ViPNet PKI Client Windows

Руководство администратора

Версия продукта: 2.0.0

infotecs

ФРКЕ.00175-02 32 03

Версия продукта 2.0.0

АО «ИнфоТеКС»

127083, Москва, улица Мишина, д. 56, стр. 2, этаж 2, помещение IX, комната 29

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

О документе

Документ описывает установку и настройку программного комплекса ViPNet® PKI Client Windows (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 Windows. 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 ее, 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.

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 OSSL для реализации всех криптографических функций**

Изменения в предыдущих версиях см. в приложении История версий.

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 компании ИнфоТеКС регулируется политикой ответственного разглашения.

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. «ViPNet PKI Client Windows. Руководство пользователя»).

Лицензия содержит:

- Разрешенные 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.

Начало работы

Установка, обновление

Особенности

- Установить, обновить ViPNet PKI Client можно с использованием установочного файла, в командной строке (см. ниже) или с помощью групповых политик.
- Если на компьютере необходимо создать замкнутую программную среду для соответствия требованиям ФСБ России к средствам криптографической защиты информации класса КС3, дополнительно установите программу ViPNet SysLocker (см. «ViPNet SysLocker. Руководство пользователя»).

Установка, обновление в обычном режиме

1. Запустите установочный файл.
2. Примите условия лицензионного соглашения.
3. Выберите папку для файла с настройками ViPNet PKI Client. Настройки из файла будут автоматически применяться в ViPNet PKI Client:
   - Папка пользователя (по умолчанию) — позволяет распространять разные настройки для разных пользователей одного компьютера. Чтобы не получать настройки автоматически, выберите эту папку и не загружайте в нее файл с настройками.
   - Общая папка — позволяет распространять одинаковые настройки для разных пользователей одного компьютера. Если выбрали эту папку, укажите путь к ней.
4. Следуйте указаниям мастера.

Установка, обновление в командной строке

```
<путь к установочному файлу>\pki_client_installer.exe -q PKI_CLIENT_EULA_ACCEPTED=yes
```

Установка с помощью групповых политик

Примечание. Подробнее об установке программного обеспечения с помощью групповых политик см. на сайте Microsoft.

Вы можете установить ViPNet PKI Client с помощью групповых политик Active Directory. Для этого потребуются файлы из комплекта поставки ViPNet PKI Client:

- файл инсталляционного пакета ViPNet PKI Client — `ViPNet_PKI_Client_<разрядность>_MUI_<версия>.msi`;
- файл инсталляционного пакета UPRNG — `iuprng_<разрядность>.msi`.

Дополнительно потребуется скачать с сайта Microsoft программу для создания MST-файлов ORCA MSI Editor.

Подготовка к установке

1 Установите программу ORCA MSI Editor.

2 Создайте файл трансформации MST в программе ORCA:

2.1 В меню **File** выберите пункт **Open** или нажмите сочетание клавиш **Ctrl+O**, затем укажите путь к файлу `ViPNet_PKI_Client_<разрядность>_MUI_<версия>.msi`.

2.2 В меню **Transform** выберите пункт **New Transform**.

2.3 В списке **Tables** выберите таблицу **Property**.

2.4 Нажмите сочетание клавиш **Ctrl+R**.

2.5 В окне **Add Row** для параметра **Property** введите значение "PKI_CLIENT_EULA_ACCEPTED".

2.6 Для строки "PKI_CLIENT_EULA_ACCEPTED" укажите Value — "yes".

2.7 В меню **Transform** выберите пункт **Generate Transform** и сохраните файл трансформации MST.

3 В произвольной сетевой папке, доступной всем компьютерам, на которые требуется установить ViPNet PKI Client, создайте папку для размещения файлов для установки.

4 Поместите в сетевую папку файлы MSI и файл MST.

Установка

1 В окне редактора групповых политик выберите раздел **Конфигурация компьютера** > **Политики** > **Конфигурация программ** > **Установка программ**.

2 Щелкните правой кнопкой мыши раздел **Установка программ**, выберите **Создать** > **Пакет**. Добавьте установочные пакеты:

2.1 Укажите сетевой путь к файлу `iuprng_<разрядность>.msi` и нажмите **Открыть**. В окне **Развертывание программ** выберите метод **Назначенный**.

2.2 Укажите сетевой путь к файлу `ViPNet_PKI_Client_<разрядность>_MUI_<версия>.msi` и нажмите **Открыть**. В окне **Развертывание программ** выберите метод **Особый**.

3 В окне свойств установочного пакета `ViPNet_PKI_Client` на вкладке **Модификации** укажите сетевой путь к файлу MST.

4 Перезагрузите компьютер пользователя.

ViPNet PKI Client будет установлен автоматически при запуске операционной системы.

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 верна;
     - сертификат в поле **Расширенное использование ключа** содержит назначение **Проверка подлинности клиента**;
     - сертификат в поле **Использование ключа** содержит назначение **Цифровая подпись** и (или) **Согласование ключей**.

     Примечание. Запрос на сертификат можно создать в ViPNet PKI Client. Подробнее см. «ViPNet PKI Client Windows. 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.

