



ViPNet PKI Client

Руководство администратора



© АО «ИнфоТекС», 2022

ФРКЕ.00175-02 32 03

Версия продукта 1.7.0

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

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

VipNet[®] является зарегистрированным товарным знаком АО «ИнфоТекС».

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

АО «ИнфоТекС»

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

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

Сайт: infotecs.ru

Служба поддержки: hotline@infotecs.ru

Содержание

Введение.....	6
О документе.....	7
Соглашения документа.....	7
О программе.....	8
Комплект поставки.....	8
Системные требования.....	8
Обратная связь.....	10
Глава 1. Назначение и состав	11
Назначение	12
Компоненты.....	13
Лицензирование.....	15
Глава 2. Начало работы	16
Установка, обновление	17
Запуск и завершение работы.....	19
TLS Unit.....	19
Активация лицензии.....	21
Обновление лицензии.....	23
Удаление.....	24
Глава 3. Подготовка к работе.....	25
Порядок подготовки к работе.....	26
Экспорт и импорт настроек.....	27
Особенности импорта настроек	27
Экспорт настроек.....	28
Импорт настроек	29
Смена языка интерфейса	30
Глава 4. Работа с сертификатами	31
Какие нужны сертификаты	32
Подготовка личного сертификата и ключа ЭП	33
Получение сертификата.....	35
Подготовка файла шаблона в формате JSON	37
Подготовка файла шаблона в формате XML	37

Установка сертификатов и CRL.....	39
Установка с помощью ViPNet PKI Client.....	39
Установка с помощью контекстного меню Windows.....	41
Экспорт сертификатов.....	42
Перенос сертификатов и ключей ЭП между компьютерами.....	43
Просмотр сертификатов.....	45
Проверка сертификатов.....	47
Удаление сертификатов.....	49
Глава 5. Автоматическое обновление CRL.....	50
Добавление точек распространения CRL.....	51
Отслеживание событий при автообновлении CRL.....	53
Файл конфигурации crlunit.cfg.....	53
Остановка и запуск службы ViPNet PKI Client CRL Unit Service.....	55
Глава 6. Использование облачных сервисов ЭП.....	56
Об облачных сервисах ЭП.....	57
Перед подключением к ПАК ViPNet PKI Service.....	58
Настройка подключения к ПАК ViPNet PKI Service.....	59
Подключение к ПАК ViPNet PKI Service.....	61
Смена пароля учетной записи пользователя.....	62
Глава 7. Подпись и шифрование файлов.....	63
Требования к сертификатам для подписи и шифрования.....	64
Настройка параметров ЭП.....	65
Импорт шаблонов XML-подписи в настройки.....	66
Настройка параметров шифрования.....	68
Настройка сетевых параметров.....	70
Глава 8. Подключение к веб-ресурсам, использующим TLS ГОСТ.....	71
Порядок настройки подключения к веб-ресурсам, использующим TLS ГОСТ.....	72
Требования к сертификатам для работы TLS Unit.....	73
Импорт сертификата и ключа ЭП на Infotecs Software Token.....	75
Импорт сертификата и ключа ЭП из хранилища.....	75
Импорт сертификата и ключа ЭП из файла *.pfx.....	76
Смена ПИНа Infotecs Software Token.....	76
Подключение к веб-ресурсу.....	77
Просмотр информации о TLS-соединениях.....	78

Глава 9. Подключение к туннелируемым ресурсам	79
Порядок настройки подключения к туннелируемым ресурсам	80
Требования к сертификатам для работы Tunnel Unit	81
Добавление туннелируемого ресурса.....	82
Подключение к туннелируемому ресурсу	84
Глава 10. Возможные неполадки и способы их устранения	85
Обращение в техническую поддержку.....	86
Общие неполадки.....	87
Не удалось установить ViPNet PKI Client	87
Ошибка при обновлении ViPNet PKI Client	87
Ошибка при импорте настроек.....	87
Ошибка при удалении сертификата.....	88
Ошибка службы регистрации событий	89
Ошибки при обновлении CRL	90
Не удается сохранить ключ ЭП на ESMART Token ГОСТ	91
Обнаружена несогласованность при внутренней проверке	92
Ошибки при совместной работе с КриптоПро CSP	92
File Unit	93
Требуемый сертификат не отображается в списке сертификатов для подписания	93
Ошибка при расшифровании.....	93
TLS Unit	94
Настройка совместной работы TLS Unit и браузера Mozilla Firefox.....	94
Невозможно установить соединение	95
Приложение А. Формат файла с шаблонами XML-подписи	97
Приложение В. Внешние устройства	102
Общие сведения	102
Список поддерживаемых внешних устройств	102
Список поддерживаемых внешних устройств для подключения к сайтам, использующим TLS ГОСТ, и туннелируемым ресурсам	105
Алгоритмы и функции, поддерживаемые внешними устройствами.....	107
Приложение С. Глоссарий	109



Введение




О документе	7
О программе	8
Обратная связь	10

О документе

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

Документ предназначен для администраторов, которые применяют ViPNet PKI Client для организации взаимодействия с инфраструктурой открытых ключей (PKI) и защиты данных. Предполагается, что читатель имеет общее представление об [инфраструктуре открытых ключей](#) (см. глоссарий, стр. 109).

Соглашения документа

Обозначение	Описание
	Внимание! Содержит критически важную информацию
	Примечание. Содержит рекомендательную информацию
	Совет. Содержит полезные приемы и хорошие практики
Название	Название элемента интерфейса: окна, вкладки, поля, кнопки, ссылки
Клавиша+Клавиша	Сочетание клавиш: нажмите первую клавишу и, не отпуская ее, нажмите вторую
Меню > Команда	Последовательность элементов или действий
Код	Имя файла, путь, фрагмент кода или команда в командной строке

О программе

Комплект поставки

- Установочный файл `pki_client_installer.exe`.
- 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

- 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 с последними пакетами обновлений:
 - Windows 7 — 32/64-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;
 - версия 2004, сборка 19041;
 - версия 20H2, сборка 19042;

- Windows 11 — 64-разрядная версии 21H2, сборка 22000.

Работа ViPNet PKI Client на компьютерах с Windows 10 или Windows 11 других версий и сборок не гарантируется;

- Браузер — Internet Explorer 11, Chromium с поддержкой ГОСТ 68.0.3440.84, КриптоПро Fox 24 или выше, а также Edge, Google Chrome, Mozilla Firefox, Опера, Яндекс.Браузер, Спутник последних версий.
- Программная платформа Microsoft .NET Framework 4.5.

Обратная связь

Дополнительная информация

Сведения о продуктах ViPNet, частые вопросы и полезная информация 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.](#)
Канал поддержки в Telegram: t.me/vhd21
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

Назначение и состав

Назначение	12
Компоненты	13
Лицензирование	15

Назначение

ViPNet PKI Client позволяет организовать взаимодействие с **PKI** (см. глоссарий, стр. 109) и защиту передаваемых данных с помощью шифрования и **электронной подписи** (см. глоссарий, стр. 112).

С помощью ViPNet PKI Client вы можете:

- Создать **запрос на сертификат** (см. глоссарий, стр. 110) и получить в **удостоверяющем центре** (см. глоссарий, стр. 111) сертификат, чтобы использовать его для защищенного обмена данными.
- Подтверждать свою личность и проверять личность других пользователей, от которых вы получаете файлы, с использованием электронной подписи (далее — ЭП) в соответствии с федеральным законом № 63-ФЗ «Об электронной подписи».
- Защищать файлы, которые вы отправляете другим пользователям, с помощью шифрования.
- Автоматически получать актуальные **списки аннулированных сертификатов (CRL)** (см. глоссарий, стр. 111) из **точек распространения** (см. глоссарий, стр. 111).
- Работать с облачным сервисом ЭП на базе ПАК ViPNet PKI Service.
- Подключаться к сайтам, использующим TLS 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 автоматического получения CRL из точек распространения.
- Разработка веб-приложений с поддержкой криптографических операций, которые смогут выполнять пользователи ViPNet PKI Client.

ViPNet PKI Client использует российские алгоритмы:

- Алгоритмы формирования и проверки ЭП ГОСТ Р 34.10-2001 с вычислением хэш-функции по ГОСТ Р 34.11-94 (только для проверки ЭП и расшифрования) 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».

Компоненты

File Unit

С помощью File Unit вы можете:

- Проверять личность отправителя файла с помощью ЭП.
- Защищать файлы путем зашифрования и расшифровывать файлы, полученные от других пользователей.

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

Web Unit

С помощью Web Unit вы можете в веб-приложениях, совместимых с ViPNet PKI Client, выполнять следующее:

- Создавать запросы на сертификат, устанавливать полученные сертификаты в хранилище.
- Подписывать данные и проверять ЭП данных.
- Зашифровывать и расшифровывать данные.

SDK

С помощью комплекта средств разработки SDK вы можете встраивать функции шифрования и ЭП в веб-приложения, разрабатываемые на языке JavaScript.

Вместе с ViPNet PKI Client на компьютер устанавливаются примеры веб-страниц, код которых вы можете использовать в своем веб-приложении для вызова криптографических функций.

На компьютерах пользователей веб-приложения потребуются установить Web Unit.

Подробнее о SDK см. «ViPNet PKI Client. Руководство разработчика».

CRL Unit

Служба CRL Unit обеспечивает автоматическое получение CRL из точек распространения и установку полученных CRL в хранилище.

Создает и управляет точками распространения CRL администратор корпоративной сети.

Certificate Unit

С помощью Certificate Unit вы можете:

- Создавать запросы на сертификаты и сохранять их в файлы.

- Устанавливать сертификаты и CRL в хранилище.
- Экспортировать сертификаты.
- Просматривать установленные сертификаты.



TLS Unit

С помощью TLS Unit вы можете установить между клиентом и веб-ресурсом защищенное TLS-соединение, поддерживающее российские алгоритмы ГОСТ 28147–89, ГОСТ Р 34.10-2012, ГОСТ Р 34.12-2015 «Магма» или «Кузнечик».



Tunnel Unit

С помощью Tunnel Unit вы можете устанавливать защищенные TLS-соединения с односторонней и двусторонней аутентификацией по алгоритмам ГОСТ с туннелируемыми ViPNet TLS Gateway ресурсами.



Cloud Unit

С помощью Cloud Unit вы можете подключиться к ПАК ViPNet PKI Service и использовать хранимые на нем сертификаты и ключи ЭП для выполнения средствами ПАК ViPNet PKI Service из интерфейса ViPNet PKI Client следующего:

- Создание запроса на сертификат по шаблонам ПАК ViPNet PKI Service с сохранением ключа ЭП на ViPNet PKI Service.
- Подписание файлов и проверка ЭП файлов.
- Расшифрование файлов.



ViPNet CSP

ViPNet CSP — криптопровайдер, к которому обращаются другие компоненты ViPNet PKI Client для выполнения криптографических операций. Также ViPNet CSP обеспечивает вызов криптографических функций из приложений сторонних производителей, использующих интерфейс CryptoAPI 2.0 (например, Microsoft Outlook).

Подробнее о ViPNet CSP см. «ViPNet CSP. Руководство пользователя».

Лицензирование

ViPNet PKI Client защищается от нелегального использования лицензией. Вы можете приобрести лицензию в [ИнфоТеКС](#) (на стр. 10).

Лицензия содержит:

- Разрешенные для использования компоненты и функции:
 - компонент File Unit для шифрования и подписания файлов;
 - компонент Web Unit для работы с ЭП и шифрованием в веб-приложениях;
 - компонент Cloud Unit для работы с облачными сервисами ЭП на базе ПАК ViPNet PKI Service версии 2.0.2;
 - компонент TLS Unit для установления TLS-соединений с односторонней аутентификацией (аутентификацией сервера);
 - функция установления TLS-соединений с двусторонней аутентификацией (взаимной аутентификацией сервера и пользователя) для TLS Unit.



Примечание. Для использования Tunnel Unit необходима лицензия, позволяющая использовать TLS Unit.

Для подключения к ПАК ViPNet PKI Service по протоколу HTTPS необходима лицензия, позволяющая использовать TLS Unit и Cloud Unit.

- Максимальную версию ViPNet PKI Client.
- Срок действия лицензии, по истечении которого в ViPNet PKI Client будет доступно только управление сертификатами и CRL.

Файл лицензии требуется указать при установке ViPNet PKI Client (см. [Установка, обновление](#) на стр. 17).

2

Начало работы

Установка, обновление	17
Запуск и завершение работы	19
Активация лицензии	21
Обновление лицензии	23
Удаление	24

Установка, обновление

Особенности установки, обновления

- Установить или обновить ViPNet PKI Client можно в обычном режиме или с использованием командной строки (см. ниже).
- Для установки и обновления ViPNet PKI Client требуется файл лицензии *.itcslic.
- Вместе с ViPNet PKI Client текущей версии устанавливается ViPNet CSP версии 4.4.2. Если на вашем компьютере уже установлен ViPNet CSP более ранней версии при установке ViPNet PKI Client он будет обновлен до версии 4.4.2 и для его работы будут использоваться данные, заданные до установки ViPNet PKI Client.



Внимание! Если локализация Windows не русская, для правильного отображения кириллицы в интерфейсе ViPNet CSP измените региональные настройки Windows (см. «ViPNet CSP. Руководство пользователя»).

Во избежание ошибок в работе ViPNet PKI Client не используйте ViPNet CSP версий выше 4.4.2.

- При обновлении с ViPNet PKI Client версии 1.0 на текущую версию сначала удалите устаревшую версию, а затем установите новую.
- Если на компьютере необходимо создать замкнутую программную среду для соответствия требованиям ФСБ России к средствам криптографической защиты информации класса КСЗ, дополнительно установите программу ViPNet SysLocker (см. «ViPNet SysLocker. Руководство пользователя»).

Установка, обновление в обычном режиме

- 1 Запустите установочный файл и следуйте указаниям мастера.
- 2 Если на компьютере нет доступа в Интернет, активируйте лицензию (см. [Активация лицензии](#) на стр. 21).

Установка, обновление с использованием командной строки

Таблица 1. Параметры установки

Параметр	Описание
/install	Установка в обычном режиме (см. выше)
/install /quiet	Тихий режим установки (без участия пользователя и демонстрации интерфейса)
-license=	Указание файла лицензии (обязательный параметр)

Параметр	Описание
<code>/ignore_os_check</code>	Параметр, разрешающий установку ViPNet CSP, входящего в состав ViPNet PKI Client, на компьютер с операционной системой версии, которая не проверялась на совместимость



Внимание! Без параметра `/ignore_os_check` ViPNet PKI Client невозможно установить на компьютер с Windows 10 или Windows 11 версии, которая не проверялась на совместимость (см. [Системные требования](#) на стр. 8). Работа ViPNet PKI Client на этих версиях Windows не гарантируется.

Пример команды:

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

Запуск и завершение работы

Для запуска нужного компонента ViPNet PKI Client в меню **Пуск** выберите **ViPNet > <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.




О подготовке ViPNet PKI Client к работе см. «ViPNet PKI Client. Руководство администратора».

Для завершения работы компонентов ViPNet PKI Client:

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

TLS Unit

Состояния TLS Unit

- **Выключена** — в области уведомлений отображается значок . Возможность подключения к веб-ресурсам, использующим TLS ГОСТ, выключена.
- **Работает** — в области уведомлений отображается значок . Подключение к веб-ресурсам, использующим TLS ГОСТ, возможно только если для сертификата сервера выполняются все проверки.
- **Работает** — в области уведомлений отображается значок . Подключение к сайтам, использующим TLS ГОСТ, возможно если для сертификата сервера выполняются не все проверки (см. [Требования к сертификатам для работы TLS Unit](#) на стр. 73).




Примечание. При первом запуске TLS Unit переходит в состояние **Выключена**.

После перезапуска TLS Unit возвращается в состояние, которое было до перезапуска.

Включение и выключение

Выполните одно из действий:

- В области уведомлений щелкните правой кнопкой мыши значок ViPNet PKI Client TLS Unit и в контекстном меню выберите **Включить** или **Выключить**.
- [Перейдите в настройки ViPNet PKI Client](#) (на стр. 19) и выберите раздел  **TLS**. Включите или выключите TLS Unit с помощью переключателя.

Первый запуск

- 1 При первом [запуске TLS Unit](#) (на стр. 19) в окне **Предупреждение о безопасности** нажмите **Да**, чтобы установить [корневой сертификат ViPNet PKI Client](#) (см. глоссарий, стр. 110). Это необходимо для работы TLS Unit.
- 2 Если в рамках текущего сеанса работы не запускалась [электронная рулетка](#) (см. глоссарий, стр. 112), выполните указания в окне **Электронная рулетка**.

Активация лицензии

Если лицензия не активирована, вы сможете использовать все компоненты и функции ViPNet PKI Client в течение пробного периода (14 дней). По окончании этого периода останутся доступны только:

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

Если ваш компьютер подключен к интернету, лицензия будет активирована автоматически при установке ViPNet PKI Client, иначе выполните активацию вручную:

- 1 [Перейдите в настройки ViPNet PKI Client](#) (на стр. 19).
- 2 В разделе  **Лицензия** нажмите  **Сохранить запрос на активацию**.

