



ViPNet PKI Client Windows

Руководство пользователя

Версия продукта: 2.1.1

© АО «ИнфоТеКС», 2025

ФРКЕ.00175-03 34 07

Версия продукта 2.1.1

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

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

ViPNet® является зарегистрированным товарным знаком АО «ИнфоТеКС».

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

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

АО «ИнфоТеКС»

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

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

Сайт: infotecs.ru

Служба поддержки: hotline@infotecs.ru

Содержание

Введение.....	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.....	14
 Глава 2. Начало работы	15
Порядок подготовки к работе.....	16
Установка и обновление	17
Запуск и завершение работы.....	18
Активация лицензии.....	19
Загрузка лицензии	19
Активация лицензии с использованием файла.....	20
Обновление лицензии.....	22
 Глава 3. Служебные функции	23
Импорт и экспорт настроек.....	24
Автоматическое получение настроек из файла.....	24
Удаление ViPNet PKI Client.....	25
 Глава 4. Управление сертификатами	26
Какие нужны сертификаты.....	27
Подготовка личного сертификата и ключа ЭП	28
Получение сертификата.....	29
Установка сертификатов и CRL.....	32
Проверка сертификатов.....	33
Смена и сброс пароля хранилища ключей.....	34
Просмотр сведений о сертификатах.....	35

Добавление точек распространения CRL	37
Экспорт сертификатов	39
Перенос сертификатов и ключей ЭП между устройствами	40
Перенос сертификатов и ключей ЭП в облачный сервис	42
Удаление сертификатов и ключей ЭП	43
Глава 5. Использование облачных сервисов ЭП	44
Об облачных сервисах ЭП	45
Перед подключением к сервису	46
Настройка подключения к сервису	47
Подключение к сервису	48
Смена пароля учётной записи пользователя	49
Глава 6. Подпись и зашифрование файлов	50
Требования к сертификатам для подписи и зашифрования	51
Порядок подписания файла	52
Настройка параметров процесса подписи	52
Подписание файла	53
Порядок зашифрования файла	55
Настройка параметров зашифрования	55
Зашифрование файла	56
Подписание и зашифрование файла	57
Глава 7. Работа с файлами, полученными от других пользователей	59
Получение подписанных и зашифрованных файлов	60
Проверка ЭП	61
Расшифрование файла	63
Глава 8. Подключение к сайтам, использующим TLS ГОСТ	65
Порядок настройки	66
Подключение к сайту	67
Просмотр информации о TLS-соединениях	68
Глава 9. Возможные неполадки	69
Обращение в техническую поддержку	70
Общие неполадки	71
Ошибка при удалении сертификата	71
Ошибка создания запроса на сертификат	71
Невозможно просмотреть созданный контейнер ключей на токене	72

File Unit	73
Нет сертификата в списке сертификатов для подписи.....	73
Ошибка при расшифровании.....	73
Приложение А. Поддерживаемые токены	74
Список поддерживаемых токенов.....	74
Аппаратная поддержка алгоритмов ГОСТ токенами	75
Приложение В. Термины и сокращения.....	76



Введение

О документе	7
О программе	8
Обратная связь	10

О документе

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

Документ предназначен для пользователей, которые используют ViPNet PKI Client для работы в инфраструктуре открытых ключей (PKI): подписания и шифрования файлов, защищенного подключения к сайтам и туннелируемым ресурсам. Предполагается, что пользователи имеют общее представление о PKI.

Для получения более подробной информации о настройке ViPNet PKI Client ознакомьтесь с документом «ViPNet PKI Client Windows. Руководство администратора».

Соглашения документа

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



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

О программе

Комплект поставки

- Установочный файл `pki_client_installer.exe`.
- Файлы для установки через Active Directory:
 - `ViPNet_PKI_Client_<разрядность>_MUI_<версия>.msi`;
 - `iuprng_<разрядность>.msi`.
- Документация:
 - ViPNet PKI Client Windows. Руководство пользователя.
 - ViPNet PKI Client Windows. Руководство администратора.
 - ViPNet PKI Client. Руководство разработчика.
 - Архив с описанием SDK `ViPNet PKI Client Web Unit SDK.zip`.

Системные требования

- Процессор — Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с двумя или более ядрами.
- Оперативная память — не менее 2 Гбайт.
- Свободное место на жёстком диске — не менее 1 Гбайт.
- Операционная система с последними пакетами обновлений:
 - Windows Server 2016 — 64-разрядная;
 - Windows Server 2019 — 64-разрядная;
 - Windows Server 2022 — 64-разрядная;
 - Windows Server 2025 — 64-разрядная;
 - Windows 10 — 32/64-разрядная следующих версий и сборок:
 - версия 1607, сборка 14393;
 - версия 1809, сборка 17763;
 - версия 21H2, сборка 19044;
 - версия 22H2, сборка 19045;
 - Windows 11 — 64-разрядная следующих версий и сборок:
 - версия 24H2, сборка 26100;

- версия 25H2, сборка 26200.