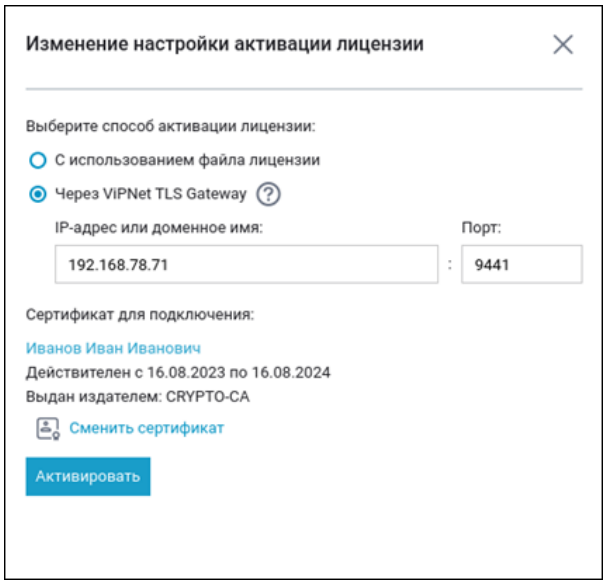


Рисунок 1. Активация через ViPNet TLS Gateway

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 ПИН.

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

В случае неуспешной активации ознакомьтесь с причиной и следуйте указаниям.

Аннулирование активации лицензии через ViPNet TLS Gateway

Если необходимо освободить лицензию, например, в случае увольнения сотрудника:

1 Перейдите в настройки ViPNet PKI Client.

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

Настройка сетевых параметров

Для вызова криптографических функций в веб-приложениях с помощью Web Unit интернет-соединение должно выполняться по протоколу IPv4. Чтобы настроить это:

1 В панели управления Windows в категории **Сеть и Интернет** нажмите **Просмотр состояния сети и задач**.

2 В окне **Центр управления сетями и общим доступом** нажмите **Изменение параметров адаптера**.

3 В окне **Сетевые подключения** щелкните правой кнопкой мыши значок вашего интернет-соединения и в контекстном меню выберите **Свойства**.

4 В окне свойств вашего интернет-соединения выберите **IP версии 4 (TCP/IPv4)** и снимите флажок **IP версии 6 (TCP/IPv6)**.

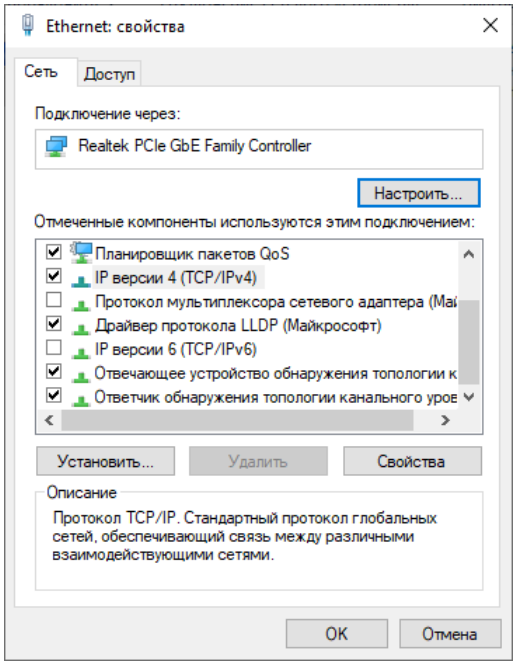


Рисунок 2. Настройка интернет-соединения по IPv4

Импорт и экспорт настроек

Часть настроек программы можно выгрузить 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 Включите настройки, которые хотите экспортировать.

4 Если необходимо, добавьте описание файла настроек.

5 Нажмите **Экспортировать** и укажите папку для сохранения файла настроек.

Импорт настроек

1 Ознакомьтесь с особенностями импорта настроек.

2 Перейдите в настройки ViPNet PKI Client.

3 В разделе  **Импорт и экспорт** нажмите **Загрузить настройки из файла**.

4 Укажите путь к файлу `*.json`.

5 Выберите настройки для импорта и нажмите **Импортировать**.

6 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. «ViPNet PKI Client Windows. 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 настройки, которые надо установить на компьютерах других пользователей.

6 Отметьте настройки, которые надо перезаписать.

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`.

Отслеживание событий при автообновлении CRL

Просмотр событий и настройка их записи

Загрузка CRL в ViPNet PKI Client выполняется с помощью службы `ViPNet PKI Client CRL Unit Service`. Для отслеживания событий, происходящих в работе службы:

1. Перейдите в папку `C:\ProgramData\Infotecs\ViPNet PKI Client\CRL Unit\Logs`.
2. Откройте для чтения файл `crlunitXXX.log` с нужной датой создания.

Чтобы изменить настройки записи событий, отредактируйте конфигурационный файл:

1. Перейдите в одну из папок (если при установке ViPNet PKI Client не была указана другая папка):
   - в 32-разрядных версиях Windows — `C:\Program Files\InfoTeCS\ViPNet PKI Client\CRL Unit`;
   - в 64-разрядных версиях Windows — `C:\Program Files (x86)\InfoTeCS\ViPNet PKI Client\CRL Unit`.
2. В текстовом редакторе, поддерживающем кодировку текста UTF-8, откройте файл `crlunit.cfg` и выполните настройки.
3. Сохраните изменения.
4. Перезапустите службу `ViPNet PKI Client CRL Unit Service` стандартными средствами Windows.