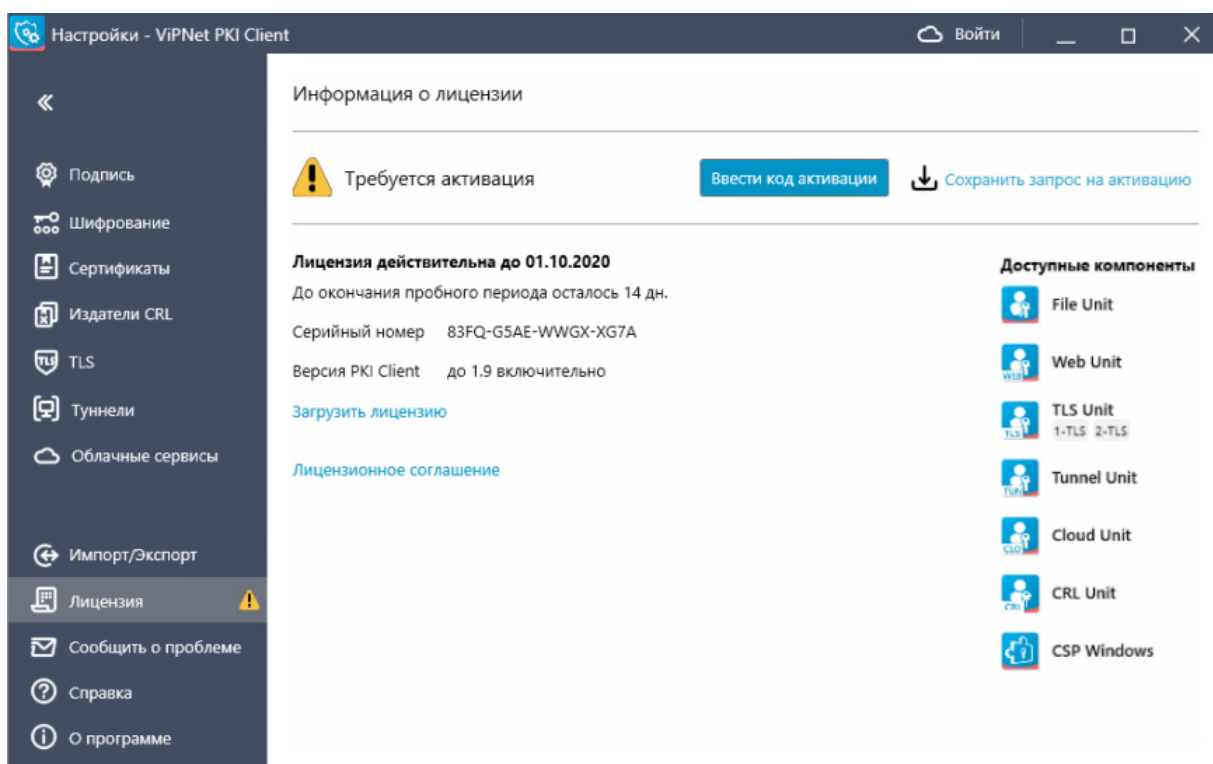
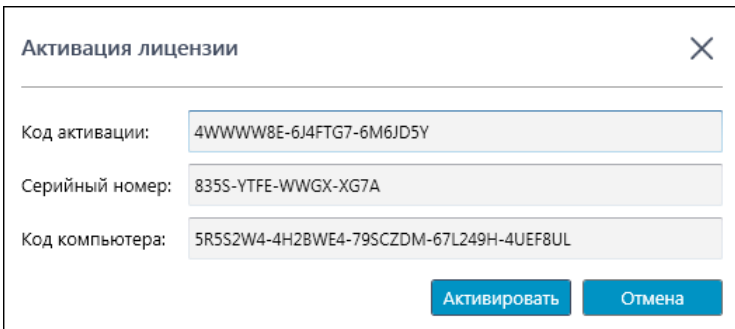


Рисунок 1. Просмотр информации о лицензии

- 3 Выполните одно из действий:
 - Если у вас установлен почтовый клиент, нажмите `Reg@infotecs.ru`. Откроется окно почтового клиента с уже сформированным письмом. Перетащите файл запроса в окно с письмом и отправьте его в ИнфоТеКС.
 - Если у вас не установлен почтовый клиент, сохраните файл запроса и создайте письмо вручную. Укажите адрес получателя письма `Reg@infotecs.ru` и прикрепите к письму файл запроса. 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**.



Активация лицензии

Код активации: 4WWWW8E-6J4FTG7-6M6JD5Y

Серийный номер: 835S-YTFE-WWGX-XG7A


Код компьютера: 5R5S2W4-4H2BWE4-79SCZDM-67L249H-4UEF8UL

Активировать Отмена

Рисунок 2. Ввод данных для активации ViPNet PKI Client


- 7 Нажмите **ОК**.

Чтобы убедиться, что лицензия активирована:

- 1 [Перейдите в настройки ViPNet PKI Client](#) (на стр. 19) и выберите раздел  **Лицензия**.
- 2 Проверьте, что на странице информации о лицензии нет надписи **Требуется активация**.

Обновление лицензии

При истечении срока действия лицензии или для расширения функций ViPNet PKI Client обновите лицензию:

- 1 Отправьте запрос на получение лицензии через [веб-форму на сайте ИнфоТеКС](#) и получите новый файл лицензии.
- 2 [Перейдите в настройки ViPNet PKI Client](#) (на стр. 19).
- 3 В разделе  **Лицензия** выполните одно из действий:
 - Нажмите **Загрузить лицензию** и укажите путь к новому файлу лицензии.
 - Перетащите новый файл лицензии в окно настроек.
- 4 Ознакомьтесь с информацией о лицензии и нажмите **Загрузить**.

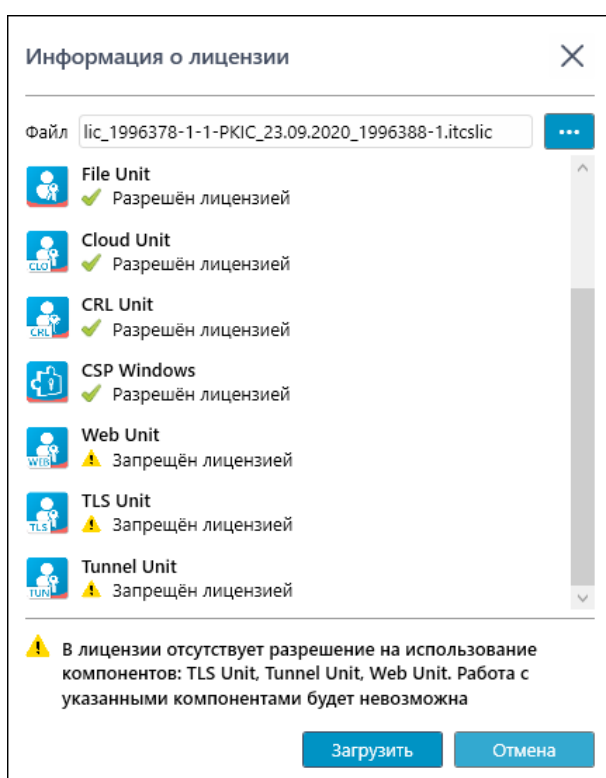


Рисунок 3. Информация о лицензии

Удаление

Удалите ViPNet PKI Client стандартными средствами Windows.

При удалении ViPNet PKI Client не удаляются:

- ViPNet CSP. Вы можете:
 - Удалить ViPNet CSP (см. «ViPNet CSP. Руководство пользователя»).
 - Продолжить использовать ViPNet CSP. Если вы не работали с ViPNet CSP до установки ViPNet PKI Client, выполните регистрацию (см. «ViPNet CSP. Руководство пользователя»).
- Пользовательские данные:
 - Сертификаты и ключи ЭП.
 - Подписанные и зашифрованные файлы.
 - Настройки ЭП, шифрования, добавленные туннели и так далее.

3

Подготовка к работе

Порядок подготовки к работе	26
Экспорт и импорт настроек	27
Смена языка интерфейса	30

Порядок подготовки к работе

Действие и ссылка

- 1 Установите ViPNet PKI Client (на стр. 17)
 - 2 Подготовьте личный сертификат и ключ ЭП (на стр. 33)
 - 3 Установите личный сертификат, сертификаты издателей и CRL в хранилище сертификатов (на стр. 39)
 - 4 Настройте автоматическое обновление CRL (на стр. 50)
 - 5 Настройте параметры ЭП (на стр. 65)
 - 6 Настройте параметры шифрования (на стр. 68)
 - 7 Настройте подключения к сайтам, использующим TLS по ГОСТ (на стр. 71)
 - 8 Настройте подключение к туннелируемым ViPNet TLS Gateway ресурсам (на стр. 79)
-

Экспорт и импорт настроек

Используйте экспорт и импорт настроек ViPNet PKI Client, если необходимо:

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

Чтобы выполнить экспорт и импорт настроек ViPNet PKI Client:

- 1 Ознакомьтесь с особенностями (см. [Особенности импорта настроек](#) на стр. 27).
- 2 На компьютере с ViPNet PKI Client экспортируйте настройки (см. [Экспорт настроек](#) на стр. 28).
- 3 На другом компьютере установите ViPNet PKI Client (см. [Установка, обновление](#) на стр. 17).
- 4 На другой компьютер:
 - 4.1 Перенесите личные сертификаты и ключи ЭП (см. [Перенос сертификатов и ключей ЭП между компьютерами](#) на стр. 43).
 - 4.2 Если вы планируете использовать перенесенные сертификаты для подключения к веб-ресурсам по протоколу TLS и туннелируемым ресурсам, импортируйте их на Infotecs Software Token (см. [Импорт сертификата и ключа ЭП из хранилища](#) на стр. 75).
 - 4.3 Импортируйте настройки (см. [Импорт настроек](#) на стр. 29).

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. 19).

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, 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 автоматического обновления CRL (см. [Добавление точек распространения CRL](#) на стр. 51).

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.

Экспорт настроек

- 1 [Перейдите в настройки ViPNet PKI Client](#) (на стр. 19).
- 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.

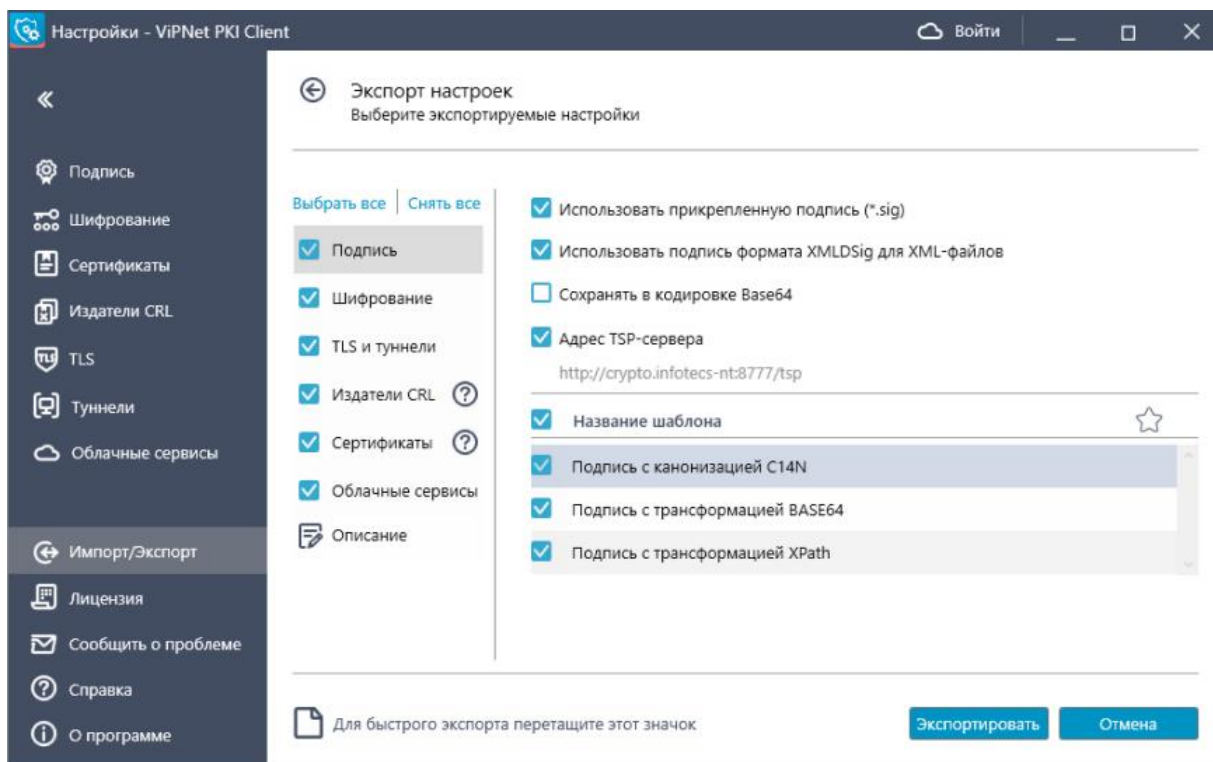




Рисунок 4. Экспорт настроек ViPNet PKI Client

- 4 Добавьте описание файла с настройками (например, укажите, для каких пользователей предназначены эти настройки), чтобы проще было его найти при импорте.
- 5 Нажмите **Экспортировать** и укажите папку для сохранения файла настроек или перетащите значок  в выбранную папку.


Импорт настроек

Чтобы импортировать настройки ViPNet PKI Client:


- 1 [Перейдите в настройки ViPNet PKI Client](#) (на стр. 19).
- 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**.

Смена языка интерфейса

- 1 [Перейдите в настройки ViPNet PKI Client](#) (на стр. 19).
- 2 Выберите раздел  **О программе**.
- 3 Измените язык в списке **Выбор языка**.
- 4 [Перезапустите ViPNet PKI Client](#) (на стр. 19).

4

Работа с сертификатами

Какие нужны сертификаты	32
Подготовка личного сертификата и ключа ЭП	33
Получение сертификата	35
Установка сертификатов и CRL	39
Экспорт сертификатов	42
Перенос сертификатов и ключей ЭП между компьютерами	43
Просмотр сертификатов	45
Проверка сертификатов	47
Удаление сертификатов	49

Какие нужны сертификаты

Для шифрования и подписания с помощью ViPNet PKI Client вам потребуются:

- Личный сертификат — для подписания, расшифрования данных, подключения к сайтам по TLS ГОСТ и туннелируемым ресурсам с аутентификацией пользователя.

Запросите его в УЦ и установите в хранилище сертификатов текущего пользователя **Личное**.

- Сертификаты издателей — для проверки подлинности личного сертификата.

Получите их в УЦ и установите в хранилище сертификатов **Доверенные корневые центры сертификации** или **Промежуточные центры сертификации**.

- CRL — для подтверждения действительности сертификатов.

Получите его в УЦ и установите в хранилище сертификатов **Промежуточные центры сертификации** > **Список отзыва сертификатов**.

В УЦ могут использоваться:

- Точки распространения CRL. В этом случае можно автоматически получать и устанавливать CRL путем опроса этих точек по URL, которые содержатся в сертификатах, изданных УЦ, в поле **Точки распространения списков отзыва (CRL)**.
 - Сервис онлайн-проверки статуса сертификатов по протоколу OCSP. В этом случае CRL не используются. Информация о поддержке сервиса содержится в сертификатах, изданных УЦ, в поле **Доступ к информации о центрах сертификации**.
- Сертификаты получателей — для зашифрования данных.

Запросите их у получателей зашифрованных файлов и установите в хранилище сертификатов **Другие пользователи**.

Подготовка личного сертификата и ключа ЭП

У меня нет сертификата и ключа ЭП

- 1 Создайте запрос на сертификат (см. [Получение сертификата](#) на стр. 35).
- 2 Передайте запрос в УЦ и получите личный сертификат, сертификаты издателей из цепочки и соответствующие им CRL.
- 3 Установите личный сертификат в хранилище сертификатов Windows или на внешнее устройство (на стр. 39).

У меня есть сертификат и ключ ЭП в папке на диске

- 1 С помощью ViPNet CSP установите контейнер ключей (см. «ViPNet CSP. Руководство пользователя» > «Установка контейнера ключей из папки»).
- 2 Установите сертификат в хранилище сертификатов текущего пользователя **Личное** с указанием расположения контейнера ключей (см. в документе «ViPNet CSP. Руководство пользователя» > «Установка сертификата в системное хранилище Windows»).

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

- 1 Подключите внешнее устройство к компьютеру (см. [Внешние устройства](#) на стр. 102).




Примечание. При подключении устройств семейства Rutoken, JaCarta и ESMART Token появится соответствующее уведомление, а в настройках ViPNet PKI Client появится раздел



Подключено устройств.

2 Выполните одно из действий:

- Для устройств семейства Rutoken, JaCarta, ESMART Token — перейдите в раздел  **Подключено устройств**, щелкните сертификат правой кнопкой мыши и выберите **Установить сертификат**.
- Для других устройств — с помощью ViPNet CSP установите контейнер ключей и сертификат в хранилище сертификатов текущего пользователя **Личное** (см. «ViPNet CSP. Руководство пользователя» > «Установка контейнера ключей с внешнего устройства»).

У меня есть сертификат и ключ ЭП на ПАК ViPNet PKI Service

- 1 [Настройте подключение к ПАК ViPNet PKI Service](#) (на стр. 56).
- 2 [Подключитесь к ПАК ViPNet PKI Service](#) (на стр. 61). Сертификат появится в списке сертификатов **Облачные**.

Примечание. Если в вашей учетной записи на ПАК ViPNet PKI Service нет сертификата или вам нужно обновить существующий сертификат:






- 1 Создайте запрос на сертификат с помощью шаблона **Облачный** (см. [Получение сертификата](#) на стр. 35).
 - 2 Установите его на ПАК ViPNet PKI Service (на стр. 39).
-

Получение сертификата

Сертификат издается в УЦ по запросу, в котором указываются необходимые данные. Изданный сертификат и соответствующие ключи могут храниться в папке на диске, внешнем устройстве (токене) или на ПАК ViPNet PKI Service.

Чтобы создать запрос на сертификат:

1 Выполните одно из действий:

- [Перейдите в настройки ViPNet PKI Client](#) (на стр. 19), выберите раздел  Сертификаты и нажмите  Создать запрос.
- В меню Пуск выберите ViPNet >  Создание запроса на сертификат.

