ViPNet PKI Client Linux

Руководство администратора

infotecs

ФРКЕ.00175-01 32 05

Версия продукта 1.5.0

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)

Веб-сайт: infotecs.ru

Служба поддержки: hotline@infotecs.ru

Содержание

Введение

О документе

Документ описывает назначение и состав программного комплекса ViPNet® PKI Client Linux (далее — ViPNet PKI Client), сценарии использования ViPNet PKI Client для защиты данных и взаимодействия с инфраструктурой открытых ключей (см. глоссарий, стр. 108), а также установку и настройку.

Для кого предназначен документ

Руководство предназначено для администраторов ViPNet PKI Client.

Предполагается, что читатель данного руководства имеет общее представление об инфраструктуре открытых ключей (см. глоссарий, стр. 108) и навыки работы с операционными системами семейства Linux.

Соглашения документа

Ниже перечислены соглашения, принятые в этом документе для выделения информации.

Таблица 1. Обозначения, используемые в примечаниях

Обозначение	Описание
	**Внимание!** Указывает на обязательное для исполнения или следования действие или информацию.
	**Примечание.** Указывает на необязательное, но желательное для исполнения или следования действие или информацию.
	**Совет.** Содержит дополнительную информацию общего характера.

Таблица 2. Обозначения, используемые для выделения информации в тексте

Обозначение	Описание
Название	Название элемента интерфейса. Например, заголовок окна, название поля, кнопки или клавиши.
Клавиша+Клавиша	Сочетание клавиш. Чтобы использовать сочетание клавиш, следует нажать первую клавишу и, не отпуская ее, нажать вторую клавишу.
Меню > Подменю > Команда	Иерархическая последовательность элементов. Например, пункты меню или разделы на панели навигации.
`Код`	Имя файла, путь, фрагмент текстового файла (кода) или команда, выполняемая из командной строки.

При описании команд в данном документе используются следующие условные обозначения:

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

  ```
  команда
  ```

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

  ```
  команда <параметр>
  ```

- Необязательные параметры или ключевые слова заключены в квадратные скобки. Например:

  ```
  команда <обязательный параметр> [необязательный параметр]
  ```

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

  ```
  команда {вариант-1 | вариант-2}
  ```

О программе

Комплект поставки

В комплект поставки ViPNet PKI Client входят:

- Архивы с пакетами в форматах DEB и RPM и установочным скриптом `install.sh` для 32- и 64-разрядных операционных систем.
- Документация в формате PDF:
  - «ViPNet PKI Client Linux. Руководство администратора».
  - «ViPNet PKI Client File Unit Linux. Руководство пользователя».
  - «ViPNet CSP Linux. Руководство пользователя».
  - «ViPNet PKI Client. Руководство разработчика».

Системные требования

Требования к компьютеру для установки ViPNet PKI Client:

- Процессор — Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более.
- Объем оперативной памяти — не менее 2 Гбайт.
- Свободное место на жестком диске — не менее 300 Мбайт.
- Операционная система — Linux, поддерживаются следующие дистрибутивы (32- и 64-разрядные):
  - Альт 8 СП Рабочая станция;
  - Альт Рабочая станция 9;
  - Альт Линукс СПТ 7.0;
  - ЛОТОС (для рабочих станций);
  - РЕД ОС 7.1 «МУРОМ», 7.2;
  - РОСА «Кобальт»;
  - Astra Linux Common Edition («Орел») 2.12;
  - Astra Linux Special Edition («Смоленск») 1.5, 1.6, в том числе в режиме замкнутой программной среды.
  - Debian 8, 9, 10;
  - Ubuntu 16.04 LTS, 18.04 LTS, 20.04 LTS;

- Ubuntu Server 16.04 LTS, 18.04 LTS, 20.04 LTS.

  Для Ubuntu и Ubuntu Server 20.04 LTS должен быть установлен пакет `libqtgui4`.

Примечание. На некоторых дистрибутивах при использовании графической оболочки GNOME могут отсутствовать иконки программы в области уведомлений. В этом случае используйте другую графическую оболочку.

- Веб-браузер — Mozilla Firefox, Chromium последних версий.

  Для ОС должны быть установлены последние пакеты обновлений.

Новые возможности версии 1.5.0

Краткий обзор изменений ViPNet PKI Client версии 1.5.0 по сравнению с 1.4.1. Информация об изменениях в предыдущих версиях содержится в приложении История версий (на стр. 102).

- **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/xmldsig/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.

Обратная связь

Дополнительная информация

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

- Информация о продуктах ViPNet.
- Информация о решениях ViPNet.
- Часто задаваемые вопросы.
- Форум пользователей продуктов ViPNet.

Контактная информация

Если у вас есть вопросы, свяжитесь со специалистами ИнфоТеКС:

- 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.

  Телефон для клиентов с расширенной поддержкой: +7 (495) 737-6196.

- Отдел продаж: soft@infotecs.ru.

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.

1

Общие сведения

Назначение

ViPNet PKI Client — это набор компонентов, который позволяет организовать взаимодействие с инфраструктурой PKI (см. глоссарий, стр. 108) и обеспечить безопасность передачи файлов и данных с помощью шифрования и электронной подписи (см. глоссарий, стр. 110).

С помощью ViPNet PKI Client вы можете:

- Создать запрос и с его помощью получить в удостоверяющем центре (УЦ) сертификат, чтобы использовать его для безопасной передачи файлов и данных.
- Подтверждать свою личность и проверять личность отправителя с помощью электронной подписи в соответствии с федеральным законом № 63-ФЗ «Об электронной подписи».
- Обеспечивать безопасность файлов, которыми вы обмениваетесь с другими пользователями, с помощью шифрования.
- Настроить автоматическое обновление списков аннулированных сертификатов (CRL) (см. глоссарий, стр. 109) из точек распространения.
- Подключаться к веб-ресурсам с помощью TLS-соединений по алгоритмам ГОСТ.
- 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 SQL.

ViPNet PKI Client предоставляет дополнительные возможности администраторам и разработчикам информационных систем:

- Настройка на рабочих местах пользователей ViPNet PKI Client автоматической загрузки CRL из точек распространения (см. глоссарий, стр. 110).
- Разработка веб-приложений с поддержкой криптографических операций, которые смогут выполнять пользователи ViPNet PKI Client.

Для выполнения криптографических операций ViPNet PKI Client использует российские криптографические алгоритмы:

- Алгоритмы формирования и проверки электронной подписи данных ГОСТ Р 34.10-2001 (с вычислением хэш-функции по ГОСТ Р 34.11-94) и ГОСТ Р 34.10-2012 (с вычислением хэш-функции по ГОСТ Р 34.11-2012).
- Алгоритм шифрования файлов ГОСТ 28147-89.
- Алгоритмы шифрования для TLS-соединений: ГОСТ 28147-89, ГОСТ Р 34.12-2015 «Магма» или «Кузнечик».

Инфраструктура открытых ключей

При обмене данными между отдельными пользователями или внутри информационной системы часто требуется защитить информацию от несанкционированного доступа или искажения. Например, если вам нужно передать кому-либо файл, содержащий ваши персональные данные, вы можете зашифровать его, чтобы только получатель имел возможность прочесть этот файл. Если вам нужно направить в какое-либо учреждение документ в электронной форме, вы можете заверить его электронной подписью, которая будет аналогом собственноручной подписи на бумажном документе.

Распространенный способ защиты электронных документов — использование асимметричных алгоритмов шифрования и электронной подписи. При этом каждый пользователь имеет пару связанных между собой асимметричных ключей — открытый и закрытый. Закрытый ключ пользователь хранит в секрете, а открытый ключ свободно распространяется среди других пользователей. Пара ключей используется следующим образом:

- Отправитель документа может зашифровать его с помощью открытого ключа получателя. Этот документ сможет расшифровать только получатель с помощью своего закрытого ключа, поэтому посторонние лица не будут иметь доступа к документу.
- Отправитель может заверить какой-либо документ электронной подписью с помощью своего закрытого ключа. С помощью открытого ключа отправителя получатели документа могут убедиться, что документ действительно подписан отправителем и не был искажен.

Примечание. В федеральном законе № 63-ФЗ «Об электронной подписи» от 6 апреля 2011 г. используются термины:

- Закрытый ключ, предназначенный для создания электронной подписи, называется ключом электронной подписи (см. глоссарий, стр. 109).
- Открытый ключ, предназначенный для проверки подлинности электронной подписи, называется ключом проверки электронной подписи (см. глоссарий, стр. 109).

Чтобы использовать асимметричные ключи для шифрования и электронной подписи, пользователям нужна возможность проверить, кому принадлежит тот или иной открытый ключ, то есть должно существовать доверие пользователей друг к другу. Для этого должна быть организована инфраструктура открытых ключей (PKI) (см. глоссарий, стр. 108). Основной элемент PKI — удостоверяющий центр, который издает сертификаты открытых ключей. Сертификат издается по запросу пользователя на определенный срок и подтверждает, что этому пользователю принадлежит открытый ключ и соответствующий ему закрытый ключ. Сертификат свободно распространяется среди других пользователей.

Примечание. В федеральном законе № 63-ФЗ «Об электронной подписи» от 6 апреля 2011 г. сертификат, подтверждающий принадлежность ключа проверки электронной подписи его владельцу, называется сертификатом ключа проверки электронной подписи (см. глоссарий, стр. 109).

Если по какой-либо причине сертификату невозможно доверять (например, владелец сертификата потерял свой закрытый ключ, и он мог быть доступен посторонним лицам), удостоверяющий центр аннулирует такой сертификат и вносит его в список аннулированных сертификатов (CRL) (см. глоссарий, стр. 109), затем CRL распространяется среди всех участников защищенного документооборота.

Таким образом, сертификат можно безопасно использовать для операций шифрования и электронной подписи, если этот сертификат издан доверенным удостоверяющим центром, срок действия сертификата не истек и сертификат отсутствует в CRL.

Компоненты ViPNet PKI Client

File Unit

File Unit — программа, которая позволяет выполнять с файлами следующие операции:

- Подтверждать и проверять личность отправителя с помощью электронной подписи (см. Заверение документа электронной подписью на стр. 23).
- Обеспечивать безопасность файлов с помощью шифрования и работать с зашифрованными файлами, полученными от других пользователей (см. Отправка зашифрованного файла на стр. 24).

Web Unit

Программа Web Unit позволяет выполнять криптографические операции в веб-приложениях, совместимых с ViPNet PKI Client, например: на порталах государственных электронных услуг, электронных торговых площадках и так далее.

С помощью программы Web Unit вы можете:

- Создавать запросы на издание сертификатов и устанавливать сертификаты в хранилище.
- Заверять данные электронной подписью и проверять электронную подпись.
- Зашифровывать и расшифровывать данные.

SDK

SDK — комплект средств разработки, который позволяет встраивать функции электронной подписи и шифрования в веб-приложения, разрабатываемые на языке JavaScript.

Вместе с ViPNet PKI Client на компьютер устанавливаются примеры веб-страниц, код которых вы можете использовать в собственных веб-приложениях для вызова криптографических функций. Для работы с вашим веб-приложением на компьютерах пользователей должна быть установлена программа Web Unit.

Подробную информацию о комплекте средств разработки SDK вы найдете в документе «ViPNet PKI Client. Руководство разработчика».

CRL Unit

CRL Unit — служба, которая обеспечивает автоматическую загрузку CRL из точек распространения и установку полученных CRL в хранилище сертификатов.

Для автоматической загрузки CRL на компьютер пользователя администратор корпоративной сети должен создать точку распространения (см. глоссарий, стр. 110), в которую будет помещать обновления CRL.

Certificate Unit

Наличие сертификатов является обязательным условием для установления доверительных отношений между пользователями, участвующими в безопасном обмене данными. С помощью сертификатов вы можете выполнять такие операции, как проверка подлинности электронной подписи, аутентификация пользователей, зашифрование данных.

Компонент Certificate Unit предоставляет следующие возможности:

- Создание запросов на издание сертификатов и сохранение их в файл.
- Установка сертификатов и CRL в хранилище сертификатов.
- Экспорт сертификатов.
- Просмотр установленных сертификатов.

TLS Unit

TLS Unit — программа, которая позволяет установить между клиентом и веб-ресурсом безопасное TLS-соединение, поддерживающее российские криптографические алгоритмы ГОСТ 28147–89, ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, ГОСТ Р 34.12-2015 «Магма» или «Кузнечик».

Tunnel Unit

Tunnel Unit — программа, которая позволяет устанавливать защищенные TLS-соединения с односторонней и двусторонней аутентификацией по алгоритмам ГОСТ с туннелируемыми ViPNet TLS Gateway ресурсами.

ViPNet CSP

ViPNet CSP представляет собой криптопровайдер (см. глоссарий, стр. 109), к которому обращаются другие компоненты ViPNet PKI Client для выполнения криптографических операций.

Подробнее об использовании криптопровайдера ViPNet CSP см. документ «ViPNet CSP Linux. Руководство пользователя».

Лицензирование

Для защиты от нелегального копирования и использования ViPNet PKI Client предусмотрен механизм лицензирования. Лицензию необходимо приобрести у представителя ОАО «ИнфоТеКС» (на стр. 12).

Файл лицензии содержит:

- Список компонентов, разрешенных для использования (File Unit, Web Unit, TLS Unit).

Примечание. Для компонента Tunnel Unit необходима лицензия, позволяющая использовать компонент TLS Unit.

- Ограничение максимальной версии программного обеспечения.
- Срок действия лицензии.

Файл лицензии необходимо поместить в каталог с установочными файлами при установке ViPNet PKI Client (см. Установка и обновление на стр. 31), иначе ПО не будет установлено.

После установки ViPNet PKI Client вам нужно активировать лицензию. Лицензия активируется одним из способов:

- Если ваш компьютер подключен к Интернету, лицензия активируется автоматически при запуске настроек ViPNet PKI Client (на стр. 33).
- Если ваш компьютер не подключен к Интернету, активируйте лицензию вручную с помощью запроса (см. Активация лицензии на стр. 35).

Если лицензия ViPNet PKI Client не активирована, вы сможете использовать ПО в течение 14 дней. По истечении пробного периода компоненты, разрешенные для использования файлом лицензии, перестанут работать.

Останутся доступны:

- управление сертификатами и CRL;
- настройка автоматической загрузки CRL.

При необходимости вы можете обновить лицензию (см. Обновление лицензии на стр. 37).

2

Сценарии использования ViPNet PKI Client

Получение нового сертификата

Чтобы получить новый сертификат для проведения криптографических операций:

1 С помощью ViPNet PKI Client сформируйте запрос на сертификат (см. Получение нового сертификата на стр. 48).

При создании запроса (см. глоссарий, стр. 108) вам нужно учитывать цели, для которых вы будете использовать сертификат. Сертификат может использоваться для шифрования, организации защищенного соединения, аутентификации пользователя и других операций.

При создании запроса на сертификат будут сформированы ключ электронной подписи и ключ проверки электронной подписи. При этом ключ электронной подписи (см. глоссарий, стр. 109) помещается в контейнер ключей (см. глоссарий, стр. 109) на диске или внешнем устройстве, а ключ проверки электронной подписи (см. глоссарий, стр. 109) — в файл запроса на сертификат.

2 Передайте запрос в удостоверяющий центр любым способом.

3 После получения запроса администратор удостоверяющего центра издает сертификат, который соответствует вашему открытому ключу.

4 Получите в удостоверяющем центре свой сертификат, корневой сертификат удостоверяющего центра и CRL.

5 Установите полученные сертификаты и CRL в хранилище сертификатов (см. Установка сертификатов и CRL на стр. 50).

Процедура передачи запроса и получения сертификата приведена на следующей схеме:

Рисунок 1. Передача пользователем запроса и получение сертификата

После установки сертификата в хранилище вы сможете заверять документы электронной подписью и расшифровывать данные, полученные от других пользователей.

Загрузка и установка CRL

Чтобы выполнять криптографические операции, требуются действительные сертификаты. Чтобы сертификат считался действительным:

- срок действия сертификата не должен быть истекшим;
- сертификат издан доверенным удостоверяющим центром;
- сертификат не аннулирован.

С помощью ViPNet PKI Client вы можете автоматически загружать CRL и проверять состояние сертификатов, которые вы используете.

Порядок обновления CRL описан ниже.

1. Укажите в настройках ViPNet PKI Client один или несколько URL-адресов точек распространения данных и настройте расписание проверки наличия обновленных CRL.
2. В соответствии с расписанием ViPNet PKI Client будет периодически проверять наличие обновленных CRL в указанных точках распространения.
3. При обнаружении обновленных CRL ViPNet PKI Client загрузит их на ваш компьютер.
4. После загрузки CRL ViPNet PKI Client автоматически установит их в хранилище сертификатов **Промежуточные центры сертификации**.

Рисунок 2. Процесс загрузки CRL с помощью ViPNet PKI Client

Заверение документа электронной подписью

Допустим, что вам нужно отправить руководителю отчет в электронной форме, и по принятым в вашей компании стандартам отчет должен быть заверен электронной подписью. Вы можете подписать отчет с помощью ViPNet PKI Client. Для этого:

1. Убедитесь, что у вас есть сертификат и соответствующий ему ключ электронной подписи.

   Если у вас нет сертификата, обратитесь в удостоверяющий центр вашей компании с запросом на сертификат. Затем получите ваш сертификат и установите его в хранилище сертификатов с помощью ViPNet PKI Client.

2. В программе File Unit используйте функцию заверения электронной подписью. Для этого укажите файл отчета и сертификат, с помощью которого вы хотите подписать файл. В результате программа File Unit создаст файл с расширением `*.sig`, который в зависимости от выбранного типа подписи содержит исходный файл отчета и его электронную подпись или отдельно электронную подпись.

   Рисунок 3. Заверение документа электронной подписью с помощью программы File Unit

3. Отправьте файл `*.sig` руководителю по электронной почте.

   Если при подписании вы использовали открепленную подпись, то вместе файлом `*.sig` отправьте исходный файл отчета.

4. Руководитель с помощью программы File Unit и вашего сертификата сможет проверить электронную подпись полученного отчета.

Отправка зашифрованного файла

Допустим, что вам нужно отправить по электронной почте документ, который содержит ваши персональные данные. Чтобы ваши персональные данные не стали доступны посторонним лицам или злоумышленникам, вы можете зашифровать файл таким образом, чтобы расшифровать его мог только получатель.

Зашифровать файл вы можете с помощью ViPNet PKI Client. Для этого:

1. Запросите сертификат у получателя, например, попросите его прислать сертификат по электронной почте.
2. Если у вас с получателем разные удостоверяющие центры, запросите в удостоверяющем центре получателя сертификат издателя и актуальный CRL и установите их в хранилище сертификатов. Сертификат издателя и CRL необходимы, чтобы убедиться в том, что сертификат получателя является действительным.