Файл crlunit.cfg

В файле `crlunit.cfg` содержится один корневой элемент `certagent` с атрибутами:

- `proxy-settings` — настройки подключения к прокси-серверам (если используются для доступа в интернет):
  - `proxy addr` — IP-адрес или доменное имя и порт;
  - `protocol` — протокол (`http`, `ftp`, `ldap`, `all`);
  - `authtype` — способ аутентификации (`basic`, `digest`, `negotiate`, `ntlm`, `any`).

- `logging` — настройки записи событий в файлы:
  - `dir` — папка для сохранения файлов. Путь к папке может содержать переменные окружения, например, `%PROGRAMDATA%`;
  - `rotationsize` — максимальный размер файла в МБайтах. При достижении этого размера создается новый файл;
  - `maxsize` — максимальный размер всех файлов в МБайтах. При достижении этого размера удаляются файлы, начиная с раннее созданного;
  - `level` — записываемые события:
    - `0` — все события, включая отладочные;
    - `1` — все события, кроме отладочных (по умолчанию);
    - `2` — предупреждения и ошибки;
    - `3` — только ошибки.

Пример файла crlunit.cfg

```
<?xml version="1.0" encoding="utf-8"?>
<certagent>
      <proxy-settings>
          <proxy addr="msk.proxy-server:3128"/>
          <proxy addr="msk.proxy-server:3128" protocol="http" authtype="negotiate"/>
          <proxy addr="msk.proxy-server:3128" protocol="ftp" authtype="negotiate"/>
      </proxy-settings>

      <logging>
          <dir>%PROGRAMDATA%\InfoTeCS\ViPNet PKI Client\CRL Unit\Logs</dir>
          <rotationsize>10</rotationsize>
          <maxsize>200</maxsize>
          <level>1</level>
      </logging>
</certagent>
```

Перезапуск ViPNet PKI Client CRL Unit Service

После установки ViPNet PKI Client служба `ViPNet PKI Client CRL Unit Service` запускается автоматически и работает в фоновом режиме.

Если вы изменили файл `crlunit.cfg`, перезапустите службу стандартными средствами Windows:

1. Нажмите сочетание клавиш **Win**+**R**.
2. В окне **Выполнить** в поле **Открыть** введите `services.msc`.

3 Выберите **Службы** > **ViPNet PKI Client CRL Unit Service**.

4 В контекстном меню выберите **Остановить**.

5 В контекстном меню выберите **Запустить**.

Настройка подключения к сайтам, использующим TLS ГОСТ

Требования к сертификатам для работы TLS Unit

Сертификат сервера

При подключении к сайту проверяется:

- что сертификат действителен;
- ЭП сертификата верна;
- адрес сайта соответствует адресу в сертификате;
- сертификат в поле **Расширенное использование ключа** содержит назначение **Проверка подлинности сервера**;
- сертификат в поле **Использование ключа** содержит назначение:
  - **Шифрование ключей** и (или) **Согласование ключей** — для TLS 1.2;
  - **Цифровая подпись** — для TLS 1.3.

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 истек или не наступил;
- не удается 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 верна;
- сертификат в поле **Расширенное использование ключа** содержит назначение **Проверка подлинности клиента**;
- сертификат в поле **Использование ключа** содержит назначение **Цифровая подпись** и (или) **Согласование ключей**.

Примечание. Для подключения к некоторым сайтам сертификат пользователя должен быть издан в определенных 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 совместной работы TLS Unit и Firefox

Если для доступа к сайтам используется браузер Firefox, импортируйте корневой сертификат `ViPNet PKI Client Root` в сертификаты Firefox. Для этого:

1 Проверьте, что в браузере Firefox используются системные параметры прокси:

1.1 Перейдите в меню **Настройки**.

1.2 Слева выберите раздел **Основные**.

1.3 В группе **Настройки сети** нажмите **Настроить**.

1.4 Проверьте, что в окне **Параметры соединения** выбрано **Использовать системные настройки прокси**.

2 Экспортируйте корневой сертификат `ViPNet PKI Client Root` с помощью менеджера сертификатов:

2.1 Нажмите сочетание клавиш **Win+R**.

2.2 В окне **Выполнить** в поле **Открыть** введите `certmgr.msc`.

2.3 Перейдите в системное хранилище **Доверенные корневые центры сертификации**, в раздел **Сертификаты**.

2.4 В списке щелкните правой кнопкой мыши сертификат `ViPNet PKI Client Root`. В меню выберите **Все задачи** > **Экспорт**.

2.5 В окне **Мастер экспорта сертификатов**:

- На странице **Экспортирование закрытого ключа** выберите **Нет, не экспортировать закрытый ключ**.
- На странице **Формат экспортируемого файла** установите переключатель в положение **Файлы X.509 (.CER) в кодировке DER**.
- На странице **Имя экспортируемого файла** нажмите **Обзор** и укажите имя и папку для сохранения экспортируемого сертификата.
- На странице **Завершение работы мастера экспорта сертификатов** нажмите **Готово**.

3 Импортируйте сертификат `ViPNet PKI Client Root` в Firefox:

3.1 В браузере перейдите в меню **Настройки.**

3.2 Слева выберите раздел **Приватность и Защита**.