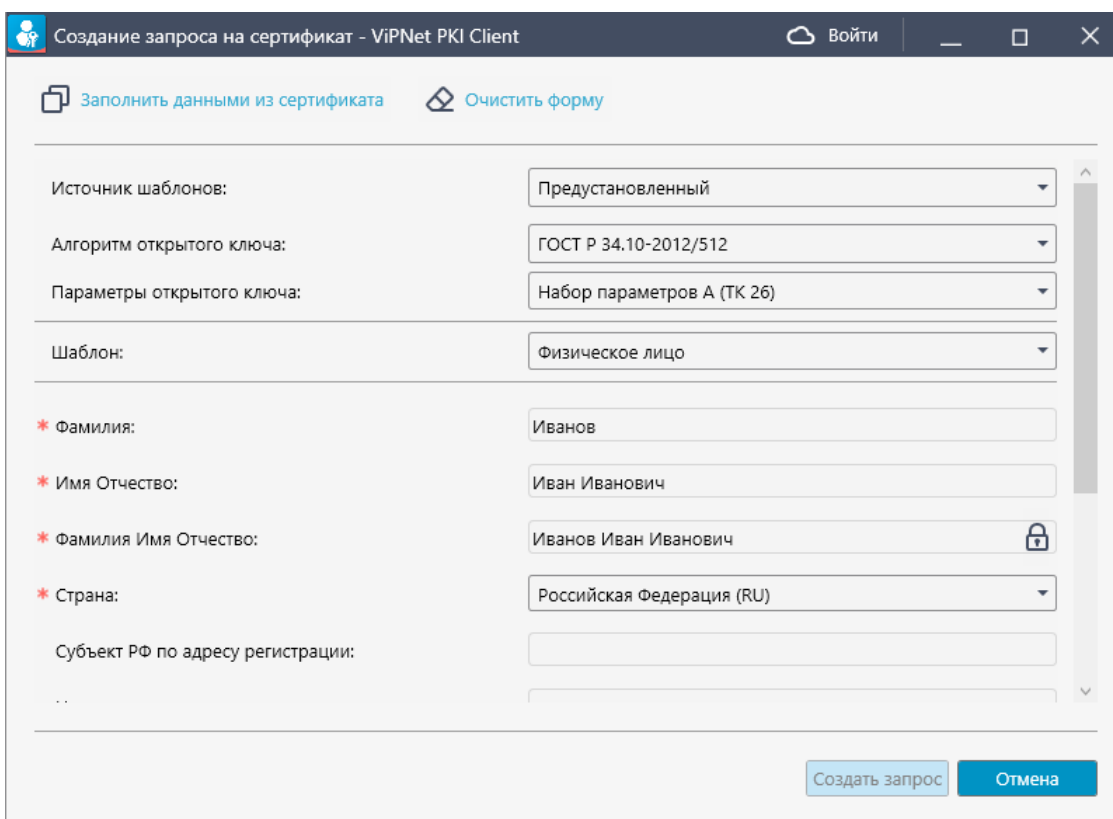



Рисунок 5. Создание запроса на сертификат



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

2 Выберите **Источник шаблонов**:

- **Предустановленный** — чтобы использовать добавленные по умолчанию шаблоны и сохранить контейнер ключей на диске или внешнем устройстве.
- **Пользовательский** — если в вашей организации требуется, чтобы в поле сертификата **Субъект (Subject)** присутствовали только определенные атрибуты:
 - Подготовьте файл в формате JSON (см. [Подготовка файла шаблона в формате JSON](#) на стр. 37) или XML (см. [Подготовка файла шаблона в формате XML](#) на стр. 37).
 - Задайте в подготовленном файле нужные атрибуты и загрузите в окно создания запроса на сертификат.

При создании запроса контейнер ключей можно сохранить на диске или внешнем устройстве.

- **Облачный** — чтобы использовать шаблоны, добавленные на ViPNet PKI Service, и сохранить контейнер ключей на ПАК ViPNet PKI Service. В этом случае требуется [настройка подключения к ПАК ViPNet PKI Service](#) (на стр. 59) и авторизация на нем.
- 3 Выберите **алгоритм** и **параметры открытого ключа** или оставьте значение по умолчанию.
 - 4 Выберите **Шаблон** сертификата и **Назначение сертификата** (если к качеству шаблона вы выбрали **Облачный**). **Шаблон** содержит разное количество и наименование атрибутов, которые попадут в поле сертификата **Субъект (Subject)**. **Назначение сертификата** содержит разное количество идентификаторов (OID), которые попадут в поле сертификата **Улучшенный ключ**.
 - 5 Заполните личные данные.
 - 6 В поле **Идентификация заявителя** выберите способ идентификации пользователя при получении сертификата. Например, чтобы получать лично, выберите **Личное присутствие**.
 - 7 Нажмите **Создать запрос**.
 - 8 Укажите имя и папку для сохранения файла запроса и нажмите **Сохранить**.
 - 9 Если контейнер ключей был сохранен не на ViPNet PKI Service (**Облачный**), в окне **ViPNet CSP — инициализация контейнера ключей**:
 - Укажите имя и место для сохранения **контейнера ключей** (см. глоссарий, стр. 110).
 - Задайте пароль для работы с контейнером ключей. Чтобы в дальнейшем не вводить пароль, установите флажок **Сохранить пароль**.
 - 10 В окне **Электронная рулетка** отобразится процесс инициализации генератора случайных чисел. Следуйте указаниям в этом окне.
 - 11 В окне сообщения об успешном создании файла запроса на сертификат выполните одно из действий:
 - Перейдите в папку с запросом.
 - Создайте еще один запрос.
 - Закройте окно.
 - 12 Передайте запрос в УЦ и получите личный сертификат, сертификаты издателей и соответствующие CRL.

После получения сертификатов установите их в хранилище или на ПАК ViPNet PKI Service (см. [Установка сертификатов и CRL](#) на стр. 39).

Подготовка файла шаблона в формате JSON

Атрибуты, которые будут добавлены в поле **Субъект (Subject)**, могут быть заданы с помощью файла шаблона в формате *.json.

Файл шаблона в формате JSON должен иметь вид:

```
[
  {
    "FieldName": "Название параметра",
    "FieldValue": "Значение по умолчанию",
    "FieldAttribute": "Атрибут",
    "ValidationRegExp": "Ограничение",
    "ValidationErrorText": "Текст ошибки"
  },
  ...
  {
    "FieldName": "Название параметра",
    "FieldValue": "Значение по умолчанию",
    "FieldAttribute": "Атрибут",
    "ValidationRegExp": "Ограничение",
    "ValidationErrorText": "Текст ошибки"
  }
]
```

Где:

- `FieldName` — название атрибута, отображаемое в списке **Поля сертификата**.
- `FieldValue` — значение атрибута, заданное по умолчанию.
- `FieldAttribute` — атрибут поля сертификата **Субъект (Subject)** в соответствии со [стандартом X.509](#), например, SN — фамилия владельца, O — компания и так далее.
- `ValidationRegExp` — ограничение на ввод данных с помощью регулярных выражений, например, `^\d*$` — возможен ввод только цифр (неограниченное количество).
- `ValidationErrorText` — текст ошибки при несоответствии введенного значения регулярному выражению.

Подготовка файла шаблона в формате XML

Список атрибутов, которые будут добавлены в поле **Субъект (Subject)**, могут быть заданы с помощью файла шаблона в формате *.xml.

Файл шаблона должен иметь вид:

```
<?xml version="1.0" encoding="utf-8"?>
<RequestTemplate>
  <Field attribute="Атрибут" name="Название параметра" value="Значение по умолчанию"
  validationRegExp="Ограничение" validationErrorText="Текст ошибки"/>
  ...
  <Field attribute="Атрибут" name="Название параметра" value="Значение по умолчанию"
  validationRegExp="Ограничение" validationErrorText="Текст ошибки"/>
</RequestTemplate>
```

Где:

- `attribute` — атрибут поля сертификата **Субъект (Subject)** в соответствии со [стандартом X.509](#), например, SN — фамилия владельца, O — компания и так далее.
- `name` — название атрибута, отображаемое в списке **Поля сертификата**.
- `value` — значение атрибута, заданное по умолчанию.
- `validationRegExp` — ограничение на ввод данных с помощью регулярных выражений, например, `^\d*$` — возможен ввод только цифр (неограниченное количество).
- `validationErrorText` — текст ошибки при несоответствии введенного значения регулярному выражению.

Установка сертификатов и CRL

Описанными ниже способами устанавливайте только те личные сертификаты, запрос на которые был создан в ViPNet PKI Client (см. [Получение сертификата](#) на стр. 35). Если вы получали сертификат иным способом, см. [Подготовка личного сертификата](#) (на стр. 33).

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

Установка с помощью ViPNet PKI Client

- 1 [Перейдите в настройки ViPNet PKI Client](#) (на стр. 19).




Примечание. Чтобы установить сертификаты издателей и CRL в хранилище сертификатов локального компьютера, запустите настройки ViPNet PKI Client от имени администратора.




- 2 В разделе  **Сертификаты** выполните одно из действий:



- Перетащите файлы сертификатов и (или) CRL на панель просмотра.




Примечание. При запуске настроек ViPNet PKI Client от имени администратора данный способ недоступен.


- Нажмите  **Добавить сертификат или CRL**, укажите путь к файлам сертификатов и (или) CRL.
- 3 В окне **Добавление сертификатов** отображается список устанавливаемых сертификатов и CRL. В этом списке:

-  **Личный** — личные сертификаты, запрос на которые был создан в ViPNet PKI Client или ViPNet CSP, а контейнер ключей сохранен на диске или внешнем устройстве (токене). Сертификаты будут установлены в хранилище сертификатов текущего пользователя **Личное**. Если нужно установить сертификат в контейнер ключей, установите соответствующий флажок, введите пароль контейнера ключей или ПИН внешнего устройства и нажмите **Ввести**.
-  **Издатель** — сертификаты УЦ. Корневые сертификаты устанавливаются в хранилище **Доверенные корневые центры сертификации**, промежуточные — **Промежуточные центры сертификации**.
-  **Другой** — сертификаты получателей. Устанавливаются в хранилище **Другие пользователи**.

-  **CRL** — списки аннулированных сертификатов. Устанавливаются в хранилище **Промежуточные центры сертификации > Список отзыва сертификатов**.
-  **Облачный** — сертификаты, контейнеры ключей которых сохранены на ПАК ViPNet PKI Service. Такие сертификаты будут установлены на ПАК ViPNet PKI Service.

Сертификаты и CRL с истекшим сроком действия или имеющие недействительную ЭП отмечаются значком  и не будут установлены в хранилище сертификатов.

При необходимости вы можете:

- 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).

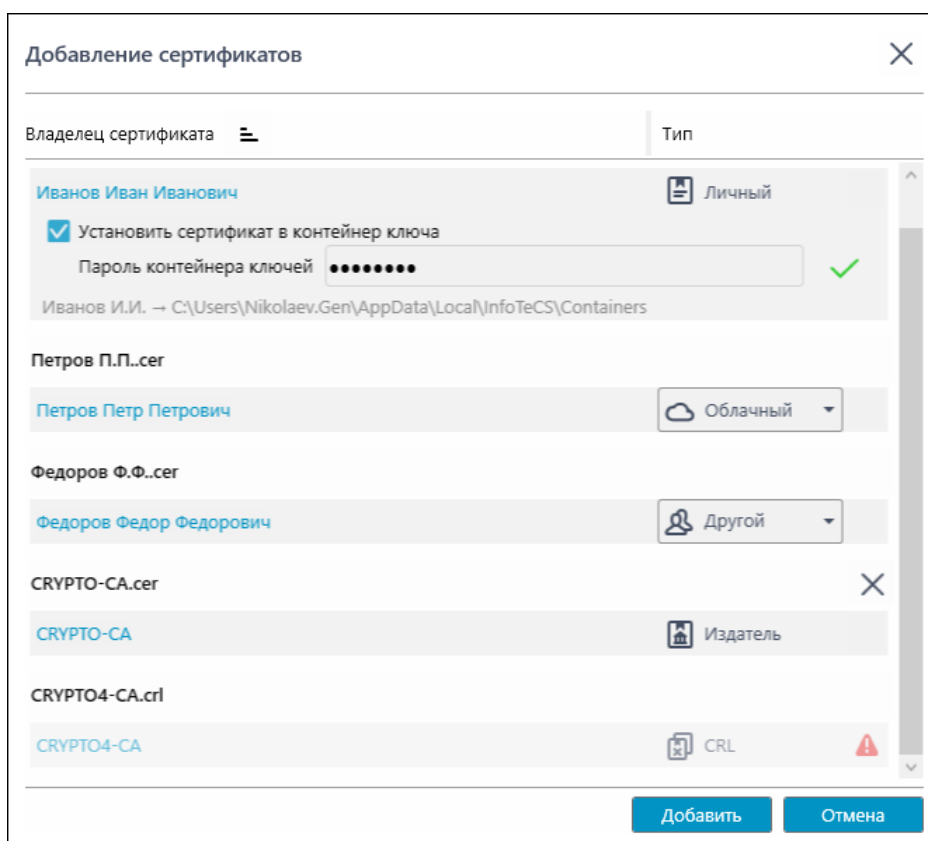





Рисунок 6. Установка сертификатов и CRL в ViPNet PKI Client

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


При установке корневых сертификатов издателей появится окно **Предупреждение системы безопасности**, в котором вам будет предложено установить сертификат. Чтобы установить сертификат, нажмите **Да**.

Результат установки отмечается значком напротив каждого установленного сертификата и CRL:

-  — установка выполнена успешно;

-  — во время установки произошла ошибка;
-  — сертификат или CRL уже установлен в системное хранилище.



Примечание. Если после установки сертификата в строке имени владельца сертификата появится предупреждающее сообщение, наведите курсор на значок , просмотрите подробные сведения об ошибках и устраните их (см. [Проверка сертификатов](#) на стр. 47).

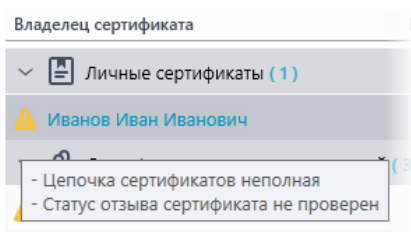


Рисунок 7. Просмотр предупреждающих сообщений

Установка с помощью контекстного меню Windows

Установка с помощью контекстного меню Windows

Вы можете устанавливать сертификаты и CRL с помощью контекстного меню Windows без вызова окна **Настройки - ViPNet PKI Client**. Установленные таким способом сертификаты появятся в ViPNet PKI Client.



Примечание. Если вы работаете не под учетной записью администратора Windows, при установке сертификата издателя он будет установлен в системное хранилище текущего пользователя, то есть будет доступен только текущему пользователю.

Для установки сертификатов или CRL с помощью контекстного меню Windows выделите их, щелкните правой кнопкой мыши и выберите **ViPNet PKI Client > Установить сертификат/список отзыва**.

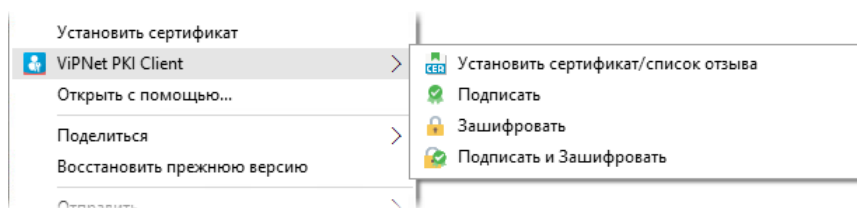


Рисунок 8. Установка сертификатов и CRL с помощью контекстного меню Windows


Экспорт сертификатов

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




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

Чтобы экспортировать сертификат в файл:

- 1 [Перейдите в настройки ViPNet PKI Client](#) (на стр. 19).
- 2 Выберите раздел  **Сертификаты**.
- 3 Щелкните сертификат правой кнопкой мыши и в контекстном меню выберите **Экспорт в CER-файл**.
- 4 В открывшемся окне укажите папку для сохранения файла и нажмите **Сохранить**.
- 5 Чтобы перейти в папку с файлом сертификата, в окне сообщения об успешном экспорте сертификата нажмите **Открыть папку назначения**.
- 6 Нажмите **Закрыть**.





Примечание. Также для экспорта сертификата в файл вы можете навести указатель мыши на значок  (появляется при выборе сертификата в списке) и перетащить его в нужную папку.

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 одном 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. 19).
- 2 Выберите раздел  Сертификаты.
- 3 Нажмите  и выберите **Личные сертификаты**.
- 4 Щелкните правой кнопкой мыши выбранный сертификат и в контекстном 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.


- 5 В окне **Экспорт в PFX-файл**:
 - 5.1 Введите пароль контейнера ключей.
 - 5.2 Задайте пароль к PFX-файлу.
 - 5.3 Укажите имя и путь для сохранения PFX-файла.
 - 5.4 Нажмите **Экспортировать**.



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



Внимание! Файл *.pfx защищен паролем, но 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. 19).
- 2 Выберите раздел  Сертификаты.

- 3 Нажмите  **Добавить сертификат или CRL** и укажите путь к файлу *.pfx, полученному в результате экспорта или перетащите его в окно настроек.
- 4 Чтобы в дальнейшем сертификат и ключ ЭП нельзя было экспортировать в PFX-файл, нажмите значок .
- 5 Введите пароль PFX-файла и нажмите **Ввести**.

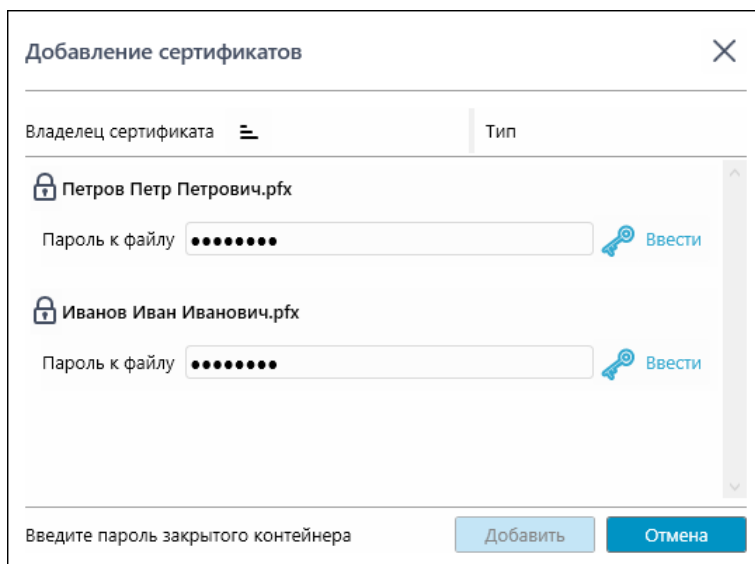


Рисунок 9. Ввод пароля для импорта сертификата с закрытым ключом

- 6 В окне ViPNet CSP — инициализация контейнера ключей укажите имя [контейнера ключей](#) (см. глоссарий, стр. 110) и его месторасположение. Нажмите **ОК**.
- 7 В окне ViPNet CSP — **пароль контейнера ключей** задайте пароль для работы с контейнером ключей. Чтобы в дальнейшем не повторять ввод пароля, выберите **Сохранить пароль**.
- 8 Выполните шаги 4-7 для других сертификатов и нажмите **Добавить**.

В результате сертификаты и ключи ЭП будут установлены в контейнеры ключей, а также сертификаты будут установлены в хранилище.