Примечание. Если у вас с получателем один и тот же удостоверяющий центр, дополнительно устанавливать сертификат издателя и CRL не требуется.

---

3. Подготовьте файл, который вы хотите отправить.
4. В программе File Unit используйте функцию шифрования. Для этого укажите файл, который нужно зашифровать, и сертификат получателя. В результате программа File Unit создаст файл с расширением `*.enc`, который содержит исходный файл в зашифрованном виде.

Рисунок 4. Шифрование документа с помощью программы File Unit

5. Отправьте файл `*.enc` получателю по электронной почте.

Получатель сможет расшифровать полученный файл с помощью своего ключа электронной подписи.

Использование электронной подписи и шифрования в веб-приложениях

Допустим, что вы используете интернет-сервисы государственных услуг, торговые площадки, интернет-банк и так далее. Чтобы обеспечить защиту данных, такие веб-порталы требуют использования электронной подписи или других криптографических функций для совершения многих операций.

Если веб-портал, который вы используете, совместим с ViPNet PKI Client, для работы с этим порталом вам потребуется установить на ваш компьютер программу Web Unit.

Примечание. Вы можете установить ViPNet PKI Client с помощью программы установки (см. Установка и обновление на стр. 31) либо загрузить непосредственно с веб-портала, на котором вы хотите получить услугу. Возможность установки ViPNet PKI Client Web Unit непосредственно с веб-портала зависит от того, предусмотрена ли такая функция разработчиком портала.

После установки программы Web Unit:

1. Сформируйте на веб-портале заявление на получение услуги.
2. Если у вас еще нет сертификата, вам нужно будет создать запрос на издание сертификата.
3. Создайте запрос с помощью программы Web Unit, дождитесь издания сертификата. Получите и установите сертификат.
4. При отправке заявления от вас потребуется подписать его электронной подписью. Появится окно программы Web Unit, в котором вы сможете просмотреть подписываемый документ и выбрать сертификат для создания электронной подписи.
5. После подписания заявление будет отправлено.

Рисунок 5. Использование электронной подписи и шифрования в веб-приложениях

Подключение к веб-ресурсу с использованием TLS-соединения

Некоторые веб-ресурсы требуют защиты соединения с помощью протокола TLS (см. глоссарий, стр. 108), который работает по российским алгоритмам ГОСТ (например, электронные торговые площадки или государственные информационные порталы). С помощью веб-браузера вы не сможете подключиться к такому ресурсу, потому что браузеры не поддерживают установку TLS-соединения по российским алгоритмам ГОСТ. Вы можете решить эту проблему, используя программу TLS Unit.

Программа TLS Unit позволяет установить TLS-соединение, реализованное по российским алгоритмам ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 и ГОСТ 28147-89. Благодаря этому вы сможете получить доступ к нужным веб-ресурсам и работать с ними.

TLS-соединение устанавливается в следующем порядке:

1. Пользователь с помощью браузера обращается к веб-ресурсу. В веб-браузере в настройках прокси-сервера задаются параметры программы TLS Unit. Программа TLS Unit выполняет функцию локального прокси-сервера, поэтому все соединения с веб-ресурсами проходят через нее.
2. Веб-ресурс и TLS Unit согласовывают параметры соединения: используемые протоколы, алгоритмы шифрования данных.
3. Если TLS-соединение должно быть организовано не по российским алгоритмам ГОСТ или соединение устанавливается не по протоколу TLS, то для его установки используются стандартные средства браузера.
4. Если для установки соединения должны использоваться алгоритмы ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 и ГОСТ 28147-89, оно устанавливается с помощью TLS Unit. Порядок установки соединения следующий:

   4.1 TLS Unit проверяет цепочку сертификации сервера (см. глоссарий, стр. 110). Вся цепочка сертификации должна быть действительной, иначе соединение не будет установлено.

   4.2 Если веб-ресурс требует аутентификации пользователя, то он запрашивает сертификат пользователя. Затем TLS Unit предлагает пользователю выбрать сертификат из списка доступных сертификатов для аутентификации пользователя и установки соединения с этим веб-ресурсом.

   Пользователь выбирает сертификат, соединение устанавливается.

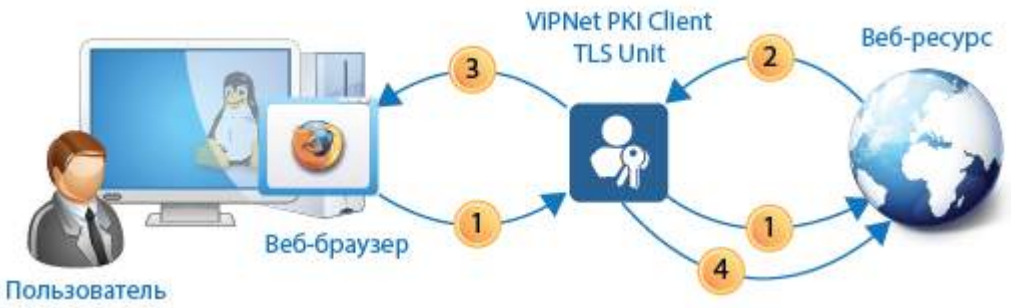

Рисунок 6. Установка TLS-соединения

Установка соединения с туннелируемыми ресурсами

При предоставлении удаленного доступа к корпоративным ресурсам (например, к удаленному рабочему месту, файловому или почтовому серверу) может возникнуть необходимость в защищенном соединении между клиентом и сервером при передаче данных через Интернет. Если в вашей корпоративной сети для разграничения доступа к ресурсам используется ViPNet TLS Gateway версии не ниже 1.3, вы можете настроить туннелирование ресурсов, использующих протоколы RDP, HTTP, SMTP, POP3, IMAP, WebDAV и протоколы взаимодействия с базами данных (например, MSSQL, PostgreSQL, MySQL).

Программа Tunnel Unit позволяет устанавливать защищенные TLS-соединения с односторонней и двусторонней аутентификацией по алгоритмам ГОСТ с этими ресурсами. Благодаря этому вы сможете получить защищенный доступ к нужным ресурсам и работать с ними.

Рисунок 7. Установка соединения с туннелируемыми ресурсами

Для установки защищенного соединения с туннелируемыми ресурсами должны выполняться следующие условия:

- На ПАК ViPNet TLS Gateway должны быть добавлены и настроены туннелируемые ресурсы. Подробнее см. документ «ViPNet TLS Gateway. Руководство администратора».
- На компьютере пользователя должны быть установлены сертификаты УЦ из цепочки доверия транспортных сертификатов ViPNet TLS Gateway.

Соединение устанавливается следующим образом:

- Пользователь в программе ViPNet PKI Client добавляет туннелируемый ресурс (см. Добавление туннелируемого ресурса на стр. 87).
- Пользователь с помощью соответствующего приложения подключается к туннелируемому ресурсу (см. Подключение к туннелируемому ресурсу на стр. 89).

3

Установка, обновление и запуск компонентов

Установка и обновление

Внимание! Для установки ViPNet PKI Client должны быть подключены репозитории, используемые вашей операционной системой по умолчанию.

Во время установки ViPNet PKI Client будет установлен криптопровайдер ViPNet CSP версии 4.4.0. Если на вашем компьютере уже установлен криптопровайдер ViPNet CSP более ранней версии, он будет автоматически обновлен до версии 4.4.0. Для работы ViPNet CSP будут использоваться данные, которые были заданы до установки ViPNet PKI Client.

Для установки и обновления потребуется файл лицензии `*.itcslic`.

Перед установкой или обновлением:

1. Распакуйте пакеты в произвольный каталог.
2. Поместите файл лицензии в каталог с пакетами.
3. Перейдите в каталог с пакетами.

Установка

1. Запустите скрипт `install.sh` с правами суперпользователя:

   ```
   sudo ./install.sh
   ```

2. Программа установки выполнит проверку пакетов:
   - Если появится сообщение, что пакеты не найдены — установите недостающие пакеты и снова запустите установку.
   - Если появится сообщение о конфликтах с пакетами ViPNet CSP прошлой версии, удалите их и снова запустите установку.
3. Если на компьютере нет доступа в Интернет, после установки активируйте лицензию (см. Активация лицензии на стр. 35).

Обновление

1. Если у вас установлена версия 1.0, удалите ее.
2. Запустите скрипт `install.sh` с правами суперпользователя:

   ```
   sudo ./install.sh
   ```

3. Программа установки выполнит проверку пакетов:
   - Если появится сообщение, что пакеты не найдены — установите недостающие пакеты и снова запустите обновление.
   - Если появится сообщение о конфликтах с пакетами ViPNet CSP прошлой версии, удалите их и снова запустите обновление.

4 После обновления перенесите сертификаты и ключи со старого Infotecs Software Token на новый. Для этого:

4.1 Перейдите в настройки ViPNet PKI Client (на стр. 33).

4.2 В разделе  **TLS** нажмите **Перенести данные Infotecs Software Token** и следуйте указаниям мастера.

Примечание. Кнопка **Перенести данные Infotecs Software Token** не отображается, если вы не использовали Infotecs Software Token.

Запуск и завершение работы компонентов

Внимание! Для запуска и завершения работы программы CRL Unit (демон `pki-client-crlunit`) необходимо обладать правами суперпользователя.

Для запуска компонентов ViPNet PKI Client выполните одно из действий:

- Чтобы запустить настройки ViPNet PKI Client, в меню приложений выберите **ViPNet PKI Client Settings** или выполните команду:

  `/opt/itcs/bin/pki-client-settings`

  При первом запуске настроек ViPNet PKI Client появится электронная рулетка (см. глоссарий, стр. 110) (если она не запускалась в рамках текущего сеанса работы криптопровайдера). Следуйте указаниям в окне **Электронная рулетка**.

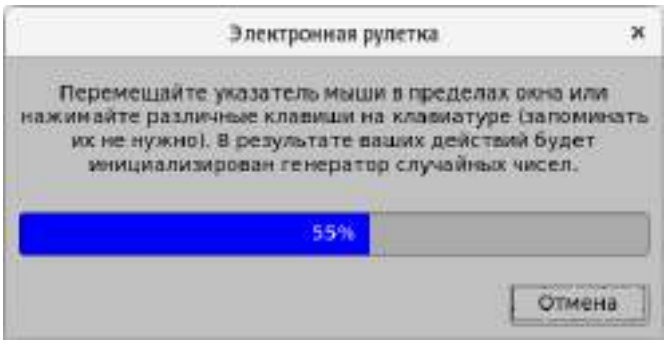

Рисунок 8. Электронная рулетка

- Программы Web Unit, TLS Unit и CRL Unit (демон `pki-client-crlunit`) запускаются автоматически после загрузки операционной системы. Если вы завершили работу программы, то для запуска выполните следующие действия:

  - Чтобы запустить программу Web Unit, в меню приложений выберите **ViPNet PKI Client Web Unit** или выполните команду:

    `/opt/itcs/bin/pki-client-web-unit`

  - Чтобы запустить программу TLS Unit, в меню приложений выберите **ViPNet PKI Client TLS Unit** или выполните команду:

    `/opt/itcs/bin/pki-client-tls-unit`

    При первом запуске TLS Unit появится электронная рулетка (см. глоссарий, стр. 110) (если она не запускалась в рамках текущего сеанса работы криптопровайдера). Следуйте указаниям в окне **Электронная рулетка**.

- Чтобы запустить программу CRL Unit, выполните одно из действий:
  - Если вы используете операционную систему Astra Linux 1.5, выполните команду:

    ```
    /etc/init.d/pki-client-crlunit start
    ```
  - Если вы используете операционную систему Ubuntu, Debian, Альт Линукс или Astra Linux 1.6, выполните команду:

    ```
    systemctl start pki-client-crlunit
    ```

- Чтобы запустить программу Tunnel Unit, в меню приложений выберите  **ViPNet PKI Client Tunnel Unit** или выполните команду:

  ```
  /opt/itcs/bin/pki-client-tunnel-unit
  ```

Для завершения работы компонентов ViPNet PKI Client выполните следующие действия:

- Чтобы завершить работу программ Web Unit и TLS Unit, в области уведомлений щелкните правой кнопкой мыши соответствующий значок и в контекстном меню выберите пункт **Выход**.
- Чтобы завершить работу программы Tunnel Unit, выполните команду:

  ```
  killall pki-client-tunnel-unit
  ```
- Чтобы завершить работу программы CRL Unit, выполните одно из следующих действий:
  - Если вы используете операционную систему Astra Linux, выполните команду:

    ```
    /etc/init.d/pki-client-crlunit stop
    ```
  - Если вы используете операционную систему Ubuntu, Debian или Альт Линукс, выполните команду:

    ```
    systemctl stop pki-client-crlunit
    ```

Активация лицензии

Если лицензия не активирована, вы сможете использовать полнофункциональную версию программы только в течение пробного периода. По окончании пробного периода большинство функций будет недоступно (см. Лицензирование на стр. 19).

Если ваш компьютер подключен к Интернету, активируйте лицензию в режиме реального времени. Для этого выполните одно из действий:

- Запустите настройки ViPNet PKI Client (на стр. 33). Лицензия будет активирована автоматически.
- Активируйте лицензию с помощью команды:

  ```
  /opt/itcs/bin/pki-client-license --register-online
  ```

Если ваш компьютер не подключен к Интернету, выполните активацию в ручном режиме. Для этого:

1 Перейдите в настройки ViPNet PKI Client (на стр. 33) и в разделе  **Лицензия** нажмите  **Запрос на активацию**.

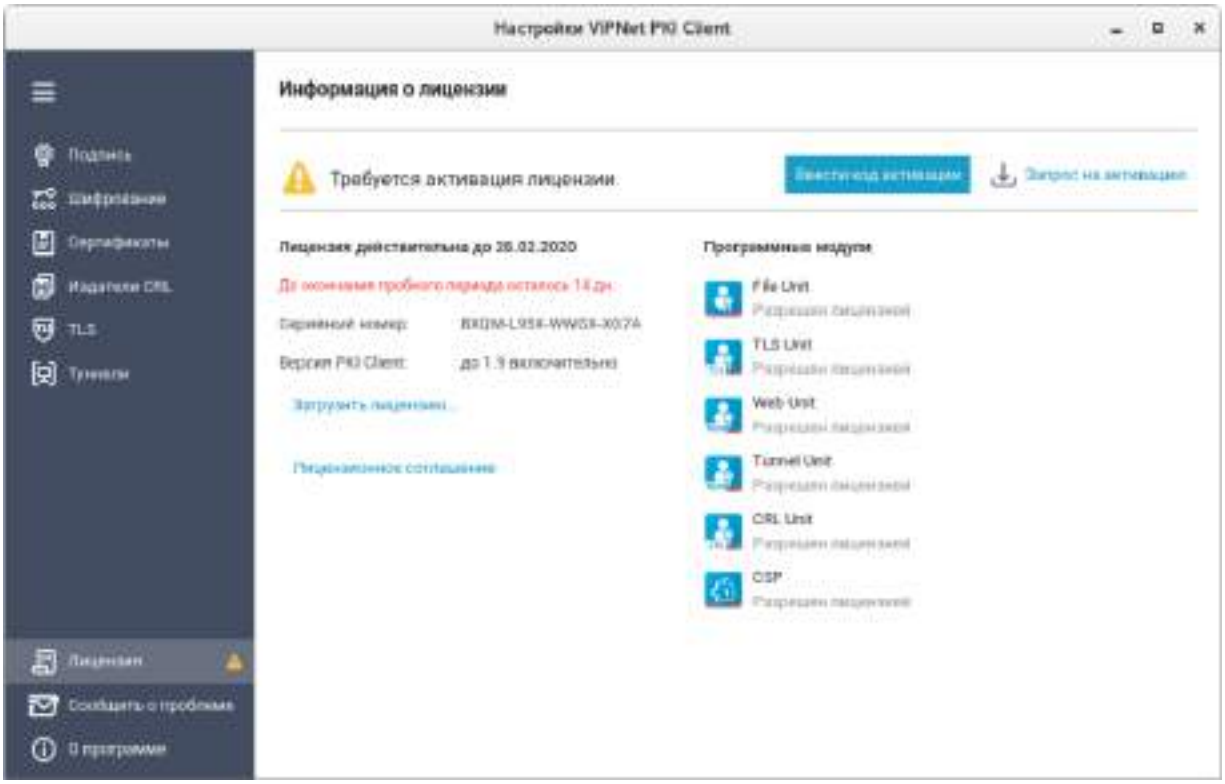

Рисунок 9. Просмотр информации о лицензии

Примечание. Также вы можете сохранить запрос на активацию с помощью команды:
`/opt/itcs/bin/pki-client-license --request <путь сохранения файла запроса>/<имя файла запроса>.txt`

---

2 Укажите имя и путь для сохранения файла запроса и отправьте его в ОАО «ИнфоТеКС».

3 Отправьте файл запроса на электронную почту `reg@infotecs.biz`. Тема и оформление письма могут быть любыми.

4 Дождитесь получения ответного письма, в котором будут указаны данные для активации.

5 Нажмите **Ввести код активации**.

6 В поле **Код активации** введите полученный регистрационный код и нажмите **Активировать**.

Рисунок 10. Ввод данных для активации ViPNet PKI Client

7 В окне сообщения об успешной активации лицензии нажмите **ОК**.

Примечание. Также вы можете активировать лицензию с помощью команды:
`/opt/itcs/bin/pki-client-license --register --serial=<серийный номер> --code=<код регистрации>`

Чтобы убедиться, что лицензия активирована:

1 Перейдите в настройки ViPNet PKI Client (на стр. 33) и выберите раздел **Лицензия**.

2 Удостоверьтесь, что на странице информации о лицензии нет надписи **Требуется активация**.

Примечание. Также вы можете проверить статус лицензии с помощью команды:
`/opt/itcs/bin/pki-client-license --status`

Обновление лицензии

Обновите лицензию для расширения функций ViPNet PKI Client Linux или при истечении срока действия текущей лицензии. Для этого:

1 Отправьте запрос на получение лицензии через веб-форму на сайте ОАО «ИнфоТеКС».

2 Перейдите в настройки ViPNet PKI Client (на стр. 33), в разделе  **Лицензия** нажмите кнопку **Загрузить лицензию** и укажите путь к файлу лицензии.

Примечание. Также вы можете обновить лицензию с помощью команды:
`/opt/itcs/bin/pki-client-license --import <путь к новому файлу лицензии>`

---

3 Ознакомьтесь с информацией о лицензии и нажмите **Установить**.