3.3 В группе **Защита** нажмите **Просмотр сертификатов**.

3.4 В окне **Управление сертификатами** выберите вкладку **Центры сертификации** и нажмите **Импортировать**.

3.5 Выберите сертификат `ViPNet PKI Client Root` и нажмите **Открыть**.

3.6 В окне **Загрузка сертификата** выберите **Доверять при идентификации веб-сайтов** и нажмите **ОК**.

3.7 Перезапустите Firefox.

Подключение к туннелируемым ресурсам

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 верна;
- адрес ViPNet TLS Gateway соответствует адресу в сертификате;
- сертификат в поле **Расширенное использование ключа** содержит назначение **Проверка подлинности сервера**.
- сертификат в поле **Использование ключа** содержит назначение:
  - **Шифрование ключей** и (или) **Согласование ключей** — для TLS 1.2;
  - **Цифровая подпись** — для TLS 1.3.

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

Сертификат пользователя

- Сертификат действителен;
- ЭП сертификата верна;
- сертификат добавлен в ViPNet TLS Gateway в список **Сертификаты пользователей** > **Разрешенные**, и разрешен доступ к туннелируемому ресурсу (см. «ViPNet TLS Gateway. Руководство администратора»);
- сертификат в поле **Расширенное использование ключа** содержит назначение **Проверка подлинности клиента**;
- сертификат в поле **Использование ключа** содержит назначение **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 необходимо указать 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 ПИН 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 .

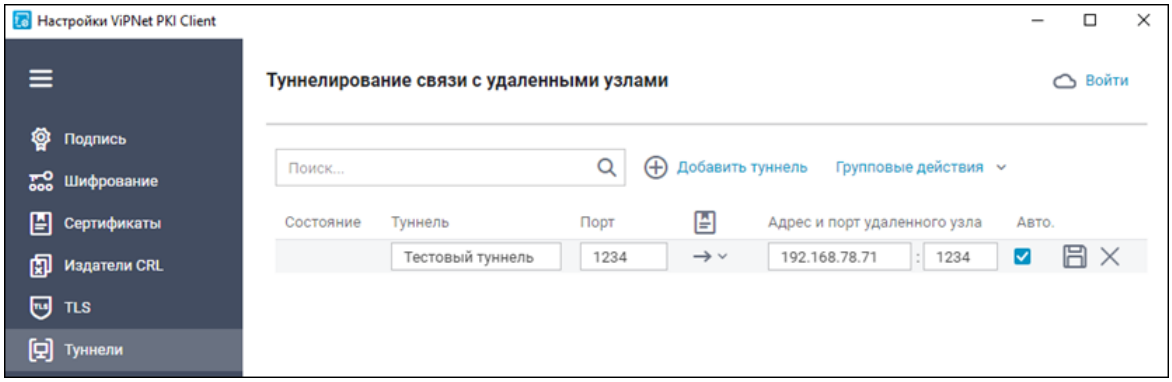


Рисунок 3. Добавление туннелируемого ресурса

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 удаленному 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 используйте кнопку **Групповые действия**:

- **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 стандартную программу Windows **Подключение к удаленному рабочему столу**.

6 В поле **Компьютер** 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

Невозможно установить соединение по TLS ГОСТ

1. Проверьте, что на компьютере установлены последние пакеты обновлений Windows.
2. Проверьте, что при выключенном TLS Unit настройки прокси-сервера, заданные на вашем компьютере, соответствуют настройкам прокси-сервера во всей локальной сети.
3. Если вы устанавливаете защищенное соединение с сервером, принадлежащим к локальной сети, убедитесь, что при выключенном TLS Unit адрес этого сервера указан в исключениях настроек параметров прокси-сервера.

Не удается запустить компоненты ViPNet PKI Client в VirtualBox

Если вам не удается запустить компоненты ViPNet PKI Client на виртуальной машине, созданной в VirtualBox:

1. Перейдите в настройки виртуальной машины.
2. Нажмите **Дисплей** и включите поддержку 3D-ускорения.

