ViPNet PKI Client

Общие сведения

infotecs

ФРКЕ.00175-01 90 01

Версия продукта 1.5.1

ОАО «ИнфоТеКС»

127287, г. Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1, 2 этаж

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

Веб-сайт: infotecs.ru

Служба технической поддержки: hotline@infotecs.ru

Содержание

Введение

О документе

Документ описывает назначение и состав программного комплекса ViPNet® PKI Client (далее — ПК ViPNet PKI Client), сценарии использования ПК ViPNet PKI Client для защиты данных и взаимодействия с инфраструктурой открытых ключей (см. глоссарий, стр. 64), а также установку программного комплекса.

Для кого предназначен документ

Документ предназначен для пользователей, которые применяют ПК ViPNet PKI Client для организации взаимодействия с инфраструктурой открытых ключей и защиты данных.

Связанные документы

В таблице ниже перечислены документы, входящие в комплект документации ПК ViPNet PKI Client помимо данного документа.

Таблица 1. Связанные документы

Документ	Содержание
ViPNet PKI Client. Руководство администратора	Назначение ViPNet PKI Client. Общие сведения об инфраструктуре открытых ключей. Сведения о компонентах комплекса. Сценарии использования компонентов комплекса. Инструкция по развертыванию комплекса. Операции с сертификатами. Настройка параметров электронной подписи и шифрования файлов. Настройка автоматической загрузки CRL. Настройка подключения к ПАК ViPNet PKI Service. Настройка подключения к сайтам, использующим TLS ГОСТ. Настройка подключения к туннелируемым ViPNet TLS Gateway ресурсам.

Документ	Содержание
ViPNet PKI Client File Unit. Руководство пользователя	Назначение ViPNet PKI Client File Unit. Настройка программы. Принцип работы. Заверение файлов электронной подписью. Шифрование файлов. Расшифрование файлов. Проверка электронной подписи.
ViPNet PKI Client. Руководство разработчика	Назначение ViPNet PKI Client SDK. Работа с комплектом средств разработки ViPNet PKI Client SDK. Добавление вызова криптографических функций в веб-приложения.
ViPNet CSP. Руководство пользователя	Использование криптографических функций в системах защиты данных. Установка и запуск криптопровайдера ViPNet CSP. Регистрация ViPNet CSP. Получение сертификата и закрытого ключа. Установка контейнеров ключей и сертификатов. Операции с контейнерами ключей.

Соглашения документа

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

Таблица 2. 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 3. 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.

О программе

Комплект поставки

В комплект поставки ПК ViPNet PKI Client входят:

- Программа установки ПК ViPNet PKI Client.
- Документация в формате PDF:
  - «ViPNet PKI Client. Общие сведения».
  - «ViPNet PKI Client. Руководство администратора».
  - «ViPNet PKI Client File Unit. Руководство пользователя».
  - «ViPNet CSP. Руководство пользователя».
  - «ViPNet PKI Client. Руководство разработчика».

Системные требования

Требования к компьютеру для работы 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 1 Гбайт.
- Операционная система:
  - Windows 7 — 32/64-разрядная;
  - Windows Server 2008 R2 — 64-разрядная;
  - Windows Server 2012 — 64-разрядная;
  - Windows 8.1 — 32/64-разрядная;
  - Windows Server 2012 R2 — 64-разрядная;
  - Windows Server 2016 — 64-разрядная;
  - Windows Server 2019 — 64-разрядная;
  - Windows 10 — 32/64-разрядная следующих версий и сборок:
    - версия 1803, сборка 17134;
    - версия 1809, сборка 17763;
    - версия 1903, сборка 18362;

- версия 1909, сборка 18363.

Для операционной системы должны быть установлены последние пакеты обновлений. Работа ViPNet PKI Client на компьютерах, работающих под управлением Windows 10 других версий, не гарантируется.

- Веб-браузер — Internet Explorer 11, Chromium с поддержкой ГОСТ 68.0.3440.84, КриптоПро Fox версии 24 и выше, а также Edge, Google Chrome, Mozilla Firefox, Opera, Яндекс.Браузер, браузер «Спутник» последних версий.
- Программная платформа Microsoft .NET Framework версии 4.5.

Новые возможности версии 1.5.1

Обзор изменений в версии 1.5.1 по сравнению с 1.4.0. Информацию о предыдущих версиях см. в приложении История версий (на стр. 46).

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

  Ранее вы могли использовать подпись формата XMLDSig для XML-файлов, но не могли изменить параметры подписи, заданные по умолчанию. Теперь вы можете создать свой шаблон XML-подписи, добавить его в настройки и использовать при подписании XML-файлов.

- **Упрощено подключение к сайтам, использующим TLS ГОСТ с аутентификацией пользователя**

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

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

  Теперь для подключения могут использоваться устройства Esmart Token, JaCarta SE, Рутокен S.

- **Добавлен английский язык**

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

Обратная связь

Дополнительная информация

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

- Единый многоканальный телефон:

  +7 (495) 737-6192,

  8-800-250-0-260 — бесплатный звонок из России (кроме Москвы).

- Служба технической поддержки: hotline@infotecs.ru.

  Форма для обращения в службу технической поддержки через сайт.

  Консультации по телефону для клиентов с расширенной схемой технической поддержки: +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 ОАО «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. 64) и обеспечить безопасность передачи файлов и данных с помощью шифрования и электронной подписи (см. глоссарий, стр. 67).

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. 66) из точек распространения.
- Подключиться к ПАК ViPNet PKI Service и с помощью сертификатов и ключей ЭП, хранящихся на нем, выполнять криптографические операции из интерфейса ViPNet PKI Client.
- 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. 66).
- 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. 65).
- Открытый ключ, предназначенный для проверки подлинности электронной подписи, называется ключом проверки электронной подписи (см. глоссарий, стр. 65).

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. 64). Основной элемент PKI — удостоверяющий центр (см. глоссарий, стр. 66), 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. 66).

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. 66), 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. 24).
- Обеспечивать безопасность файлов с помощью шифрования и работать с зашифрованными файлами, полученными от других пользователей (см. Отправка зашифрованного файла на стр. 25).

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. 66), 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.

Cloud Unit

Компонент Cloud Unit позволяет подключиться к ПАК ViPNet PKI Service и с помощью сертификатов и ключей ЭП, хранящихся на нем, выполнять криптографические операции из интерфейса ViPNet PKI Client:

- создание запроса на сертификат по шаблонам ViPNet PKI Service с сохранением ключа ЭП на ViPNet PKI Service;
- заверение файлов электронной подписью;
- проверка электронной подписи файлов;
- расшифрование файлов.

ViPNet CSP

ViPNet CSP — обязательный компонент ПК ViPNet PKI Client. ViPNet CSP представляет собой криптопровайдер, к которому обращаются другие компоненты ViPNet PKI Client для выполнения криптографических операций. Также криптопровайдер ViPNet CSP обеспечивает вызов

криптографических функций из приложений сторонних производителей, использующих интерфейс CryptoAPI 2.0 (например, Microsoft Outlook).

Подробнее об использовании криптопровайдера ViPNet CSP см. документ «ViPNet CSP. 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, Cloud Unit).

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

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

Файл лицензии требуется указать при установке ViPNet PKI Client (см. Установка и обновление на стр. 32), иначе ПО не будет установлено на компьютер.

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

- Если ваш компьютер подключен к Интернету, лицензия активируется автоматически во время установки ViPNet PKI Client.
- 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 (см. глоссарий, стр. 65). 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.

   При создании запроса (см. глоссарий, стр. 65) 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. 65) помещается в контейнер ключей (см. глоссарий, стр. 65) на диске или внешнем устройстве, а ключ проверки электронной подписи (см. глоссарий, стр. 65) — 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.

