` командами:

```
wget
http://ru.archive.ubuntu.com/ubuntu/pool/universe/g/gconf/libgconf-2-4_3.2.6-6ubuntu1_amd64.deb

wget
http://ru.archive.ubuntu.com/ubuntu/pool/universe/g/gconf/gconf2-common_3.2.6-6ubuntu1_all.deb
```

- 2 Установите пакеты командами:

```
sudo dpkg -i libgconf-2-4_3.2.6-6ubuntu1_amd64.deb
sudo dpkg -i gconf2-common_3.2.6-6ubuntu1_all.deb
```

- 3 Повторите установку ViPNet PKI Client.

Если используется Ubuntu версии 22.04 и ниже

- 1 Установите пакет `libgconf-2-4` командами:

```
sudo apt install libgconf-2-4
sudo apt --fix-broken install
```

- 2 Повторите установку ViPNet PKI Client.

Ошибка при установке ViPNet PKI Client на ОСнова

При установке ViPNet PKI Client на компьютеры под управлением ОСнова с включённым режимом замкнутой программной среды выводится сообщение **Отказано в доступе**.

Возможная причина № 1

Файл `install.sh` из архива с пакетами был распакован некорректно.

Способ устранения

- 1 В папке с пакетами просмотрите информацию о подписи файла `install.sh`:

```
evmctl show ./install.sh
```
- 2 Если информация о подписи не отображается, [повторите установку ViPNet PKI Client](#).

Возможная причина № 2

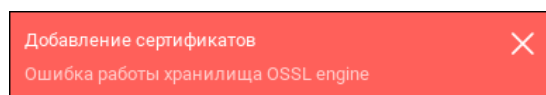
Установка ViPNet PKI Client была выполнена некорректно (для ОС с выключенным режимом замкнутой программной среды).

Способ устранения

[Повторите установку ViPNet PKI Client для ОСнова в режиме замкнутой программной среды](#).

Ошибка при установке сертификата на устройство Рутокен

Если вы создали запрос на сертификат с сохранением ключа на устройстве Рутокен и при установке изданного сертификата в ViPNet PKI Client возникает ошибка:



[Установите библиотеку librtpkcs11ecp версии 2.8.1.0:](#)

- Astra Linux, Debian или Ubuntu:
`librtpkcs11ecp_2.8.1.0-1_<разрядность>.deb`
- Альт, РЕД ОС или РОСА:
`librtpkcs11ecp-2.8.1.0-1.<разрядность>.rpm`

Ошибка при запуске компонентов ViPNet PKI Client в РЕД ОС

На компьютерах под управлением РЕД ОС могут не запускаться компоненты ViPNet PKI Client. При запуске компонентов из командой строки появляется сообщение об отсутствии пакета `libQt5WebEngine.so.5`.

Способ устранения

Установите пакет `qt5-qtwebengine`:

```
sudo dnf install qt5-qtwebengine
```

После смены PIN-кода токена в ViPNet PKI Client не удастся ввести новый PIN-код

Если вы сменили PIN-кода токена при помощи утилиты обслуживания токена и при вводе нового PIN-кода в ViPNet PKI Client появляется сообщение о том, что PIN-код неверный:

- 1 Убедитесь, что на токене отсутствует аппаратная поддержка алгоритмов ГОСТ (см. «Руководство пользователя»).
- 2 Подключите токен и узнайте его `Slot Id`:

Семейство устройств	Команда для выполнения
Рутокен	<code>/opt/itcs/bin/ngost_token_manager enum-slots --dll /opt/itcs/lib/libsofttoken_ngost_rutoken.so</code>
JaCarta	<code>/opt/itcs/bin/ngost_token_manager enum-slots --dll /opt/itcs/lib/libsofttoken_ngost_jacarta.so</code>

```
tester@astra:/opt/itcs/bin$ ./ngost_token_manager enum-slots --dll /opt/itcs/lib/libsofttoken_ngost_jacarta.so
Command: Slot enumeration (enumerate slots with token attached and show information about token attached).

Integrity check failed:
  module name: ngost_token_manager
  event type: 0
  error code: 28
Integrity check failed:
  module name: libsofttoken_ngost_jacarta.so
  event type: 0
  error code: 28
=====
Number of slots with token attached: 1
=====
Slot Id: 196607
PKCS11 storage presented.
-----
Token info:
-----
Label: JaCarta PRO
Manufacture id: ITCS
Model: PRO
Serial number: 4E46001747663839
=====
Command successfully finished.
```

Рисунок 3. Определение `Slot Id` подключенного токена

- 3 Смените PIN-код токена. Новый PIN-код токена должен совпадать с тем, который вы задали в утилите обслуживания токена:

Семейство устройств	Команда для выполнения
Рутокен	<pre>/opt/itcs/bin/ngost_token_manager correct-pin --dll /opt/itcs/lib/libsofttoken_ngost_rutoken.so --slotid <Slot Id токена> --old-pin <старый PIN-код> --new-pin <новый PIN-код></pre>
JaCarta	<pre>/opt/itcs/bin/ngost_token_manager correct-pin --dll /opt/itcs/lib/libsofttoken_ngost_jacarta.so --slotid <Slot Id токена> --old-pin <старый PIN-код> --new-pin <новый PIN-код></pre>

```
tester@astra:/opt/itcs/bin$ ./ngost_token_manager correct-pin --dll /opt/itcs/lib/libsofttoken_ngost_jacarta.so
--slotid 196607 --old-pin 11111111 --new-pin 22222222
Command: Pin correction after changing original token pin outside library.

Integrity check failed:
  module name: ngost_token_manager
  event type: 0
  error code: 28
Integrity check failed:
  module name: libsofttoken_ngost_jacarta.so
  event type: 0
  error code: 28
Command successfully finished.
```

Рисунок 4. Смена PIN-кода токена

- 4 Проверьте готовность токена для использования:

Семейство устройств	Команда для выполнения
Рутокен	<pre>/opt/itcs/bin/ngost_token_manager login-check --dll /opt/itcs/lib/libsofttoken_ngost_rutoken.so --slotid <Slot Id токена> --pin <PIN-код токена></pre>
JaCarta	<pre>/opt/itcs/bin/ngost_token_manager login-check --dll /opt/itcs/lib/libsofttoken_ngost_jacarta.so --slotid <Slot Id токена> --pin <PIN-код токена></pre>

```
tester@astra:/opt/itcs/bin$ ./ngost_token_manager login-check --dll /opt/itcs/lib/libsofttoken_ngost_jacarta.so
--pin 22222222 --slotid 196607
Command: Login check to PKCS11 storage.

Integrity check failed:
  module name: ngost_token_manager
  event type: 0
  error code: 28
Integrity check failed:
  module name: libsofttoken_ngost_jacarta.so
  event type: 0
  error code: 28
PKCS11 storage presented.
C_Loading is SUCCESSFUL.
```

Рисунок 5. Проверка готовности токена для использования

В

История версий

Что нового в версии 2.1.0

- **Перенос сертификата и ключа ЭП в облачный сервис**

Теперь вы можете перенести сертификат и ключ ЭП из локального хранилища в облачный сервис через ViPNet PKI Client.

- **Дополнена проверка усиленной квалифицированной ЭП**

В соответствии с Федеральным законом 06.04.2011 № 63-ФЗ (ред. 04.08.2023) «Об электронной подписи» добавлена возможность при проверке усиленной квалифицированной ЭП проверять дополнительные параметры (например, срок действия ключа ЭП).

- **Просмотр информации о сертификате**

Ранее информация о сертификатах отображалась средствами ОС. Теперь вы можете просмотреть подробную информацию о сертификате в ViPNet PKI Client.

- **Новые шаблоны на сертификат**

- **Специальный** — для управления атрибутами и расширениями в запросе на сертификат. С помощью шаблона вы можете запрашивать сертификаты в УЦ, которые предъявляют специальные требования к запросу.
- **Сертификат безопасности клиента** — для издания сертификата, используемого при подключении к веб-ресурсам по TLS ГОСТ.

- **Возможность задать срок действия ключа ЭП при создании запроса на сертификат**

- **Подтверждение операций в облачном сервисе ЭП**

Теперь в ViPNet PKI Client поддерживается выполнение операций в облачном сервисе ЭП, требующих подтверждение: подписание и расшифрование файла, а также создание запроса на сертификат.

- Возможность подписывать XML-файлы в облачном сервисе ЭП
- Возможность подписывать несколько XML-файлов в веб-приложениях с Web Unit
- Расширен список поддерживаемых ОС
 - РЕД ОС 8 — 64-разрядная;
 - ОСнова 2.11, 2.12, в том числе в режиме замкнутой программной среды — 64-разрядные;
 - Astra Linux Special Edition 1.8, в том числе в режиме замкнутой программной среды — 64-разрядная;
 - Debian 11, 12 — 64-разрядные;
 - Ubuntu 24.04 LTS — 64-разрядная.
- Прекращена поддержка ОС
 - РЕД ОС 7.2 — 32/64-разрядная;
 - ОСнова 2.9 — 64-разрядная;
 - Debian 10, 11 — 32/64-разрядные.