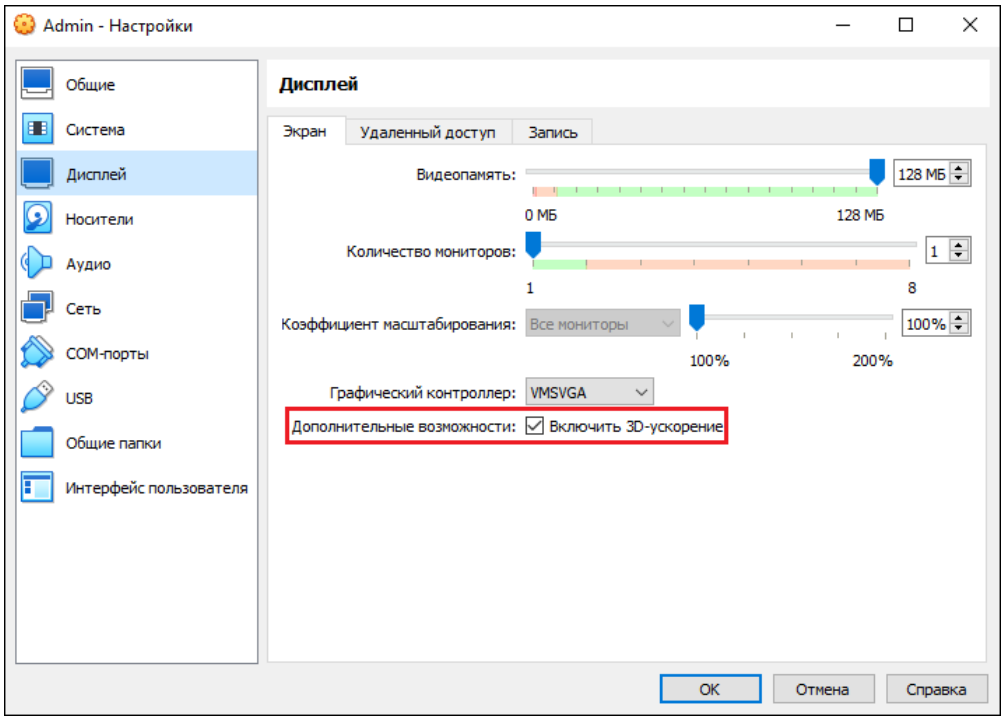
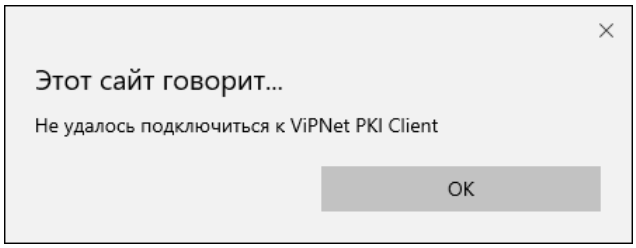


Рисунок 4. Включение поддержки 3D-ускорения

Ошибка при работе в Web Unit

При работе в Web Unit браузер может отобразить ошибку:



Убедитесь, что у вас установлена последняя версия браузера.

Ошибки при обновлении CRL

Для определения причины сбоя:

1. Откройте файл `pki-client-crl-unit.log`, в который записываются события службы `ViPNet PKI Client CRL Unit Service` (по умолчанию находится в папке `C:\ProgramData\Infotecs\ViPNet PKI Client\Logs\pki-client-crl-unit`).
2. В строке события посмотрите значение `Error code`.

Неправильный URL (Error code: -3)

Проверьте правильность URL точки распространения CRL.

Ошибка данных (Error code: -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 (Error code: -5)

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

Для устранения ошибки:

1. Проверьте доступ в интернет.
2. Проверьте доступ к точке 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.

Ошибка хранилища сертификатов (Error code: -6)

Возможно, у используемой учетной записи недостаточно прав для установки CRL.

Сертификат не найден (Error code: -7)

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

CRL просрочен (Error code: -8)

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

Недостаточно памяти (Error code: -9)

Нехватка оперативной памяти.

CRL уже установлен (Error code: -11)

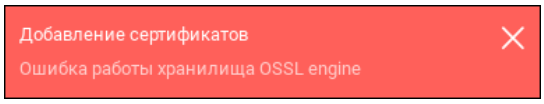
Попытка установить CRL, который уже есть в хранилище сертификатов.

Ошибка сети (Error code: -12)

Сбой в сети во время загрузки CRL.

Ошибки при работе с устройствами Рутокен

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



Или если у вас возникают ошибки при попытке подписать или расшифровать файл сертификатом, хранящимся на устройстве Рутокен:

1. Узнайте версию установленного приложения «Панель управления Рутокен».
2. Если у вас установлено приложение версии 4.17.0.0, удалите его стандартными средствами Windows.
3. Установите приложение «Панель управления Рутокен» версии 4.16.0.0.

После отключения автозагрузки TLS Unit не устанавливается интернет-соединение

Если вы отключили автозагрузку TLS Unit, перезагрузили компьютер и не смогли установить интернет-соединение, включите и выключите TLS Unit (см. «ViPNet PKI Client Windows. Руководство пользователя»).

После смены ПИНа токена в ViPNet PKI Client не удается ввести новый ПИН

Если вы сменили ПИН токена при помощи утилиты обслуживания токена и при вводе нового ПИНа в ViPNet PKI Client появляется сообщение о том, что ПИН неверный:

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

ОС	Семейство устройств	Команда для выполнения
Windows 32-разрядная	Рутокен	`"C:\Program Files\InfoTeCS\ViPNet PKI Client\bin\ngost_token_manager.exe" enum-slots --dll "C:\Program Files\InfoTeCS\ViPNet PKI Client\bin\softtoken_ngost_rutoken.dll"`
Windows 32-разрядная	JaCarta	`"C:\Program Files\InfoTeCS\ViPNet PKI Client\bin\ngost_token_manager.exe" enum-slots --dll "C:\Program Files\InfoTeCS\ViPNet PKI Client\bin\softtoken_ngost_jacarta.dll"`
Windows 64-разрядная	Рутокен	`"C:\Program Files (x86)\InfoTeCS\ViPNet PKI Client\bin\ngost_token_manager.exe" enum-slots --dll "C:\Program Files (x86)\InfoTeCS\ViPNet PKI Client\bin\softtoken_ngost_rutoken.dll"`
Windows 64-разрядная	JaCarta	`"C:\Program Files (x86)\InfoTeCS\ViPNet PKI Client\bin\ngost_token_manager.exe" enum-slots --dll "C:\Program Files (x86)\InfoTeCS\ViPNet PKI Client\bin\softtoken_ngost_jacarta.dll"`