Рисунок 11. Информация о лицензии

Удаление

Чтобы удалить ViPNet PKI Client, но сохранить пользовательские данные (настройки шифрования, электронной подписи, добавленные туннели и так далее), выполните команду:

```
sudo apt-get remove 'pki-client-*'
```

Чтобы удалить ViPNet PKI Client и пользовательские данные, выполните команду:

```
sudo apt-get remove --purge 'pki-client-*'
```

В процессе удаления ViPNet PKI Client не удаляются:

- Криптопровайдер ViPNet CSP. Вы можете удалить его отдельно или зарегистрировать в течение 30 дней (см. документ «ViPNet CSP Linux. Руководство пользователя»). Криптопровайдер ViPNet CSP регистрировать не нужно, если он был установлен на вашем компьютере до развертывания ViPNet PKI Client. Для работы ViPNet CSP будут использоваться данные, которые были заданы до развертывания ViPNet PKI Client.
- Сертификаты и ключи ЭП.
- Подписанные и зашифрованные файлы.

4

Подготовка к работе

Порядок действий при подготовке к работе

Таблица 3. Порядок действий

	Действие
☐	Подготовьте личный сертификат и ключ ЭП (на стр. 46)
☐	Установите сертификаты издателей и CRL в хранилище сертификатов (на стр. 50)
☐	Настройте параметры электронной подписи (на стр. 61)
☐	Настройте параметры шифрования (на стр. 63)
☐	Настройте параметры обновления CRL (на стр. 65)
☐	Настройте параметры подключения к сайтам, использующим TLS ГОСТ (на стр. 71)
☐	Настройте параметры подключения к туннелируемым ViPNet TLS Gateway ресурсам (на стр. 85)

Экспорт и импорт настроек

Экспортируйте настройки ViPNet PKI Client Linux в файл или импортируйте настройки из файла, чтобы перенести ViPNet PKI Client Linux на другой компьютер, применить одинаковые настройки на нескольких компьютерах или создать резервную копию настроек в случае неисправности компьютера. Для этого:

1 Выполните экспорт настроек (см. Экспорт настроек на стр. 41).

2 На другом компьютере установите ViPNet PKI Client Linux (см. Установка и обновление на стр. 31) и активируйте лицензию (см. Активация лицензии на стр. 35).

3 На другом компьютере импортируйте настройки из созданного ранее файла (см. Импорт настроек на стр. 42).

Экспорт настроек

Примечание. Сначала прочитайте Особенности импорта настроек (на стр. 43).

Чтобы экспортировать настройки ViPNet PKI Client Linux в файл:

1 Перейдите в настройки ViPNet PKI Client (на стр. 33).

2 В разделе  **Импорт/Экспорт** нажмите **Экспорт**.

3 Выберите настройки, которые хотите экспортировать.

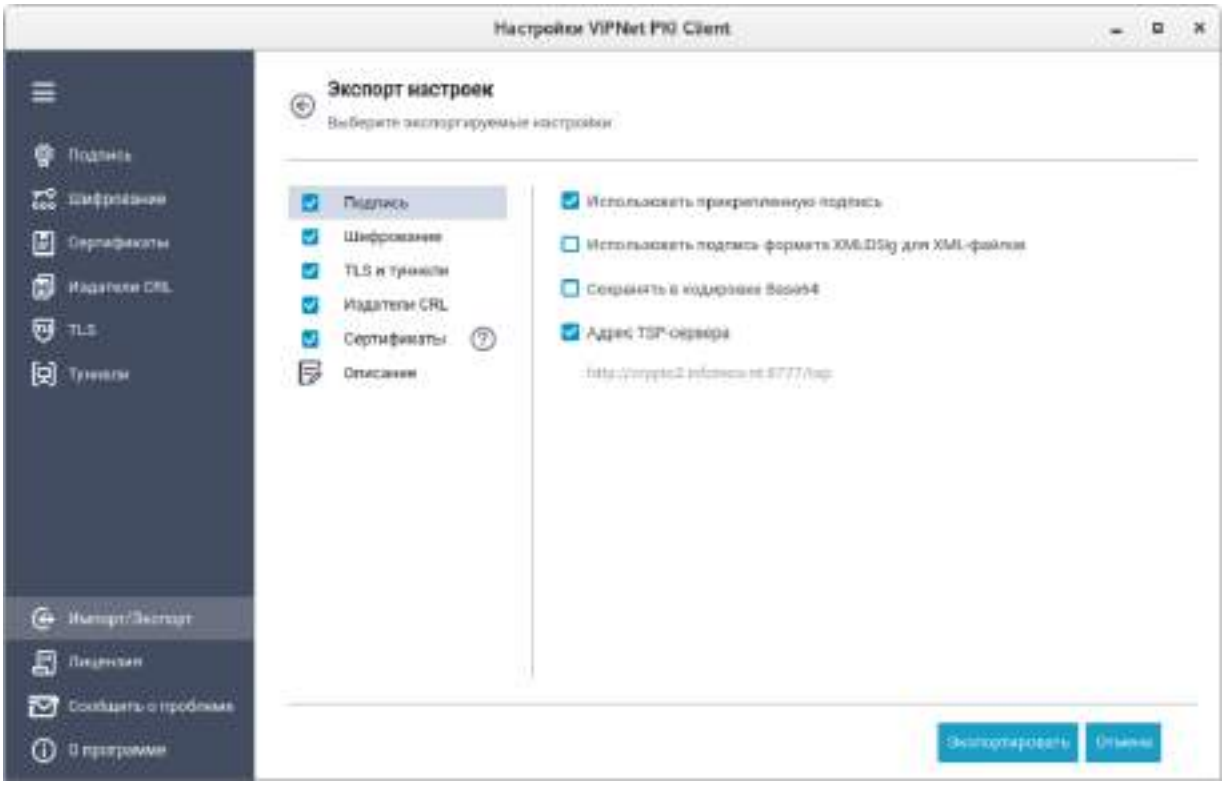

Рисунок 12. Экспорт настроек ViPNet PKI Client

4 При необходимости добавьте описание файла с настройками, например укажите, для каких пользователей предназначены эти настройки. Это описание будет отображаться при импорте настроек (см. Импорт настроек на стр. 42) на новом компьютере.

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

Импорт настроек

Внимание! Сначала прочитайте Особенности импорта настроек (на стр. 43).

Вы можете импортировать настройки ViPNet PKI Client Linux одним из следующих способов:

- Если в файл были экспортированы настройки автоматического обновления CRL, запустите настройки ViPNet PKI Client Linux с правами суперпользователя и импортируйте настройки обновления CRL (раздел **Издатели CRL**), сертификаты издателей и CRL (раздел **Сертификаты**). Затем запустите настройки ViPNet PKI Client Linux с правами текущего пользователя и импортируйте остальные настройки.
- Если в файл не были экспортированы настройки автоматического обновления CRL или вам не нужно их импортировать, запустите настройки ViPNet PKI Client Linux с правами текущего пользователя.

Чтобы импортировать настройки ViPNet PKI Client Linux:

1 В окне **Настройки - ViPNet PKI Client** перейдите в раздел **Импорт/Экспорт** и нажмите кнопку **Импорт**.

2 В открывшемся окне выберите файл с настройками.

3 Выберите настройки, которые вы хотите импортировать, и нажмите **Импортировать**.

Особенности импорта настроек

Шифрование

При импорте списка получателей зашифрованных файлов сертификаты этих пользователей не импортируются. Для импорта списка получателей зашифрованных файлов необходимо выполнение одного из условий:

- Сертификаты получателей экспортированы в файл настроек.
- Сертификаты получателей не экспортированы в файл настроек, но установлены в хранилище текущего пользователя **Другие пользователи**.

TLS и туннели

Для применения настройки **Разрешать соединения при неполном доверии к сертификату сервера** после импорта перезапустите программу TLS Unit (на стр. 33).

По умолчанию не импортируются туннелируемые ресурсы, если уже существует туннелируемый ресурс с таким же номером локального порта (будет помечен значком ⚠). Чтобы импортировать такой ресурс, установите флажок напротив его названия. Туннелируемый ресурс с таким же номером порта будет перезаписан.

Также по умолчанию не импортируются туннелируемые ресурсы с аутентификацией пользователя. Чтобы импортировать такой ресурс, в столбце укажите личный сертификат.

Примечание. Если у вас нет личного сертификата для подключения к туннелируемым ресурсам:

1 Выберите режим без аутентификации пользователя и импортируйте настройки.

2 Получите новый сертификат (см. Получение нового сертификата на стр. 48), установите его в хранилище (на стр. 50), а затем импортируйте его на Infotecs Software Token.

3 В настройках перейдите в раздел **Туннели** и измените тип подключения к туннелируемому ресурсу (см. Добавление туннелируемого ресурса на стр. 87).

Издатели CRL

При импорте настроек обновления CRL сертификаты издателей этих CRL не импортируются. Для импорта настроек обновления CRL необходимо выполнение одного из условий:

- Сертификаты издателей, образующие цепочку сертификации (см. глоссарий, стр. 110), экспортированы в файл настроек, а при импорте настройки ViPNet PKI Client Linux запущены с правами суперпользователя.
- Сертификаты издателей, образующие цепочку сертификации, не экспортированы в файл настроек, но установлены в хранилище локального компьютера.

Сертификаты

Импорт личных сертификатов не предусмотрен.

Для импорта сертификатов издателей и CRL в хранилище локального компьютера настройки ViPNet PKI Client Linux должны быть запущены с правами суперпользователя. В противном случае они будут импортированы в хранилище текущего пользователя, и вы не сможете их использовать для настройки автоматической загрузки CRL (см. Настройка автоматической загрузки CRL на стр. 66).

5

Операции с сертификатами

Подготовка личного сертификата и ключа ЭП

У меня нет сертификата и ключа ЭП

1 Создайте запрос на сертификат (см. Получение нового сертификата на стр. 48).

2 Передайте запрос в УЦ и получите личный сертификат, сертификат издателя и CRL, а если ваш УЦ не является корневым, все сертификаты издателей из цепочки сертификации и соответствующие CRL.

3 Установите личный сертификат в хранилище сертификатов (на стр. 50).

У меня есть сертификат и ключ ЭП в папке на диске

Примечание. Этот вариант подходит, если у вас имеется 1 файл: контейнер ключей, включающий сертификат, или 2 файла: контейнер ключей и сертификат.

Если ваш сертификат и ключ ЭП хранятся в файле PFX, следуйте указаниям раздела Перенос сертификатов и ключей ЭП между компьютерами (на стр. 56).

---

1 Скопируйте контейнер ключей в каталог `/home/<user name>/.itcs/vipnet-csp/containers`.

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

3 В окне **Хранилище сертификатов** выберите хранилище **Текущий пользователь**  .

4 На левой панели выберите раздел **Личное (My)** и на панели инструментов нажмите **Импорт**  .

5 Если у вас имеется только контейнер ключей:

5.1 Установите переключатель в положение **Сертификат из контейнера ключей** и выберите контейнер ключей. Нажмите **Далее**.

5.2 Пропустите остальные шаги и завершите работу мастера.

6 Если у вас имеется контейнер ключей и сертификат:

6.1 Установите переключатель в положение **Сертификат или CRL на диске** и выберите файл сертификата. Нажмите **Далее**.

6.2 В списке выберите контейнер ключей. Нажмите **Далее**.

6.3 Завершите работу мастера.

У меня есть сертификат и ключ ЭП на внешнем устройстве (токене)

1 Подключите внешнее устройство к компьютеру.

2 Перейдите в раздел  **Подключено устройств**, нажмите в строке сертификата и в меню выберите **Установить в хранилище**.

Получение нового сертификата

Чтобы выполнять криптографические операции, вам необходимо иметь контейнер ключей и сертификат. Сертификат издается удостоверяющим центром по вашему запросу, в котором указываются необходимые данные. Контейнер ключей и сертификат могут храниться в папке на диске или внешнем устройстве (токене).

Чтобы создать запрос на сертификат:

1 Перейдите в настройки ViPNet PKI Client (на стр. 33) и в разделе **Сертификаты** и нажмите **Создать запрос**.

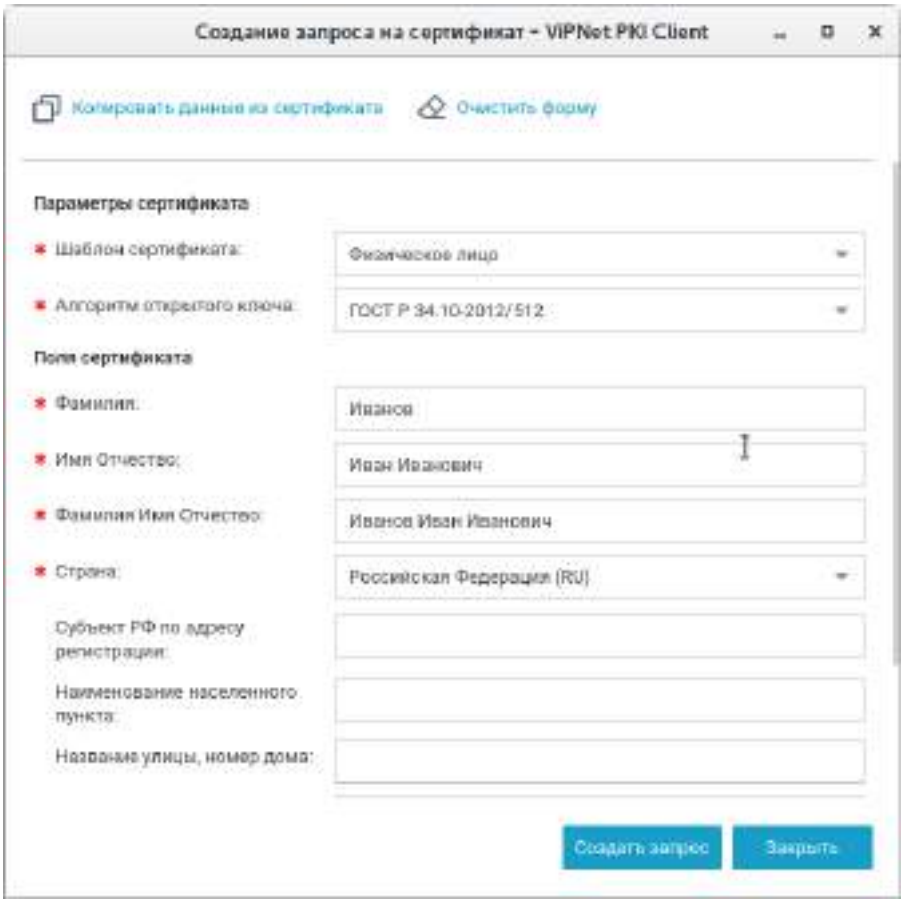

Рисунок 13. Создание запроса на сертификат

Примечание. Если у вас есть сертификат, вы можете создать запрос на его основе. Для этого нажмите **Копировать данные из сертификата** и выберите сертификат для автоматического заполнения полей. Если нужно, измените информацию в полях запроса вручную.

---

2 Выберите **Шаблон** сертификата. В каждом шаблоне содержится разное количество и наименование атрибутов, которые попадут в поле сертификата **Субъект (Subject)**.

3 Выберите **Алгоритм открытого ключа** или оставьте значение по умолчанию.

4 Заполните поля и нажмите **Создать запрос**.

5 Укажите имя и папку для сохранения файла запроса и нажмите **Сохранить**.

6 В окне **ViPNet CSP — инициализация контейнера ключей:**

- Укажите имя и место для сохранения контейнера ключей (см. глоссарий, стр. 109).
- Задайте пароль для работы с контейнером ключей.

7 В окне **Электронная рулетка** отобразится процесс инициализации генератора случайных чисел. Следуйте указаниям в этом окне.

8 В окне сообщения об успешном создании файла запроса нажмите кнопку **OK**.

9 Передайте запрос в УЦ и получите личный сертификат, сертификат издателя и CRL, а если ваш УЦ не является корневым, все сертификаты издателей из цепочки сертификации и соответствующие CRL.

После получения сертификата установите его в хранилище (см. Установка сертификатов и CRL на стр. 50).

Установка сертификатов и CRL

Указанным способом устанавливайте только те личные сертификаты, запрос на которые был создан в ViPNet PKI Client (см. Получение нового сертификата на стр. 48). Если вы получали сертификат иным способом, следуйте указаниям раздела Подготовка личного сертификата (на стр. 46).

ViPNet PKI Client также поддерживает работу с файлами формата PKSC#7. Установка сертификатов из таких файлов осуществляется аналогично. Если файл формата PKSC#7 помимо сертификатов содержит CRL, они также могут быть установлены в хранилище сертификатов.

Чтобы установить сертификаты и (или) CRL:

1 Перейдите в настройки ViPNet PKI Client (на стр. 33).

Внимание! Чтобы установить сертификаты издателей и CRL в хранилище локального компьютера, запустите настройки ViPNet PKI Client с правами суперпользователя. В этом случае не устанавливайте личные сертификаты и сертификаты получателей, поскольку они будут установлены в хранилище сертификатов пользователя root и вы не сможете работать с ними после запуска настроек под своей учетной записью.

---

2 В разделе  **Сертификаты** нажмите  **Добавить сертификат или CRL** и укажите путь к файлу сертификата или CRL.

3 В окне **Добавление сертификатов и CRL** отображаются устанавливаемые сертификаты и (или) CRL.

Сертификаты и CRL с истекшим сроком действия или имеющие недействительную цифровую подпись отмечаются значком  .

При необходимости вы можете:

- Установить в контейнер ключей сертификат, запрос на который был создан в ViPNet PKI Client. Для этого в окне **Добавление сертификатов и CRL** установите соответствующий флажок.
- Посмотреть подробную информацию об устанавливаемых сертификатах и CRL, для этого щелкните имя владельца сертификата или CRL.
- Удалить сертификат или CRL из списка, для этого щелкните значок  (появляется при наведении курсора на строку сертификата или CRL).

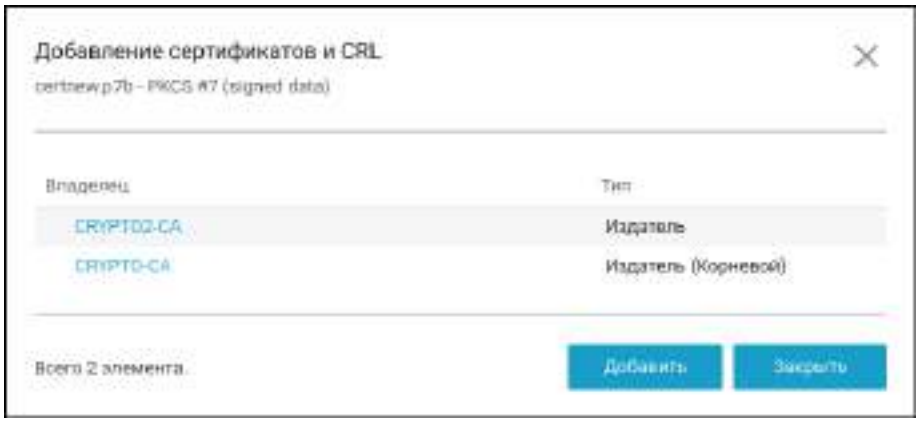

Рисунок 14. Установка сертификатов и CRL

4 В окне **Добавление сертификатов** нажмите **Добавить**, а затем **Закрыть**.