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

- Браузер — Chromium-Gost, Microsoft Edge, Mozilla Firefox, Google Chrome, Opera, Яндекс.Браузер последних версий.
- Для использования сертификатов, хранящихся в облачном сервисе ЭП — ViPNet PKI Service версии 2.0 или выше.

Обратная связь

Контактная информация

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

Дополнительная информация на сайте ИнфоТеКС

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

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



1

Назначение и состав

Назначение	12
Компоненты	13
Лицензирование	14

Назначение

ViPNet PKI Client — средство криптографической защиты информации и электронной подписи (далее — ЭП).

С помощью ViPNet PKI Client вы можете:

- Создать [запрос на сертификат](#) и, передав его в удостоверяющий центр (далее — УЦ), получить сертификат.
- Подписать файлы и проверить [ЭП файлов](#).
- Зашифровать и расшифровать файлы.
- Подключиться к сайтам по TLS ГОСТ, в том числе с [аутентификацией пользователя](#).
Поддерживаемые версии [протокола TLS](#): 1.2, 1.3.
- Работать в облачном сервисе ЭП на базе [ViPNet PKI Service](#): подписывать файлы, проверять ЭП файлов, расшифровать файлы.
- Установить TLS-соединения с ресурсами, которые туннелирует ViPNet TLS Gateway.
Поддерживаемые протоколы: RDP, HTTP, SMTP, POP3, IMAP, WebDAV и SQL.

ViPNet PKI Client можно использовать для встраивания криптографических функций в пользовательские веб-приложения (см. «Руководство разработчика»).

ViPNet PKI Client использует российские криптографические алгоритмы:

- Алгоритм проверки ЭП: ГОСТ Р 34.10-2012 с вычислением хэш-функции по ГОСТ Р 34.11-2012.
- Алгоритм создания ЭП: ГОСТ Р 34.10-2012 с вычислением хэш-функции по ГОСТ Р 34.11-2012.
- Алгоритм шифрования для TLS-соединений: ГОСТ 28147-89 и ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018) «Магма» и «Кузнечик».
- Алгоритм шифрования для файлов: ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018) «Магма» и «Кузнечик».

Компоненты

Компонент	Назначение
 Certificate Unit	Управление сертификатами: создание запросов на сертификаты, установка, просмотр, экспорт сертификатов
 CRL Unit	Автоматическое обновление CRL
 Cloud Unit	Выполнение криптографических операций средствами облачного сервиса ЭП на базе ViPNet PKI Service
 File Unit	Подпись, шифрование файлов Проверка ЭП, расшифрование файлов
 TLS Unit	Подключение к сайтам, использующим TLS ГОСТ
 Tunnel Unit	Подключение к туннелируемым ViPNet TLS Gateway ресурсам (см. «Руководство администратора»)
 Web Unit	Управление сертификатами, использование ЭП, шифрования в веб-приложениях

Лицензирование

При работе в ViPNet PKI Client без лицензии доступно только [управление сертификатами и CRL](#).

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

Лицензирование с помощью файла

- 1 Получите файл лицензии одним из способов:
 - обратитесь в [ИнфоТеКС](#);
 - обратитесь к своему администратору.
- 2 [Загрузите файл лицензии](#) в ViPNet PKI Client.
- 3 Если лицензия загружена, но не активирована — [активируйте её](#).

Лицензирование через ViPNet TLS Gateway

Если в вашей организации для лицензирования используется ViPNet TLS Gateway, см. «Руководство администратора».

2

Начало работы

Порядок подготовки к работе	16
Установка и обновление	17
Запуск и завершение работы	18
Активация лицензии	19
Обновление лицензии	22

Порядок подготовки к работе

- 1 Установите ViPNet PKI Client.
- 2 Активируйте лицензию.
- 3 Подготовьте личный сертификат и ключ ЭП.
- 4 Установите в хранилище личный сертификат, корневой сертификат УЦ, а также при наличии сертификаты всех УЦ из цепочки и соответствующие CRL.
- 5 Настройте автообновление CRL.
- 6 Если в вашей организации используется облачный сервис ЭП на базе ViPNet PKI Service, настройте подключение к нему.
- 7 Настройте параметры процесса подписи.
- 8 Настройте параметры зашифрования.
- 9 Вы можете настроить подключение к сайтам по TLS ГОСТ.

Установка и обновление



Совет. Если у вас установлен ViPNet PKI Client версии 1.x, сначала удалите устаревшую версию, затем установите новую. При удалении ViPNet PKI Client настройки сохранятся на компьютере.