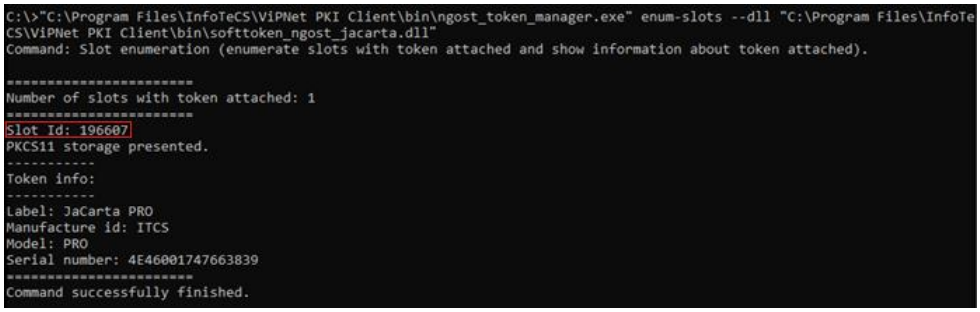


Рисунок 5. Определение Slot Id подключенного токена

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

ОС	Семейство устройств	Команда для выполнения
Windows 32-разрядная	Рутокен	`"C:\Program Files\InfoTeCS\ViPNet PKI Client\bin\ngost_token_manager.exe" correct-pin --dll "C:\Program Files\InfoTeCS\ViPNet PKI Client\bin\softtoken_ngost_rutoken.dll" --slotid <Slot Id токена> --old-pin <старый ПИН> --new-pin <новый ПИН>"`
Windows 32-разрядная	JaCarta	`"C:\Program Files\InfoTeCS\ViPNet PKI Client\bin\ngost_token_manager.exe" correct-pin --dll "C:\Program Files\InfoTeCS\ViPNet PKI Client\bin\softtoken_ngost_jacarta.dll" --slotid <Slot Id токена> --old-pin <старый ПИН> --new-pin <новый ПИН>"`
Windows 64-разрядная	Рутокен	`"C:\Program Files (x86)\InfoTeCS\ViPNet PKI Client\bin\ngost_token_manager.exe" correct-pin --dll "C:\Program Files (x86)\InfoTeCS\ViPNet PKI Client\bin\softtoken_ngost_rutoken.dll" --slotid <Slot Id токена> --old-pin <старый ПИН> --new-pin <новый ПИН>"`

ОС	Семейство устройств	Команда для выполнения
Windows 64-разрядная	JaCarta	"C:\Program Files (x86)\InfoTeCS\ViPNet PKI Client\bin\ngost_token_manager.exe" correct-pin --dll "C:\Program Files (x86)\InfoTeCS\ViPNet PKI Client\bin\softtoken_ngost_jacarta.dll" --slotid <Slot Id токена> --old-pin <старый ПИН> --new-pin <новый ПИН>"

Рисунок 6. Смена ПИНа токена

4 Проверьте готовность токена для использования:

ОС	Семейство устройств	Команда для выполнения
Windows 32-разрядная	Рутокен	"C:\Program Files\InfoTeCS\ViPNet PKI Client\bin\ngost_token_manager.exe" login-check --dll "C:\Program Files\InfoTeCS\ViPNet PKI Client\bin\softtoken_ngost_rutoken.dll" --slotid <Slot Id токена> --pin <ПИН токена>"
Windows 32-разрядная	JaCarta	"C:\Program Files\InfoTeCS\ViPNet PKI Client\bin\ngost_token_manager.exe" login-check --dll "C:\Program Files\InfoTeCS\ViPNet PKI Client\bin\softtoken_ngost_jacarta.dll" --slotid <Slot Id токена> --pin <ПИН токена>"
Windows 64-разрядная	Рутокен	"C:\Program Files (x86)\InfoTeCS\ViPNet PKI Client\bin\ngost_token_manager.exe" login-check --dll "C:\Program Files (x86)\InfoTeCS\ViPNet PKI Client\bin\softtoken_ngost_rutoken.dll" --slotid <Slot Id токена> --pin <ПИН токена>"
Windows 64-разрядная	JaCarta	"C:\Program Files (x86)\InfoTeCS\ViPNet PKI Client\bin\ngost_token_manager.exe" login-check --dll "C:\Program Files (x86)\InfoTeCS\ViPNet PKI Client\bin\softtoken_ngost_jacarta.dll" --slotid <Slot Id токена> --pin <ПИН токена>"

Рисунок 7. Проверка готовности токена для использования

История версий

Что нового в версии 1.7.0

- **Поддержка Windows 11 (версия 21H2, сборка 22000)**
- **Изменения в лицензировании TLS Unit**

  Теперь возможности установления TLS-соединений с односторонней аутентификацией 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 аутентификацией и двухсторонней аутентификацией. Обновлять их не требуется.
- **Поддержка подключения к веб-ресурсам по протоколу TLS версии 1.3**
- **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.
- **Совместимость с КриптоПро CSP**

  Установка новой версии ViPNet PKI Client на компьютер, на котором используется КриптоПро CSP, не влияет на работоспособность КриптоПро CSP. При возникновении ошибок см. «ViPNet CSP. Руководство пользователя» > «Установка и запуск программы» > «Совместимость с программным обеспечением КриптоПро CSP».