Результат установки отмечается значком напротив каждого установленного сертификата и CRL.

Примечание. Если после установки сертификата в строке имени владельца сертификата появится предупреждающее сообщение, наведите курсор на значок ⚠, просмотрите более подробные сведения об ошибках и устраните их (см. Предупреждающие сообщения на стр. 58).

Рисунок 15. Просмотр предупреждающих сообщений

Экспорт сертификатов

Вы можете экспортировать сертификаты пользователей, установленные в программе ViPNet PKI Client, в файлы формата X.509 (`*.cer`, `*.pem`). Экспорт сертификатов может потребоваться, например, при архивировании сертификатов или при передаче сертификатов внешним пользователям.

Примечание. Экспорт сертификатов издателей в программе ViPNet PKI Client не предусмотрен.

Чтобы экспортировать сертификат в файл:

1. Перейдите в настройки ViPNet PKI Client (на стр. 33) и выберите раздел **Сертификаты**.
2. Нажмите кнопку напротив сертификата и в меню выберите нужный пункт.
3. В открывшемся окне укажите папку для сохранения файла.
4. В окне сообщения об успешном экспорте сертификата нажмите кнопку **OK**.

В результате сертификат пользователя будет сохранен в файле с расширением `*.cer`, `*.pem` в выбранной папке.

Просмотр установленных сертификатов

Вы можете просмотреть сертификаты пользователей, установленные в программе ViPNet PKI Client, чтобы получить подробную информацию о назначении сертификата, его издателе, составе полей, причине недействительности и так далее.

Примечание. Просмотр подробной информации о сертификатах издателя в программе ViPNet PKI Client не предусмотрен.

Для просмотра информации об установленном сертификате:

1 Перейдите в настройки ViPNet PKI Client (на стр. 33) и выберите раздел **Сертификаты**.

2 На панели инструментов нажмите и выберите группу сертификатов:

- **Личные сертификаты** (выбрана по умолчанию).
- **Сертификаты других пользователей**.
- **Сертификаты на внешних устройствах**.
- **Все сертификаты**.

3 По умолчанию за 60 дней ViPNet PKI Client предупредит об истечении срока действия сертификатов. Вы можете изменить этот срок. Для этого на панели инструментов щелкните .

Примечание. Количество столбцов списка можно изменять, для этого нажмите и в открывшемся меню установите соответствующие флажки.

При необходимости вы можете отсортировать сертификаты по любому столбцу. Для этого щелкните по названию столбца.

Также при необходимости вы можете отфильтровать список сертификатов, для этого в поле поиска введите часть имени владельца или издателя сертификата.

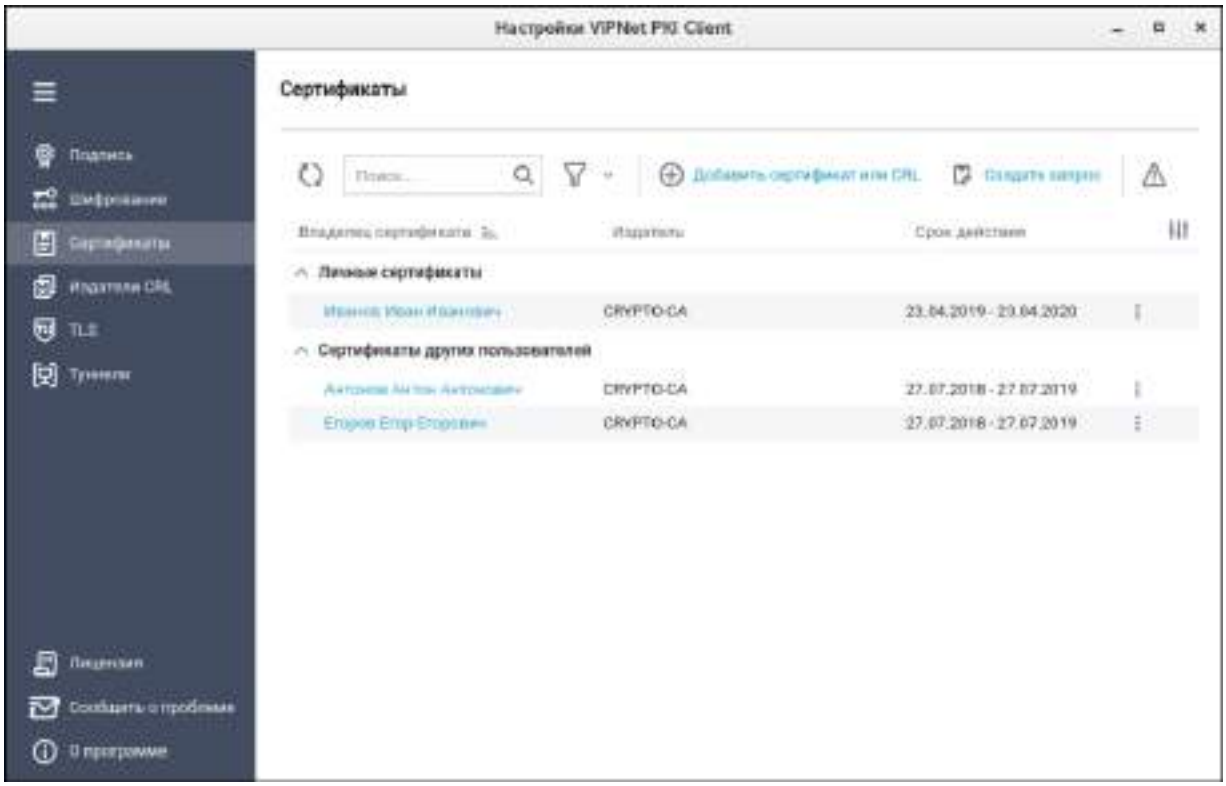

Рисунок 16. Просмотр установленных сертификатов

4 Щелкните имя владельца сертификата, в появившемся окне будут представлены подробные сведения о сертификате.

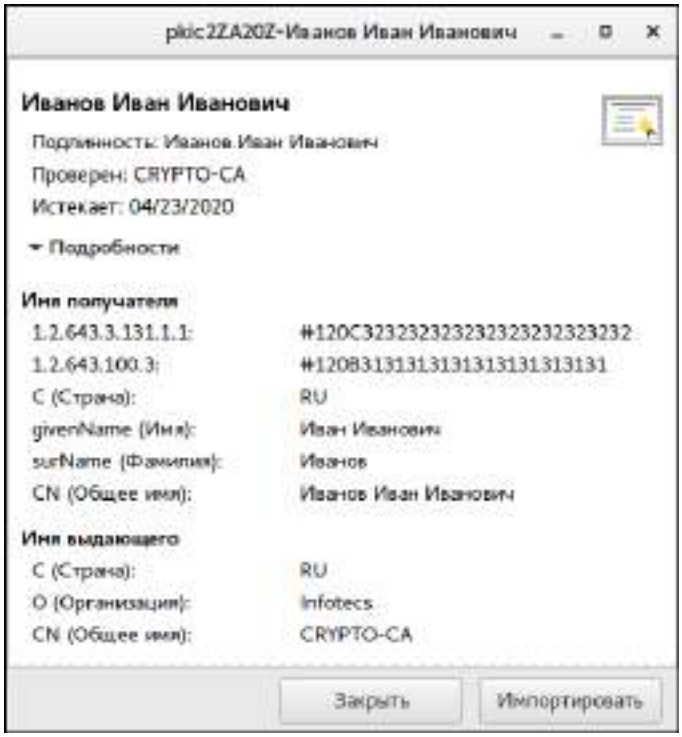

Рисунок 17. Просмотр сведений о сертификате

Удаление сертификатов

Удаляйте сертификаты, если у них истек срок действия или они были аннулированы. Для этого:

1. Перейдите в настройки ViPNet PKI Client (на стр. 33) и выберите раздел **Сертификаты**.
2. На панели инструментов нажмите и в списке выберите группу сертификатов.
3. Нажмите в строке сертификата и в меню выберите **Удалить**.
4. Установите флажок **Подтверждаю удаление <имя владельца сертификата>**.
5. Чтобы удалить ключ ЭП, соответствующий сертификату, например при аннулировании сертификата, установите соответствующий флажок и нажмите **Удалить сертификат**.

Примечание. Пункт **Удалить ключ электронной подписи, соответствующий сертификату** не отображается, если сертификат не содержит информации о расположении ключа электронной подписи (например, при удалении сертификата получателя).

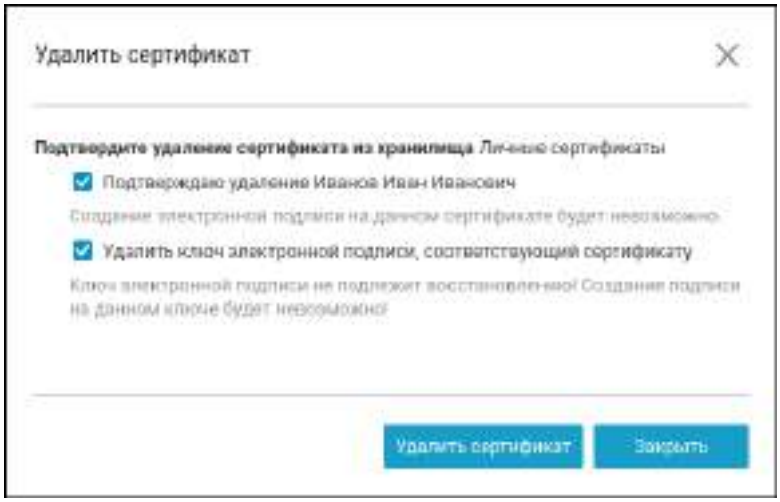

Рисунок 18. Подтверждение удаления сертификата

Внимание! Ключ ЭП не подлежит восстановлению. Создание электронной подписи на данном ключе будет невозможно.

Перенос сертификатов и ключей ЭП между компьютерами

Если вы хотите перенести сертификаты и ключи ЭП с компьютера, на котором установлен ViPNet PKI Client, на другой компьютер с ViPNet PKI Client:

1 На компьютере с ViPNet PKI Client экспортируйте сертификат и ключ ЭП в файл.

2 На другом компьютере с ViPNet PKI Client импортируйте сертификат и ключ ЭП из файла.

Экспорт сертификата и ключа ЭП в файл

1 Перейдите в настройки ViPNet PKI Client (на стр. 33). и выберите раздел **Сертификаты**.

2 Нажмите и выберите **Личные сертификаты**.

3 Нажмите напротив сертификата и в меню выберите **Экспорт в PFX-файл**.

Примечание. Вы можете экспортировать сертификат вместе ключом ЭП, только если при создании запроса на этот сертификат ключ ЭП был помечен как экспортируемый. При создании запроса на сертификат в ViPNet PKI Client ключ ЭП всегда помечается как экспортируемый.

4 Укажите путь и имя файла с экспортируемым сертификатом и ключом ЭП.

5 Задайте и подтвердите пароль PFX-файла.

6 Введите пароль контейнера ключей.

7 В окне сообщения об успешном экспорте нажмите **OK**.

В результате сертификат и ключ ЭП будут сохранены в файл с расширением `*.pfx`, который вы можете перенести на другой компьютер.

Внимание! Несмотря на то что файл формата PFX защищен паролем, по требованиям безопасности он должен передаваться на другой компьютер только доверенным способом.

Импорт сертификата и ключа ЭП из файла

1 Перейдите в настройки ViPNet PKI Client (на стр. 33). и выберите раздел **Сертификаты**.

2 Нажмите **Добавить сертификат или CRL** и укажите путь к файлу с расширением `*.pfx`, полученному в результате экспорта или перетащите его в окно настроек.

3 Введите пароль PFX-файла.

4 В окне **ViPNet CSP — инициализация контейнера ключей**:

4.1 Укажите имя контейнера ключей (см. глоссарий, стр. 109) и его месторасположение.

4.2 Задайте и подтвердите пароль для работы с контейнером ключей.

5 В окне **Добавление сертификатов и CRL** нажмите **Добавить**.

Рисунок 19. Импорт сертификата и ключа ЭП

В результате сертификат и ключ ЭП будут установлены в контейнер ключей, а также сертификат будет установлен в хранилище сертификатов.

Предупреждающие сообщения

Предупреждающие сообщения предназначены для информирования пользователя о невозможности использования установленных сертификатов для выполнения криптографических операций (заверения электронной подписью, шифрования, расшифрования).

Во время установки сертификатов ViPNet PKI Client выполняет проверку сертификатов на соответствие следующим требованиям:

- Срок действия сертификата не истек.
- Сертификат не находится в списке аннулированных сертификатов доверенного удостоверяющего центра.
- Цепочка сертификации (см. глоссарий, стр. 110) полна, и все входящие в нее сертификаты удостоверяющих центров действительны.

Вы можете выполнить проверку установленных сертификатов вручную. Для этого:

1 Перейдите в настройки ViPNet PKI Client (на стр. 33) и выберите раздел  **Сертификаты**.

2 На панели инструментов нажмите  .

В случае если устанавливаемый сертификат не соответствует указанным требованиям, в строке имя владельца сертификата появится предупреждающее сообщение (см. рисунок на стр. 51):

- **Ошибка построения цепочки сертификатов**

  Установите в хранилище все сертификаты, образующие цепочку сертификации (на стр. 50).

- **Сертификат отозван**

  Получите новый сертификат (см. Получение нового сертификата на стр. 48) и установите его в хранилище (см. Установка сертификатов и CRL на стр. 50).

- **Подпись неверна**

  Сертификат или один из сертификатов, образующих цепочку сертификации, искажен. Переустановите все сертификаты, образующие цепочку сертификации.

- **Срок действия ключа электронной подписи истек**

  - Если вы устанавливаете личный сертификат, получите новый сертификат (см. Получение нового сертификата на стр. 48) и установите его в хранилище (см. Установка сертификатов и CRL на стр. 50).
  - Если вы устанавливаете сертификат получателя, запросите у получателя новый сертификат.

- **Статус отзыва не определен**

  При появлении данного предупреждающего сообщения установите актуальный CRL в хранилище сертификатов (на стр. 50).

6

Настройка параметров электронной подписи и шифрования файлов

Требования к сертификатам для заверения электронной подписью и шифрования

Для заверения электронной подписью и шифрования файлов сертификаты должны удовлетворять следующим требованиям:

- Сертификат должен быть действителен:
  - Срок действия сертификата не истек.
  - Срок действия ключа ЭП не истек.
  - Сертификат не аннулирован.
  - Вся цепочка сертификации (см. глоссарий, стр. 110) полна, и все входящие в нее сертификаты удостоверяющих центров действительны.
- Для шифрования сертификаты получателей должны быть установлены в хранилище сертификатов **Другие пользователи** и иметь в поле **Использование ключа** хотя бы одно из назначений: **Шифрование данных**, **Шифрование ключей**, **Согласование ключей**.
- Для заверения файлов электронной подписью ваш сертификат должен быть установлен в хранилище сертификатов текущего пользователя **Личное** и иметь назначение **Цифровая подпись** в поле **Использование ключа**. В случае если запрос на сертификат был создан не с помощью ViPNet PKI Client, должна быть установлена связь между сертификатом и контейнером с ключом ЭП (см. документ «ViPNet CSP Linux 4.2. Руководство пользователя», раздел «Установка сертификата в системное хранилище»).

Внимание! В случае если ваш сертификат или сертификат получателя не соответствует указанным требованиям, вы не сможете выбрать его для заверения электронной подписью или шифрования.

Настройка параметров электронной подписи

Настройте параметры электронной подписи, которые будут использоваться по умолчанию в программах File Unit и Web Unit. Для этого:

1 Перейдите в настройки ViPNet PKI Client (на стр. 33).

2 В разделе **Подпись** нажмите **Выберите сертификат**.

3 Выберите сертификат и нажмите **Выбрать**.

Отобразится информация о выбранном сертификате. Для просмотра подробной информации об используемом сертификате щелкните имя владельца сертификата.

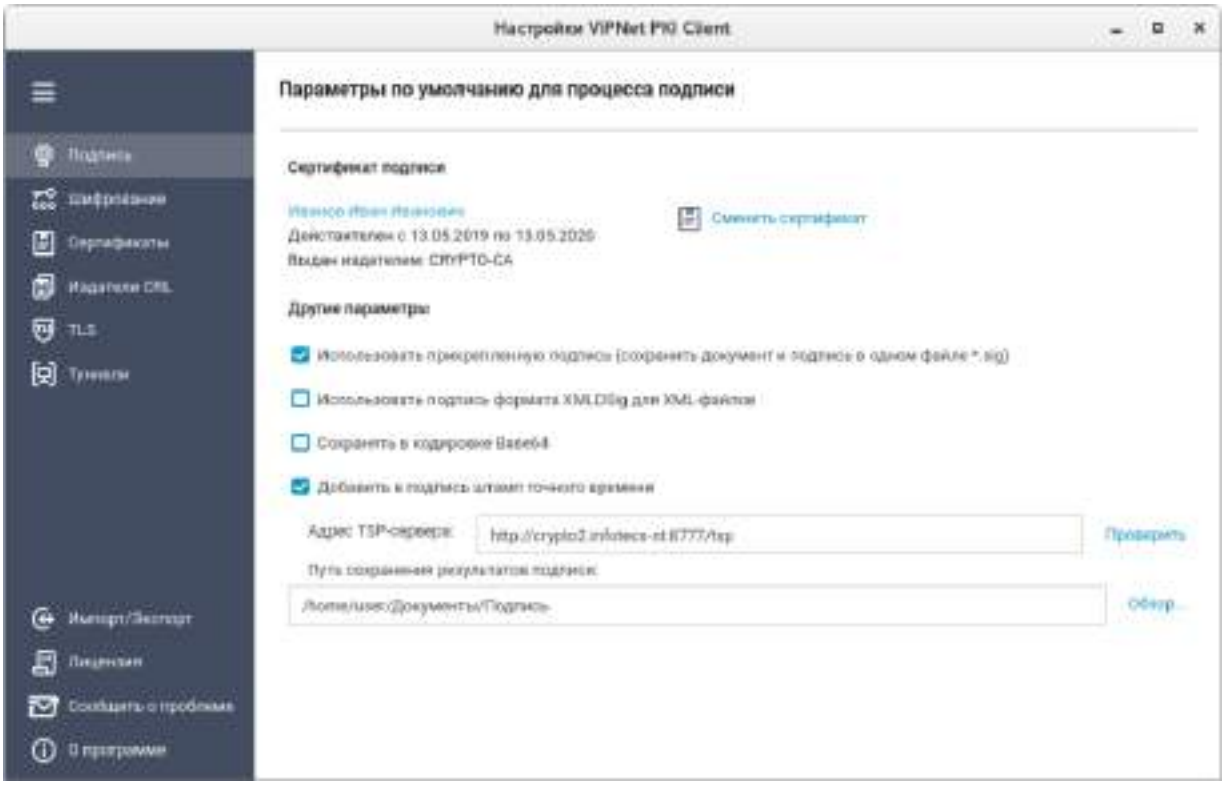

Рисунок 20. Настройка параметров электронной подписи

4 Чтобы сохранять подпись отдельно от подписываемого файла, снимите флажок **Использовать прикрепленную подпись (сохранить документ и подпись в одном файле *.sig)**. По умолчанию подпись прикрепляется к подписываемому файлу.