Что нового в версии 2.0.0

- **Лицензирование через ViPNet TLS Gateway**

Теперь активировать лицензию ViPNet PKI Client можно через ViPNet TLS Gateway. Для этого необходимо настроить параметры активации. Активация лицензии будет выполняться автоматически при установлении соединения с ViPNet TLS Gateway.
- **Централизованное распространение настроек**

Для централизованного распространения настроек необходимо создать общедоступную папку и добавить в нее файл с настройками. Настройки будут применяться автоматически, без необходимости настраивать ViPNet PKI Client на каждом компьютере вручную.
- **Возможность подписывать несколько файлов в веб-приложениях с Web Unit**
- **Новые параметры при создании запроса на сертификат**
 - возможность экспорта в PFX-файл сертификата и ключа ЭП;
 - выбор кодировки сохранения запроса на сертификат.
- **Поддержка ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018) «Магма» и «Кузнечик» для шифрования файлов**
- **Возможность выбора алгоритма шифрования для шифрования файлов и при экспорте сертификата и ключа ЭП в PFX-файл**
- **Прекращена поддержка ГОСТ 28147-89 для шифрования файлов**
- **Использование ViPNet OSSSL для реализации всех криптографических функций**
- **Добавлена поддержка:**

- Альт Рабочая станция 10 (32- и 64-разрядная);
- Альт СП Рабочая станция релиз 10 (64-разрядная);
- ПК «СинтезМ-Клиент» (64-разрядная);
- РОСА «КОБАЛЬТ» (64-разрядная);
- Debian 11 (32- и 64-разрядная);
- Ubuntu 20.04 LTS, 22.04 LTS (64-разрядные).
- **Прекращена поддержка:**
 - Debian 9 (32- и 64-разрядная).

Что нового в версии 1.7.0

- **Изменения в лицензировании TLS Unit**

Теперь возможности установления TLS-соединений с односторонней и двухсторонней аутентификацией с помощью TLS Unit лицензируются отдельно.

Лицензии с TLS Unit, приобретенные до выхода версии 1.7.0, будут по-прежнему разрешать TLS-соединения с односторонней и двухсторонней аутентификацией. Обновлять их не требуется.

- **Выбор параметров ключа проверки ЭП при создании запроса на сертификат**

Теперь при создании запроса на сертификат вы можете выбрать параметры ключа проверки ЭП, рекомендованные техническим комитетом ТК 26 или компанией КриптоПро.

- **Автоматическое восстановление подключения к туннелируемому ресурсу**

Теперь при разрыве связи Tunnel Unit автоматически переподключается к ресурсу, с которым работал.

- **Скрипты для удаления ViPNet PKI Client**

Теперь для удаления ViPNet PKI Client, ViPNet CSP и ViPNet OSSSL можно использовать входящие в состав дистрибутива скрипты.

- **Изменения в списке поддерживаемых дистрибутивов Linux**

Добавлена поддержка:

- РОСА «Хром» 12.

Прекращена поддержка:

- ЛОТОС (для рабочих станций);
- РОСА «Кобальт»;
- Ubuntu 20.04 LTS;
- Ubuntu Server 18.04 LTS;
- Ubuntu Server 20.04 LTS.

Что нового в версии 1.6.0

- **Поддержка работы с облачными сервисами ЭП**

Теперь, если в вашей организации используется облачный сервис ЭП на базе ПАК ViPNet PKI Service версии 2.0, вы можете работать с ним из программы ViPNet PKI Client.

- **Поддержка протокола TLS версии 1.3**

- **Поддержка внешних устройств для подключения к туннелируемым ресурсам**

Теперь для подключения к туннелируемым ресурсам с аутентификацией пользователя могут использоваться сертификаты и ключи ЭП, хранящиеся на внешних устройствах.

- **Смена PIN-кода Infotecs Software Token**

Теперь вы можете сменить PIN-код Infotecs Software Token.

- **Изменения в списке поддерживаемых дистрибутивов Linux**

Добавлена поддержка:

- РЕД ОС 7.3;
- Astra Linux Special Edition («Смоленск») 1.7.

Прекращена поддержка:

- Альт Линукс СПТ 7.0;
- РЕД ОС 7.1 «МУРОМ»;
- Astra Linux Special Edition («Смоленск») 1.5;
- Debian 8;
- Ubuntu и Ubuntu Server 16.04 LTS.