- 1 Запустите установочный файл.
- 2 Ознакомьтесь с лицензионным соглашением.
- 3 Чтобы принять условия лицензионного соглашения, выберите **Я принимаю условия лицензионного соглашения** и нажмите **Далее**.
- 4 На шаге **Автоматическое получение настроек из файла** выберите папку пользователя.



Примечание. Папку пользователя можно сменить после установки ViPNet PKI Client, например, по указаниям вашего администратора.

- 5 Следуйте указаниям мастера.

Запуск и завершение работы

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

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

Для завершения работы:

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

Если [электронная рулетка](#) не запускалась в рамках текущего сеанса работы TLS Unit, следуйте указаниям в открывшемся окне.

Активация лицензии

Вы можете активировать лицензию с использованием файла лицензии или через ViPNet TLS Gateway.

При использовании файла лицензии:

- 1 [Загрузите лицензию](#) в ViPNet PKI Client.
- 2 Если лицензия не была активирована сразу (например, из-за отсутствия интернет-соединения), [активируйте её вручную](#).



Примечание. Если в вашей организации для лицензирования используется ViPNet TLS Gateway, см. «Руководство администратора».

Загрузка лицензии

- 1 [Перейдите в настройки ViPNet PKI Client](#).
- 2 Выберите  **Лицензия**.
- 3 Нажмите **Выбрать способ** > **С использованием файла лицензии**.
- 4 Выберите файл лицензии и в окне **Загрузка лицензии** нажмите **Загрузить**.

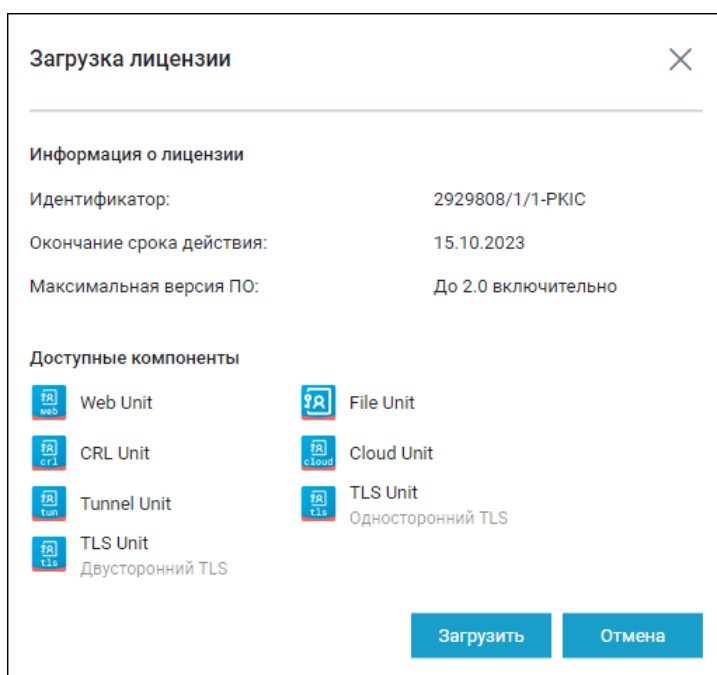


Рисунок 1. Просмотр информации о лицензии

Если связь с сервером регистрации ИнфоТеКС установлена, лицензия будет активирована автоматически. Если лицензия не была активирована, [активируйте её вручную](#).

Активация лицензии с использованием файла

1 Перейдите в настройки ViPNet PKI Client.

2 Выберите  **Лицензия**.

3 Нажмите **Активировать**.