Что нового в версии 1.6.0

- **Поддержка работы с новой версией ViPNet PKI Service**

  Теперь вы можете подключаться к облачным сервисам на базе ViPNet PKI Service 2.0. Поддержка работы с ViPNet PKI Service 1.0.4 прекращена.
- **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.
- **Новое поле при создании запроса на сертификат — Идентификация заявителя**

  В запросы на сертификаты добавлено поле **Идентификация заявителя**. Реализовано в соответствии с приказом ФСБ РФ 27.12.2011 №795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи».
- **Изменение поддержки сертификатов ГОСТ Р 34.10–2001**

Сертификаты ГОСТ Р 34.10–2001 больше нельзя использовать для подписания и зашифрования файлов, а также для подключения к сайтам, использующим TLS ГОСТ, и туннелируемым ресурсам. Теперь эти сертификаты можно использовать только для проверки ЭП и расшифрования файлов. Реализовано в соответствии с документом ФСБ России №149/7/1/3-58 от 31.01.2014 «О порядке перехода к использованию новых стандартов ЭЦП и функции хэширования».

- **Изменения в шаблонах XML-подписи**
  - Добавлена поддержка подписи формата WS-Security.
  - Добавлена поддержка трансформации СМЭВ 3 (urn://smev-gov-ru/xmldsig/transform).
- **Смена ПИНа Infotecs Software Token**

  Теперь вы можете сменить ПИН Infotecs Software Token.

Что нового в версии 1.5.1

- **Добавлена поддержка шаблонов XML-подписи (XMLDSig)**

  Ранее вы могли использовать подпись формата XMLDSig для XML-файлов, но не могли изменить параметры подписи, заданные по умолчанию. Теперь вы можете создать свой шаблон XML-подписи, добавить его в настройки и использовать при подписании XML-файлов.
- **Упрощено подключение к сайтам, использующим TLS ГОСТ с аутентификацией пользователя**

  Вы можете хранить сертификаты для подключения к сайтам, использующим TLS ГОСТ с аутентификацией пользователя, на разных устройствах. Например, Rutoken Lite и Infotecs Software Token. При этом ранее перед подключением к сайту в настройках нужно было выбрать это устройство. Теперь этого делать не нужно. ViPNet PKI Client автоматически опросит все поддерживаемые устройства и покажет список подходящих для подключения сертификатов.
- **Расширен список внешних устройств для подключения к сайтам, использующим TLS ГОСТ с аутентификацией пользователя**

  Теперь для подключения могут использоваться устройства Esmart Token, JaCarta SE, Рутокен S.
- **Добавлен английский язык**

  Теперь ViPNet PKI Client доступен на английском языке. Переключить язык можно в настройках **О Программе**.

Что нового в версии 1.4.0

- **Выполнение криптографических операций на ViPNet PKI Service**

  Если в вашей организации для хранения сертификатов и ключей ЭП используется ViPNet PKI Service, вы можете подключиться к нему для выполнения криптографических операций из интерфейса ViPNet PKI Client.

- **Установка личного сертификата в контейнер ключей**

  Теперь при установке личного сертификата в хранилище сертификатов Windows вы можете дополнительно установить его в контейнер ключей. Может быть полезно, если при создании запроса на сертификат вы сохранили ключ ЭП на внешнем устройстве.

- **Работа 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.

- **Изменения в программе TLS Unit**

  - Расширен список внешних устройств для подключения к сайтам, использующим TLS ГОСТ с аутентификацией пользователя.

    Раньше поддерживались только устройства Infotecs Software Token и Rutoken Lite. 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».

- **Новая версия криптопровайдера ViPNet CSP**

  Вместе с ViPNet PKI Client теперь устанавливается криптопровайдер ViPNet CSP версии 4.4 (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.

- **Изменения в программе Tunnel Unit**

  - Добавлена возможность устанавливать защищенные TLS-соединения с двусторонней аутентификацией по алгоритмам ГОСТ с туннелируемыми ViPNet TLS Gateway ресурсами.
  - Добавлена возможность работы с туннелируемыми ресурсами через контекстное меню значка программы в области уведомлений.
  - Изменен интерфейс раздела **Туннели** в окне настроек:
    - В новой версии туннелирование связи с удаленными узлами включается автоматически при запуске программы Tunnel Unit. В связи с этим был убран переключатель в верхней части окна.
    - Для упрощения работы с большим количеством туннелируемых ресурсов была добавлена кнопка  **Групповые действия**.

- Столбец **Статус связи** переименован в **Состояние**. Переключатель в этом столбце заменен с **Установлена/Ошибка** на **Вкл./Выкл**.
- Столбец **Название туннеля** переименован в **Туннель**.
- Столбец **Локальный порт** переименован в **Порт**.
- Добавлен столбец **Защита соединения сертификатом** для отображения типа TLS-соединения (с односторонней или двусторонней аутентификацией) с туннелируемыми ресурсами.
- Добавлен столбец **Авто**, содержащий флажки для автоматического установления связи с туннелируемыми ресурсами при запуске программы Tunnel Unit.