5 Чтобы использовать подпись формата XMLDSig для XML-файлов, установите соответствующий флажок и выберите шаблон. По умолчанию в настройки добавлен шаблон с параметрами:

- Подписывается весь XML-документ, подпись помещается в корневой тег.
- Алгоритм каноникализации — `http://www.w3.org/TR/2001/REC-xml-c14n-20010315`.

- Алгоритм трансформации — `http://www.w3.org/2000/09/xmldsig#enveloped-signature`.

Если этот шаблон не подходит, создайте свой и импортируйте его в настройки.

6 Чтобы сохранять файл подписи в кодировке Base64, установите соответствующий флажок.

7 Чтобы добавлять к электронной подписи подтверждение точного времени заверения файла, настройте подключение к службе штампов времени. Для этого:

7.1 Установите флажок **Добавить в подпись штамп точного времени**.

7.2 В поле **Адрес TSP-сервера** укажите URL-адрес TSP-сервера в формате `http://<IP-адрес или доменное имя>:<порт>/`. Для проверки соединения с указанным TSP-сервером нажмите **Проверить**. Поддерживается только протокол HTTP.

8 Чтобы все подписанные файлы по умолчанию сохранялись в определенной папке, в соответствующем поле с помощью кнопки **Обзор** укажите путь к нужной папке. Если папка по умолчанию не будет указана, то подписанные файлы будут сохраняться в папку `/home/<имя пользователя>`.

9 Нажмите кнопку **Сохранить**.

Настройка параметров шифрования

Настройте параметры шифрования, которые будут использоваться по умолчанию в программах File Unit и Web Unit. Для этого:

1 Обменяйтесь сертификатами с пользователями, которым вы хотите передавать зашифрованные файлы, например, с помощью электронной почты или съемных носителей.

2 Установите полученные сертификаты в хранилище (см. Установка сертификатов и CRL на стр. 50).

3 Перейдите в настройки ViPNet PKI Client (на стр. 33) и выберите раздел **Шифрование**.

4 Чтобы каждый раз при шифровании файлов не приходилось выбирать сертификат получателя, сформируйте список получателей файлов. Для этого:

4.1 В группе **Получатели зашифрованных файлов** нажмите **Добавить**.

4.2 Выберите сертификат и нажмите **Выбрать**.

4.3 Аналогичным образом добавьте сертификаты других получателей.

Чтобы удалить сертификат получателя из списка, щелкните значок .

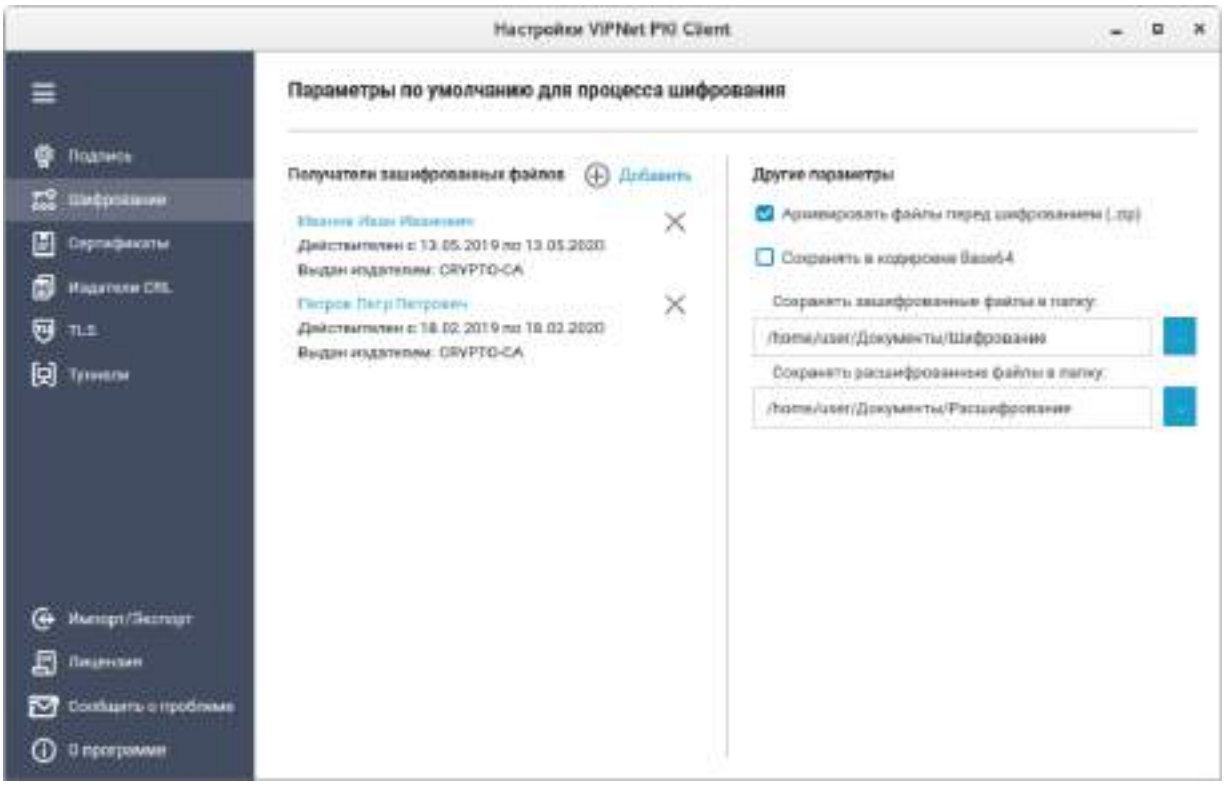

Рисунок 21. Настройка параметров шифрования

5 Чтобы перед шифрованием файлы помещались в архив, установите соответствующий флажок.

6 Чтобы сохранять зашифрованные файлы в кодировке Base64, установите соответствующий флажок.

7 С помощью кнопок  укажите папки для сохранения зашифрованных и расшифрованных файлов.

8 Нажмите кнопку **Сохранить**.

В результате будут настроены параметры шифрования файлов.

7

Настройка обновления CRL

Настройка автоматической загрузки CRL

Примечание. Вы можете настроить автоматическую загрузку CRL из точек распространения только для сертификатов издателей, установленных в хранилище локального компьютера.

Чтобы настроить автоматическое обновление CRL:

1 Перейдите в настройки ViPNet PKI Client (на стр. 33) и выберите раздел **Издатели CRL**.

2 В левой части панели просмотра нажмите **Добавить.**

3 Выберите сертификат издателя и нажмите **Выбрать**.

4 В правой части панели просмотра нажмите **Добавить**.

5 Задайте URL-адрес точки распространения, период обновления и нажмите .

Примечание. Информация об URL-адресах точек распространения CRL содержится в изданных сертификатах в поле **Точки распространения списков отзыва (CRL)**.

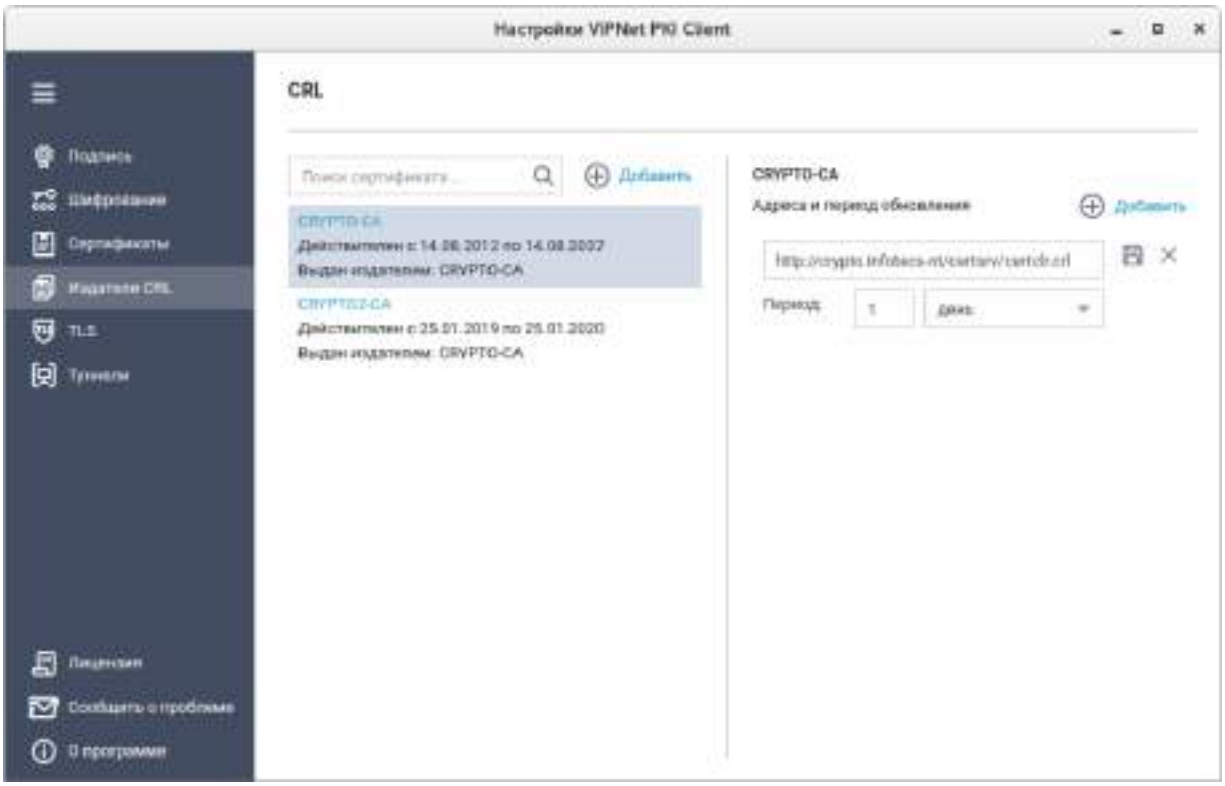

Рисунок 22. Задание точки распространения

Примечание. Если у вас несколько сертификатов издателей, образующих цепочку сертификации, добавьте точки распространения CRL для каждого из них.

6 Нажмите кнопку **Сохранить**.

7 Чтобы отредактировать или удалить точку распространения CRL, нажмите  или  соответственно (появляются при наведении курсора на адрес точки распространения CRL).

В результате по указанным ссылкам будут загружаться обновленные CRL и автоматически устанавливаться в хранилище сертификатов **Промежуточные центры сертификации** > **Список отзыва сертификатов**.

Настройка параметров подключения к прокси-серверам

Если в вашей организации доступ в Интернет осуществляется через один или несколько прокси-серверов, задайте параметры подключения к прокси-серверам. Для этого выполните следующие действия:

1 Перейдите в каталог `/opt/itcs/share/pki-client/pki-client-crl-unit` и откройте в текстовом редакторе файл конфигурации `crlunit.cfg`.

2 Внесите следующие изменения:

- Замените секцию `<proxy-info>` на `<proxy-settings>`. Если секция `<proxy-info>` отсутствует в файле конфигурации, то добавьте секцию `<proxy-settings>`.
- Раскомментируйте строку `<!--proxy addr="msk-tmg-04.Sample-nt:3128" protocol="http" authtype="negotiate" /-->` и укажите параметры прокси-сервера для HTTP-соединений, где:
  - атрибут `proxy addr` — IP-адрес или DNS-имя прокси-сервера и номер порта для подключения к нему;
  - атрибут `protocol` — тип протокола, с помощью которого компьютер с ViPNet PKI Client соединяется с прокси-сервером (HTTP, FTP);
  - атрибут `authtype` — метод аутентификации на сервере (any, ntlm, negotiate).

  Если ваш прокси-сервер использует авторизацию по логину и паролю, задайте эти значения в атрибуте `proxy addr`:

  ```
  </proxy addr="http://<имя пользователя>:<пароль>@<адрес прокси-сервера>:<номер порта>" authtype="any"/>
  ```
- Раскомментируйте строку `<!--proxy addr="msk-tmg-04.Sample-nt:3128" protocol="ftp" authtype="negotiate" /-->` и укажите параметры прокси-сервера для FTP-соединений, где:
  - атрибут `proxy addr` — IP-адрес или DNS-имя прокси-сервера и порт для подключения к нему;
  - атрибут `protocol` — тип протокола, с помощью которого клиент соединяется с прокси-сервером (HTTP, FTP);
  - атрибут `authtype` — метод аутентификации на сервере (`any`, `ntlm`, `negotiate`).

3 Сохраните изменения, внесенные в файл конфигурации, и перезапустите программу CRL Unit (на стр. 33).

Примеры файла конфигурации

Пример 1. Настройка 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 2. Настройка 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 автоматической загрузке CRL

В большинстве дистрибутивов Linux по умолчанию события регистрируются в файле журнала, расположение которого задается в конфигурации установленной системы логирования (в большинстве случаев `/var/log/messages` или `/var/log/syslog`). Файл журнала обычно доступен пользователям с правами суперпользователя.

Для удобства просмотра журнала событий мы рекомендуем использовать одну из следующих команд:

- Если вы используете Astra Linux, Ubuntu или Debian, выполните команду:

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

- Если вы используете Альт Линукс, выполните команду:

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

8

Настройка подключения к сайтам, использующим TLS ГОСТ

Порядок действий при настройке подключения к сайтам, использующим TLS ГОСТ

Таблица 4. Порядок действий

	Действие
☐	Если вы хотите подключаться к веб-ресурсам, которые требуют аутентификации пользователя, убедитесь, что ваш сертификат соответствует требованиям к сертификатам для работы TLS Unit (на стр. 73)
☐	Настройте совместную работу TLS Unit и веб-браузера (на стр. 77)
☐	Если в вашей организации доступ в Интернет организован через прокси-сервер, задайте параметры подключения TLS Unit к прокси-серверам (на стр. 75)
☐	Настройте прокси-сервер в веб-браузере (на стр. 79)
☐	Запустите программу TLS Unit (на стр. 33)
☐	Подключитесь к веб-ресурсу (на стр. 83)
☐	При необходимости просмотрите информацию о текущих TLS-соединениях (на стр. 84)

Требования к сертификатам для работы TLS Unit

Сертификат сервера

При подключении пользователя к веб-ресурсу программа TLS Unit проверяет соответствие сертификата сервера следующим условиям:

- срок действия сертификата не истек;
- сертификат не аннулирован;
- все сертификаты из цепочки сертификации (см. глоссарий, стр. 110) действительны и установлены в хранилище;
- подпись сертификата верна;
- адрес веб-ресурса соответствует адресу в сертификате;
- сертификат имеет назначение **Проверка подлинности сервера** в поле **Улучшенный ключ**.

Если не выполняется хотя бы одно из этих условий, соединение с сервером не будет установлено.

Вы можете разрешить установку TLS-соединения при неполном доверии к сертификату сервера. Для этого:

1. Перейдите в настройки ViPNet PKI Client (на стр. 33) и выберите раздел  **TLS**.
2. Установите флажок **Разрешать соединение при неполном доверии к сертификату сервера**.
3. Нажмите кнопку **Сохранить**.

В этом случае соединение может быть установлено, если:

- не удается выяснить, аннулирован сертификат или нет;
- цепочка сертификации неполная или ее невозможно проверить;
- истек срок действия сертификата.

В одном из этих случаев вы увидите оповещение, что сертификат сервера недействителен или не удалось проверить сертификат на аннулирование, но соединение будет установлено.

Сертификат пользователя

Если веб-ресурс, к которому вы пытаетесь подключиться с помощью TLS Unit, требует аутентификации пользователя, проверьте, что для вашего сертификата выполнены условия:

- Сертификат действителен и имеет расширение **Улучшенный ключ** со значением **Проверка подлинности клиента**.
- Сертификат установлен в хранилище сертификатов текущего пользователя **Личное**.

- Сертификат и соответствующий ему ключ ЭП хранятся на программном токене Infotecs Software Token (см. Способы импорта сертификата и ключа ЭП на Infotecs Software Token на стр. 81) или на внешнем устройстве (см. Список поддерживаемых внешних устройств для подключения к сайтам, использующим TLS ГОСТ на стр. 99).
- В хранилище установлены все сертификаты, образующие цепочку сертификации (см. глоссарий, стр. 110).
- Все сертификаты в цепочке сертификации действительны.

Примечание. Для доступа к некоторым веб-ресурсам сертификат пользователя должен быть издан в определенных удостоверяющих центрах. В этом случае:

1. Обратитесь в техническую поддержку или ознакомьтесь со справочным разделом веб-ресурса и получите информацию об удостоверяющих центрах, в которых может быть издан сертификат для подключения к выбранному веб-ресурсу.
2. В сертификате пользователя просмотрите информацию об издателе и сравните ее с информацией об удостоверяющих центрах, полученной на веб-ресурсе. Если издателя сертификата нет в списке удостоверяющих центров веб-ресурса, создайте запрос на сертификат, направьте его в нужный удостоверяющий центр и получите сертификат (см. Получение нового сертификата на стр. 48).

Настройка подключения TLS Unit к прокси-серверам

Если в вашей организации доступ в Интернет осуществляется через один или несколько прокси-серверов, задайте параметры подключения TLS Unit к прокси-серверам. Для этого выполните следующие действия:

1. Перейдите в каталог `/opt/itcs/share/pki-client/pki-client-tls-unit`.
2. Откройте в текстовом редакторе файл конфигурации `tlsunit.cfg`.
3. Внесите изменения в следующие секции:
   - В секции `#Here you can specify parent proxy bypass list` укажите адреса ресурсов, при подключении к которым не используется прокси-сервер. Адреса разделяются с помощью запятой.