Просмотр сертификатов


Вы можете просмотреть сертификаты пользователей, установленные в 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 ViPNet PKI Client не предусмотрен.

Для просмотра информации о сертификате:

- 1 [Перейдите в настройки ViPNet PKI Client](#) (на стр. 19).
- 2 Выберите раздел  **Сертификаты**.
- 3 На панели инструментов нажмите  и выберите группу сертификатов:
 - **Все сертификаты** (выбрана по умолчанию).
 - **Личные сертификаты**.
 - **Сертификаты других пользователей**.
 - **Сертификаты на внешних устройствах**.
 - **Сертификаты в облаке** (для просмотра нужно подключиться к ПАК ViPNet PKI Service).
- 4 По умолчанию ViPNet PKI Client предупредит об истечении срока действия сертификатов за 60 дней. Вы можете изменить этот срок. Для этого на панели инструментов щелкните .

Примечание. Чтобы изменить состав отображаемых столбцов, нажмите  и установите соответствующие флажки.



Чтобы изменить порядок расположения столбцов, используйте перетаскивание.

Чтобы отсортировать сертификаты по любому столбцу, дважды щелкните название столбца.

Чтобы отфильтровать список сертификатов, в поле поиска введите часть имени владельца или издателя сертификата.

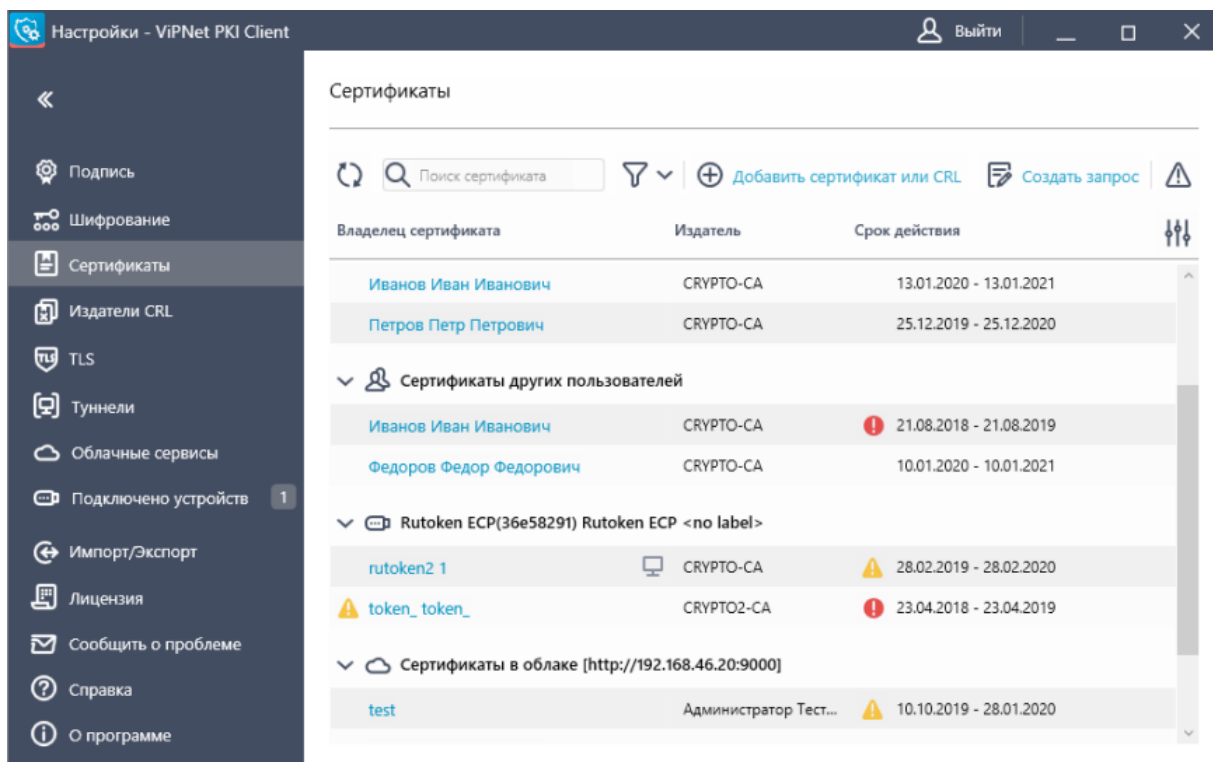


Рисунок 10. Просмотр установленных сертификатов

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

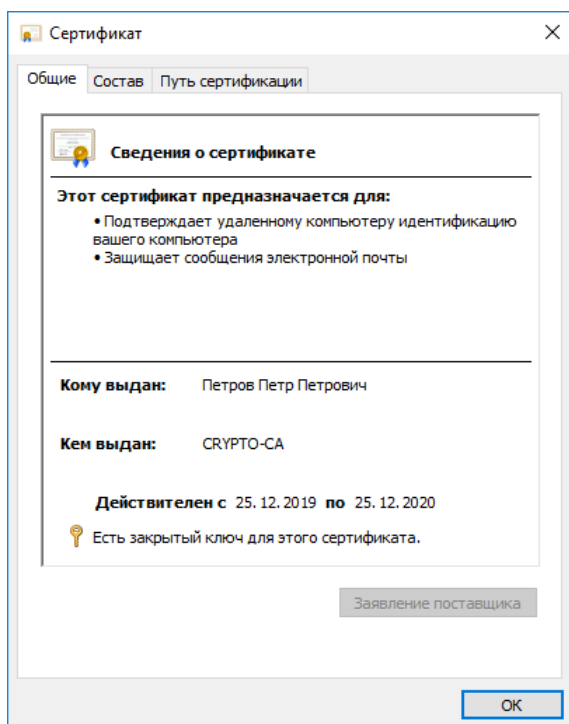


Рисунок 11. Просмотр сведений о сертификате

Проверка сертификатов

Предупреждающие сообщения информируют пользователя о невозможности использования установленных сертификатов для подписания, зашифрования, расшифрования.

Во время установки сертификатов ViPNet PKI Client проверяет сертификаты на соответствие следующим требованиям:


- Срок действия сертификата наступил и не истек.
- Сертификат не аннулирован (не находится в CRL доверенного УЦ).
- Цепочка сертификатов полна, и все входящие в нее сертификаты УЦ действительны.

Вы можете проверить установленные сертификаты вручную. Для этого:

1 [Перейдите в настройки ViPNet PKI Client](#) (на стр. 19).

2 Выберите раздел  **Сертификаты**.

3 На панели инструментов нажмите .

В случае если устанавливаемый сертификат не соответствует указанным требованиям, в строке с именем владельца сертификата появится значок . Наведите курсор на значок, чтобы просмотреть предупреждающие сообщения:

- **Цепочка сертификации неполная**

В хранилище установлены не все сертификаты, образующие цепочку.

Установите в хранилище недостающие сертификаты, чтобы образовалась полная цепочка (см. [Установка сертификатов и CRL](#) на стр. 39).

- **Сертификат отозван**

Сертификат или один из сертификатов, образующих цепочку, аннулирован.

Получите новый сертификат (см. [Получение сертификата](#) на стр. 35) и установите его в хранилище (см. [Установка сертификатов и CRL](#) на стр. 39).

- **Сертификат в цепочке содержит недействительную ЭП**

Сертификат или один из сертификатов, образующих цепочку, искажен.

Переустановите все сертификаты, образующие цепочку.

- **Срок действия ключа ЭП истек**

Истек срок действия ключа ЭП.

Выполните одно из действий:

- Если вы устанавливаете личный сертификат, получите новый сертификат (см. [Получение сертификата](#) на стр. 35) и установите его в хранилище (см. [Установка сертификатов и CRL](#) на стр. 39).

- Если вы устанавливаете сертификат получателя, запросите у получателя новый сертификат.
- **Статус отзыва сертификата не проверен**



Возможные причины:

- В хранилище сертификатов не установлен CRL.
- В хранилище сертификатов установлен CRL с истекшим сроком действия.
- ЭП CRL неверна.

[Установите актуальный CRL в хранилище](#) (на стр. 39).

Удаление сертификатов


Чтобы удалить аннулированные сертификаты и сертификаты с истекшим сроком действия:

- 1 [Перейдите в настройки ViPNet PKI Client](#) (на стр. 19).
- 2 Выберите раздел  Сертификаты.
- 3 На панели инструментов нажмите  и в списке выберите группу сертификатов.
- 4 Щелкните сертификат правой кнопкой мыши и в контекстном меню выберите **Удалить**.
- 5 Выберите **Подтверждаю удаление <имя владельца сертификата>**.
- 6 Чтобы удалить ключ ЭП, соответствующий сертификату, например при аннулировании сертификата, установите соответствующий флажок и нажмите **Удалить сертификат**.



Примечание. Пункт **Удалить ключ ЭП данного сертификата** не отображается, если сертификат не содержит информации о расположении ключа ЭП (например, при удалении сертификата получателя).

Удалить сертификат ✕

Подтвердите удаление сертификата из хранилища  Личные сертификаты

Подтверждаю удаление **Иванов Иван Иванович**
Создание электронной подписи на данном сертификате будет невозможно

Удалить **ключ ЭП** данного сертификата
Ключ электронной подписи не подлежит восстановлению! Создание подписи на данном ключе будет невозможно

Удалить сертификат **Закрыть**

Рисунок 12. Подтверждение удаления сертификата



Внимание! Ключ ЭП не подлежит восстановлению. Создание ЭП с использованием данного ключа будет невозможно.

5

Автоматическое обновление CRL

Добавление точек распространения CRL	51
Отслеживание событий при автообновлении CRL	53

Добавление точек распространения CRL





Если в сертификатах пользователей и промежуточных сертификатах УЦ содержатся URL точек распространения списков аннулированных сертификатов, CRL будут обновляться автоматически.

Если URL точек распространения нет в сертификатах, для автоматического обновления CRL добавьте их в ViPNet PKI Client:



Примечание. Автоматическое обновление CRL из точек распространения можно настроить только для сертификатов издателей, установленных в хранилище локального компьютера.

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

- 1 [Перейдите в настройки ViPNet PKI Client](#) (на стр. 19).
- 2 Выберите раздел  **Издатели CRL**.
- 3 В левой части панели просмотра нажмите  **Добавить**.
- 4 Выберите сертификат издателя и нажмите **Выбрать**.
- 5 В правой части панели просмотра нажмите  **Добавить**.
- 6 Задайте URL точки распространения, период ее опроса и нажмите .
- 7 Если необходимо, добавьте URL и период опроса следующей точки.

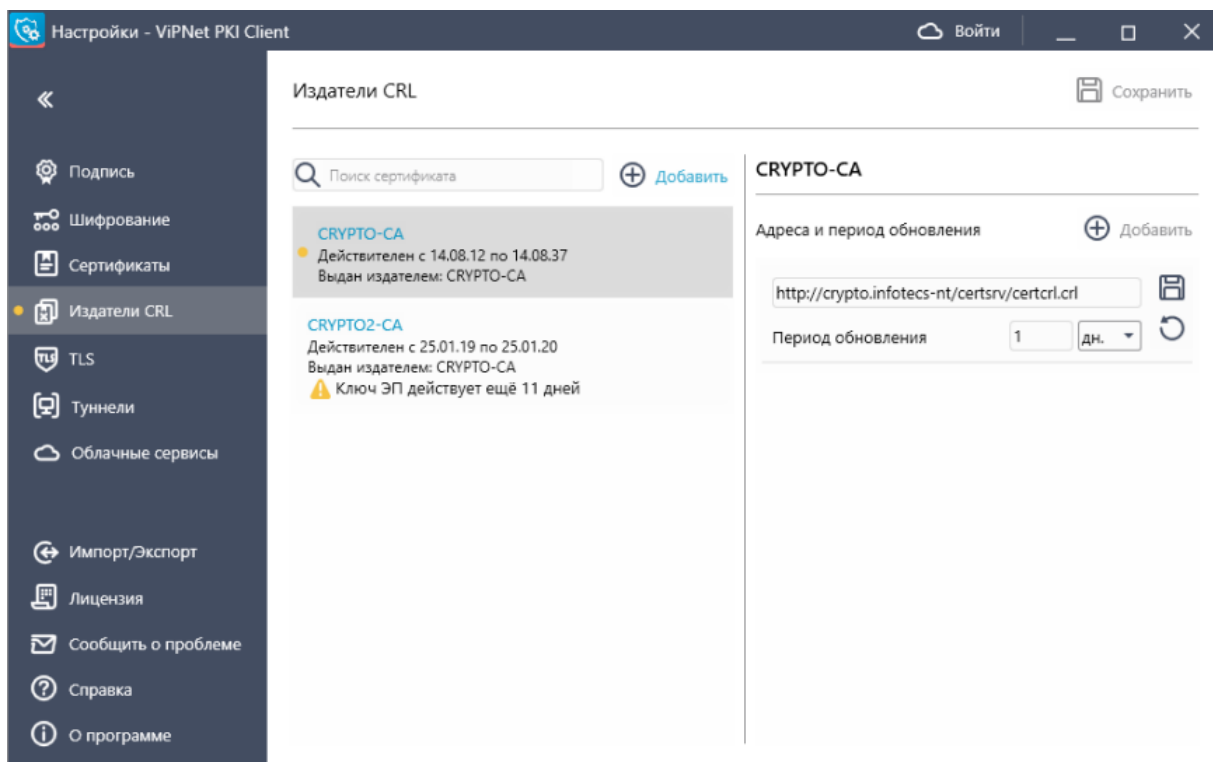




Рисунок 13. Добавление точки распространения

8 Нажмите  Сохранить.

В результате актуальные CRL будут автоматически скачиваться и устанавливаться в хранилище сертификатов **Промежуточные центры сертификации > Список отзыва сертификатов.**



Примечание. Чтобы отредактировать или удалить точку распространения CRL, выберите ее и нажмите  или  соответственно.

Отслеживание событий при автообновлении CRL

Загрузка CRL в ViPNet PKI Client выполняется с помощью службы ViPNet PKI Client CRL Unit Service. Для отслеживания информации о работе службы:

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

Чтобы изменить настройки записи событий, отредактируйте файл конфигурации:

- 1 Перейдите в одну из папок (если в процессе установки ViPNet PKI Client не была указана другая папка):
 - в 32-разрядных версиях Windows — `C:\Program Files\InfoTeCS\ViPNet PKI Client\CRL Unit`;
 - в 32-разрядных версиях Windows — `C:\Program Files (x86)\InfoTeCS\ViPNet PKI Client\CRL Unit`.
- 2 Откройте в текстовом редакторе, поддерживающем кодировку текста UTF-8, файл конфигурации `crlunit.cfg` (на стр. 53).
- 3 Измените настройки:
 - `<dir>` — папка, в которой будут храниться журналы событий;
 - `<rotationsize>` — максимальный размер файла для записи событий (МБ);
 - `<maxsize>` — максимальный размер всех файлов с событиями (МБ);
 - `<level>` — тип событий, которые будут записываться в файл;
 - Если в вашей организации доступ в Интернет осуществляется через один или несколько прокси-серверов, в секции `<proxy-settings>` задайте параметры подключения к прокси-серверам.
- 4 Сохраните изменения.
- 5 Перезапустите службу ViPNet PKI Client CRL Unit Service стандартными средствами Windows (см. [Остановка и запуск службы ViPNet PKI Client CRL Unit Service](#) на стр. 55).

Файл конфигурации `crlunit.cfg`

Файл конфигурации `crlunit.cfg` содержит настройки записи событий, происходящих при работе службы ViPNet PKI Client CRL Unit.

Структура файла конфигурации crlunit.cfg

Элемент	Допустимые вложенные элементы	Описание
certagent	logging proxy-settings	Корневой элемент документа.
logging	<ul style="list-style-type: none">• dir• rotationsize• maxsize• level	Настройки записи событий.
dir		Папка сохранения файлов журнала событий. Путь к папке сохранения может содержать переменные окружения, например, %PROGRAMDATA%.
rotationsize		Максимальный размер файла в МБ, при достижении которого создается новый файл для записи событий.
maxsize		Суммарный максимальный размер в МБ всех файлов с записанными событиями. При достижении этого размера из папки будут удалены файлы, начиная с файла с самой ранней датой создания.
level		Параметр, определяющий, запись каких событий будет выполняться: <ul style="list-style-type: none">• 0 — все типы событий, включая отладочные;• 1 — все типы событий, кроме отладочных (значение по умолчанию);• 2 — предупреждения и ошибки;• 3 — только ошибки.
proxy-settings		Сведения о прокси-сервере, если доступ в Интернет организован через прокси-сервер. Атрибуты <proxy settings>: <ul style="list-style-type: none">• proxy addr — IP-адрес или DNS-имя прокси-сервера и порт для подключения к нему.• protocol — это тип протокола, с помощью которого клиент соединяется с прокси-сервером (http, ftp, ldap, all).• authtype — метод аутентификации на сервере basic, digest, negotiate, ntlm, any.

Пример файла конфигурации crlunit.cfg

```
<?xml version="1.0" encoding="utf-8"?>
<certagent>
  <logging>
    <dir>%PROGRAMDATA%\InfoTeCS\ViPNet PKI Client\CRL Unit\Logs</dir>
```

```
<rotationsize>10</rotationsize>
<maxsize>200</maxsize>
<level>1</level>
</logging>

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

</certagent>
```

Остановка и запуск службы ViPNet PKI Client CRL Unit Service

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

После изменения файла конфигурации `crlunit.cfg` перезапустите службу стандартными средствами Windows:

- 1 Нажмите сочетание клавиш **Win+R**.
- 2 В окне **Выполнить** в поле **Открыть** введите `services.msc`.
- 3 В открывшемся окне на панели навигации выберите **Службы**.
- 4 На панели просмотра выберите службу **ViPNet PKI Client CRL Unit Service**.
- 5 Вызовите контекстное меню и выберите **Остановить**.
- 6 Еще раз вызовите контекстное меню и выберите **Запустить**.

6

Использование облачных сервисов ЭП

Об облачных сервисах ЭП	57
Перед подключением к ПАК ViPNet PKI Service	58
Настройка подключения к ПАК ViPNet PKI Service	59
Подключение к ПАК ViPNet PKI Service	61
Смена пароля учетной записи пользователя	62

Об облачных сервисах ЭП

Использование облачных сервисов ЭП удобно в корпоративных сетях, в которых пользователи взаимодействуют друг с другом в рамках электронного документооборота. С помощью облачного сервиса ЭП пользователи могут выполнять различные операции: подписывать файлы, проверять ЭП, зашифровывать и расшифровывать данные.