Процедура передачи запроса и получения сертификата приведена на следующей схеме:

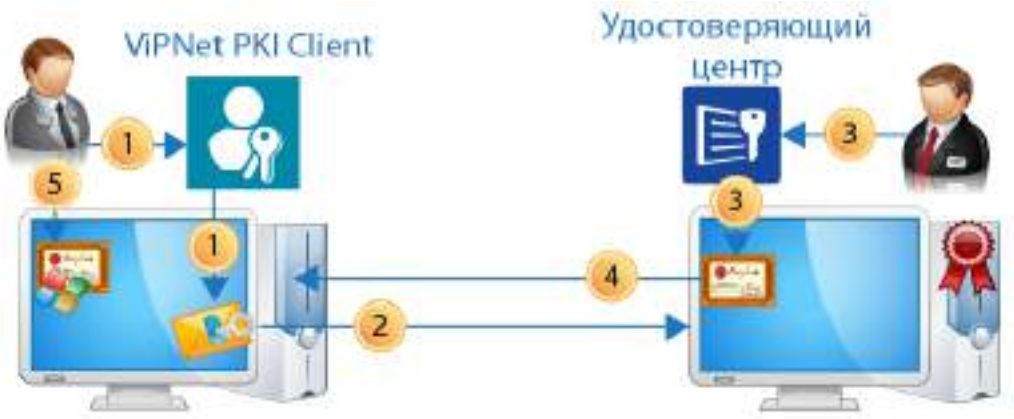

Рисунок 1. Передача пользователем запроса и получение сертификата

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. 32) 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. 64), 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. Программа TLS Unit выполняет функцию локального прокси-сервера, поэтому все соединения с веб-ресурсами проходят через нее.

   Пока программа TLS Unit работает, ее настройки используются в качестве параметров локального прокси-сервера. Если выключить TLS Unit, то для работы прокси-сервера будут использоваться настройки, заданные по умолчанию.

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. 66). 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.

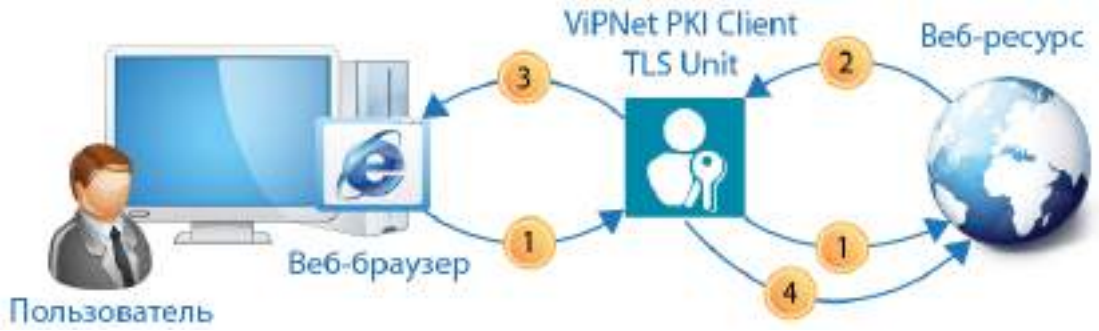

Рисунок 6. Установка TLS-соединения

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.
- Пользователь с помощью соответствующего приложения подключается к туннелируемому ресурсу.

3

Установка, обновление и запуск компонентов

Установка и обновление

Во время установки ПК 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 ПК ViPNet PKI Client.

Внимание! Если локализация Windows не русская, то для правильного отображения кириллицы в интерфейсе ViPNet CSP измените региональные настройки Windows.

Установить или обновить ПК ViPNet PKI Client можно в обычном режиме или с использованием командной строки.

Для установки и обновления потребуется файл лицензии `*.itcslic`. Если на компьютере нет доступа в Интернет, после установки активируйте лицензию (см. Активация лицензии на стр. 35).

Установка и обновление в обычном режиме

Запустите установочный файл и следуйте указаниям мастера.

Установка и обновление с использованием командной строки

Таблица 4. Параметры режима установки

Параметр	Описание
`/install`	Установка в обычном режиме (см. выше).
`/quiet`	Тихий режим, без взаимодействия с пользователем (без демонстрации интерфейса). Параметр действует только в сочетании с параметром `/install`.
`-license=`	Указание файла лицензии. Параметр является обязательным.
`/ignore_os_check`	Параметр, разрешающий установку криптопровайдера ViPNet CSP, входящего в состав ПК ViPNet PKI Client, на компьютер с версией ОС Windows 10, которая не проверялась на совместимость.

Внимание! Без параметра `/ignore_os_check` ПК ViPNet PKI Client невозможно будет установить на компьютер с версией ОС Windows 10, которая не проверялась на совместимость (см. Системные требования на стр. 9). Работа ПК ViPNet PKI Client на этих версиях ОС не гарантируется.

Пример команды:

```
pki_client_installer.exe /install /quiet
-license="C:\Users\tester\Desktop\license_tls.itcslic" /ignore_os_check
```

Примечание. Если на компьютере необходимо создать замкнутую программную среду для соответствия требованиям ФСБ России к средствам криптографической защиты информации класса КС3, дополнительно установите программу ViPNet SysLocker. Подробнее о работе с ViPNet SysLocker см. документ «ViPNet SysLocker. Руководство пользователя».

Особенности обновления

- При обновлении с версии 1.0 на текущую версию сначала удалите старую версию, а затем установите новую.
- Начиная с версии 1.4, изменился формат Infotecs Software Token. После обновления сертификаты и ключи ЭП для установления TLS-соединений, хранящиеся на Infotecs Software Token, будут недоступны. Чтобы продолжить их использовать в новой версии, перенесите их на новый Infotecs Software Token. Для этого перейдите в настройки ViPNet PKI Client (на стр. 34), в разделе  **TLS** нажмите соответствующую кнопку и следуйте указаниям мастера.

Примечание. Кнопка **Перенести данные Infotecs Software Token** не отображается, если вы не использовали Infotecs Software Token для TLS-соединений.

Запуск и завершение работы компонентов

Для запуска нужного компонента ViPNet PKI Client в меню **Пуск** выберите **ViPNet** и название компонента. По умолчанию Web Unit, TLS Unit и Tunnel Unit запускаются автоматически после загрузки Windows.

Чтобы перейти к настройкам ViPNet PKI Client, в меню **Пуск** выберите **ViPNet** > **Настройки PKI Client** или дважды щелкните ярлык на рабочем столе.

Для завершения работы компонентов ViPNet PKI Client:

- File Unit — закройте главное окно программы.
- Web Unit, TLS Unit, Tunnel Unit или SDK — в области уведомлений щелкните правой кнопкой мыши соответствующий значок и в контекстном меню выберите **Выход**.

Активация лицензии

Если лицензия не активирована, вы сможете использовать полнофункциональную версию программы только в течение пробного периода (см. глоссарий, стр. 65). По окончании пробного периода большинство функций будет недоступно (см. Лицензирование на стр. 20).

Если ваш компьютер подключен к Интернету, лицензия будет активирована автоматически при установке, иначе выполните активацию в ручном режиме. Для этого:

1 Перейдите в настройки ViPNet PKI Client (на стр. 34) и в разделе **Лицензия** нажмите **Сохранить запрос на активацию**.