     ```
     allow * * <IP-адреса ресурсов, при подключении к которым не используется прокси-сервер>
     ```

   - В секции `#Here you can specify parent HTTPS proxy` раскомментируйте строку `#parent 1000 connect 10.0.4.245 3128` и укажите IP-адрес прокси-сервера для HTTPS-соединений.

     ```
     parent 1000 connect <IP-адрес прокси-сервера для HTTPS-соединений> <номер порта>
     ```

   - В секции `#Here you can specify parent HTTP proxy` раскомментируйте строку `#parent 1000 http 10.0.4.245 3128` и укажите IP-адрес прокси-сервера для HTTP-соединений.

     ```
     parent 1000 http <IP-адрес прокси-сервера для HTTP-соединений> <номер порта>
     ```
4. Сохраните изменения, внесенные в файл конфигурации.
5. Перезапустите программу TLS Unit (на стр. 33).

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

Пример файла конфигурации

```
#!/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
#Here you can specify parent HTTP proxy
allow * * * * HTTP
parent 1000 http 10.0.4.245 3128
proxy -p9998 -T -n -a
```

Настройка совместной работы TLS Unit и веб-браузера

Для совместной работы программы TLS Unit и используемого веб-браузера необходимо импортировать корневой сертификат ViPNet PKI Client Root в настройки веб-браузера.

Импорт сертификата ViPNet PKI Client Root в Mozilla Firefox

Чтобы импортировать корневой сертификат ViPNet PKI Client Root в веб-браузер Mozilla Firefox, выполните следующие действия:

1 В веб-браузере Mozilla Firefox перейдите в меню **Настройки** и выберите раздел **Приватность и Защита**.

2 В группе **Сертификаты** нажмите кнопку **Просмотр сертификатов**.

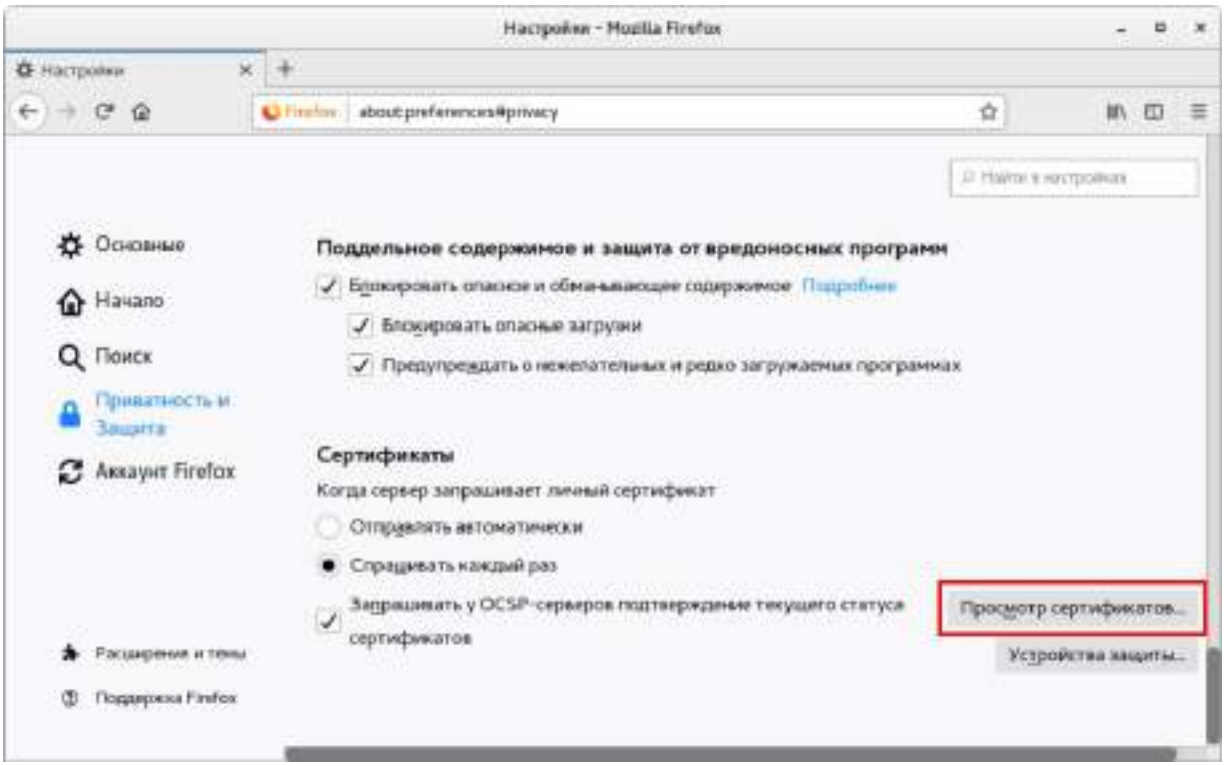

Рисунок 23. Настройки браузера Mozilla Firefox

3 В окне **Управление сертификатами** перейдите на вкладку **Центры сертификации** и нажмите кнопку **Импортировать**.

4 В каталоге `/opt/itcs/share/pki-client/certs` выберите сертификат `root.pem` и нажмите кнопку **Открыть**.

5 В окне **Загрузка сертификата** установите флажок **Доверять при идентификации веб-сайтов** и нажмите кнопку **ОК**.

6 Перезагрузите браузер.

Импорт сертификата ViPNet PKI Client Root в Chromium

Чтобы импортировать корневой сертификат ViPNet PKI Client Root в веб-браузер Chromium, выполните следующие действия:

1 Перейдите в меню **Настройки** веб-браузера Chromium.

2 В разделе **Конфиденциальность и безопасность** выберите пункт **Настроить сертификаты**.

3 Перейдите на вкладку **ЦЕНТРЫ СЕРТИФИКАЦИИ** и нажмите кнопку **ИМПОРТ**.

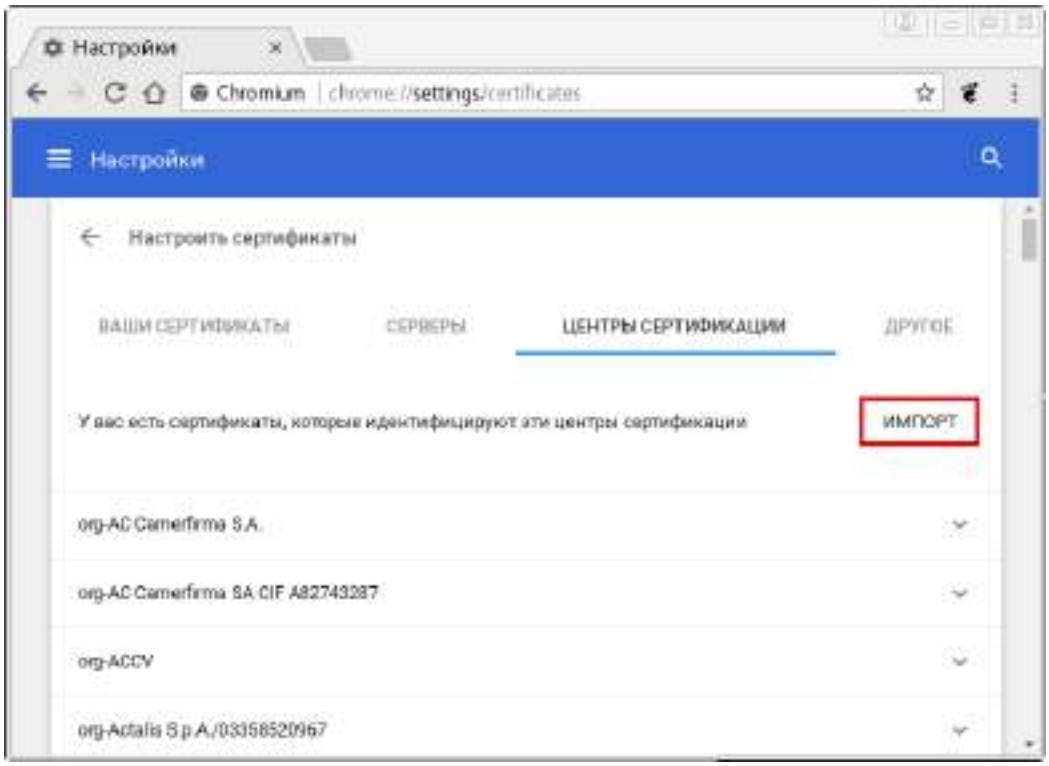

Рисунок 24. Настройки браузера Chromium

4 В каталоге `/opt/itcs/share/pki-client/certs` выберите сертификат `root.pem` и нажмите кнопку **Открыть**.

5 В окне **Центр сертификации** установите флажок **Доверять этому сертификату при идентификации сайтов** и нажмите кнопку **ОК**.

6 Перезагрузите браузер.

Настройка прокси-сервера в веб-браузере

Программа TLS Unit выполняет роль прокси-сервера (см. Подключение к веб-ресурсу с использованием TLS-соединения на стр. 27). Чтобы все соединения с веб-ресурсами проходили через нее, задайте настройки TLS Unit в используемом веб-браузере.

Настройка прокси-сервера в Mozilla Firefox

Чтобы настроить прокси-сервер в браузере Mozilla Firefox:

1 В веб-браузере Mozilla Firefox перейдите в меню **Настройки** и выберите раздел **Основные**.

2 В группе **Параметры сети** нажмите кнопку **Настроить**.

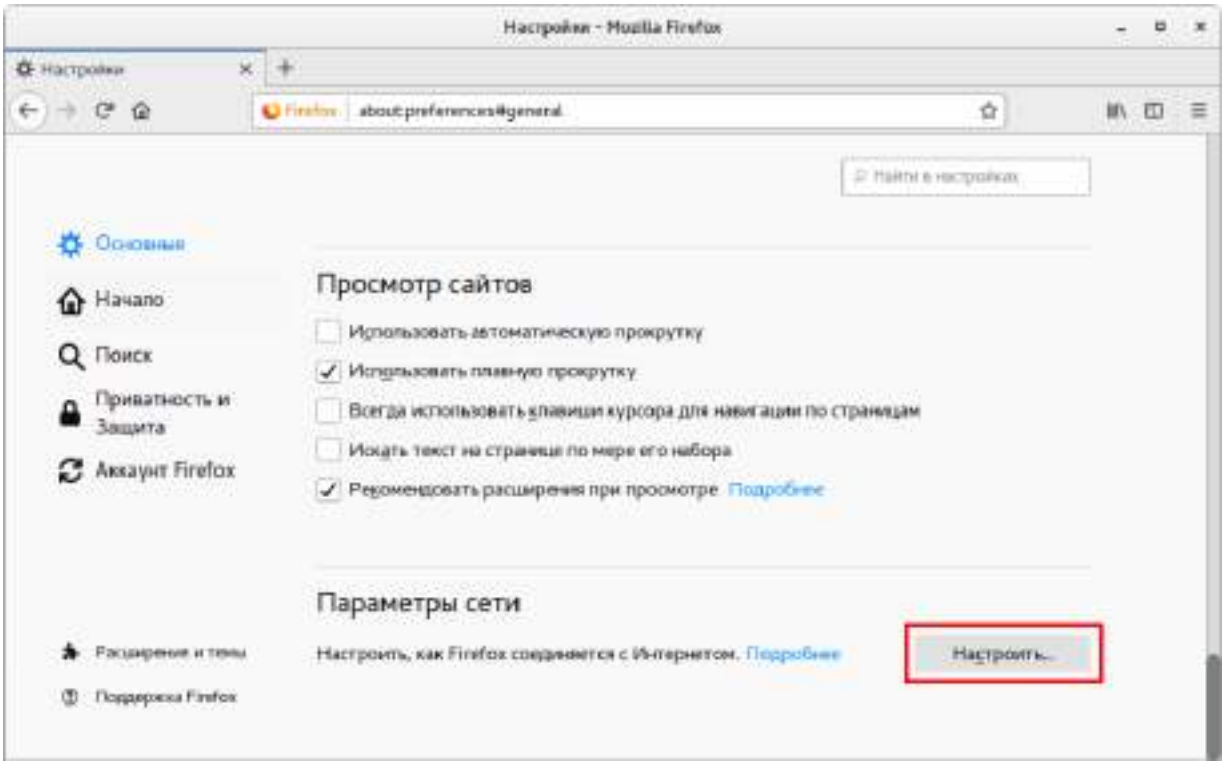

Рисунок 25. Настройки браузера Mozilla Firefox

3 В окне **Параметры соединения** выполните следующие действия:

3.1 Установите переключатель в положение **Ручная настройка сервиса прокси**.

3.2 В поле **HTTP прокси** укажите IP-адрес прокси-сервера — `127.0.0.1`.

3.3 В поле **Порт** укажите номер порта для подключения к прокси-серверу — `9998`.

3.4 Задайте аналогичные параметры в поле **SSL прокси**.

4 В поле **Не использовать прокси для** укажите адреса ресурсов, при подключении к которым не используется прокси-сервер — `localhost, 127.0.0.1`.

5 Нажмите кнопку **OK**.

Настройка прокси-сервера в Chromium

Чтобы настроить прокси-сервер в браузере Chtomium:

1 В браузере Chromium перейдите в меню **Настройки**.

2 В группе **Система** выберите пункт **Настройки прокси-сервера**.

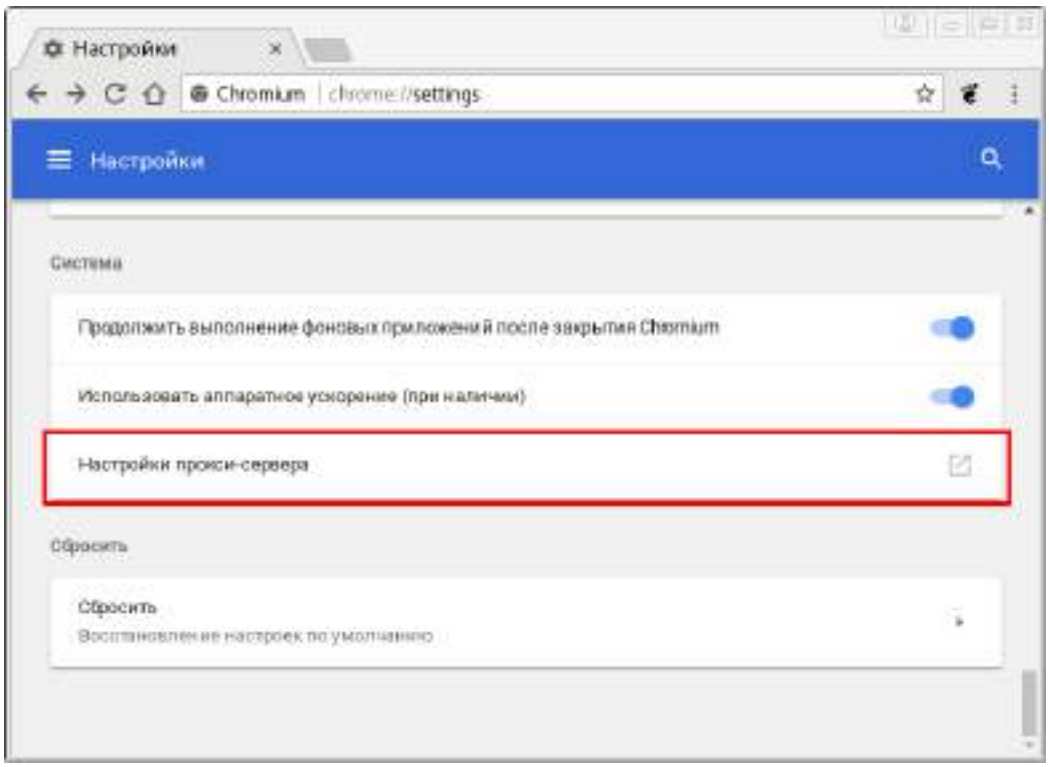

Рисунок 26. Настройки браузера Chromium

3 В окне **Сеть** перейдите в раздел **Сетевая прокси-служба** и в меню **Метод** выберите пункт **Ручной**.

4 В поле **Прокси для HTTP** укажите IP-адрес прокси-сервера — `127.0.0.1` и порт для подключения к прокси-серверу — `9998`.

5 Задайте аналогичные параметры в поле **Прокси для HTTPS**.

6 В поле **Игнорировать узлы** укажите адреса ресурсов, при подключении к которым не используется прокси-сервер — `localhost, 127.0.0.1`.

7 Нажмите кнопку **Закрыть**.

Способы импорта сертификата и ключа ЭП на Infotecs Software Token

Программа TLS Unit поддерживает работу только с теми сертификатами пользователя, ключ ЭП которых хранится на Infotecs Software Token (см. глоссарий, стр. 108) или внешнем устройстве (см. Список поддерживаемых внешних устройств для подключения к сайтам, использующим TLS ГОСТ на стр. 99).

Чтобы импортировать сертификат и ключ ЭП на Infotecs Software Token, выполните одно из действий:

- Если сертификат установлен в системное хранилище (см. Установка сертификатов и CRL на стр. 50) и имеется контейнер ключей, содержащий соответствующий ключ электронной подписи, выполните действия, описанные в разделе Импорт сертификата и ключа ЭП на Infotecs Software Token (на стр. 81).
- Если сертификат и ключ ЭП находятся в файле PFX, выполните действия, описанные в разделе Импорт сертификата и ключа ЭП на Infotecs Software Token из файла PFX (на стр. 82).

Импорт сертификата и ключа ЭП на Infotecs Software Token

Чтобы импортировать сертификат и ключ ЭП на Infotecs Software Token (см. глоссарий, стр. 108):

1. Перейдите в настройки ViPNet PKI Client (на стр. 33) и выберите раздел  **Сертификаты**.
2. Нажмите  и в списке выберите **Личные сертификаты**.
3. Нажмите напротив сертификата и в меню выберите **Скопировать ключ в Infotecs Software Token**.
4. Появится электронная рулетка (см. глоссарий, стр. 110), если она еще не запускалась в рамках текущего сеанса работы программы. Следуйте указаниям в окне **Электронная рулетка**.
5. Введите пароль контейнера ключей.
6. В окне сообщения об успешном импорте нажмите **OK**.

В результате сертификат и ключ ЭП будут импортированы на Infotecs Software Token.

Импорт сертификата и ключа ЭП на Infotecs Software Token из файла PFX

Чтобы импортировать сертификат и ключ ЭП из файла PFX:

1. Перейдите в настройки ViPNet PKI Client (на стр. 33) и выберите раздел  **TLS**.
2. Нажмите **Импортировать PFX-файл на Infotecs Software Token** и укажите путь к PFX-файлу.
3. Введите пароль PFX-файла.
4. В окне сообщения об успешном импорте нажмите **OK**.

В результате сертификат и ключ ЭП будут импортированы на Infotecs Software Token (см. глоссарий, стр. 108).