Если в вашей компании используется облачный сервис ЭП на базе ПАК ViPNet PKI Service 2.0, вы можете работать с ним из интерфейса ViPNet PKI Client.



Внимание! В ViPNet PKI Client поддерживается только выполнение операций, не требующих подтверждения пользователя.

Перед подключением к ПАК ViPNet PKI Service

1 Получите у оператора сервера подписи:

- Адрес ПАК ViPNet PKI Service.
- Способ подключения и дополнительные данные (см. таблицу).

Таблица 2. Способы подключения и дополнительные данные

Способ подключения	Дополнительные данные
По протоколу HTTP с помощью имени учетной записи и пароля	Имя учетной записи и разовый пароль.
По протоколу HTTPS (TLS ГОСТ) с помощью имени учетной записи и пароля	<ul style="list-style-type: none">• Имя учетной записи и разовый пароль.• Корневой и промежуточные сертификаты издателей сертификата ПАК ViPNet PKI Service и CRL.
По протоколу HTTPS (TLS ГОСТ) с помощью сертификата	<ul style="list-style-type: none">• Корневой и промежуточные сертификаты издателей сертификата ПАК ViPNet PKI Service и CRL.• Список УЦ, в которых можно получить сертификат для подключения к ПАК ViPNet PKI Service.






2 Для подключения по протоколу HTTPS [установите полученные сертификаты издателей и CRL](#) (на стр. 39).

3 Для подключения с помощью сертификата подготовьте его:

- 3.1 Чтобы сохранить ключ ЭП, а затем и сертификат на токене, подключите его к компьютеру.
- 3.2 Создайте запрос на сертификат (см. [Получение сертификата](#) на стр. 35).
- 3.3 Передайте его в УЦ из полученного списка.
- 3.4 Получите личный сертификат, корневой и промежуточные (если есть) сертификаты издателей и CRL.
- 3.5 [Установите полученные сертификаты и CRL](#) (на стр. 39):
 - Корневые и промежуточные сертификаты издателей и CRL — в хранилище.
 - Личный — в хранилище или в хранилище и на токен.
- 3.6 Если личный сертификат и ключ ЭП хранятся не на токене, импортируйте их на Infotecs Software Token (см. [Импорт сертификата и ключа ЭП из хранилища](#) на стр. 75).
- 3.7 Передайте личный сертификат оператору сервера подписи. После его добавления в вашу учетную запись вы сможете подключиться к ПАК ViPNet PKI Service.

После этого [настройте подключение к ПАК ViPNet PKI Service](#) (на стр. 59).

Настройка подключения к ПАК ViPNet PKI Service

- 1 Перейдите в настройки ViPNet PKI Client (на стр. 19).
- 2 Выберите раздел  **Облачные сервисы**.
- 3 Включите  **Использовать функции облачного сервиса**.
- 4 Нажмите  **Добавить** и укажите:
 - Название облачного сервиса.
 - Адрес и порт ПАК ViPNet PKI Service.
 - Способ аутентификации. При выборе способа аутентификации **Сертификат** выберите сертификат для подключения к ПАК ViPNet PKI Service.
 - Нажмите .
- 5 Чтобы проверить соединение с ПАК ViPNet PKI Service, нажмите .

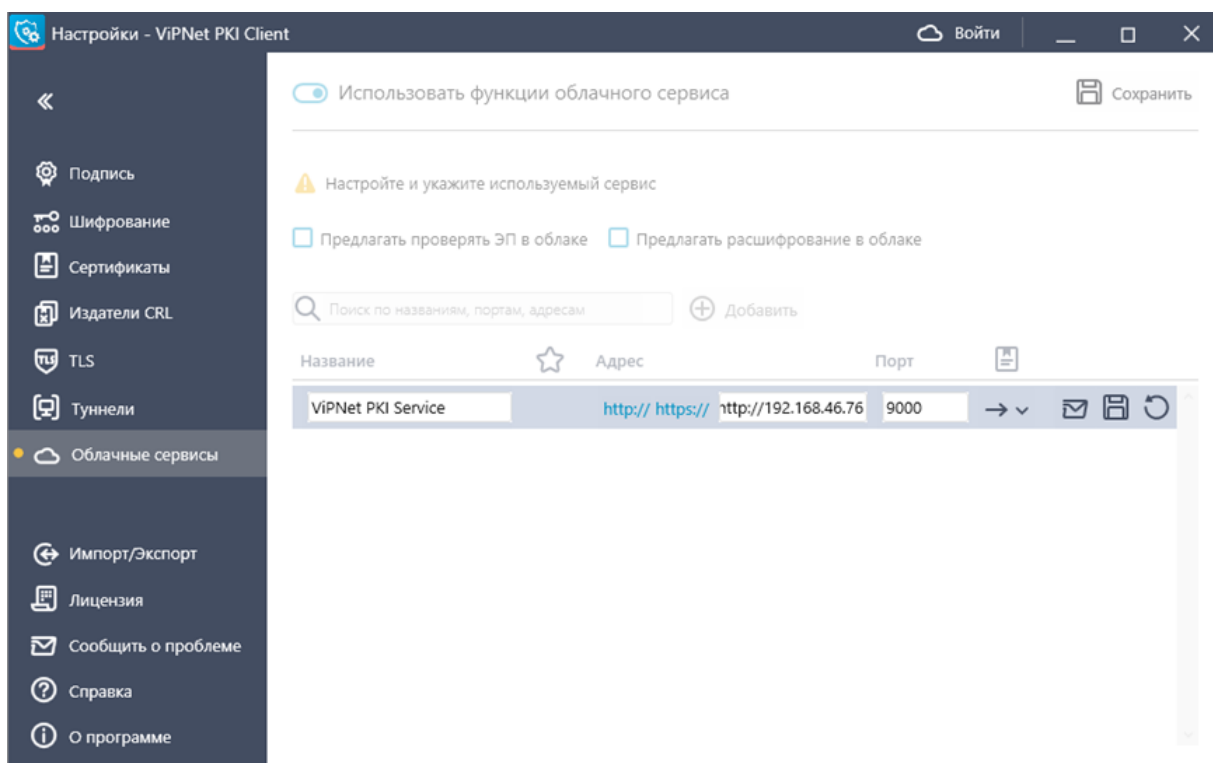



Рисунок 14. Настройка подключения к облачному сервису ЭП (на базе ViPNet PKI Service)

- 6 Чтобы ViPNet PKI Client предлагал проверять подпись на ПАК ViPNet PKI Service, если при проверке подписи не удалось проверить сертификат подписанта с помощью сертификатов, установленных в хранилище, выберите **Предлагать проверять ЭП в облаке**.

- 7 Чтобы ViPNet PKI Client предлагал расшифровывать файл на ПАК ViPNet PKI Service, если подходящий для расшифрования сертификат не найден в хранилище, выберите **Предлагать расшифрование в облаке**.
- 8 Если вы добавили несколько ПАК ViPNet PKI Service, в списке **Используемый сервис** выберите ПАК ViPNet PKI Service, к которому будете подключаться по умолчанию.
- 9 В верхней части окна нажмите  **Сохранить**.

Теперь вы можете [подключиться к ПАК ViPNet PKI Service](#) (на стр. 61).

Подключение к ПАК ViPNet PKI Service


После настройки ViPNet PKI Client будет подключаться к ПАК ViPNet PKI Service в следующих случаях:

- При выполнении операций с помощью сертификатов и ключей ЭП, хранящихся на ПАК ViPNet PKI Service.
- При просмотре и выборе сертификатов для подписи, хранящихся на ПАК ViPNet Service.
- При создании запроса на сертификат с помощью шаблона **Облачный**.

Подключение с помощью сертификата

- 1 Запустите программу [TLS Unit](#) (на стр. 19) и переведите ее в состояние **Работает** (см. [TLS Unit](#) на стр. 19).
- 2 Если сертификат для подключения хранится на токене, введите ПИН-код в окне подключения.

Подключение с помощью логина и пароля

- 1 Для подключения по протоколу HTTPS запустите программу [TLS Unit](#) (на стр. 19) и переведите ее в состояние **Работает** (см. [TLS Unit](#) на стр. 19).
- 2 Перейдите в настройки [ViPNet PKI Client](#) (на стр. 19).
- 3 На панели заголовка нажмите  **Войти**.
- 4 Введите ваши учетные данные и нажмите **Войти**.

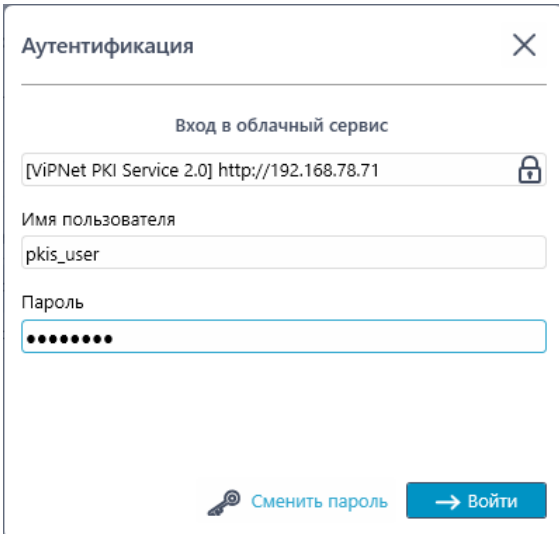





Рисунок 15. Подключение к ПАК ViPNet PKI Service с помощью логина и пароля

Продолжительность сессии — 1 час. После этого потребуется повторное подключение.

Смена пароля учетной записи пользователя

Я знаю свой пароль и хочу его сменить

- 1 [Перейдите в настройки ViPNet PKI Client](#) (на стр. 19).
- 2 В разделе  **Облачные сервисы** выберите **Используемый сервис**.
- 3 На панели заголовка нажмите  **Войти**.
- 4 Введите ваши учетные данные и нажмите  **Сменить пароль**.
- 5 Введите и повторите новый пароль и нажмите **Изменить**.

Я забыл пароль и хочу получить новый

Обратитесь к оператору сервера подписи и получите разовый пароль. При первом подключении его нужно будет сменить на постоянный.

7

Подпись и шифрование файлов

Требования к сертификатам для подписи и шифрования	64
Настройка параметров ЭП	65
Настройка параметров шифрования	68
Настройка сетевых параметров	70

Требования к сертификатам для подписи и шифрования

Для подписи и шифрования файлов вам нужны сертификаты, для которых выполняется следующее:



- Сертификат действителен:
 - срок действия сертификата наступил и не истек;
 - сертификат не аннулирован;
 - все сертификаты цепочки действительны и установлены в хранилище.
- Для зашифрования сертификат получателя файла:
 - установлен в хранилище сертификатов **Другие пользователи**;
 - в поле **Использование ключа** содержит хотя бы одно из назначений: **Шифрование данных**, **Шифрование ключей**, **Согласование ключей**.
- Для подписи сертификат:
 - установлен в хранилище сертификатов текущего пользователя **Личное**;
 - в поле **Использование ключа** содержит назначение **Цифровая подпись**;
 - если запрос на сертификат создан не с помощью ViPNet PKI Client, установлена связь между сертификатом и контейнером с ключом ЭП (см. «ViPNet CSP. Руководство пользователя» > «Установка сертификата в системное хранилище Windows»).



Внимание! Если ваш сертификат или сертификат получателя не соответствует выше указанным требованиям, вы не сможете выбрать его для подписи или зашифрования.

Настройка параметров ЭП

Чтобы настроить параметры ЭП, которые будут использоваться по умолчанию в File Unit и Web Unit:

- 1 Перейдите в настройки ViPNet PKI Client (на стр. 19).
- 2 В разделе  Подпись нажмите  Выбрать сертификат.
- 3 Выберите сертификат и нажмите **Выбрать**.

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

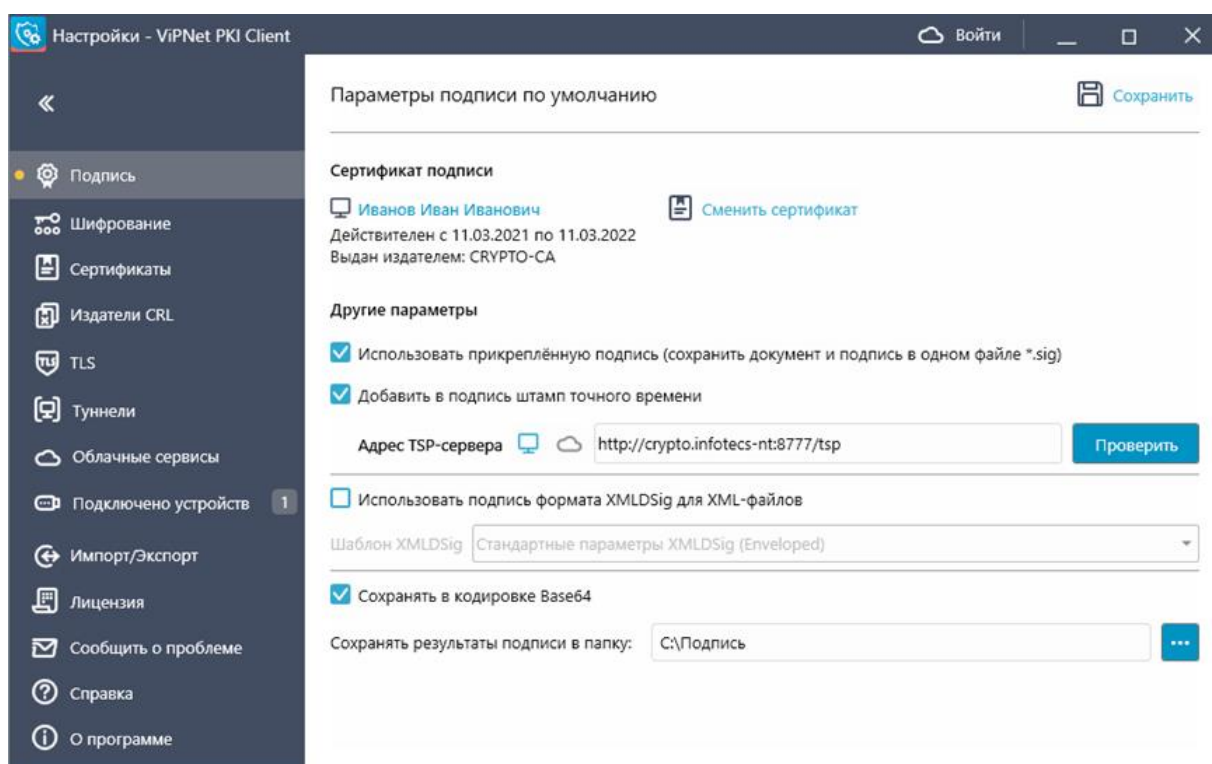


Рисунок 16. Настройка параметров ЭП

- 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** (см. глоссарий, стр. 110).
- 5 Чтобы использовать подпись формата **XMLDSig** (см. глоссарий, стр. 109) для XML-файлов, установите соответствующий флажок и выберите шаблон. По умолчанию в настройке 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/xmlsig#enveloped-signature>.

Если этот шаблон не подходит, [создайте свой](#) (на стр. 97) и [импортируйте его в настройки](#) (на стр. 66).


6 Чтобы сохранять файл подписи в кодировке Base64, выберите соответствующую настройку.

7 Чтобы добавлять к ЭП точное время подписания файла, настройте подключение к службе штампов времени:

7.1 Включите **Добавить в подпись штамп точного времени**.

7.2 Если вы не настраивали подключение к облачному сервису ЭП, в строке **Адрес TSP-сервера** укажите URL [TSP-сервера](#) (см. глоссарий, стр. 109) в формате `http://<IP-адрес или доменное имя>:<порт>/`. Поддерживаются протоколы HTTP и HTTPS. Для проверки соединения с указанным TSP-сервером нажмите **Проверить**.


7.3 Если вы настроили подключение к облачному сервису ЭП:


- Чтобы задать TSP-сервер вручную, в строке **Адрес TSP-сервера** щелкните значок  и укажите URL [TSP-сервера](#) (см. глоссарий, стр. 109) в формате `http://<IP-адрес или доменное имя>:<порт>/`. Поддерживаются протоколы HTTP и HTTPS. Для проверки соединения с указанным TSP-сервером нажмите **Проверить**.

Внимание! Чтобы использовать указанный TSP-сервер при подписании с помощью сертификата и ключа ЭП, хранящихся на ПАК ViPNet PKI Service:



- На ПАК ViPNet PKI Service должен быть установлен сертификат издателя и CRL, выпустивший сертификат TSP-сервера, а если сертификат издателя не является корневым, все сертификаты цепочки.
- ПАК ViPNet PKI Service должен иметь доступ к TSP-серверу.

-
- Чтобы использовать облачный TSP-сервер, в строке **Адрес TSP-сервера** щелкните значок  и в списке выберите TSP-сервер.

8 Нажмите  и укажите папку для сохранения подписанных файлов.

9 Нажмите  **Сохранить**.

Импорт шаблонов XML-подписи в настройки

Чтобы выбирать [свои шаблоны XML-подписи](#) (на стр. 97), импортируйте их в настройки:

1 [Перейдите в настройки ViPNet PKI Client](#) (на стр. 19).


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

3 Выполните одно из действий:

- Перетащите файл с шаблонами в выделенную область.






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

- Нажмите  **Выбрать** и выберите файл с шаблонами.
- 4 Выберите шаблоны, которые вы хотите импортировать, и нажмите **Импортировать**.

Настройка параметров шифрования

Чтобы настроить параметры шифрования, которые будут использоваться по умолчанию в File Unit и Web Unit:

- 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. 39).
- 3 [Перейдите в настройки ViPNet PKI Client](#) (на стр. 19).
- 4 Выберите раздел  **Шифрование**.
- 5 Чтобы каждый раз при шифровании файлов не приходилось выбирать сертификат получателя, сформируйте список получателей файлов:
 - 5.1 В группе **Получатели зашифрованных файлов** нажмите  **Добавить**.
 - 5.2 Выберите один или несколько сертификатов и нажмите **Выбрать**.

Чтобы удалить сертификат получателя из списка, щелкните значок  (появляется при наведении курсора на строку сертификата).