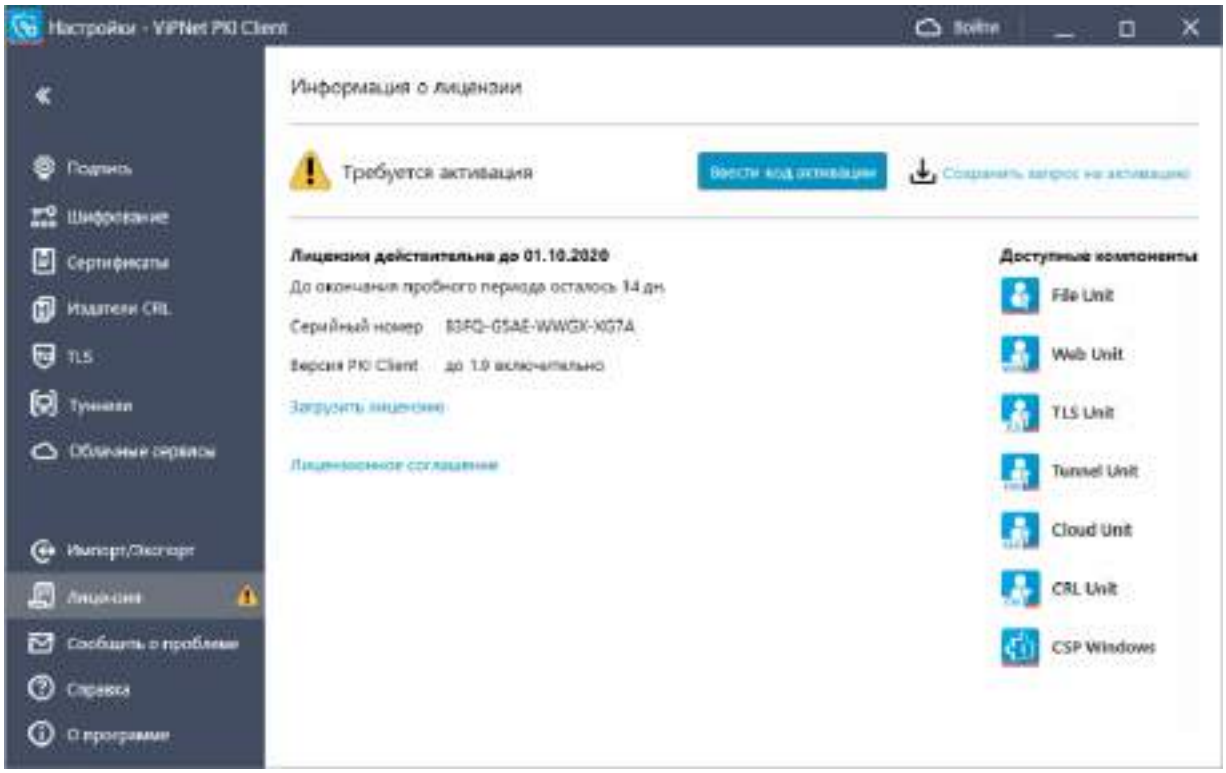

Рисунок 8. Просмотр информации о лицензии

2 В открывшемся окне выполните одно из действий:

- Если у вас установлен почтовый клиент, щелкните ссылку `Reg@infotecs.biz`. Откроется окно вашего почтового клиента с уже сформированным письмом. Перетащите файл запроса в окно создания письма и отправьте в ОАО «ИнфоТеКС».
- Если у вас не установлен почтовый клиент, сохраните файл запроса и создайте письмо самостоятельно. В качестве получателя добавьте адрес электронной почты `Reg@infotecs.biz`, прикрепите к письму файл запроса. Тема и оформление письма могут быть любыми.

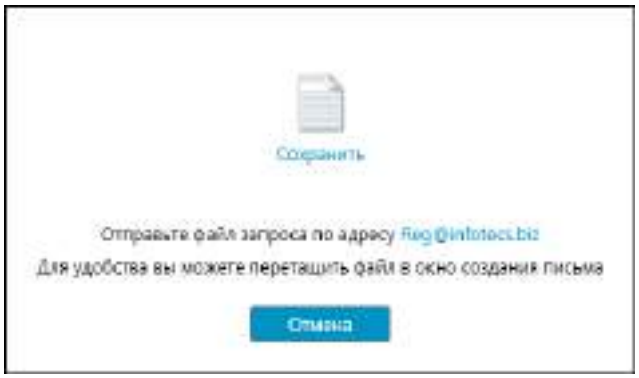

Рисунок 9. Сохранение запроса на активацию

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

4 Нажмите **Ввести код активации**.

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

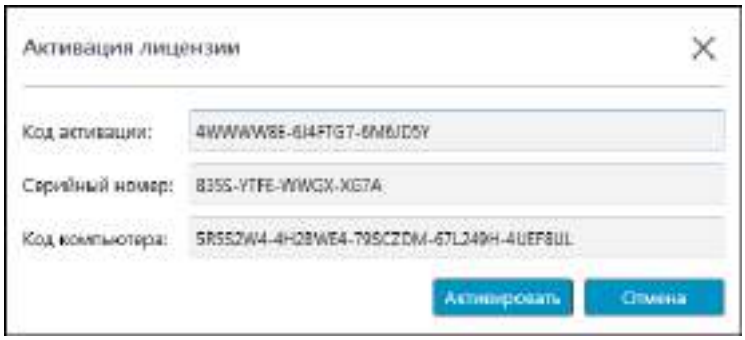

Рисунок 10. Ввод данных для активации ViPNet PKI Client

6 В окне сообщения об успешной активации лицензии нажмите **OK**.

Чтобы убедиться, что лицензия активирована:

1 Перейдите в настройки ViPNet PKI Client (на стр. 34) и выберите раздел **Лицензия**.

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

Обновление лицензии

Обновите лицензию для расширения функций ViPNet PKI Client 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. 34) и в разделе **Лицензия** выполните одно из действий:

- Щелкните ссылку **Загрузить лицензию** и укажите путь к файлу с новой лицензией.
- Перетащите файл с новой лицензией в окно настроек.

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

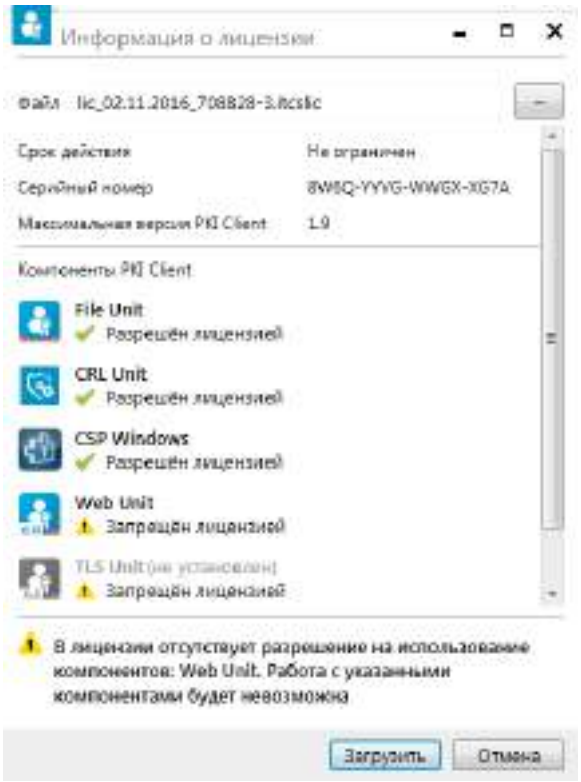

Рисунок 11. Информация о лицензии

4 Чтобы начать использовать новые компоненты, удалите (см. Удаление компонентов на стр. 38), а затем заново установите ПК ViPNet PKI Client (см. Установка и обновление на стр. 32). При установке укажите путь к файлу с новой лицензией.

Удаление компонентов

Удалите ПК ViPNet PKI Client стандартными средствами ОС Windows.

В процессе удаления ПК ViPNet PKI Client не удаляются:

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

4

Подготовка к работе

Порядок действий при подготовке к работе

Таблица 5. Порядок действий

	Действие
☐	Подготовьте личный сертификат и ключ ЭП (см. документ «ViPNet PKI Client. Руководство администратора», раздел «Подготовка личного сертификата и ключа ЭП»)
☐	Установите личный сертификат, сертификаты издателей и CRL в хранилище сертификатов Windows (см. документ «ViPNet PKI Client. Руководство администратора», раздел «Установка сертификатов и CRL»)
☐	Настройте параметры электронной подписи (см. документ «ViPNet PKI Client. Руководство администратора», раздел «Настройка параметров электронной подписи»)
☐	Настройте параметры шифрования (см. документ «ViPNet PKI Client. Руководство администратора», раздел «Настройка параметров шифрования»)
☐	Настройте автоматическое обновление CRL (см. документ «ViPNet PKI Client. Руководство администратора», раздел «Настройка обновления CRL»)
☐	Настройте подключения к сайтам, использующим TLS по ГОСТ (см. документ «ViPNet PKI Client. Руководство администратора», раздел «Настройка подключения к сайтам, использующим TLS ГОСТ»)
☐	Настройте подключение к туннелируемым ViPNet TLS Gateway ресурсам (см. документ «ViPNet PKI Client. Руководство администратора», раздел «Настройка подключения к туннелируемым ресурсам»)

Экспорт и импорт настроек

Экспортируйте настройки ViPNet PKI Client в файл или импортируйте настройки из файла, чтобы перенести ViPNet PKI Client 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 (см. Установка и обновление на стр. 32) и активируйте лицензию (см. Активация лицензии на стр. 35).
3. Перенесите личные сертификаты и ключи электронной подписи. Если вы планируете использовать эти сертификаты для подключения к веб-ресурсам по протоколу TLS и туннелируемым ресурсам, импортируйте их на Infotecs Software Token.
4. 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 в файл:

1. Перейдите в настройки ViPNet PKI Client (на стр. 34).
2. В разделе **Импорт/Экспорт** нажмите **Экспорт**.
3. Выберите настройки, которые хотите экспортировать.