Подключение к веб-ресурсу с помощью TLS Unit

Чтобы подключиться к сайту, использующему TLS ГОСТ, в браузере введите адрес сайта:

- Если для подключения не требуется аутентификация пользователя, соединение будет установлено.
- Если для подключения требуется аутентификация пользователя, в открывшемся окне выберите сертификат. Соединение будет установлено.

  При дальнейших подключениях к этому сайту во время текущей сессии выбирать сертификат не нужно — программа TLS Unit запоминает сертификаты, которые были выбраны при первом подключении. Если вы завершите работу программы, то кэш сертификатов будет очищен.

Примечание. Чтобы выбрать другой сертификат для подключения, очистите кэш сертификатов. Для этого в области уведомлений щелкните правой кнопкой мыши значок ViPNet PKI Client TLS Unit и в контекстном меню выберите **Очистить кэш сертификатов**.

Просмотр информации о текущих TLS-соединениях

Чтобы просмотреть информацию о текущих TLS-соединениях, сертификатах сервера и пользователя:

1. В области уведомлений щелкните значок TLS Unit правой кнопкой мыши и в контекстном меню выберите **Последние соединения**.

   В открывшемся окне будут отображены соединения, установленные в течение последних десяти минут.

2. Щелкните значок ✉, расположенный слева от информации о соединении. Будут отображены более подробные сведения о соединении:
   - версия протокола TLS, используемая для установки соединения;
   - алгоритм, по которому выполняется согласование ключей;
   - алгоритм, по которому проводится шифрование передаваемых данных и контроль их целостности.

Рисунок 27. Просмотр сведений о TLS-соединениях

9

Настройка подключения к туннелируемым ресурсам

Требования к сертификатам для работы Tunnel Unit

Сертификат сервера

При подключении к туннелируемому ресурсу программа Tunnel Unit проверяет соответствие транспортного сертификата ViPNet TLS Gateway следующим условиям:

- срок действия сертификата не истек;
- сертификат не аннулирован;
- электронная подпись сертификата верна;
- адрес ViPNet TLS Gateway соответствует адресу в сертификате;
- сертификат имеет назначение **Проверка подлинности сервера** в поле **Улучшенный ключ**.

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

Сертификат пользователя

Для подключения к туннелируемым ресурсам с аутентификацией пользователя, проверьте, что для вашего сертификата выполнены условия:

- Сертификат установлен в хранилище сертификатов текущего пользователя **Личное**.
- Установлены все сертификаты УЦ, образующие цепочку сертификации (см. глоссарий, стр. 110).
- Все сертификаты в цепочке сертификации действительны.
- В хранилище сертификатов установлены актуальные CRL (см. глоссарий, стр. 109).
- Сертификат пользователя действителен (см. глоссарий, стр. 108) и имеет расширение **Улучшенный ключ** со значением **Проверка подлинности клиента**.
- Сертификат и ключ ЭП хранятся на программном токене Infotecs Software Token (см. Импорт сертификата и ключа ЭП на Infotecs Software Token из файла PFX на стр. 82).
- Сертификат добавлен на ViPNet TLS Gateway в список **Сертификаты пользователей** > **Разрешенные** и разрешен доступ к туннелируемому ресурсу. Подробнее см. документ «ViPNet TLS Gateway. Руководство администратора».

Добавление туннелируемого ресурса

Чтобы добавить туннелируемый ресурс:

1 Перейдите в настройки ViPNet PKI Client (на стр. 33), выберите раздел **Туннели** и нажмите **Добавить туннель**.

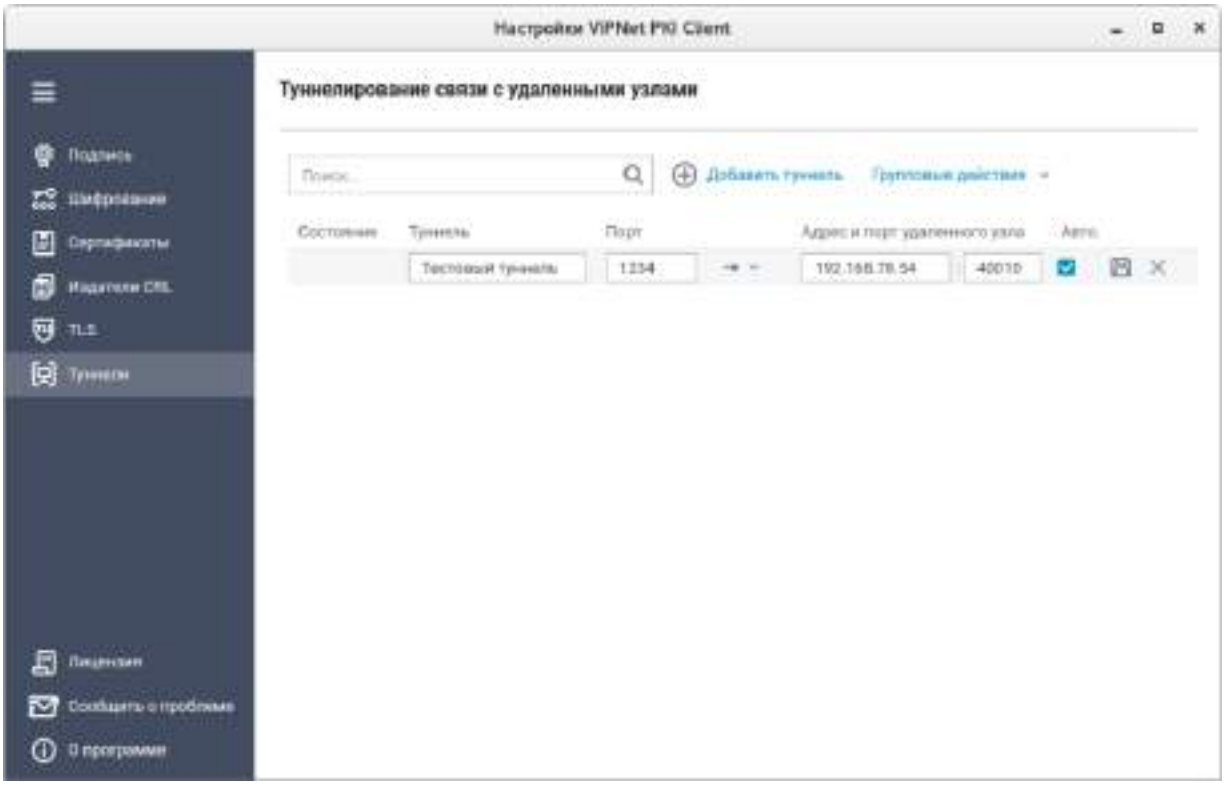

Рисунок 28. Добавление туннелируемого ресурса

2 В соответствующих полях укажите:

- В поле **Туннель** введите произвольное наименование туннелируемого ресурса.
- В поле **Порт** введите номер порта локального сетевого интерфейса для обмена данными с туннелируемым ресурсом, который не занят другим приложением. Этот номер порта необходимо будет указать в настройках приложения для подключения к туннелируемому ресурсу.

Примечание. Доступность портов можно проверить с помощью консольной утилиты `netstat`.

- В поле **Адрес и порт удаленного узла** укажите адрес и порт ViPNet TLS Gateway для подключения к туннелируемому ресурсу. Эти данные необходимо получить у администратора ViPNet TLS Gateway.
- В списке  **Защита соединения сертификатом** выберите тип подключения к туннелируемому ресурсу:
  -  — для подключения к туннелируемому ресурсу без аутентификации пользователя.
  -  — для подключения к туннелируемому ресурсу с аутентификацией пользователя. При выборе данного типа подключения появится окно **Выбор сертификата**, в котором нужно выбрать сертификат для аутентификации на туннелируемом ресурсе.
- Чтобы после запуска программы Tunnel Unit (на стр. 33) автоматически устанавливалась связь с туннелируемым ресурсом, установите флажок в столбце **Авто**.

3 Нажмите  .

4 При необходимости вы можете отредактировать или удалить туннелируемый ресурс, для этого нажмите  или  соответственно (появляется при выборе туннелируемого ресурса).

В результате туннелируемый ресурс будет добавлен в ViPNet PKI Client и вы сможете устанавливать с ним защищенное соединение (см. Подключение к туннелируемому ресурсу на стр. 89).

Подключение к туннелируемому ресурсу

Примечание. Описание приведено на примере подключения к удаленному рабочему столу по протоколу RDP. Подключение к туннелируемым ресурсам с помощью других приложений и по другим протоколам осуществляется аналогично.

Для подключения к туннелируемому ресурсу:

1 Запустите программу Tunnel Unit (на стр. 33).

2 Перейдите в настройки ViPNet PKI Client (на стр. 33) и выберите раздел **Туннели**.

3 В списке выберите нужный ресурс и с помощью переключателя в столбце **Состояние** установите соединение с туннелируемым ресурсом. Если при добавлении туннелируемого ресурса вы установили флажок в столбце **Авто**, связь с этим ресурсом будет установлена автоматически при запуске программы Tunnel Unit.

Примечание. Для работы сразу со всеми туннелируемыми ресурсами вы можете использовать кнопку **Групповые действия**. С ее помощью вы сможете:

- **Включить все туннели** — установить соединение со всеми туннелируемыми ресурсами.
- **Включить автозапускаемые** — установить соединение с туннелируемыми ресурсами, для которых включено автоматическое установление связи при запуске программы Tunnel Unit (установлен флажок в столбце **Авто**), если соединение было прервано вручную.
- **Выключить все туннели** — разорвать соединение со всеми туннелируемыми ресурсами.
- **Удалить все туннели** — удалить все туннелируемые ресурсы.

4 Запустите клиент удаленного рабочего стола, например Remmina.

5 На панели инструментов в списке протоколов выберите **RDP** и в поле рядом введите адрес подключения в формате `127.0.0.1:<Порт>`, где `<Порт>` — номер порта локального сетевого интерфейса, заданный при добавлении туннелируемого ресурса (см. Добавление туннелируемого ресурса на стр. 87).

6 Нажмите кнопку **Подключиться**.

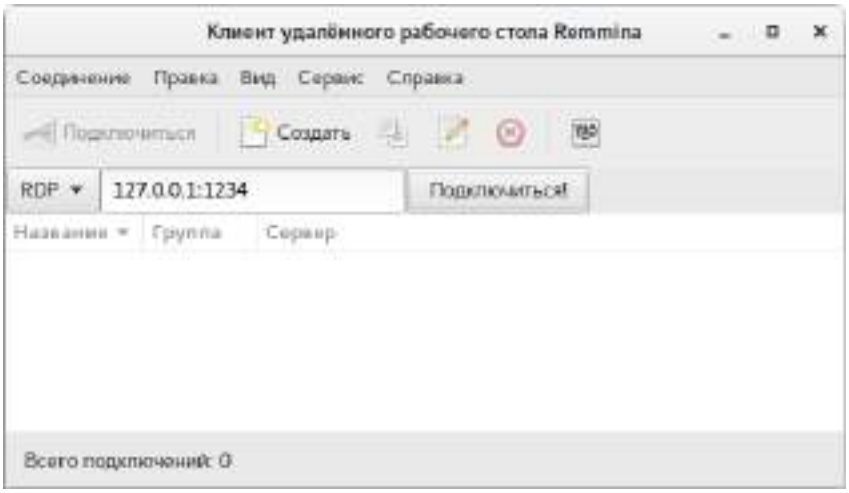

Рисунок 29. Подключение к удаленному рабочему столу

В результате вы подключитесь к туннелируемому ресурсу по защищенному TLS-протоколу.

10

Возможные неполадки и способы их устранения

Обращение в службу технической поддержки

Чтобы передать сведения о неполадках в работе ПО ViPNet PKI Client:

1 Перейдите в настройки ViPNet PKI Client (на стр. 33) и на панели навигации нажмите **Сообщить о проблеме**.

Рисунок 30. Создание архива с данными, необходимыми для анализа проблемы

2 В открывшемся окне выполните одно из действий:

- Если у вас установлен почтовый клиент, щелкните ссылку **hotline@infotecs.ru**. Откроется окно вашего почтового клиента с уже сформированным письмом. Опишите проблему в теле письма, перетащите архив с данными в окно создания письма и отправьте в ОАО «ИнфоТеКС».
- Если у вас не установлен почтовый клиент, сохраните архив и создайте письмо самостоятельно. В качестве получателя добавьте адрес электронной почты `hotline@infotecs.ru`, в теле письма опишите возникшую проблему и прикрепите к письму архив с данными.

Примечание. ViPNet PKI Client не собирает вашу конфиденциальную информацию. ОАО «ИнфоТеКС» ответственно подходит к защите вашей личной информации и принимает все меры для предотвращения несанкционированного доступа или разглашения информации, которую вы нам предоставляете.

Ошибка при установке или запуске на компьютерах с Astra Linux Special Edition («Смоленск») 1.6 с включенным режимом замкнутой программной среды

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

Ошибка может возникать из-за отсутствия пакета `astra-digsig-oldkeys`.

Для устранения проверьте, что это пакет установлен с помощью команды:

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

Если пакет не установлен, установите его с помощью команды:

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

Ошибки при обновлении CRL

Для определения причины сбоя откройте журнал (см. Отслеживание событий при автоматической загрузке CRL на стр. 70), в который записываются события службы и в строке события посмотрите значение `ErrorCode`.

Неправильный URL-адрес (ErrorCode=3)

Перейдите в настройки автоматической загрузки CRL (см. Настройка автоматической загрузки CRL на стр. 66) и проверьте правильность введенного URL-адреса точки распространения CRL.

Ошибка данных (ErrorCode=4)

- Проверьте доступность точки распространения CRL. Для этого загрузите список CRL вручную: скопируйте URL-адрес точки распространения CRL в адресную строку браузера и перейдите по нему. Если после этого на ваш компьютер загрузился файл `*.crl`, значит, точка распространения доступна.
- Если в вашей организации доступ в Интернет осуществляется через прокси-сервер, то в файле конфигурации `crlunit.cfg` укажите настройки прокси-сервера (см. Настройка параметров подключения к прокси-серверам на стр. 68).

Ошибка загрузки (ErrorCode=5)

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

Ошибка хранилища сертификатов (ErrorCode=6)

В большинстве случаев означает, что у используемой учетной записи недостаточно прав для установки CRL.

Сертификат не найден (ErrorCode=7)

Получите сертификат издателя выбранной точки распространения CRL и установить его в хранилище локального компьютера (см. Установка сертификатов и CRL на стр. 50).

CRL просрочен (ErrorCode=8)

Указывает на то, что срок действия CRL, загруженного из указанной точки распространения, истек. Обратитесь к администратору удостоверяющего центра.

Недостаточно памяти (ErrorCode=9)

Указывает на нехватку оперативной памяти.

CRL уже установлен (ErrorCode=11)

Указывает на попытку установить CRL, который уже установлен в хранилище сертификатов.

Ошибка сети (ErrorCode=12)

Указывает на сбой в сети во время загрузки CRL.

Требуемый сертификат не отображается в списке сертификатов для настройки обновления CRL

При настройке автоматической загрузки CRL (на стр. 65) в окне **Выбор сертификата** нужный сертификат издателя может не отображаться.

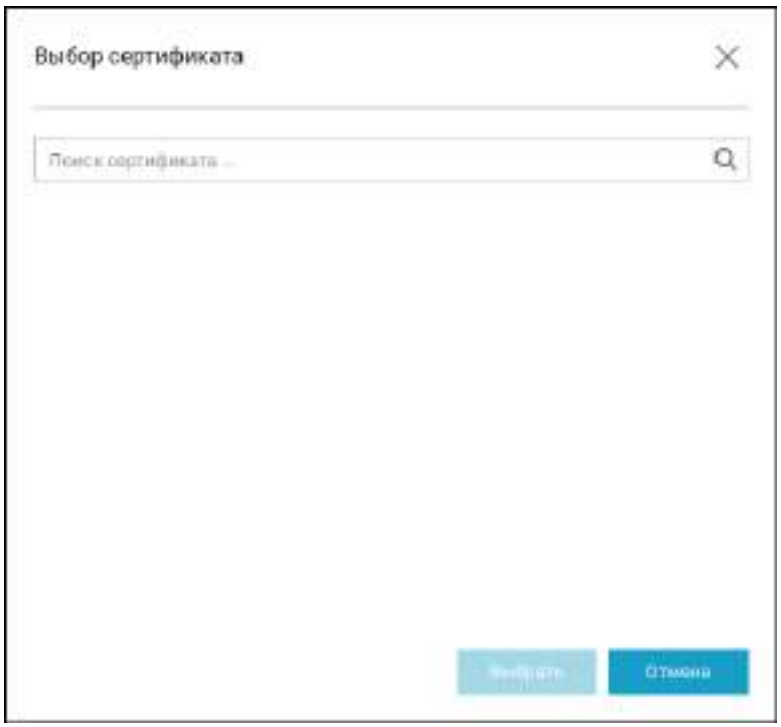

Рисунок 31. Сертификат не отображается в списке сертификатов для подписи

В этом случае убедитесь, что соответствующий сертификат издателя установлен в хранилище локального компьютера (на стр. 50).

A

Внешние устройства

Общие сведения

Внешние устройства предназначены для хранения контейнеров ключей (см. глоссарий, стр. 109), которые вы можете использовать для аутентификации, формирования электронной подписи (см. глоссарий, стр. 110) или для других целей.

На внешнем устройстве могут храниться ключи, созданные по различным алгоритмам в программном обеспечении ViPNet или в сторонних программах. Максимальное количество контейнеров ключей, которое может храниться на одном внешнем устройстве, зависит от объема памяти устройства.

Все операции с контейнерами ключей и внешними устройствами вы можете выполнить в программе ViPNet CSP. Чтобы использовать какое-либо внешнее устройство, на компьютер необходимо установить драйверы этого устройства. Перед записью ключей на устройство убедитесь, что оно отформатировано.

Список поддерживаемых внешних устройств

Перед использованием внешнего устройства убедитесь, что применяемая операционная система соответствует системным требованиям устройства, изложенным в документации к нему.

В таблице перечислены внешние устройства, которые могут быть использованы при работе с ViPNet PKI Client. Для каждого семейства устройств в таблице приведено описание, указаны условия и особенности работы с устройствами.