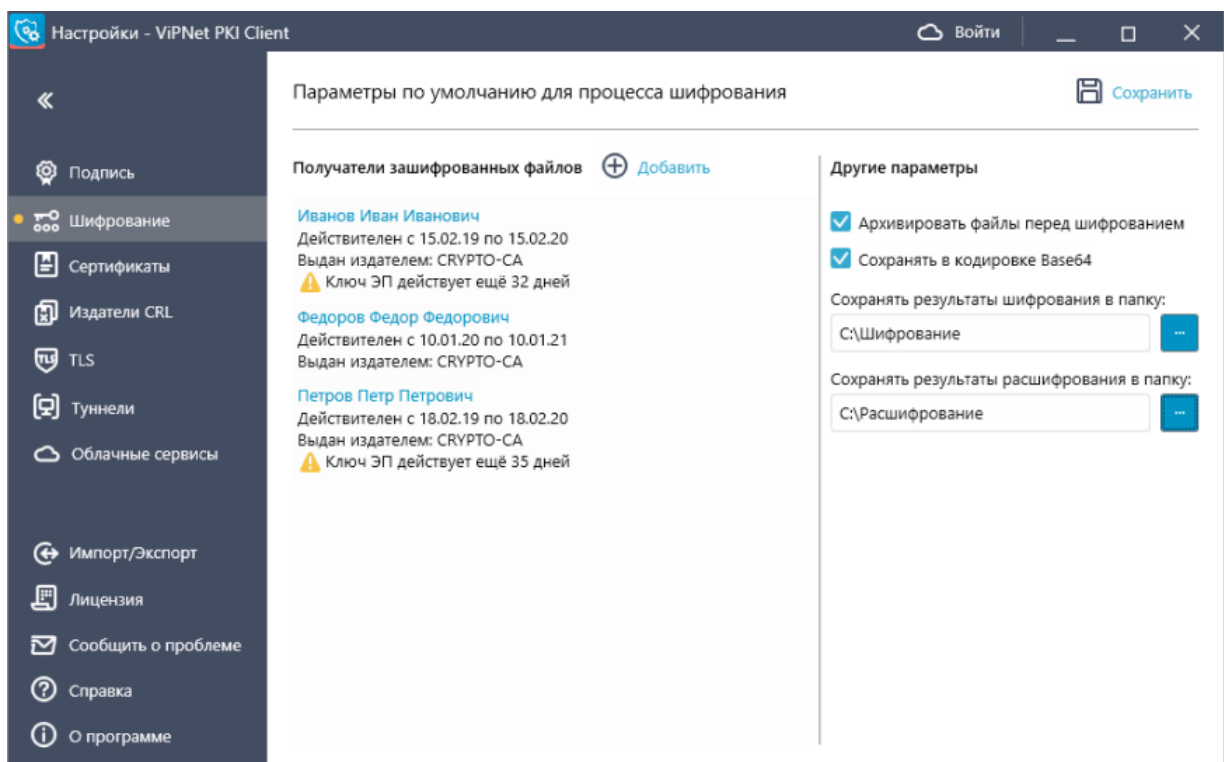




Рисунок 17. Настройка параметров шифрования

- 6 Чтобы перед шифрованием файлы помещались в архив, установите соответствующий флажок.
- 7 Чтобы сохранять зашифрованные файлы в кодировке Base64, установите соответствующий флажок.
- 8 Нажмите  и укажите папки для сохранения зашифрованных и расшифрованных файлов.
- 9 Нажмите  Сохранить.

Настройка сетевых параметров

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

- 1 В панели управления Windows в категории **Сеть и Интернет** щелкните **Просмотр состояния сети и задач**.
- 2 В окне **Центр управления сетями и общим доступом** щелкните **Изменение параметров адаптера**.
- 3 В окне **Сетевые подключения** щелкните правой кнопкой мыши значок вашего интернет-соединения и в контекстном меню выберите **Свойства**.
- 4 В окне свойств вашего интернет-соединения убедитесь, что выбрано **IP версии 4 (TCP/IPv4)**, а флажок **IP версии 6 (TCP/IPv6)** снят.

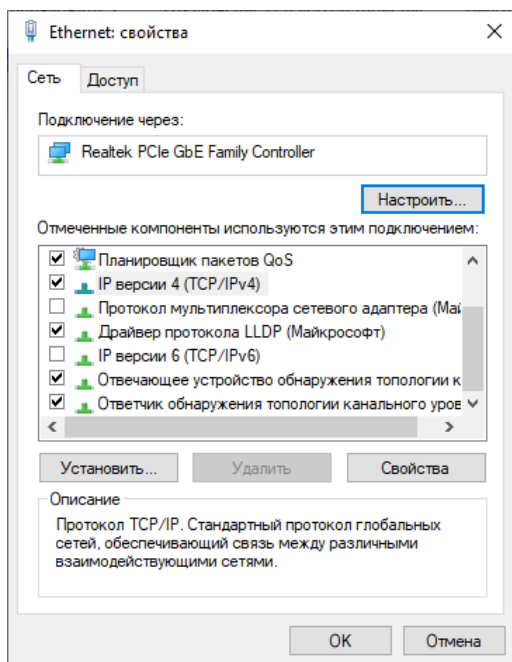


Рисунок 18. Проверка настроек интернет-соединения

8

Подключение к веб-ресурсам, использующим TLS ГОСТ

Порядок настройки подключения к веб-ресурсам, использующим TLS ГОСТ	72
Требования к сертификатам для работы TLS Unit	73
Импорт сертификата и ключа ЭП на Infotecs Software Token	75
Подключение к веб-ресурсу	77
Просмотр информации о TLS-соединениях	78

Порядок настройки подключения к веб-ресурсам, использующим TLS ГОСТ

Действие и ссылка

- 1 Чтобы подключаться к веб-ресурсам, которые требуют аутентификации пользователя:
 - Убедитесь, что сертификат, который вы будете использовать для подключения, соответствует [требованиям](#) (на стр. 73).
 - Если сертификат и ключ ЭП хранятся на внешнем устройстве — подключите внешнее устройство к компьютеру (см. [Список поддерживаемых внешних устройств для подключения к сайтам, использующим TLS ГОСТ, и туннелируемым ресурсам](#) на стр. 105).
 - Если сертификат и ключ ЭП хранятся на компьютере — [импортируйте сертификат и ключ ЭП на Infotecs Software Token](#) (на стр. 75).
- 2 Переведите TLS Unit в состояние **Работает** (на стр. 19).
- 3 Подключитесь к веб-ресурсу (на стр. 77).
- 4 Просмотрите информацию о текущих TLS-соединениях (на стр. 78).

Требования к сертификатам для работы TLS Unit

Сертификат сервера

При подключении к веб-ресурсу TLS Unit проверяет, что:



- Сертификат сервера действителен:
 - срок действия сертификата сервера наступил и не истек;
 - сертификат сервера не аннулирован;
 - все сертификаты цепочки действительны и установлены в хранилище.
- ЭП сертификата сервера верна.
- Адрес веб-ресурса соответствует адресу в сертификате сервера.
- Сертификат сервера имеет назначение **Проверка подлинности сервера** в поле **Улучшенный ключ**.

По умолчанию, если хотя бы одна проверка не выполняется, соединение с сервером не устанавливается.

Вы можете разрешить установку соединений, если часть проверок не выполнена, а именно:

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

Для этого:

- 1 [Перейдите в настройки ViPNet PKI Client](#) (на стр. 19).
- 2 Выберите раздел  **TLS**.
- 3 Если **TLS Unit** включен, **выключите его** (см. [TLS Unit](#) на стр. 19).
- 4 Выберите **Разрешать соединение при неполном доверии к сертификату сервера**.
- 5 Нажмите  **Сохранить**.

Сертификат пользователя

Для подключения с помощью TLS Unit к веб-ресурсам, требующим аутентификацию пользователя, вам нужен сертификат, для которого выполняется следующее:

- сертификат действителен и имеет расширение **Улучшенный ключ** со значением **Проверка подлинности клиента**;

- сертификат и соответствующий ключ ЭП хранятся одним из способов:
 - на программном токене Infotecs Software Token (см. [Импорт сертификата и ключа ЭП на Infotecs Software Token](#) на стр. 75);
 - на внешнем устройстве (см. [Список поддерживаемых внешних устройств для подключения к сайтам, использующим TLS ГОСТ, и туннелируемым ресурсам](#) на стр. 105);
- сертификат установлен в хранилище сертификатов текущего пользователя **Личное**;
- все сертификаты цепочки действительны и установлены в хранилище;
- актуальные CRL установлены в хранилище.

Примечание. Для подключения к некоторым веб-ресурсам сертификат пользователя должен быть издан в определенных УЦ. В этом случае:



- 1 Обратитесь в техническую поддержку или ознакомьтесь со справочным разделом на сайте и получите информацию об УЦ, в которых может быть издан сертификат.
- 2 В сертификате просмотрите информацию об издателе и сравните ее с информацией об УЦ, полученной на сайте. Если издателя сертификата нет в списке УЦ на сайте, создайте запрос на сертификат, передайте его в нужный УЦ и получите сертификат (см. [Получение сертификата](#) на стр. 35).

Импорт сертификата и ключа ЭП на Infotecs Software Token



TLS Unit может использовать для подключения только сертификаты пользователя, ключ ЭП которых хранится одним из способов:

- на [Infotecs Software Token](#) (см. глоссарий, стр. 109), для защиты в этом случае используется ПИН (см. [Смена ПИНа Infotecs Software Token](#) на стр. 76);
- на внешнем устройстве (см. [Список поддерживаемых внешних устройств для подключения к сайтам, использующим TLS ГОСТ, и туннелируемым ресурсам](#) на стр. 105), для защиты в этом случае используются прикладные средства устройства.

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


- Если сертификат установлен в хранилище и имеется контейнер ключей с соответствующим ключом ЭП, см. [Импорт сертификата и ключа ЭП из хранилища](#) (на стр. 75).
- Если сертификат не установлен в хранилище и имеется контейнер ключей с сертификатом и ключом ЭП:
 - Экспортируйте сертификат и ключ ЭП в файл (см. «ViPNet CSP. Руководство пользователя» > «Операции с контейнерами ключей» > «Экспорт сертификата и закрытого ключа в файл»).
 - Импортируйте полученный файл на Infotecs Software Token (см. [Импорт сертификата и ключа ЭП из файла *.rfx](#) на стр. 76).
- Если сертификат и ключ ЭП находятся в файле *.rfx, см. [Импорт сертификата и ключа ЭП из файла *.rfx](#) (на стр. 76).

Импорт сертификата и ключа ЭП из хранилища

- 1 [Перейдите в настройки ViPNet PKI Client](#) (на стр. 19).
- 2 Выберите раздел  Сертификаты.
- 3 Нажмите  и в списке выберите **Личные сертификаты**.
- 4 Щелкните правой кнопкой мыши выбранный сертификат и в контекстном меню выберите **Скопировать ключ в Infotecs Software Token**.
- 5 При первом импорте появится [электронная рулетка](#) (см. глоссарий, стр. 112). Следуйте указаниям в окне **Электронная рулетка**.
- 6 Введите пароль контейнера ключей.

7 В окне сообщения об успешном импорте нажмите **ОК**.

Импорт сертификата и ключа ЭП из файла *.pfx


- 1 [Перейдите в настройки ViPNet PKI Client](#) (на стр. 19).
- 2 Выберите раздел  **TLS**.
- 3 Нажмите **Импортировать PFX-файл на Infotecs Software Token** и укажите путь к PFX-файлу.
- 4 Введите пароль PFX-файла.
- 5 В окне сообщения об успешном импорте нажмите **ОК**.

Смена ПИНа Infotecs Software Token

По умолчанию ПИН Infotecs Software Token — 11111111 и не запрашивается при работе с Infotecs Software Token. Если по требованиям безопасности вашей организации не допускается использование такого ПИНа, смените его:



Внимание! После смены ПИНа при выполнении операций с сертификатами и ключами, хранящимися на Infotecs Software Token, потребуется вводить ПИН.

- 1 [Перейдите в настройки ViPNet PKI Client](#) (на стр. 19).
- 2 Выберите раздел  **TLS**.
- 3 Нажмите **Сменить пароль Infotecs Software Token**.
- 4 Введите текущий пароль (по умолчанию — 11111111) и нажмите **Ввести**.
- 5 Задайте и подтвердите новый пароль.
- 6 Нажмите **Изменить**.

Подключение к веб-ресурсу

Чтобы подключиться к веб-ресурсу, использующему TLS ГОСТ, в браузере введите адрес сайта:

- Если для подключения не требуется аутентификация пользователя, соединение будет установлено.

Появится сообщение об установке соединения в области уведомлений.

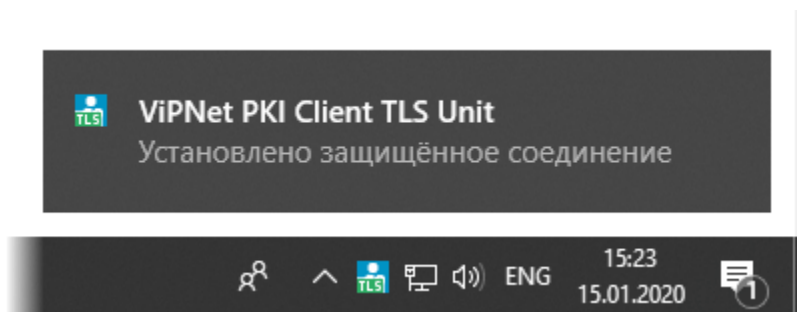


Рисунок 19. Сообщение об успешной установке соединения

- Если для подключения требуется аутентификация пользователя, выберите сертификат. Соединение будет установлено.


Примечание. При первом подключении к веб-ресурсу выбранный сертификат сохраняется в кэш, и при последующих подключениях к этому веб-ресурсу в текущей сессии выбирать сертификат не требуется. Сертификат удаляется из кэша:



- автоматически при завершении работы TLS Unit;
 - вручную, если необходимо выбрать другой сертификат для подключения. 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 TLS-соединениях

Чтобы просмотреть информацию о TLS-соединениях, установленных за последние 10 минут:

- 1 В области уведомлений щелкните правой кнопкой мыши значок TLS Unit и в контекстном меню выберите **Информация о соединениях**.
- 2 Чтобы просмотреть подробную информацию об одном из соединений, слева от него щелкните значок  и просмотрите:
 - версию протокола TLS;
 - алгоритм согласования ключей;
 - алгоритм шифрования передаваемых данных и контроля их целостности;
 - процесс Windows, который инициировал установку защищенного соединения.

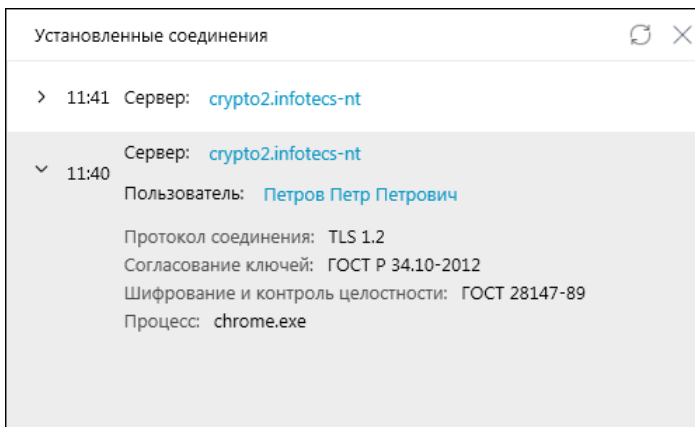


Рисунок 20. Просмотр информации о TLS-соединениях

9

Подключение к туннелируемым ресурсам

Порядок настройки подключения к туннелируемым ресурсам	80
Требования к сертификатам для работы Tunnel Unit	81
Добавление туннелируемого ресурса	82
Подключение к туннелируемому ресурсу	84

Порядок настройки подключения к туннелируемым ресурсам

Действие

- 1 У администратора ViPNet TLS Gateway получите:
 - сертификат УЦ, в котором изданы транспортные сертификаты ViPNet TLS Gateway, и соответствующий CRL; если УЦ не является корневым, также получите все сертификаты из цепочки и соответствующие CRL;
 - адрес и порт для подключения к туннелируемому ресурсу.
 - 2 Установите полученные сертификаты и CRL в хранилище (на стр. 39).
 - 3 Чтобы подключаться к туннелируемым ресурсам, которые требуют аутентификации пользователя, убедитесь, что сертификат, который вы будете использовать для подключения, соответствует [требованиям](#) (на стр. 81).
 - 4 Добавьте туннелируемый ресурс в ViPNet PKI Client (на стр. 82).
 - 5 Подключитесь к туннелируемому ресурсу (на стр. 84).
-

Требования к сертификатам для работы Tunnel Unit

Сертификат сервера (транспортный сертификат ViPNet TLS Gateway)

При подключении к туннелируемому ресурсу Tunnel Unit проверяет, что:

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

Если хотя бы одна проверка не выполняется, соединение с ViPNet TLS Gateway не устанавливается.


Сертификат пользователя


Для подключения с помощью Tunnel Unit к туннелируемым ресурсам, требующим аутентификацию пользователя, вам нужен сертификат, для которого выполняется следующее:

- сертификат действителен и имеет расширение **Улучшенный ключ** со значением **Проверка подлинности клиента**;
- сертификат и соответствующий ключ ЭП хранятся одним из способов:
 - на программном токене Infotecs Software Token (см. [Импорт сертификата и ключа ЭП на Infotecs Software Token](#) на стр. 75);
 - на внешнем устройстве (см. [Список поддерживаемых внешних устройств для подключения к сайтам, использующим TLS ГОСТ, и туннелируемым ресурсам](#) на стр. 105);
- сертификат установлен в хранилище сертификатов текущего пользователя **Личное**;
- все сертификаты цепочки действительны и установлены в хранилище.
- актуальные CRL установлены в хранилище;
- сертификат добавлен на ViPNet TLS Gateway в список **Сертификаты пользователей > Разрешенные** и разрешен доступ к туннелируемому ресурсу (см. «ViPNet TLS Gateway. Руководство администратора»).

Добавление туннелируемого ресурса

1 Перейдите в настройки ViPNet PKI Client (на стр. 19).

2 Выберите раздел  Туннели.

3 Нажмите  **Добавить туннель**.