Что нового в версии 1.5.0

- **Расширена функция программы Web Unit — signXML для подписи XML-файлов**

- Добавлен параметр `signatureType`, с помощью которого можно выбирать формат электронной XML-подписи: XAdES, XMLDSig, WSS-Security. В предыдущей версии выбор был недоступен (использовался формат XMLDSig).
- Добавлена поддержка трансформации СМЭВ (`urn://smev-gov-ru/xmlldsig/transform`), применяемой в государственном документообороте.
- Добавлена поддержка шаблонов XML-подписи, которые можно добавлять в подписываемые XML-файлы. В шаблонах содержатся параметры XML-подписи, которые в новой версии ViPNet PKI Client Web Unit будет учитывать при выполнении операции подписи.

Подробнее см. в документе «ViPNet PKI Client. Руководство разработчика».

- **Изменен список поддерживаемых дистрибутивов Linux**

Добавлена поддержка дистрибутивов (32- и 64-разрядных):

- Альт Рабочая станция 9;
- ЛОТОС (для рабочих станций);
- РЕД ОС 7.2;
- РОСА «Кобальт»;
- Debian 10;
- Ubuntu и Ubuntu Server 18.04 LTS, 20.04 LTS;

Прекращена поддержка Ubuntu 14.04 LTS.

Что нового в версии 1.4.1

- Добавлена поддержка устройств Rutoken Lite и Jacarta PKI для подключения к сайтам, использующим TLS ГОСТ.
- Прекращена поддержка сертификатов ГОСТ Р 34.10-2001 для заверения электронной подписью и шифрования файлов, а также для подключения к сайтам, использующим TLS ГОСТ. Сертификаты ГОСТ Р 34.10-2001 могут использоваться только для проверки электронной подписи и расшифрования.
- Улучшена внутренняя функциональность и исправлены незначительные ошибки, выявленные в процессе эксплуатации версии 1.4.0.

Что нового в версии 1.4.0

- **Поддержка работы в режиме замкнутой программной среды Astra Linux Special Edition («Смоленск») 1.5, 1.6**

Предыдущая версия ViPNet PKI Client поддерживала работу в режиме замкнутой программной среды Astra Linux Special Edition («Смоленск») только в «режиме для проверки электронной подписи в специальном программном обеспечении». В новой версии добавлена поддержка работы в остальных режимах. Подробнее о режиме замкнутой программной среды Astra Linux см. в документе «Операционная система специального назначения Astra Linux Special Edition. Руководство администратора».

- **Перенос личного сертификата с ключом ЭП между компьютерами**

Теперь вы можете экспортировать свой личный сертификат и ключ ЭП в файл PFX и перенести его на другой компьютер или мобильное устройство с установленным ViPNet PKI Client, а также импортировать файлы PFX в разделе **Сертификаты**.

- **Изменения в программе TLS Unit**

- Поддержка устройств Rutoken, JaCarta и ESMART Token.

Раньше поддерживалось только устройство Infotecs Software Token. В новой версии для подключения вы можете использовать устройства семейств Rutoken, JaCarta и ESMART Token с аппаратной поддержкой российских криптографических алгоритмов.

- Добавлены новые алгоритмы шифрования.

Теперь вы сможете подключаться к сайтам, использующим TLS ГОСТ, с алгоритмами шифрования ГОСТ Р 34.12-2015 «Магма» или «Кузнечик».

- Упрощен перенос ключа ЭП на Infotecs Software Token

Теперь для копирования ключа ЭП на Infotecs Token необязательно, чтобы он находился в файле PFX вместе с сертификатом. Скопировать ключ ЭП на Infotecs Software Token можно в разделе **Сертификаты**.

- **Новая версия криптопровайдера ViPNet CSP**

Вместе с ViPNet PKI Client теперь устанавливается криптопровайдер ViPNet CSP версии 4.4.0 (в прошлой версии — 4.2.8).

Что нового в версии 1.3.1

- **Добавлена возможность экспорта и импорта настроек**

Вы можете экспортировать настройки ViPNet PKI Client в файл или импортировать настройки из файла, например, для переноса ViPNet PKI Client на новый компьютер или для восстановления настроек из резервной копии.

- **Добавлена возможность работы с файлами в кодировке Base64**

Теперь вы можете сохранять файлы электронной подписи и зашифрованные файлы в кодировке Base64, а также проверять электронную подпись файлов и расшифровывать файлы в кодировке Base64.

- **Изменен список поддерживаемых дистрибутивов ОС Linux**

Добавлена поддержка ОС Альт 8 СП «Рабочая станция» (32- и 64-разрядной).

Что нового в версии 1.3

- **Добавлен графический интерфейс для настройки компонентов ViPNet PKI Client**

В предыдущей версии настройка компонентов ViPNet PKI Client была возможна только с помощью консоли или файлов конфигурации. В новой версии вы можете настроить все компоненты ViPNet PKI Client с помощью удобного графического интерфейса.