Примечание. Экспорт сертификатов издателей и CRL, установленных в хранилище текущего пользователя недоступен.

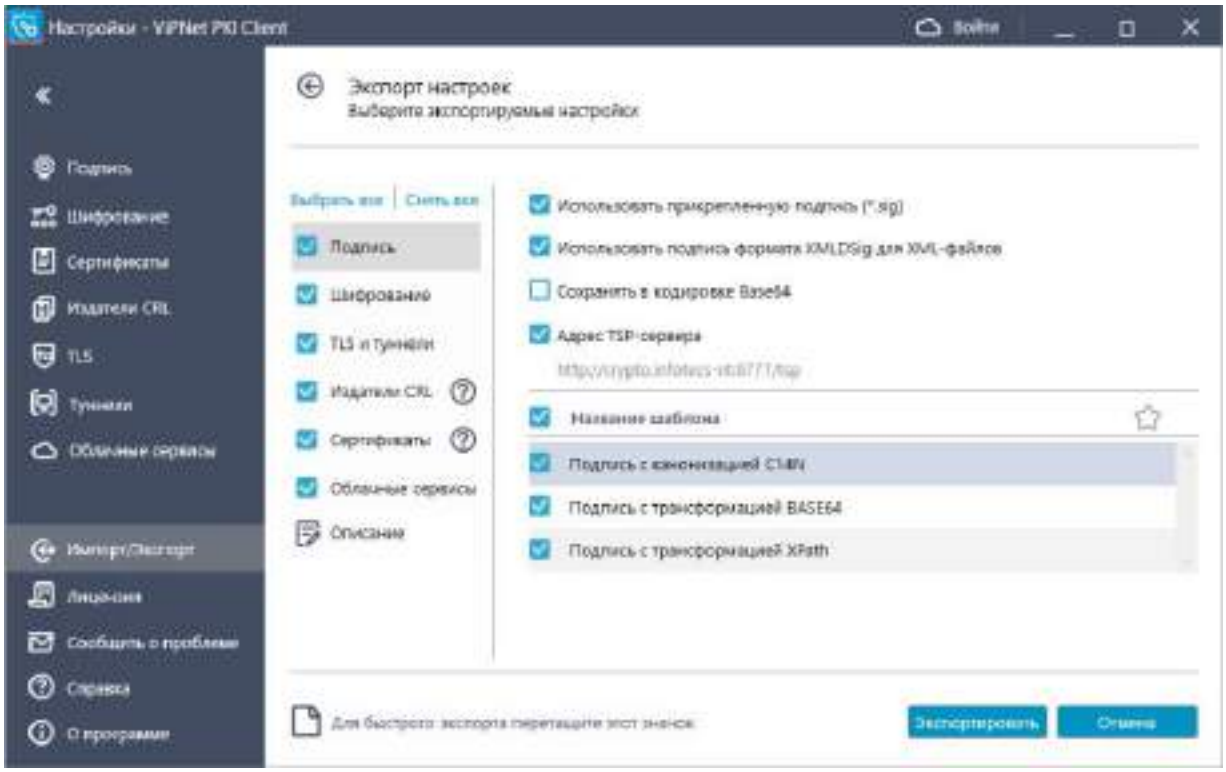

Рисунок 12. Экспорт настроек ViPNet PKI Client

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 или перетащите значок в выбранную папку.

Импорт настроек

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

Чтобы импортировать настройки ViPNet PKI Client:

1 Перейдите в настройки ViPNet PKI Client (на стр. 34).

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

3 Выполните одно из действий:

- Перетащите файл с настройками в выделенную область.

Примечание. При запуске настроек ViPNet PKI Client с правами администратора данный способ недоступен.

- Нажмите **Выбрать** и выберете файл с настройками.

4 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. 34).

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.

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. 66), экспортированы в файл настроек, а при импорте настройки ViPNet PKI Client запущены от имени администратора.
- Сертификаты издателей, образующие цепочку сертификации, не экспортированы в файл настроек, но установлены в хранилище локального компьютера. Настройки ViPNet PKI Client должны быть запущены от имени администратора.

Сертификаты

Импорт личных сертификатов не предусмотрен.

Для импорта сертификатов издателей и CRL в хранилище локального компьютера настройки ViPNet PKI Client должны быть запущены от имени администратора. В противном случае они будут импортированы в хранилище текущего пользователя, и вы не сможете их использовать для настройки автоматической загрузки CRL.

Облачные сервисы

Если уже существует облачный сервис с таким же адресом и номером порта, он будет перезаписан.

Используемым будет назначен облачный сервис, указанный в файле настроек.

Смена языка

Чтобы изменить язык интерфейса ViPNet PKI Client:

1. Перейдите в настройки ViPNet PKI Client (на стр. 34) и выберите раздел  **О программе**.
2. Измените язык в списке **Выбор языка**.
3. Перезапустите компоненты ViPNet PKI Client (на стр. 34).

A

История версий

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

Новые возможности версии 1.4.0

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

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

  Если в вашей организации для хранения сертификатов и ключей ЭП используется ПАК ViPNet PKI Service (см. глоссарий, стр. 65), вы можете подключиться к нему для выполнения криптографических операций из интерфейса ViPNet PKI Client.

- **Установка личного сертификата в контейнер ключей**

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

- **Работа с файлами в кодировке Base64**

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

- **Изменения в программе TLS Unit**

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

    Раньше поддерживались только устройства Infotecs Software Token и Rutoken Lite. В новой версии для подключения вы можете использовать устройства семейств Rutoken, JaCarta и ESMART Token с аппаратной поддержкой российских криптографических алгоритмов (см. Список поддерживаемых внешних устройств для подключения к сайтам, использующим TLS ГОСТ на стр. 59).

  - Добавлены новые алгоритмы шифрования.

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

- **Новая версия криптопровайдера ViPNet CSP**

  Вместе с ПК ViPNet PKI Client теперь устанавливается криптопровайдер ViPNet CSP версии 4.4 (в прошлой версии — 4.2.8).

Новые возможности версии 1.3.1

В этом разделе представлен краткий обзор изменений и новых возможностей ПК ViPNet PKI Client версии 1.3.1 по сравнению с версией 1.3.

- **Добавлена возможность экспорта и импорта настроек**

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

- **Изменения в программе Tunnel Unit**
  - Добавлена возможность устанавливать защищенные TLS-соединения с двусторонней аутентификацией по алгоритмам ГОСТ с туннелируемыми ViPNet TLS Gateway ресурсами.
  - Добавлена возможность работы с туннелируемыми ресурсами через контекстное меню значка программы в области уведомлений.
  - Изменен интерфейс раздела **Туннели** в окне настроек
    - В новой версии туннелирование связи с удаленными узлами включается автоматически при запуске программы Tunnel Unit. В связи с этим был убран переключатель в верхней части окна.
    - Для упрощения работы с большим количеством туннелируемых ресурсов была добавлена кнопка  **Групповые действия**.
    - Столбец **Статус связи** переименован в **Состояние**. Переключатель в этом столбце заменен с **Установлена/Ошибка** на **Вкл./Выкл**.
    - Столбец **Название туннеля** переименован в **Туннель**.
    - Столбец **Локальный порт** переименован в **Порт**.
    - Добавлен столбец **Защита соединения сертификатом** для отображения типа TLS-соединения (с односторонней или двусторонней аутентификацией) с туннелируемыми ресурсами.
    - Добавлен столбец **Авто**, содержащий флажки для автоматического установления связи с туннелируемыми ресурсами при запуске программы Tunnel Unit.
- **Изменения в интерфейсе**
  - Раздел **CRL** переименован в **Издатели CRL**.
  - Добавлен раздел **Импорт/Экспорт**.