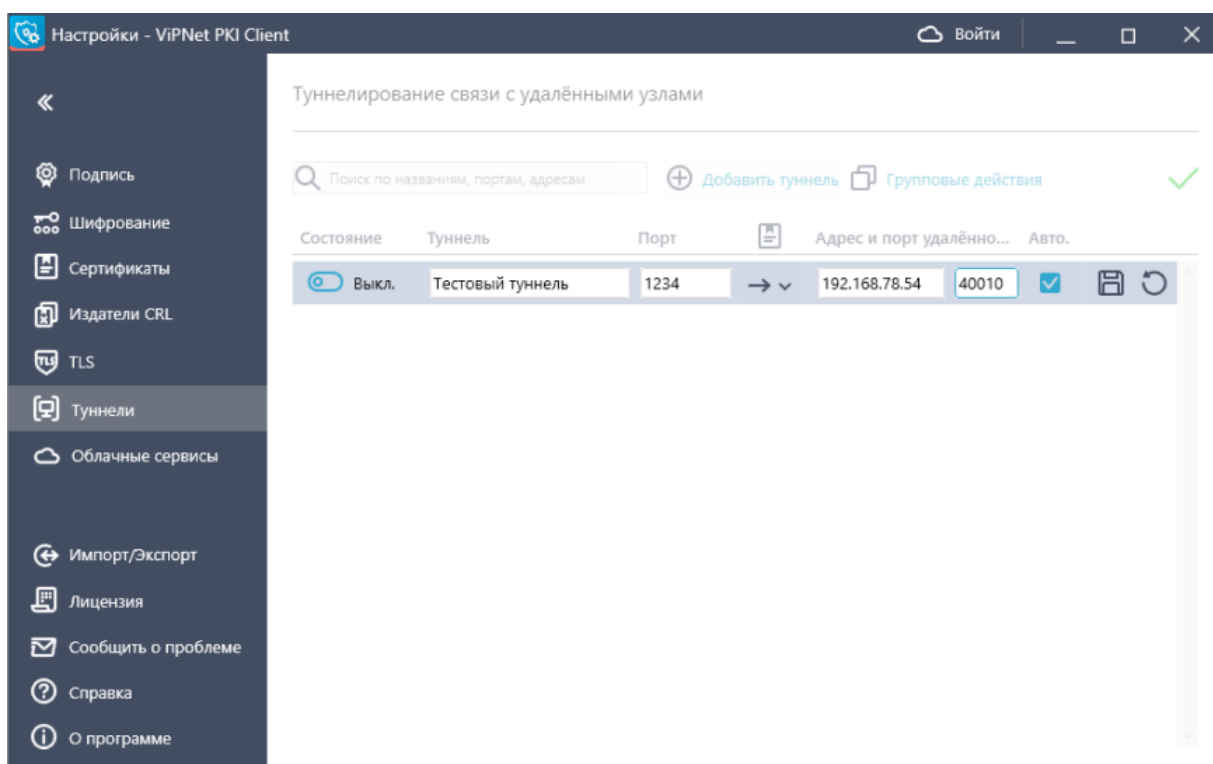


Рисунок 21. Добавление туннелируемого ресурса





4 В поле **Туннель** введите произвольное наименование туннелируемого ресурса.

5 В поле **Порт** введите номер порта локального сетевого интерфейса для обмена данными с туннелируемым ресурсом. Этот же номер порта необходимо указать в настройках приложения для подключения к туннелируемому ресурсу.





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

6 В поле **Адрес и порт удаленного узла** укажите адрес и порт ViPNet TLS Gateway для подключения к туннелируемому ресурсу. Эти данные вы можете получить у администратора ViPNet TLS Gateway.

- 7 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. В этом случае в окне **Выбор сертификата** выберите сертификат (см. [Требования к сертификатам для работы Tunnel Unit](#) на стр. 81).
- 8 Чтобы подключение к туннелируемому ресурсу выполнялось автоматически после [запуска Tunnel Unit](#) (на стр. 19), установите флажок в столбце **Авто**.
- 9 Нажмите .




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

Подключение к туннелируемому ресурсу



Примечание. Если при добавлении туннелируемого ресурса вы установили флажок в столбце **Авто** (см. [Добавление туннелируемого ресурса](#) на стр. 82), связь с этим ресурсом будет установлена автоматически при запуске программы Tunnel Unit.

Ниже описано подключение к удаленному рабочему столу по протоколу RDP. Подключение к туннелируемым ресурсам с помощью других приложений и по другим протоколам выполняется аналогично.

- 1 Запустите **Tunnel Unit** (на стр. 19).
- 2 Перейдите в настройки **ViPNet PKI Client** (на стр. 19).
- 3 Выберите раздел  **Туннели**.
- 4 В списке выберите туннелируемый ресурс и с помощью переключателя в столбце **Состояние** установите соединение с ним.

Примечание. Для работы сразу со всеми туннелируемыми ресурсами используйте кнопку



Групповые действия:



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

Также эти действия, кроме **Удалить все туннели**, вы можете выполнить с помощью контекстного меню значка Tunnel Unit в области уведомлений.


- 5 Запустите стандартную программу Windows **Подключение к удаленному рабочему столу**.
- 6 В поле **Компьютер** 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. 82).
- 7 Нажмите **Подключить**.

10

Возможные неполадки и способы их устранения

Обращение в техническую поддержку	86
Общие неполадки	87
File Unit	93
TLS Unit	94

Обращение в техническую поддержку

- 1 Перейдите в настройки ViPNet PKI Client (на стр. 19).
- 2 На панели слева нажмите  Сообщить о проблеме.

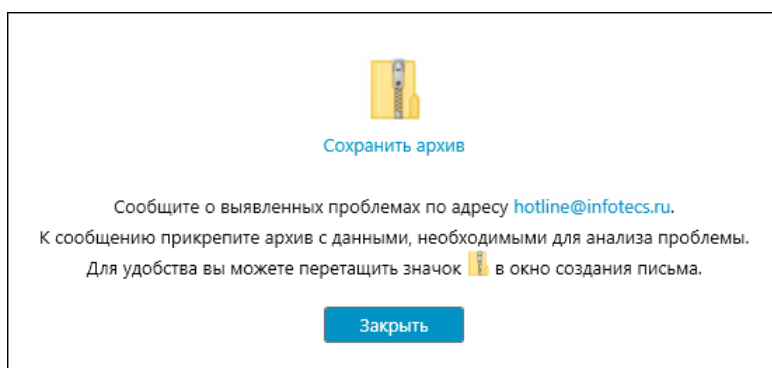



Рисунок 22. Создание архива с данными для анализа проблемы

- 3 Выберите, какая информация будет включена в отчёт, и нажмите  Собрать данные.
- 4 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 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. ИнфоТеКС ответственно подходит к защите вашей личной информации и принимает все меры для предотвращения несанкционированного доступа или разглашения информации, которую вы нам предоставляете.

Общие неполадки

Не удалось установить ViPNet PKI Client

Данная ошибка может возникнуть, если на компьютере установлено ПО Microsoft Visual C++ 2017 Redistributable (x86) версии выше 14.16.27012.

Для устранения ошибки:

- 1 Удалите ПО Microsoft Visual C++ 2017 Redistributable (x86).
- 2 Установите ViPNet PKI Client (см. [Установка, обновление](#) на стр. 17).
- 3 Заново установите ПО Microsoft Visual C++ 2017 Redistributable (x86).

Ошибка при обновлении ViPNet PKI Client

При обновлении версии ViPNet PKI Client на этапе выбора лицензии может возникнуть ошибка:



Рисунок 23. Ошибка при обновлении ViPNet PKI Client

Для устранения ошибки:

- 1 Удалите папку %ProgramData%\InfoTeCS\ViPNet PKI Client\LicenseStorage.
- 2 Заново выполните обновление.

Ошибка при импорте настроек

При импорте настроек может возникнуть ошибка:

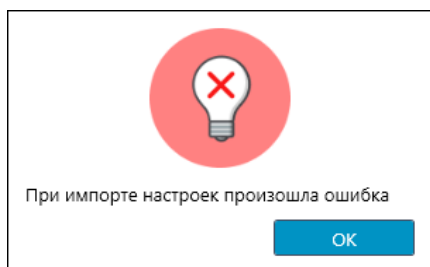


Рисунок 24. Ошибка при импорте настроек

Для устранения ошибки:

- 1 Переустановите ViPNet PKI Client.
- 2 Заново выполните [импорт настроек](#) (на стр. 29).

Ошибка при удалении сертификата

При удалении сертификатов получателей с помощью ViPNet PKI Client (см. [Удаление сертификатов](#) на стр. 49) может возникнуть ошибка:

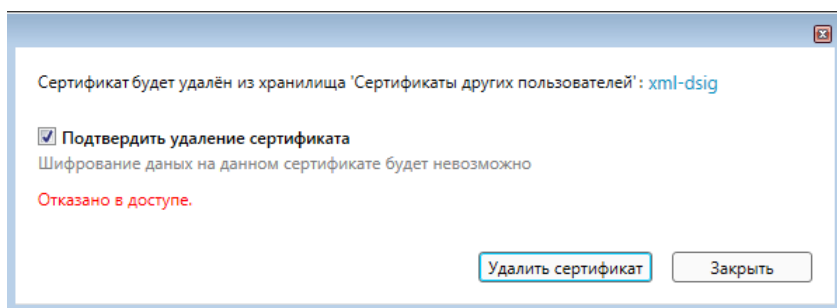


Рисунок 25. Ошибка при удалении сертификата

Данное ошибка возникает, если сертификат получателя установлен в системное хранилище компьютера, а у пользователя недостаточно прав для работы с этим хранилищем.

Чтобы удалить сертификат:

- 1 Откройте консоль MMC:
 - Нажмите сочетание клавиш **Win+R**.
 - В поле **Открыть** введите `mmc` и нажмите **ОК**.
- 2 В меню **Файл** окна консоли выберите **Добавить или удалить оснастку**.
- 3 В окне **Добавление и удаление оснасток** в списке **Доступные оснастки** выберите оснастку **Сертификаты** и нажмите **Добавить**.
- 4 В окне **Оснастка диспетчера сертификатов** выберите тип оснастки **Учетной записи компьютера** и нажмите **Далее**, а затем **Готово**.
- 5 На панели навигации консоли выберите **Сертификаты (локальный компьютер) > Другие пользователи > Сертификаты**.

- 6 Щелкните правой кнопкой мыши нужный сертификат и в контекстном меню выберите **Удалить**.
- 7 В окне подтверждения удаления нажмите **Да**.

Ошибка службы регистрации событий

При работе с ViPNet PKI Client может возникнуть ошибка:

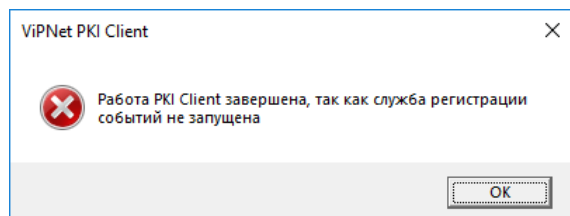


Рисунок 26. Ошибка службы регистрации событий

Данная ошибка может возникать, если после перезагрузки компьютера не запустилась служба регистрации событий `Infotecs.SecurityAuditService`. В этом случае использование ViPNet PKI Client будет невозможно.

Для устранения ошибки:

- 1 Запустите службу `Infotecs.SecurityAuditService`:
 - Запустите «Диспетчер задач» с помощью сочетания клавиш **Ctrl+Shift+Esc**.
 - В окне **Диспетчер задач** перейдите на вкладку **Службы**.
 - В списке найдите службу `Infotecs.SecurityAuditService`, щелкните эту службу правой кнопкой мыши и в контекстном меню выберите **Запустить службу**.
- 2 Если служба `Infotecs.SecurityAuditService` не запускается, с помощью консольной утилиты `netstat` проверьте, что порт 62000, по умолчанию используемый службой `Infotecs.SecurityAuditService`, не занят другим приложением.
- 3 Если порт 62000 занят, измените порт для службы `Infotecs.SecurityAuditService`:
 - Если запущены компоненты ViPNet PKI Client, **завершите их работу** (на стр. 19).
 - Перейдите в папку с файлом конфигурации. По умолчанию:
 - для 32-разрядных версий Windows — `C:\Program Files\InfoTeCS\ViPNet PKI Client\Audit`;
 - для 64-разрядных версий Windows — `C:\Program Files (x86)\InfoTeCS\ViPNet PKI Client\Audit`.
 - Откройте в текстовом редакторе, поддерживающем кодировку текста UTF-8, файл конфигурации `Infotecs.SecurityAuditService.exe.config`.
 - В параметре `baseAddresses` укажите порт из диапазона 49151–65535.

```
<add baseAddress="http://localhost:63158/webhost"/>
```

- Сохраните изменения.
- Запустите службу `Infotecs.SecurityAuditService`.

Ошибки при обновлении CRL

Для определения причины сбоя откройте файл `crlunit.log`, в который записываются события службы, и в строке события посмотрите значение `ErrorCode`. По умолчанию файл располагается в папке `C:\ProgramData\Infotecs\ViPNet PKI Client\CRL Unit\Logs`.

Неправильный URL-адрес (ErrorCode=3)

Данная ошибка указывает на то, что неправильно введен URL точки распространения CRL.

Для устранения ошибки проверьте правильность введенного URL точки распространения CRL (см. [Добавление точек распространения CRL](#) на стр. 51).

Ошибка данных (ErrorCode=4)

Для устранения ошибки выполните одно из действий:

- Проверьте доступность точки распространения CRL. Для этого загрузите список CRL вручную: скопируйте URL точки распространения CRL в адресную строку браузера и перейдите по нему. Если на ваш компьютер загрузился файл `*.crl`, значит, точка распространения доступна.
- Если в вашей организации доступ в интернет осуществляется через прокси-сервер, в файле конфигурации `crlunit.cfg` укажите настройки прокси-сервера (см. [Файл конфигурации `crlunit.cfg`](#) на стр. 53).

Ошибка загрузки (ErrorCode=5)

Данная ошибка указывает на отсутствие доступа к Интернету или недоступности точки распространения CRL.

Для устранения ошибки:

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

Ошибка хранилища сертификатов (ErrorCode=6)

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

Сертификат не найден (ErrorCode=7)

Для устранения ошибки получите сертификат издателя выбранной точки распространения CRL и установите его в хранилище локального компьютера (см. [Установка сертификатов и CRL](#) на стр. 39).

CRL просрочен (ErrorCode=8)

Данная ошибка указывает на то, что срок действия CRL, загруженного из указанной точки распространения, истек.

Для устранения ошибки обратитесь к администратору вашего УЦ.

Недостаточно памяти (ErrorCode=9)

Данная ошибка указывает на нехватку оперативной памяти.

CRL уже установлен (ErrorCode=11)

Данная ошибка указывает на попытку установить CRL, который уже установлен в хранилище сертификатов.

Ошибка сети (ErrorCode=12)

Данная ошибка указывает на сбой в сети во время загрузки CRL.

Не удастся сохранить ключ ЭП на ESMART Token ГОСТ

На устройстве ESMART Token ГОСТ нельзя создать запрос на сертификат, в поле **Назначение** которого присутствует **Шифрование**.

При создании запроса на сертификат с помощью ViPNet PKI Client не предусмотрена возможность выбора назначения сертификата и по умолчанию устанавливается назначение **Подпись и шифрование**.

В этом случае создайте запрос на сертификат с помощью ViPNet CSP (см. «ViPNet CSP. Руководство пользователя» > «Создание запроса на сертификат и формирование закрытого ключа») и в поле **Назначение** выберите значение **Подпись**.

Обнаружена несогласованность при внутренней проверке

Может возникнуть при попытке создать запрос на сертификат с сохранением ключа ЭП на внешнее устройство с аппаратной поддержкой ГОСТ, если данное устройство не поддерживает выбранный набор параметров ключа проверки ЭП.

Для устранения ошибки при создании запроса на сертификат выполните одно из действий:

- используйте для сохранения ключа ЭП устройство с аппаратной поддержкой ГОСТ и поддержкой выбранного набора параметров ключа проверки ЭП или устройство с программной поддержкой ГОСТ;
- выберите другой набор параметров ключа проверки ЭП.

Ошибки при совместной работе с КриптоПро CSP

Не рекомендуется использовать несколько криптопровайдеров на одной компьютере.

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

File Unit

Требуемый сертификат не отображается в списке сертификатов для подписания

При подписании файлов с помощью File Unit нужный сертификат может не отображаться в окне **Выбор сертификата**.

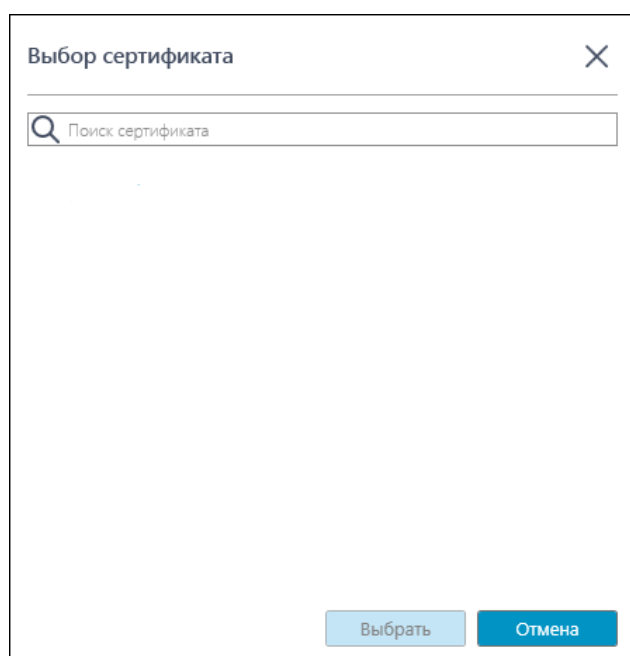



Рисунок 27. Сертификат не отображается в списке сертификатов для подписи

Проверьте, что сертификат соответствует требованиям (см. [Требования к сертификатам для подписи и шифрования](#) на стр. 64).

Ошибка при расшифровании

Ошибка может возникать, если ключ ЭП был создан сторонним ПО и вместе с сертификатом хранится на внешнем устройстве. Текущая версия ViPNet PKI Client не поддерживает расшифрование с помощью таких сертификатов и ключей.