Также с помощью графического интерфейса вы сможете:

- Обновить или расширить лицензию.

- При возникновении неполадок в работе ViPNet PKI Client сформировать архив с данными, необходимыми для анализа проблемы, и отправить его в службу технической поддержки ИнфоТеКС.
- Просмотреть подробные сведения о ПК ViPNet PKI Client.

- **Добавлен компонент Certificate Unit для работы с сертификатами**

С помощью компонента Certificate Unit вы сможете:

- Создавать запросы на издание сертификатов и сохранять их в файл.
- Устанавливать сертификаты и CRL в хранилище сертификатов.
- Экспортировать установленные сертификаты в файлы формата X.509 (*.cer, *.pem).
- Просматривать установленные сертификаты.

Подробнее см. раздел Управление сертификатами.

- **Добавлен компонент Tunnel Unit для подключения к туннелируемым ресурсам**

С помощью компонента Tunnel Unit вы сможете устанавливать защищенные TLS-соединения с односторонней и двусторонней аутентификацией по алгоритмам ГОСТ с туннелируемыми ViPNet TLS Gateway ресурсами, использующими протоколы RDP, HTTP, SMTP, POP3, IMAP, WebDAV и протоколы взаимодействия с базами данных (например MSSQL, PostgreSQL, MySQL). Для компонента Tunnel Unit необходима лицензия, позволяющая использовать компонент TLS Unit. Подробнее см. раздел Подключение к туннелируемым ресурсам.

- **Добавлен компонент File Unit для выполнения криптографических операций с файлами**

С помощью компонента File Unit вы сможете:

- Заверять файлы электронной подписью и проверять электронную подпись файлов.
- Зашифровывать и расшифровывать файлы.

Подробнее см. документ «ViPNet PKI Client File Unit Linux. Руководство пользователя».

- **Изменен список поддерживаемых дистрибутивов ОС Linux**

Добавлена поддержка дистрибутивов ОС Linux (32- и 64-разрядных):

- РЕД ОС 7.1 «МУРОМ»;
- Astra Linux Special Edition («Смоленск») 1.6;
- Astra Linux Common Edition («Орел») 2.12.8;
- Debian 8.11, 9.8;
- Ubuntu Server 16.04 LTS.

Прекращена поддержка дистрибутивов Linux:

- Astra Linux Special Edition («Смоленск») 1.4;
- Astra Linux Common Edition («Орел») 1.11, 2.11.1, 2.11.3;
- Debian 8.10, 9.3;
- Ubuntu 14.10.

- **Изменен комплект документации**

В связи с добавлением компонента File Unit в комплект поставки добавлен документ «ViPNet PKI Client File Unit Linux. Руководство пользователя».

Что нового в версии 1.2

- **Объединение компонентов ПК ViPNet PKI Client предыдущих версий**

Компоненты ViPNet PKI Client предыдущих версий были объединены в единый программный комплекс.

- **Новый компонент CRL Unit**

Добавлен компонент CRL Unit, который обеспечивает автоматическую загрузку списков аннулированных сертификатов (CRL) из точек распространения и установку полученных CRL в хранилище сертификатов ViPNet CSP.

- **Поддержка новых операционных систем**

Добавлена поддержка дистрибутивов ОС Linux (32- и 64-разрядных):

- Альт Линукс СПТ 7.0;
- Astra Linux Common Edition (Опел) 1.11, 2.11.1, 2.11.3;
- Debian 7.11, 9.3;
- Ubuntu 14.04 LTS, 14.10.

- **Изменения в TLS Unit**

- Теперь импорт сертификата и закрытого ключа на Infotecs Software Token осуществляется с помощью контекстного меню программы TLS Unit.
- Добавлено окно выбора сертификата при подключении к веб-ресурсам, требующим аутентификации пользователя.
- Добавлена возможность просмотра информации о TLS-соединениях.
- Интеграция с хранилищем сертификатов ViPNet CSP.

Раньше сертификаты, используемые для установки двусторонних TLS-соединений, хранились в виде файлов в каталогах операционной системы. В новой версии ViPNet PKI Client эти сертификаты, устанавливаются в хранилище сертификатов ViPNet CSP.



Термины и сокращения

Infotecs Software Token

Программное устройство для хранения ключей с интерфейсом PKCS#11.

Аккредитованный удостоверяющий центр

Удостоверяющий центр, аккредитованный уполномоченным федеральным органом исполнительной власти и издающий квалифицированные сертификаты.

Корневой сертификат ViPNet PKI Client Root

Сертификат, используемый TLS Unit при издании служебных сертификатов для подключения к сайтам.