- **Изменения в интерфейсе**
  - Раздел **CRL** переименован в **Издатели CRL**.
  - Добавлен раздел **Импорт/Экспорт**.
- **Добавлена возможность экспорта сертификатов в CER-файлы**

  В предыдущей версии ViPNet PKI Client можно было экспортировать только личные сертификаты вместе с ключом ЭП в PFX-файлы. В новой версии вы можете экспортировать личные сертификаты и сертификаты получателей в CER-файлы (формат X509 с кодировкой DER). Подробнее см. документ «ViPNet PKI Client. Руководство администратора», раздел «Экспорт сертификатов».
- **Изменен список поддерживаемых операционных систем**

  Начиная с версии 1.3.1, добавлена поддержка ОС Windows Server 2016 (64-разрядная) и Windows 10 версии 1803.

  Прекращена поддержка ОС Windows 8 в связи с прекращением ее поддержки производителем.

Что нового в версии 1.3.0

- **Добавлен новый компонент Tunnel Unit**

  С помощью компонента Tunnel Unit вы сможете устанавливать защищенные TLS-соединения с односторонней аутентификацией по алгоритмам ГОСТ с туннелируемыми ViPNet TLS Gateway ресурсами, использующими протоколы RDP, HTTP, SMTP, POP3, IMAP, WebDAV и SQL. Для компонента Tunnel Unit необходима лицензия, позволяющая использовать компонент TLS Unit.
- **Добавлена возможность обращения в службу технической поддержки**

  Теперь при возникновении неполадок в работе ViPNet PKI Client вы сможете сформировать архив с данными, необходимыми для анализа проблемы, и отправить его в службу технической поддержки АО «ИнфоТеКС». Подробнее см. документ «ViPNet PKI Client. Руководство администратора», раздел «Обращение в службу технической поддержки».
- **Обновлен интерфейс ViPNet PKI Client**

  Переработан дизайн интерфейса ViPNet PKI Client в соответствии с корпоративным стилем.

- **Улучшена работа с сертификатами и CRL**
  - Вы можете устанавливать несколько сертификатов и CRL одновременно.
  - Вы можете устанавливать сертификаты и CRL, перетащив их в окно **Настройки - ViPNet PKI Client** в раздел  **Сертификаты**.
- **Изменения в программе File Unit**
  - Вы можете выполнять криптографические операции для нескольких файлов одновременно.
  - Вы можете добавлять файлы для выполнения криптографических операций, перетащив их в главное окно программы File Unit.

Что нового в версии 1.2.0

- **Расширенная поддержка алгоритма ГОСТ Р 34.10-2012**

  Добавлена возможность организации защищенного TLS-соединения с использованием внешних устройств, поддерживающих хранение ключей, созданных по алгоритму ГОСТ Р 34.10-2012.

- **Изменения в интерфейсе**

  В интерфейс окна **Настройки ViPNet PKI Client** были внесены следующие изменения:

  - Вкладка **Менеджер сертификатов** заменена на вкладку **Сертификаты**.
  - Добавлена вкладка **CRL**. Информация о сертификатах издателей и точках распространения CRL теперь отображается здесь.
  - Добавлена вкладка **TLS** для настройки TLS-соединений.

- **Работа с сертификатами и CRL**

  В предыдущей версии установка сертификатов и CRL осуществлялась с помощью оснастки **Сертификаты**.

  В новой версии ViPNet PKI Client в работе с сертификатами и CRL произошли следующие изменения:

  - Добавлена возможность установки сертификатов и CRL с помощью окна **Настройки ViPNet PKI Client**.
  - Добавлена возможность просмотра установленных сертификатов и подробной информации о них.
  - Добавлена возможность сортировки установленных сертификатов по группам (**Личные сертификаты**, **Сертификаты других пользователей**, **Сертификаты на внешних устройствах**, **Все сертификаты**) и имени владельца.
  - Добавлена возможность фильтрации установленных сертификатов по имени владельца или издателя.

- **Настройка TLS-соединений**

В некоторых случаях может возникнуть необходимость подключения к веб-ресурсам, у которых либо истек срок действия сертификата, либо цепочка сертификации неполная, либо ее невозможно проверить. В новой версии вы можете устанавливать TLS-соединение с такими веб-ресурсами (подробнее см. документ «ViPNet PKI Client. Руководство администратора», главу «Настройка подключения к веб-ресурсу по протоколу TLS», раздел «Требования к сертификату сервера для установки TLS-соединения»).

Также добавлена возможность выбора внешнего устройства, поддерживающего хранение ключей, для установки TLS-соединения.

Что нового в версии 1.1.0

- **Реализован компонент ViPNet PKI Client TLS Unit.**

  Этот компонент позволяет установить TLS-соединение по российским алгоритмам ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 и ГОСТ 28147-89. Вы сможете получить доступ к веб-ресурсам, которые требуют установки такого соединения для работы с ними.

Термины и сокращения

Infotecs Software Token

Программное устройство для хранения ключей с интерфейсом PKCS#11.

Корневой сертификат ViPNet PKI Client Root

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