Чтобы узнать в каком ПО был создан ключ ЭП:

- 1 [Перейдите в настройки ViPNet PKI Client](#) (на стр. 19).
- 2 В разделе  **Сертификаты** откройте сертификат.
- 3 На вкладке **Состав** найдите поле **Средство электронной подписи владельца**.

TLS Unit

Настройка совместной работы TLS Unit и браузера Mozilla Firefox

Если для доступа к веб-ресурсам вы используете браузер Mozilla Firefox, настройте совместную работу TLS Unit и браузера Mozilla Firefox.

Примечание. Перед импортом сертификата проверьте, что в браузере Mozilla Firefox используются системные параметры прокси:



- 1 Перейдите в меню **Настройки** и выберите вкладку **Дополнительные**, а затем **Сеть**.
- 2 В группе **Соединение** нажмите **Настроить**.
- 3 Проверьте, что в окне **Параметры соединения** включите **Использовать системные настройки системы**.

Для этого импортируйте корневой сертификат `ViPNet PKI Client Root` в сертификаты Mozilla Firefox.

- 1 Экспортируйте корневой сертификат `ViPNet PKI Client Root` с помощью менеджера сертификатов:
 - 1.1 Запустите менеджер сертификатов. Для этого в меню **Пуск** выберите **Выполнить**, введите команду `certmgr.msc` и нажмите **ОК**.
 - 1.2 Перейдите в системное хранилище **Доверенные корневые центры сертификации**, в раздел **Сертификаты**.
 - 1.3 В списке щелкните правой кнопкой мыши сертификат `ViPNet PKI Client Root`. В меню выберите **Все задачи > Экспорт**.
 - 1.4 В **Мастере экспорта сертификатов**:
 - На странице **Экспортирование закрытого ключа** выберите вариант **Нет, не экспортировать закрытый ключ**.
 - На странице **Формат экспортируемого файла** установите переключатель в положение **Файлы X.509 (.CER) в кодировке DER**.
 - На странице **Имя экспортируемого файла** нажмите **Обзор** и задайте имя для экспортируемого сертификата и папку его сохранения.
 - На странице **Завершение работы мастера экспорта сертификатов** нажмите **Готово**.По окончании экспорта вы увидите сообщение с подтверждением завершения операции.
- 2 Импортируйте сертификат `ViPNet PKI Client Root` в браузер Mozilla Firefox:
 - 2.1 В браузере перейдите в меню **Настройки**.

2.2 В разделе **Приватность и Защита** в группе **Защита** нажмите **Просмотр сертификатов**.

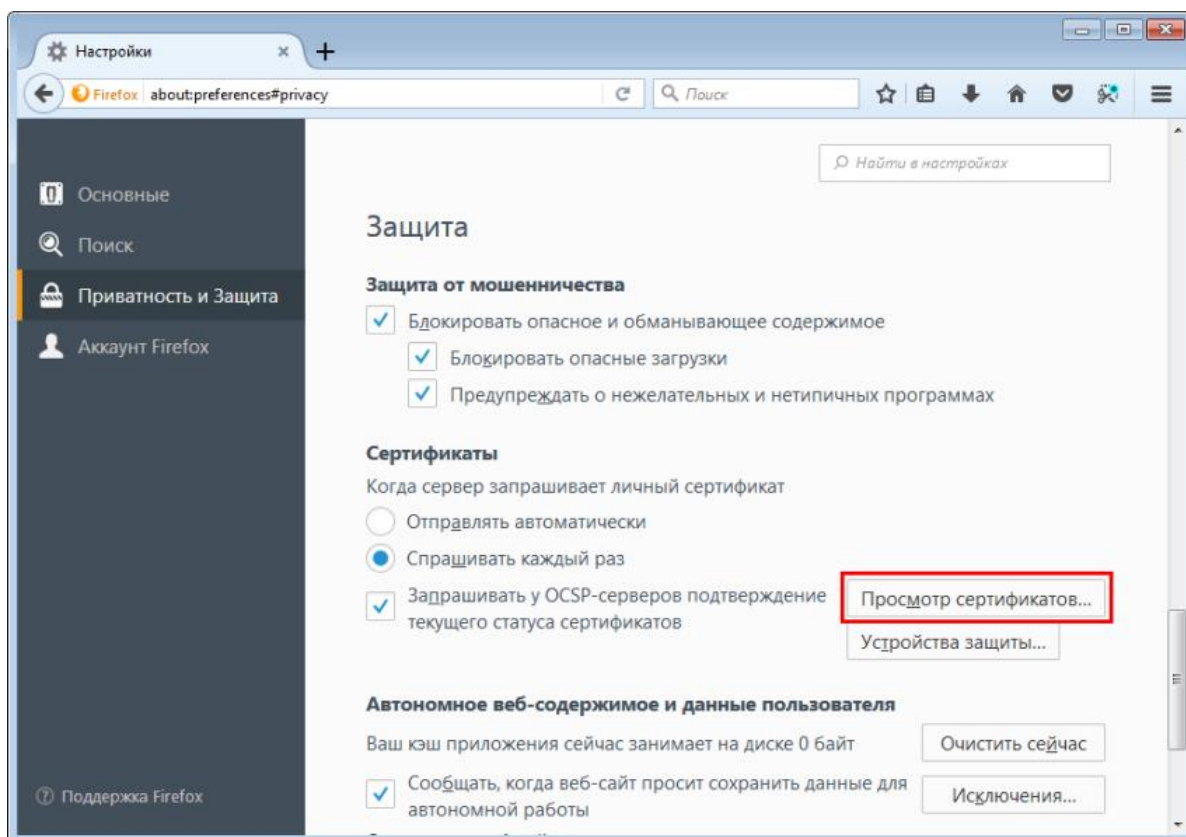


Рисунок 28. Настройки браузера Mozilla Firefox

- 2.3 В окне **Управление сертификатами** перейдите на вкладку **Центры сертификации**, нажмите **Импортировать**.
- 2.4 Выберите сертификат `ViPNet PKI Client Root`, который вы экспортировали до этого. Нажмите **Открыть**.
- 2.5 В окне **Загрузка сертификата** установите флажок **Доверять при идентификации веб-сайтов** и нажмите **ОК**.
- 2.6 В окне **Управление сертификатами** нажмите **ОК**.
- 2.7 Перезапустите браузер.

Невозможно установить соединение

Если после развертывания TLS Unit не получается устанавливать соединения с веб-ресурсами:

- 1 Проверьте, что на компьютере установлены последние обновления Windows.
- 2 Проверьте, что при выключенном TLS Unit настройки прокси-сервера, заданные на вашем компьютере, соответствуют настройкам прокси-сервера во всей локальной сети.

- 3 Если вы пытаетесь установить защищенное соединение с сервером, принадлежащим к локальной сети, убедитесь, что при выключенном TLS Unit адрес этого сервера указан в исключениях настроек параметров прокси-сервера.

A

Формат файла с шаблонами XML-подписи

Шаблоны XML-подписи описываются в формате JSON. Вы можете использовать шаблон по умолчанию или создать свой.

JSON-структура файла с шаблонами XML-подписи

Таблица 3. Параметры

Параметр	Формат	Описание	Возможные значения
SignSettings (обязательный)	SignSettings	Элемент, определяющий параметры подписи	Объект SignSettings

Таблица 4. Объект SignSettings

Параметр	Формат	Описание	Возможные значения
XmlTemplates (обязательный)	XmlTemplates	Элемент, определяющий параметры шаблонов	Объект XmlTemplates

Таблица 5. Объект XmlTemplates

Параметр	Формат	Описание	Возможные значения
Description (необязательный)	String	Описание файла шаблонов, отображаемое в настройках при импорте	—

Параметр	Формат	Описание	Возможные значения
DefaultId (необязательный)	String	Идентификатор шаблона (TemplateId), который будет выбран по умолчанию после импорта	—
Templates (обязательный)	Array <Templates>	Список шаблонов	Объект Templates

Таблица 6. Объект Templates

Параметр	Формат	Описание	Возможные значения
Name (обязательный)	String	Имя шаблона, отображаемое в настройках	—
TemplateId (обязательный)	String	Идентификатор шаблона, уникальный в пределах данного файла	—
DSignatureType (необязательный)	String	Формат XML-подписи. Если не задан, будет использоваться подпись формата XAdES.	<ul style="list-style-type: none"> • <code>xades</code> — расширенная XML-подпись в формате XAdES; • <code>xmlsig</code> — стандартная XML-подпись в формате XMLDSig; • <code>wsse-security</code> — XML-подпись в формате WS-Security, применяется при работе с протоколом SOAP.
DSignatureTypeParam (необязательный)	DSignatureTypeParam	Задаёт дополнительные параметры для подписи в формате WS-Security	Объект DSignatureTypeParam
CanonicalizationMethod (обязательный)	String	Алгоритм каноникализации	<ul style="list-style-type: none"> • http://www.w3.org/TR/2001/REC-xml-c14n-20010315/; • http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments; • http://www.w3.org/2001/10/xml-exc-c14n#; • http://www.w3.org/2001/10/xml-exc-c14n#WithComments; • http://www.w3.org/2006/12/xml-c14n11; • http://www.w3.org/2006/12/xml-c14n11#WithComments.

Параметр	Формат	Описание	Возможные значения
SignatureId (необязательный)	String	Идентификатор для распознавания подписи в подписанном документе, например, в случае ее поиска. При отсутствии будет подставляться случайное значение.	—
SignatureLocationPath (необязательный)	String	Место встраивания подписи в XML-документ. Может быть задан с помощью идентификатора тега, абсолютного или относительного Xpath. При отсутствии подпись будет встраиваться в корневой тег XML-документа.	—
References (необязательный)	Array <References>	Список ссылок на фрагменты документа, которые нужно подписать. При отсутствии будут использоваться параметры шаблона по умолчанию.	Объект References

Таблица 7. Объект DSignatureTypeParam

Параметр	Формат	Описание	Возможные значения
bsTokenId	String	Идентификатор BinarySecurityToken. Если не задан, будет сгенерирован автоматически.	—
actor	String	Идентификатор подписанта. По умолчанию будет отсутствовать в подписываемом файле.	—

Таблица 8. Объект References

Параметр	Формат	Описание	Возможные значения
Id (необязательный)	String	Идентификатор объекта Reference	—

Параметр	Формат	Описание	Возможные значения
Uri (необязательный)	String	Идентификатор тега, содержимое которого нужно подписать. При отсутствии будет подписан весь документ.	—
Type (необязательный)	String	URL-адрес, указывающий на подписываемые трансформированные данные	—
Transforms (обязательный)	Array <Transforms>	Список трансформаций выбранных фрагментов XML-документа	Объект Transforms

Таблица 9. Объект Transforms

Параметр	Формат	Описание	Возможные значения
Algorithm (обязательный)	String	Алгоритм трансформации исходных данных	<ul style="list-style-type: none"> • http://www.w3.org/TR/1999/REC-xpath-19991116; • http://www.w3.org/2000/09/xmldsig#base64; • http://www.w3.org/2000/09/xmldsig#enveloped-signature; • http://www.w3.org/2002/06/xmldsig-filter2; • urn://smev-gov-ru/xmldsig/transform.
TransformValue (обязательный для некоторых алгоритмов)	String	Дополнительные данные в текстовом формате, если они предполагаются выбранным алгоритмом	—

Пример файла с шаблонами для XML-подписи

```
{
  "SignSettings": {
    "XmlTemplates": {
      "Description": "Пример набора шаблонов подписи XML",
      "DefaultId": "template_1",
      "Templates": [
        {
          "Name": "Подпись XML с дополнительными параметрами",
          "Description": "Будет подписан тег с Id='props'",
          "TemplateId": "template_1",

```

```
"CanonicalizationMethod": "http://www.w3.org/2001/10/xml-exc-c14n#",
"SignatureId": "PropsSignature",
"SignatureLocationPath": "#props",
"References": [
  {
    "Id": "PropsReferense",
    "Uri": "#props",
    "Type": "http://www.w3.org/2000/09/xmldsig#Object",
    "Transforms": [
      {
        "Algorithm": "http://www.w3.org/2000/09/xmldsig#enveloped-signature"
      }
    ]
  }
],
{
  "Name": "Подпись нескольких частей документа",
  "Description": "Будут подписаны теги с Id='1' и Id='2'. Тег Signature будет встроен в тег Data",
  "TemplateId": "template_2",
  "CanonicalizationMethod": "http://www.w3.org/2001/10/xml-exc-c14n#",
  "SignatureLocationPath": "/Root/Data",
  "References": [
    {
      "Uri": "#1",
      "Transforms": [
        {
          "Algorithm": "http://www.w3.org/2000/09/xmldsig#enveloped-signature"
        }
      ]
    },
    {
      "Uri": "#2",
      "Transforms": [
        {
          "Algorithm": "http://www.w3.org/2000/09/xmldsig#enveloped-signature"
        }
      ]
    }
  ]
}
]
}
}
```

В

Внешние устройства

Общие сведения

Внешние устройства предназначены для хранения [контейнеров ключей](#) (см. глоссарий, стр. 110), которые вы можете использовать для аутентификации, формирования [электронной подписи](#) (см. глоссарий, стр. 112) 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 10. Поддерживаемые внешние устройства

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

Название семейства устройств в 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 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.»	<p>На компьютере должно быть установлено ПО «Единый Клиент JaCarta» компании «Аладдин Р.Д.» (рекомендуемая минимальная версия — 2.12).</p> <p>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.</p> <p>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.».</p>
Rutoken	Электронные идентификаторы Рутокен ЭЦП 2.0 и Рутокен Lite производства компании «Актив»	<p>На компьютере должны быть установлены драйверы Rutoken (рекомендуемая версия — 4.8.5.0).</p> <p>Перенос ключей подписи с устройств, а также на устройства Рутокен ЭЦП 2.0 невозможен, так как на устройствах используется аппаратная криптография с неизвлекаемым ключом.</p>
Rutoken S	Электронные идентификаторы Рутокен S производства компании «Актив»	<p>На компьютере должны быть установлены драйверы Rutoken (рекомендуемая версия — 4.8.5.0).</p>
R301 Foros	Смарт-карты и токены R301 Форос PKCS производства компании «СмартПарк»	<p>На компьютере должна быть установлена библиотека <code>foros_pkcs11.dll</code> (для 32-разрядной либо 64-разрядной архитектуры процессора), предоставленная компанией «СмартПарк».</p> <p>Перенос ключей подписи с устройств и на устройства данного семейства невозможен, так как на устройствах используется аппаратная криптография с неизвлекаемым ключом.</p>

Название семейства устройств в 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.»	<p>Если компьютер работает под управлением ОС Windows 10, на нем должно быть установлено ПО SafeNet Authentication Client (рекомендуемая версия — 10.6.146).</p> <p>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).</p> <p>Смарт-карта eToken PRO может использоваться с любым стандартным PC/SC-совместимым устройством считывания карт.</p> <p>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.</p>



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, и туннелируемым ресурсам

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

Таблица 11. Поддерживаемые внешние устройства для подключения к сайтам, использующим TLS ГОСТ, и туннелируемым ресурсам

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	<p>Входит в поставку ViPNet PKI Client.</p> <p>По умолчанию создан программный токен 8888.</p> <p>С помощью утилиты token_manager.exe на компьютере может быть создан другой программный токен.</p>
ESMART Token	Смарт-карты и токены типов ESMART Token, ESMART Token ГОСТ	<p>На компьютере должно быть установлено ПО ESMART PKI Client для Windows (рекомендуемая версия — 4.5 RC).</p> <p>Перенос ключей подписи с устройства и на устройство ESMART Token ГОСТ невозможен, так как на устройстве используется аппаратная криптография с неизвлекаемым ключом.</p>
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.»	<p>На компьютере должно быть установлено ПО «Единый Клиент JaCarta» компании «Аладдин Р.Д.» (рекомендуемая версия — 2.12).</p> <p>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.</p>
Rutoken	Электронные идентификаторы Рутокен ЭЦП, Рутокен ЭЦП 2.0 и Рутокен Lite производства компании «Актив»	<p>Необходимо загрузить и установить библиотеку PKCS#11 (загружается с сайта Rutoken).</p> <p>Перенос ключей подписи на данный тип устройств невозможен.</p>
Rutoken S	Электронные идентификаторы Рутокен S производства компании «Актив»	<p>На компьютере должны быть установлены драйверы Rutoken (рекомендуемая версия — 4.8.5.0).</p>

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 12. Алгоритмы и функции, поддерживаемые внешними устройствами

Название семейства устройств в 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 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 JaCarta PKI/ГОСТ и JaCarta-2 PKI/ГОСТ с апплетом ГОСТ, JaCarta-2 ГОСТ)	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 (короткий ключ 256 бит)	отсутствует	Да	Да
Rutoken	Рутокен ЭЦП 2.0 — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012; Рутокен Lite — отсутствует	Рутокен ЭЦП 2.0 — отсутствует; Рутокен Lite — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	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.

С

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 (Transport Layer Security)

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.

TSP-сервер (служба штампов времени)

Доверенный субъект инфраструктуры открытых ключей, обладающий точным и надежным источником времени и оказывающий услуги по созданию штампов времени.

XMLDSig

Формат подписи, позволяющий подписывать не только весь XML-документ, но и его часть, причем разные части XML-документа могут быть подписаны разными пользователями.

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 (ключ проверки ЭП)

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 несекретной 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 (ключ ЭП)

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.

Корневой сертификат ViPNet PKI Client Root

Сертификат, используемый компонентом ViPNet PKI Client TLS Unit для создания служебных сертификатов, с помощью которых устанавливаются соединения с веб-порталами.

Открепленная подпись

Тип электронной подписи, при использовании которого электронная подпись и служебная информация помещаются в отдельный контейнер `<имя_файла>.detached.sig`. Для проверки электронной подписи требуется не только данный контейнер, но и исходный файл, который в контейнер не входит.

Прикрепленная подпись

Тип электронной подписи, при использовании которой исходный файл, электронная подпись и служебная информация помещаются совместно в один контейнер с расширением `*.sig`.

Например, файл `file.txt` заверяется прикрепленной электронной подписью и помещается в контейнер `file.txt.sig`. Далее для проверки электронной подписи требуется только данный контейнер, который содержит и электронную подпись, и исходный файл.

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 (УЦ)

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 *.PFX (PKCS#12)

Одно из расширений стандарта PKCS#12. С помощью файла этого формата можно переносить закрытые ключи и сертификаты пользователя.

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).

Электронная подпись (ЭП)

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.