Таблица 5. Поддерживаемые внешние устройства

Название семейства устройств ViPNet CSP Linux	Полные названия и типы устройств	Необходимые и рекомендуемые условия работы с семейством устройств
ESMART Token	Смарт-карты и токены семейств **ESMART Token**, **ESMART Token ГОСТ**	Необходимо загрузить и установить библиотеки PKCS#11 (загружаются с сайта ESMART).
Infotecs Software Token	**Infotecs Software Token** — программная реализация стандарта PKCS#11	Входит в поставку ViPNet PKI Client. По умолчанию создан программный токен 8888. С помощью утилиты token_manager на компьютере может быть создан другой программный токен.
ViPNet HSM	Программно-аппаратный комплекс **ViPNet HSM** производства ОАО «ИнфоТеКС»	Необходимо задать параметры подключения к серверу ViPNet HSM.
JaCarta	Персональные электронные ключи и смарт-карты **JaCarta PKI, JaCarta SE, JaCarta LT, eToken ГОСТ, JaCarta ГОСТ, JaCarta-2 PKI/ГОСТ**, **JaCarta-2 ГОСТ** производства компании «Аладдин Р.Д.»	На компьютере должно быть установлено ПО «Единый Клиент JaCarta» компании «Аладдин Р.Д.» (рекомендуемая минимальная версия — 2.12). Перенос ключей подписи с устройств **eToken ГОСТ**, **JaCarta ГОСТ**, **JaCarta PKI/ГОСТ** и **JaCarta-2 PKI/ГОСТ** с апплетом ГОСТ, **JaCarta-2 ГОСТ** и на эти устройства невозможен, так как на устройствах используется аппаратная криптография с неизвлекаемым ключом.
Rutoken ECP/ Rutoken Lite	Электронные идентификаторы **Рутокен ЭЦП** и **Рутокен Lite** производства компании «Актив»	Необходимо загрузить и установить библиотеку PKCS#11 (загружается с сайта Rutoken). Перенос ключей подписи на данный тип устройств невозможен.
SafeNet eToken (eToken Aladdin)	Персональные электронные ключи **eToken PRO (Java)**, **eToken PRO**, смарт-карты **eToken PRO (Java)**, **eToken PRO**, **JaCarta PRO** производства компании «Аладдин Р.Д.»	На компьютере должно быть установлено ПО SafeNet Authentication Client для Linux. При необходимости получения ПО следует обратиться в службу поддержки компании Gemalto. Смарт-карта eToken PRO может использоваться с любым стандартным PC/SC совместимым устройством считывания карт.

Примечание. Список поддерживаемых операционных систем для каждого из приведенных устройств вы найдете на официальном веб-сайте производителя этого устройства.

Список поддерживаемых внешних устройств для подключения к сайтам, использующим TLS ГОСТ

Перед использованием внешнего устройства убедитесь, что применяемая операционная система соответствует системным требованиям устройства, изложенным в документации к нему.

В таблице перечислены внешние устройства, которые могут быть использованы в ViPNet PKI Client для подключения к сайтам, использующим TLS ГОСТ. Для каждого семейства устройств в таблице приведено описание, указаны условия и особенности работы с устройствами.

Таблица 6. Поддерживаемые внешние устройства для подключения к сайтам, использующим TLS ГОСТ

Название семейства устройств в программе ViPNet CSP	**Полные названия и типы устройств**	**Необходимые и рекомендуемые условия работы с семейством устройств**
Infotecs Software Token	**Infotecs Software Token** — программная реализация стандарта PKCS#11	Входит в поставку ViPNet PKI Client. По умолчанию создан программный токен 8888. С помощью утилиты token_manager на компьютере может быть создан другой программный токен.
ESMART Token	Смарт-карты и токены **ESMART Token ГОСТ**	Необходимо загрузить и установить библиотеки PKCS#11 (загружаются с сайта ESMART).
JaCarta	Персональные электронные ключи и смарт-карты **JaCarta PKI**, **eToken ГОСТ**, **JaCarta ГОСТ**, **JaCarta PKI/ГОСТ** и **JaCarta-2 PKI/ГОСТ** с апплетом ГОСТ, **JaCarta-2 ГОСТ** производства компании «Аладдин Р.Д.»	На компьютере должно быть установлено ПО «Единый Клиент JaCarta» компании «Аладдин Р.Д.» (рекомендуемая минимальная версия — 2.12). Перенос ключей подписи с устройств **eToken ГОСТ**, **JaCarta ГОСТ**, **JaCarta PKI/ГОСТ** и **JaCarta-2 PKI/ГОСТ** с апплетом ГОСТ, **JaCarta-2 ГОСТ** и на эти устройства невозможен, так как на устройствах используется аппаратная криптография с неизвлекаемым ключом.
Rutoken ECP/ Rutoken Lite	Электронные идентификаторы **Рутокен ЭЦП** и **Рутокен Lite** производства компании «Актив»	Необходимо загрузить и установить библиотеку PKCS#11 (загружается с сайта Rutoken). Перенос ключей подписи на данный тип устройств невозможен.

Алгоритмы и функции, поддерживаемые внешними устройствами

В следующей таблице перечислены криптографические алгоритмы, поддерживаемые внешними устройствами, приведена информация о возможности использования устройств в качестве датчиков случайных чисел, а также информация о поддержке стандарта PKCS#11.

Примечание. Стандарт PKCS#11 (также известный как Cryptoki) — один из стандартов семейства PKCS (Public Key Cryptography Standards — криптографические стандарты ключа проверки электронной подписи), разработанных компанией RSA Laboratories. Стандарт определяет независимый от платформы интерфейс API для работы с криптографическими устройствами идентификации и хранения данных.

Таблица 7. Алгоритмы и функции, поддерживаемые внешними устройствами

Название семейства устройств ViPNet CSP Linux	Аппаратная поддержка российских криптографических алгоритмов (на устройстве)	Программная поддержка российских криптографических алгоритмов (в ViPNet CSP Linux)	Использование ДСЧ в ViPNet CSP Linux	Поддержка PKCS#11
ESMART Token	**ESMART Token** — отсутствует; **ESMART Token ГОСТ** — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 (может не поддерживаться на старых устройствах)	**ESMART Token** — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 **ESMART Token ГОСТ** — отсутствует	Нет	Да
Infotecs Software Token	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 (изолированная программная реализация)	отсутствует	Нет	Да
ViPNet HSM	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	отсутствует	Нет	Да

Название семейства устройств ViPNet CSP Linux	Аппаратная поддержка российских криптографических алгоритмов (на устройстве)	Программная поддержка российских криптографических алгоритмов (в ViPNet CSP Linux)	Использование ДСЧ в ViPNet CSP Linux	Поддержка PKCS#11
JaCarta (устройства JaCarta PKI, JaCarta SE, JaCarta LT, JaCarta PKI/ГОСТ и JaCarta-2 PKI/ГОСТ с апплетом Laser)	отсутствует	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	Нет	Да
JaCarta (устройства eToken ГОСТ, JaCarta ГОСТ, JaCarta PKI/ГОСТ и JaCarta-2 PKI/ГОСТ с апплетом ГОСТ, JaCarta-2 ГОСТ)	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	отсутствует	Да	Да
eToken GOST/ JaCarta GOST	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 (короткий ключ)	отсутствует	Да	Да
Rutoken ECP/ Rutoken Lite	**Рутокен ЭЦП** — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 (короткий ключ); **Рутокен Lite** — отсутствует	**Рутокен ЭЦП** — отсутствует; **Рутокен Lite** — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	**ЭЦП** — да **Lite** — нет	Да
SafeNet eToken (eToken Aladdin)	отсутствует	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	Нет	Да

Примечание. Выработка ключей шифрования (функция `C_DeriveKey` интерфейса PKCS#11) поддерживается не всеми перечисленными устройствами. Для получения более подробной информации см. документацию по необходимому устройству.

B

История версий

В данном приложении описаны основные изменения в предыдущих версиях программы ViPNet PKI Client Linux.

Новые возможности версии 1.4.1

Краткий обзор изменений ViPNet PKI Client версии 1.4.1 по сравнению с 1.4.0.

- Добавлена поддержка устройств Rutoken Lite и Jacarta PKI для подключения к сайтам, использующим TLS ГОСТ (см. Список поддерживаемых внешних устройств для подключения к сайтам, использующим TLS ГОСТ на стр. 99).
- Улучшена внутренняя функциональность и исправлены незначительные ошибки, выявленные в процессе эксплуатации версии 1.4.0.

Новые возможности версии 1.4.0

Краткий обзор изменений ViPNet PKI Client версии 1.4.0 по сравнению с 1.3.1.

- **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 (см. Список поддерживаемых внешних устройств для подключения к сайтам, использующим TLS ГОСТ на стр. 99).

  - 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).

Новые возможности версии 1.3.1

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet PKI Client версии 1.3.1 по сравнению с версией 1.3.0.

- **Добавлена возможность экспорта и импорта настроек**

  Вы можете экспортировать настройки ViPNet PKI Client Linux в файл или импортировать настройки из файла, например для переноса ViPNet PKI Client Linux 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).

Новые возможности версии 1.3

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet PKI Client версии 1.3 по сравнению с версией 1.2.

- **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.

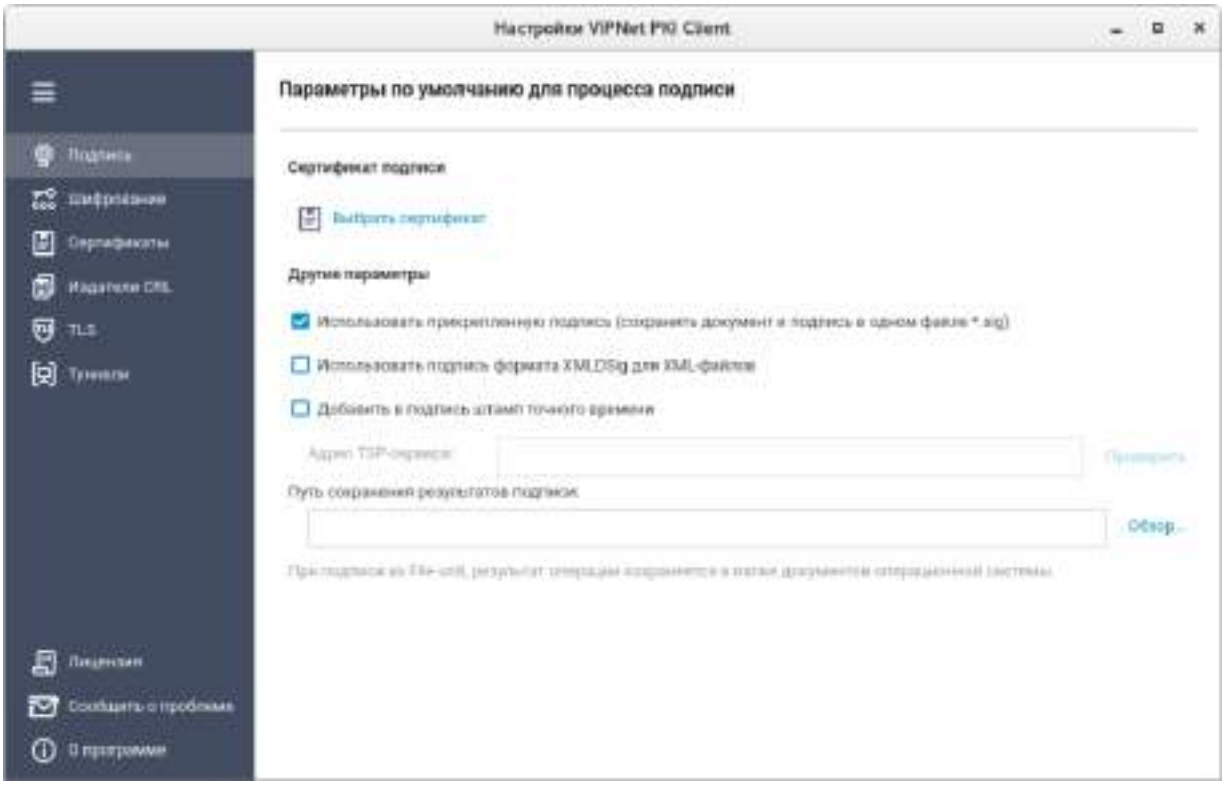

Рисунок 32. Графический интерфейс настроек ViPNet PKI Client

  Также с помощью графического интерфейса вы сможете:

  - Обновить (см. Обновление лицензии на стр. 37) 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 ОАО «ИнфоТеКС» (см. Обращение в службу технической поддержки на стр. 92).
  - 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 (см. глоссарий, стр. 109) в хранилище сертификатов.
  - Экспортировать установленные сертификаты в файлы формата X.509 (`*.cer`, `*.pem`).

- Просматривать установленные сертификаты.

Подробнее см. раздел Операции с сертификатами (на стр. 45).

- **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 Настройка подключения к туннелируемым ресурсам (на стр. 85).

- **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».

Новые возможности версии 1.2

В этом разделе представлен краткий обзор изменений и новых возможностей ПК ViPNet PKI Client 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 (Орел) 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.

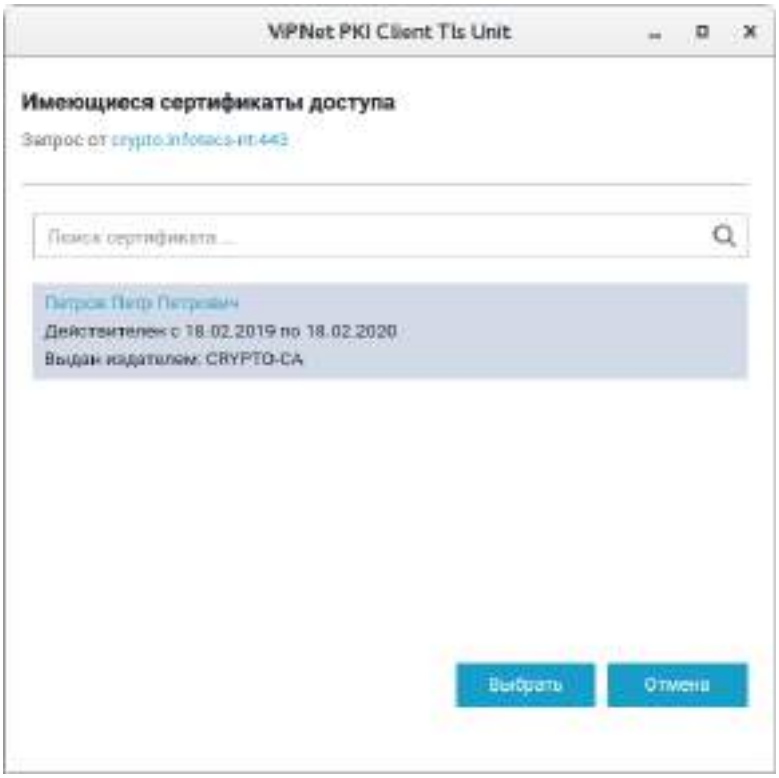

Рисунок 33. Выбор сертификата при подключении к веб-ресурсу

  - Добавлена возможность просмотра информации о TLS-соединениях.

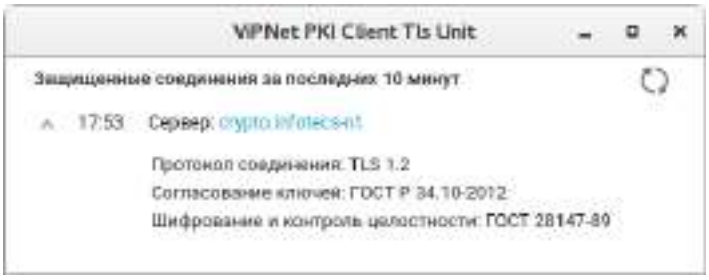

Рисунок 34. Сведения о соединении

- 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.

Глоссарий

Infotecs Software Token

Программное устройство для хранения ключей, реализующее стандарт PKCS#11.

PKI (Public Key Infrastructure)

Инфраструктура открытых ключей — комплекс аппаратных и программных средств, политик и процедур, обеспечивающих распространение доверительного отношения к открытым ключам (в том числе ключам проверки электронной подписи) в распределенных системах через создание сертификатов ключей проверки электронной подписи и поддержание их жизненного цикла.

TLS

Криптографический протокол, обеспечивающий защищенную передачу данных между узлами в Интернете. Использует асимметричную криптографию для обмена ключами, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений.

Действительность сертификата

Сертификат считается действительным, если на текущую дату он не аннулирован, а срок его действия уже начался и еще не истек.

Запрос на сертификат

Защищенное электронной подписью сообщение, содержащее имя пользователя, ключ проверки электронной подписи и его параметры, желаемый срок действия сертификата, предполагаемые назначения сертификата и другие параметры (полный набор параметров зависит от формата запроса и программного обеспечения, в котором он был сформирован).

Ключ проверки электронной подписи

В соответствии с федеральным законом N 63-ФЗ «Об электронной подписи» от 6 апреля 2011 г. ключом проверки электронной подписи называется открытый ключ, который является не секретной частью пары асимметричных ключей и представляет собой уникальную последовательность символов, однозначно связанную с закрытым ключом и предназначенную для проверки подлинности электронной подписи.

Ключ электронной подписи

В соответствии с федеральным законом N 63-ФЗ «Об электронной подписи» от 6 апреля 2011 г. ключом электронной подписи называется закрытый ключ, который является секретной частью пары асимметричных ключей и представляет собой уникальную последовательность символов, предназначенную для создания электронной подписи.

Контейнер ключей

Файл или устройство, в котором хранятся ключ электронной подписи и соответствующий ему сертификат ключа проверки электронной подписи.

Криптопровайдер

Независимый программный модуль, позволяющий выполнять криптографические функции в операционной системе.

Пробный период

Составляет 14 дней, в течение которых рекомендуется активировать лицензию ПК ViPNet PKI Client. Если не выполнить активацию в течение пробного периода, работа с ПК будет невозможна.

Сертификат издателя

Сертификат удостоверяющего центра, которым заверяются издаваемые сертификаты.

Сертификат ключа проверки электронной подписи

Электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Список аннулированных сертификатов (CRL)

Список сертификатов, которые до истечения срока их действия были аннулированы или приостановлены администратором Удостоверяющего центра и потому недействительны на момент, указанный в данном списке аннулированных сертификатов.

Точка распространения данных

Источник, доступный по общеизвестным протоколам (например, HTTP или LDAP), используемый для размещения сформированной в удостоверяющем центре информации (сертификатов издателей и списков аннулированных сертификатов).

Удостоверяющий центр

Организация, осуществляющая выпуск сертификатов ключей проверки электронной подписи, а также сертификатов другого назначения.

Цепочка сертификации

Упорядоченная последовательность сертификатов, соответствующая иерархии издателей этих сертификатов. Сертификат считается действительным, если цепочка сертификации полна (то есть завершается корневым сертификатом) и все входящие в нее сертификаты также действительны.

Электронная подпись

Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Электронная рулетка

Встроенный компонент программного обеспечения ViPNet, позволяющий инициализировать датчик случайных чисел по действиям пользователя. Полученная последовательность используется при формировании криптографических ключей.