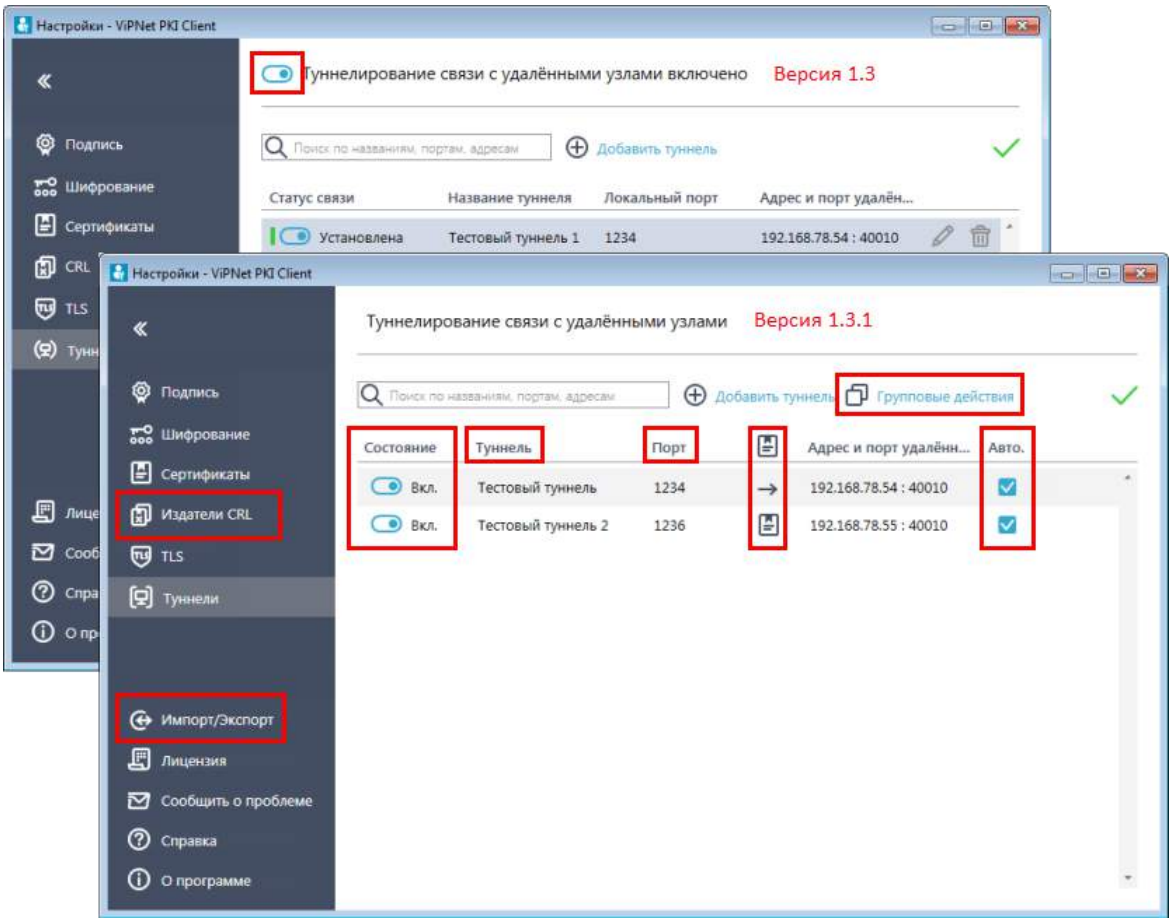

Рисунок 13. Изменения интерфейса в разделе Туннели

- **Добавлена возможность экспорта сертификатов в CER-файлы**

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

- **Изменен список поддерживаемых операционных систем**

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

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

Новые возможности версии 1.3

В этом разделе представлен краткий обзор изменений и новых возможностей ПК ViPNet PKI Client версии 1.3 по сравнению с версией 1.2. Информация об изменениях в предыдущих версиях приведена в приложении История версий (на стр. 46).

- **Добавлен новый компонент Tunnel Unit**

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

- **Добавлена возможность обращения в службу технической поддержки**

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

- **Обновлен интерфейс программы**

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

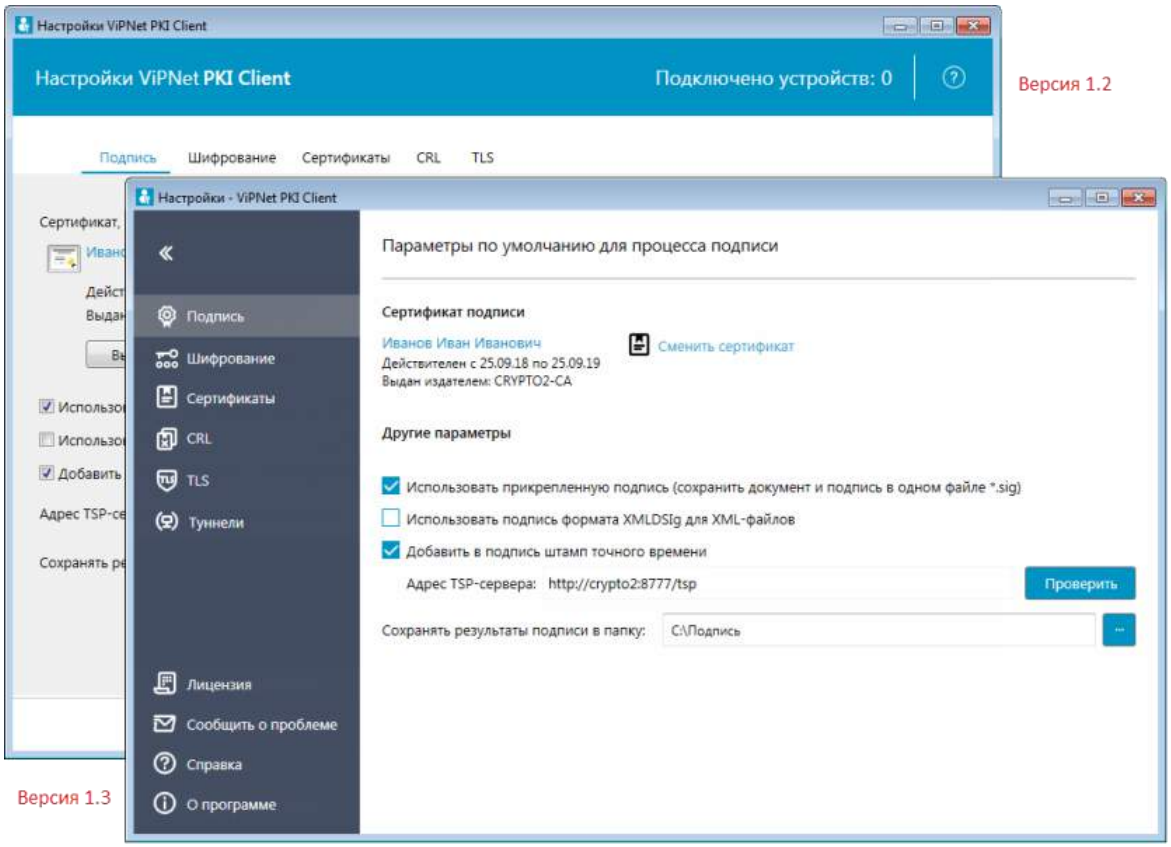

Рисунок 14. Интерфейс программы ViPNet PKI Client 1.3

- **Улучшена работа с сертификатами и CRL**

- Вы можете устанавливать несколько сертификатов и CRL одновременно.
- Вы можете устанавливать сертификаты и CRL, перетащив их в окно **Настройки - ViPNet PKI Client** в раздел  **Сертификаты**.

- **Изменения в программе File Unit**
  - Вы можете выполнять криптографические операции для нескольких файлов одновременно.
  - Вы можете добавлять файлы для выполнения криптографических операций, перетащив их в главное окно программы File Unit.

Новые возможности версии 1.2

В этом разделе представлен краткий обзор изменений и новых возможностей ПК ViPNet PKI Client версии 1.2 по сравнению с версией 1.1.

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

  Добавлена возможность организации защищенного TLS-соединения (см. глоссарий, стр. 64) с использованием внешних устройств, поддерживающих хранение ключей, созданных по алгоритму ГОСТ Р 34.10-2012.

- **Изменения в интерфейсе**

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

  - Вкладка **Менеджер сертификатов** заменена на вкладку **Сертификаты**.
  - Добавлена вкладка **CRL**. Информация о сертификатах издателей и точках распространения CRL (см. глоссарий, стр. 66) теперь отображается здесь.
  - Добавлена вкладка **TLS** для настройки TLS-соединений.

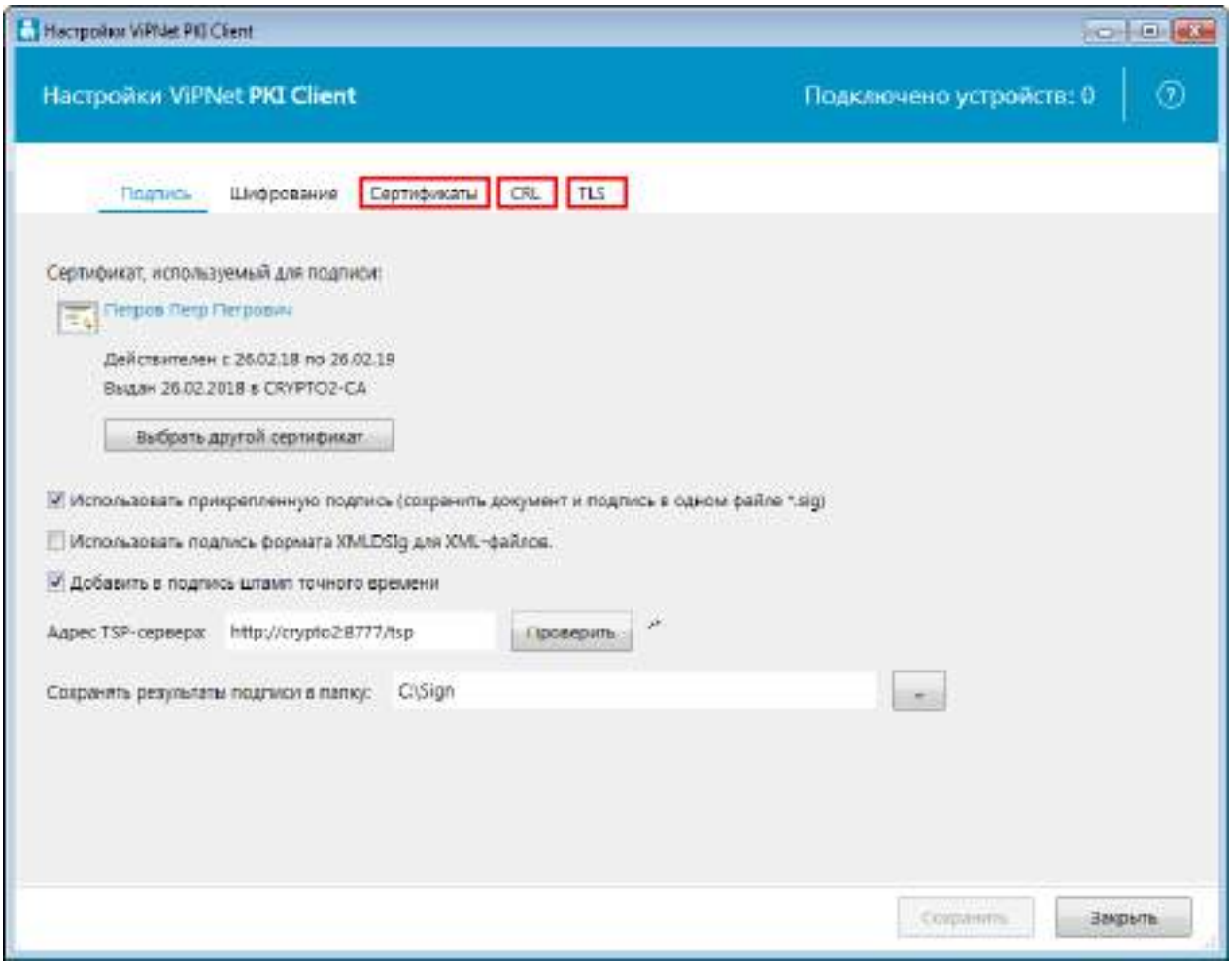

Рисунок 15. Изменения в интерфейсе окна с настройками ViPNet PKI Client

- **Работа с сертификатами и CRL**

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

  В новой версии программы в работе с сертификатами и CRL произошли следующие изменения:

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

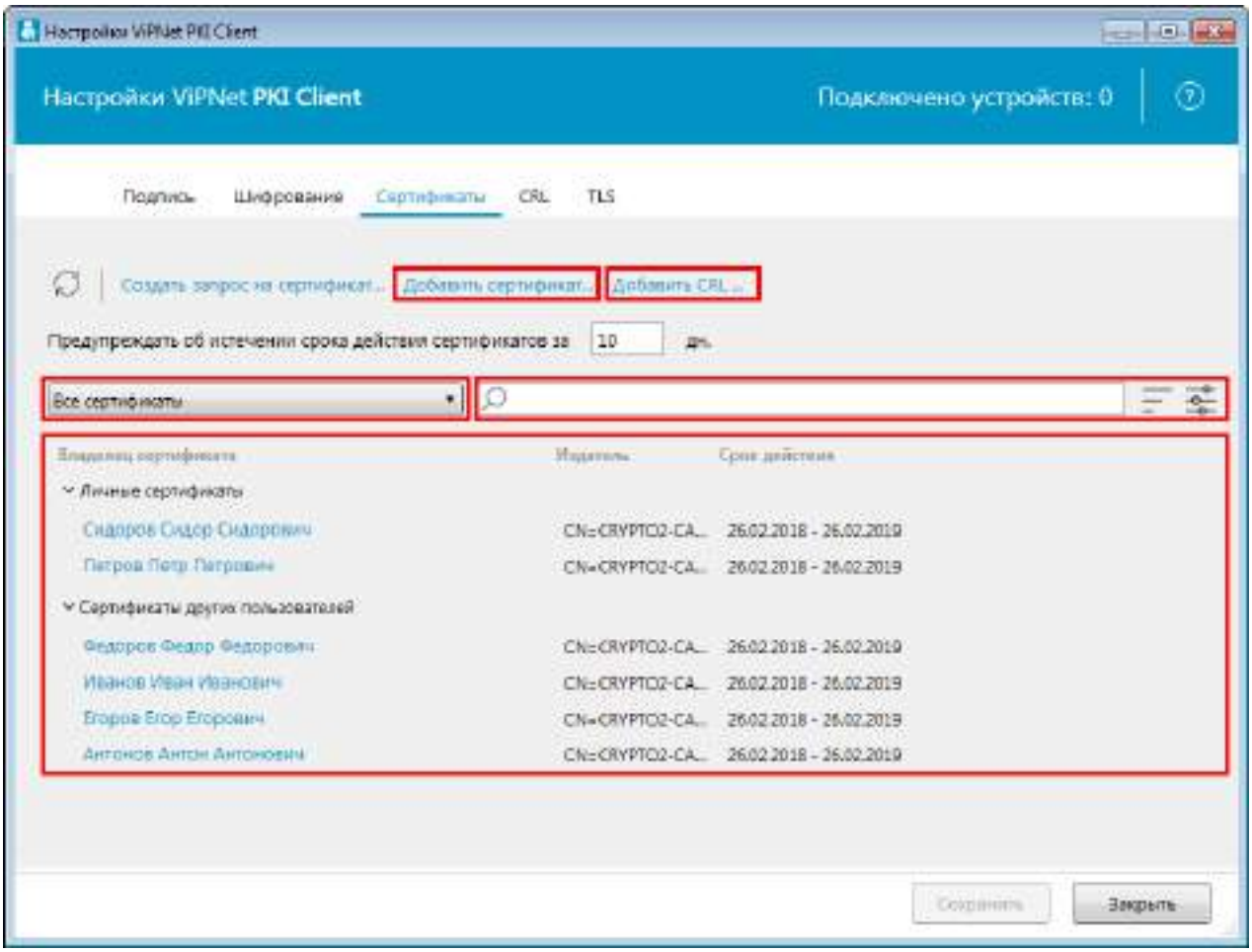

Рисунок 16. Изменения в работе с сертификатами и CRL

- **Настройка TLS-соединений**

  В некоторых случаях может возникнуть необходимость подключения к веб-ресурсам, у которых либо истек срок действия сертификата, либо цепочка сертификации неполная, либо ее

невозможно проверить. В новой версии вы можете устанавливать TLS-соединение с такими веб-ресурсами (подробнее см. документ «ViPNet PKI Client. Руководство администратора», главу «Настройка подключения к веб-ресурсу по протоколу TLS», раздел «Требования к сертификату сервера для установки TLS-соединения»).

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

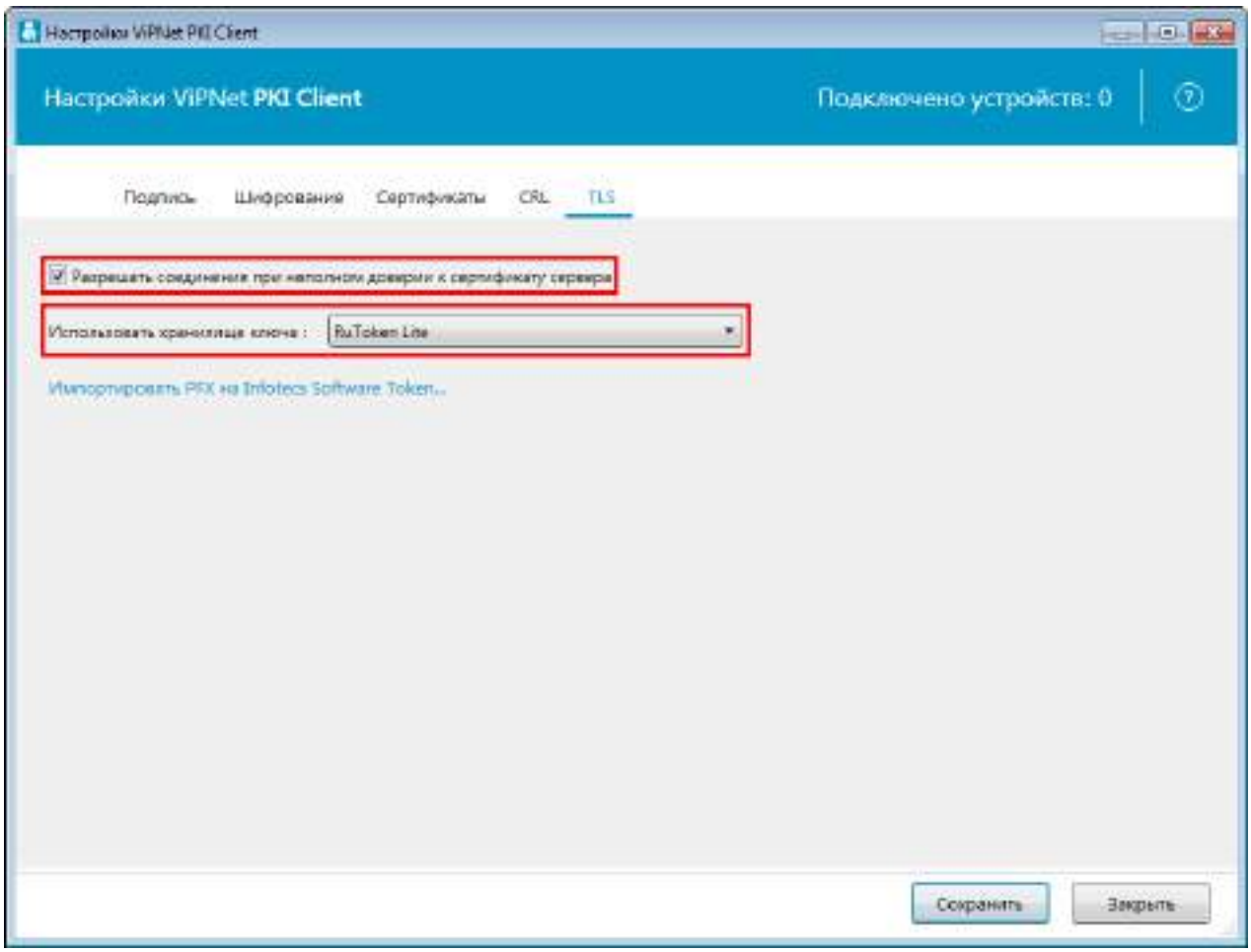

Рисунок 17. Настройка TLS-соединения

Новые возможности версии 1.1

В этом разделе представлен краткий обзор изменений и новых возможностей программы ViPNet PKI Client 1.1 по сравнению с версией 1.0.

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

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

B

Внешние устройства

Общие сведения

Внешние устройства предназначены для хранения контейнеров ключей (см. глоссарий, стр. 65), которые вы можете использовать для аутентификации, формирования электронной подписи (см. глоссарий, стр. 67) 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

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

Таблица 6. Поддерживаемые внешние устройства

Название семейства устройств в программе ViPNet CSP	Полные названия и типы устройств	Необходимые и рекомендуемые условия работы с семейством устройств
ESMART Token	Смарт-карты и токены типов **ESMART Token**, **ESMART Token ГОСТ**	На компьютере должно быть установлено ПО ESMART PKI Client для Windows (рекомендуемая версия — 4.5 RC). Устройства типа ESMART Token необходимо отформатировать с помощью ПО ESMART PKI Client для Windows с профилем ViPNet2. Перенос ключей подписи с устройства и на устройство ESMART Token ГОСТ невозможен, так как на устройстве используется аппаратная криптография с неизвлекаемым ключом.
Infotecs Software Token	**ViPNet SoftToken** — программная реализация стандарта PKCS#11	Необходимо установить компонент ViPNet SoftToken (входит в состав ПО ViPNet OpenSSL). С помощью программы `token_manager.exe` на компьютере должен быть создан программный токен. Подробную информацию о работе с программным токеном см. в документе «ViPNet SoftToken. Руководство разработчика», раздел «Использование утилиты token_manager для работы с программными токенами».
aKey	Смарт-карты **aKey S1000**, **aKey S1003**, **aKey S1004** производства компании Ak Kamal Security	На компьютере должна быть установлена библиотека `akpkcs11.dll`, предоставленная компанией Ak Kamal Security. Устройство имеет два ПИН-кода: администратора и пользователя. Значение этих ПИН-кодов по умолчанию — `12345678`. Перенос ключей подписи с устройств и на устройства данного семейства невозможен, так как на устройствах используется аппаратная криптография с неизвлекаемым ключом.
ViPNet HSM	Программно-аппаратный комплекс **ViPNet HSM** производства ОАО «ИнфоТеКС»	На компьютере должно быть установлено ПО ViPNet HSM SDK. В программе ViPNet CSP необходимо задать параметры подключения к серверу ViPNet HSM.

Название семейства устройств в программе ViPNet CSP	Полные названия и типы устройств	Необходимые и рекомендуемые условия работы с семейством устройств
JaCarta	Персональные электронные ключи и смарт-карты **eToken ГОСТ**, **eToken PRO (Java), JaCarta ГОСТ**, **JaCarta PKI**, **JaCarta LT**, **JaCarta SE, JaCarta PKI/ГОСТ, JaCarta PRO, JaCarta-2 PKI/ГОСТ, JaCarta-2 ГОСТ, JaCarta-2 PRO/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 апплетов «Криптотокен» и «Криптотокен 2 ЭП» (модели JaCarta со словом «ГОСТ» в названии) и на эти апплеты невозможен, так как на устройствах используется аппаратная криптография с неизвлекаемым ключом. Работа с апплетом PRO через ПО «Единый Клиент JaCarta» версии 2.12 не поддерживается. Необходимо установить последнее обновление ПО «Единый Клиент JaCarta» с сайта производителя либо обратиться в службу поддержки компании «Аладдин Р.Д.».
Rutoken	Электронные идентификаторы **Рутокен ЭЦП**, **Рутокен ЭЦП 2.0** и **Рутокен Lite** производства компании «Актив»	На компьютере должны быть установлены драйверы Rutoken (рекомендуемая версия — 4.8.5.0). Перенос ключей подписи с устройств, а также на устройства Рутокен ЭЦП и Рутокен ЭЦП 2.0 невозможен, так как на устройствах используется аппаратная криптография с неизвлекаемым ключом.
Rutoken S	Электронные идентификаторы **Рутокен S** производства компании «Актив»	На компьютере должны быть установлены драйверы Rutoken (рекомендуемая версия — 4.8.5.0).
R301 Foros	Смарт-карты и токены **R301 Форос PKCS** производства компании «СмартПарк»	На компьютере должна быть установлена библиотека `foros_pkcs11.dll` (для 32-разрядной либо 64-разрядной архитектуры процессора), предоставленная компанией «СмартПарк». Перенос ключей подписи с устройств и на устройства данного семейства невозможен, так как на устройствах используется аппаратная криптография с неизвлекаемым ключом.

Название семейства устройств в программе ViPNet CSP	Полные названия и типы устройств	Необходимые и рекомендуемые условия работы с семейством устройств
SafeNet eToken (eToken Aladdin)	Персональные электронные ключи **Gemalto SafeNet eToken 5100/5105**, **5200/5205**, **5110**, **7300**, смарт-карта **Gemalto SafeNet eToken 4100** производства компании Gemalto (SafeNet) Персональные электронные ключи **eToken PRO**, смарт-карты **eToken PRO** производства компании «Аладдин Р.Д.»	Если компьютер работает под управлением ОС Windows 10, на нем должно быть установлено ПО SafeNet Authentication Client (рекомендуемая версия — 10.6.146). Если компьютер работает под управлением другой ОС, на нем должно быть установлено либо ПО PKI Client версии 5.1 SP1, либо ПО SafeNet Authentication Client (рекомендуемая версия — 10.6.146). Смарт-карта **eToken PRO** может использоваться с любым стандартным PC/SC-совместимым устройством считывания карт. **Примечание**. Если вам необходимо работать с устройством из семейства **SafeNet eToken (eToken Aladdin),** то во избежание появления ошибок при выполнении криптографических операций не устанавливайте на компьютер одновременно ПО «Единый Клиент JaCarta» и ПО SafeNet Authentication Client. Работа с устройствами JaCarta PRO с помощью драйверов SafeNet возможна, но не рекомендуется производителем.

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

В таблице перечислены внешние устройства, которые могут быть использованы в программном обеспечении ViPNet для организации защищенного TLS-соединения. Для каждого семейства устройств в таблице приведено описание, указаны условия и особенности работы с устройствами.

Таблица 7. 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.exe на компьютере может быть создан другой программный токен.
ESMART Token	Смарт-карты и токены типов **ESMART Token**, **ESMART Token ГОСТ**	На компьютере должно быть установлено ПО ESMART PKI Client для Windows (рекомендуемая версия — 4.5 RC). Перенос ключей подписи с устройства и на устройство ESMART Token ГОСТ невозможен, так как на устройстве используется аппаратная криптография с неизвлекаемым ключом.
JaCarta	Персональные электронные ключи и смарт-карты **JaCarta PKI**, **eToken ГОСТ**, **JaCarta ГОСТ**, **JaCarta SE**, **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 версия — 2.12). Перенос ключей подписи с устройств eToken ГОСТ, JaCarta ГОСТ, JaCarta PKI/ГОСТ и JaCarta-2 PKI/ГОСТ на эти устройства невозможен, так как на устройствах используется аппаратная криптография с неизвлекаемым ключом.
Rutoken ECP	Электронные идентификаторы **Рутокен ЭЦП**, **Рутокен ЭЦП 2.0** 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.
Rutoken S	Электронные идентификаторы **Рутокен S** производства компании «Актив»	На компьютере должны быть установлены драйверы Rutoken (рекомендуемая версия — 4.8.5.0).

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 8. Алгоритмы и функции, поддерживаемые внешними устройствами

Название семейства устройств в программе ViPNet CSP	Аппаратная поддержка российских криптографических алгоритмов (на устройстве)	Программная поддержка российских криптографических алгоритмов (в ViPNet CSP)	Использование ДСЧ в ViPNet CSP	Поддержка PKCS#11
ESMART Token	**ESMART Token** — отсутствует; **ESMART Token ГОСТ** — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 (короткий ключ 256 бит)	**ESMART Token** — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 **ESMART Token ГОСТ** — отсутствует	Да	Да
Infotecs Software Token	Изолированная программная реализация: ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012		Нет	Да
aKey	**aKey S1000**, **aKey S1003**, **aKey S1004** — ГОСТ Р 34.10-2012; **aKey S1000**, **aKey S1003** — ГОСТ Р 34.10-2001	отсутствует	Нет	Да
ViPNet HSM	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	отсутствует	Нет	Да

Название семейства устройств в программе ViPNet CSP	Аппаратная поддержка российских криптографических алгоритмов (на устройстве)	Программная поддержка российских криптографических алгоритмов (в ViPNet CSP)	Использование ДСЧ в ViPNet CSP	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
Rutoken	**Рутокен ЭЦП** — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 (короткий ключ); **Рутокен ЭЦП 2.0** — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012; **Рутокен Lite** — отсутствует	**Рутокен ЭЦП** — отсутствует; **Рутокен ЭЦП 2.0** — отсутствует; **Рутокен Lite** — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	**ЭЦП** — да; **ЭЦП 2.0** — да; **Lite** — нет	Да
Rutoken S	отсутствует	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	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.

Глоссарий

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.

ViPNet CSP

Криптопровайдер, обеспечивающий вызов криптографических функций из различных приложений. Может использоваться как средство электронной подписи — для формирования ключей электронной подписи.

Аннулирование сертификата

Признание сертификата недействительным до истечения его срока действия (например, в случае компрометации соответствующего ключа электронной подписи).

Асимметричное шифрование

Система шифрования, при которой алгоритмы используют два математически связанных ключа. Открытый ключ используется для зашифрования и передается по незащищенному каналу. Закрытый ключ служит для расшифрования.

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.

ПАК ViPNet PKI Service

Программно-аппаратный комплекс предназначенный для защищенного хранения сертификатов и ключей ЭП, а также для выполнения криптографических операций по запросам пользователей.

Пробный период

Составляет 14 дней, в течение которых рекомендуется активировать ПК ViPNet PKI Client. Если не выполнить активацию в течение пробного периода, большинство функций программы будут недоступны. В программе останутся следующие возможности:

- создание запросов на получение сертификата,
- управление сертификатами и CRL.

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.

Файл *.enc

Файл с расширением `*.enc`, который содержит в себе файл, зашифрованный с использованием ключа проверки электронной подписи получателя или нескольких получателей.

Файл *.sig

Файл с расширением `*.sig`, который содержит в себе электронную подпись, служебную информацию, сертификат ключа проверки электронной подписи, с помощью которого была сформирована данная электронная подпись, а также исходный файл (в случае использования прикрепленной подписи).

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.