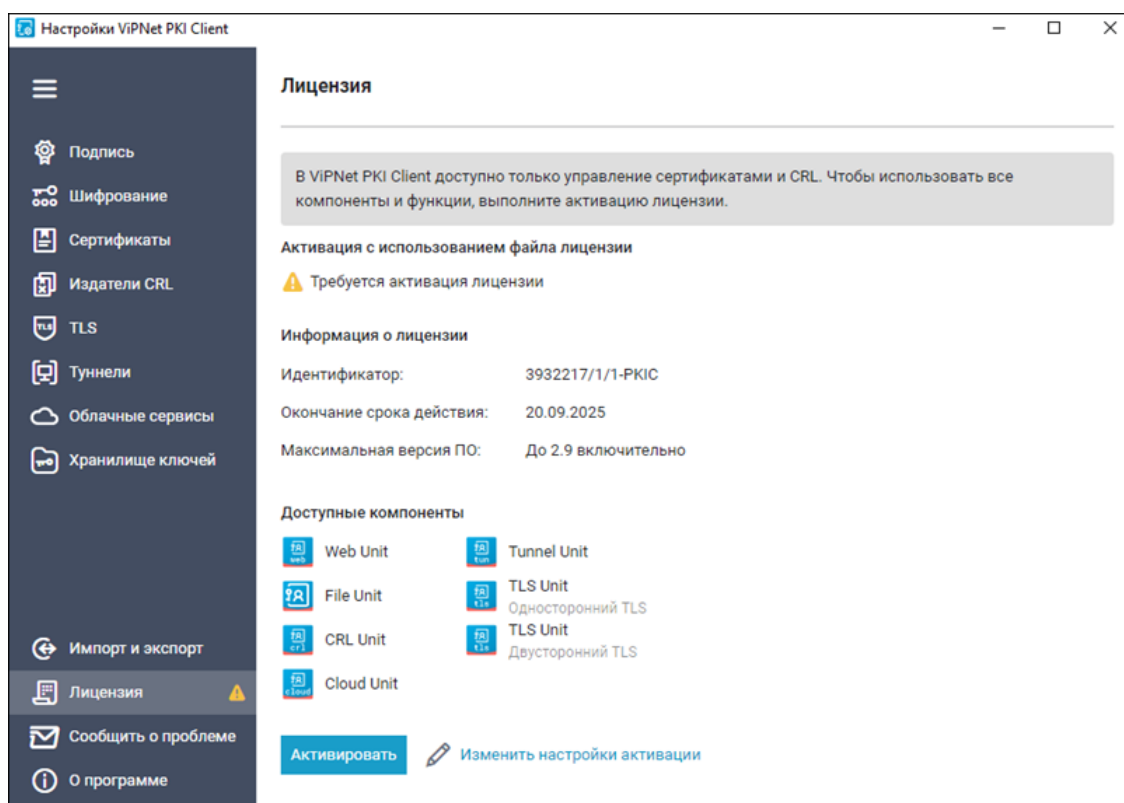


Рисунок 2. Просмотр информации о лицензии

4 Нажмите  **Сохранить запрос**.

5 Укажите имя и путь для сохранения файла запроса.

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

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

8 В поле **Код регистрации**, полученный в ответном письме введите регистрационный код и нажмите **Активировать**.

Активация лицензии по коду регистрации

✕

Для активации лицензии требуется получить код регистрации. Для этого сохраните запрос, отправьте его по адресу reg@infotecs.ru и дождитесь ответного письма.

↓ Сохранить запрос

Код регистрации, полученный в ответном письме:

4WWW8E-6J4FTG7-6M6JD5Y

Серийный номер:

8XKR-JLMS-WWG2-XG7A

Код компьютера:

5RMA2W4-5F5HSW4-4M3LNP6-57L7Y7X-6A89Q7L

Активировать

Отмена

Рисунок 3. Ввод данных для активации ViPNet PKI Client

9 Нажмите ОК.

Обновление лицензии

Если [лицензия](#) была активирована с использованием файла и вам необходимо обновить её по истечении срока действия или для расширения функций ViPNet PKI Client:

- 1 Отправьте запрос на получение лицензии в [ИнфоТеКС](#) и получите новый файл лицензии.
- 2 [Перейдите в настройки ViPNet PKI Client.](#)
- 3 Выберите  **Лицензия**.
- 4 Нажмите **Изменить настройки активации** > **С использованием файла лицензии** > **Выбрать файл**.
- 5 Выберите файл лицензии и нажмите **Открыть**.
- 6 В окне **Загрузка лицензии** нажмите **Загрузить**.
- 7 Если лицензия загрузилась и не активировалась автоматически, [активируйте её вручную](#).



Примечание. Если при активации лицензии её статус сменился на  **Лицензия недействительна**, отправьте запрос на получение нового файла лицензии в [ИнфоТеКС](#).

3

Служебные функции

Импорт и экспорт настроек	24
Удаление ViPNet PKI Client	25

Импорт и экспорт настроек

Часть настроек программы можно выгрузить в файл и использовать:

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

Подробнее об импорте и экспорте настроек см. «Руководство администратора».

Автоматическое получение настроек из файла

Выбор папки настроек

Папка для файла с настройками указывается при установке ViPNet PKI Client. Вы можете изменить её по просьбе администратора:

- 1 [Перейдите в настройки ViPNet PKI Client.](#)
- 2 Выберите  **Импорт и экспорт.**
- 3 Нажмите **Настроить.**
- 4 Выберите папку, из которой вы будете получать настройки:
 - папка пользователя — если файл с настройками помещён в вашу папку;
 - общая папка — если файл с настройками помещён в общую папку, путь к которой вам передал администратор.
- 5 Нажмите **Сохранить.**

Отключить автоматическое получение настроек

- 1 [Перейдите в настройки ViPNet PKI Client.](#)
- 2 Выберите  **Импорт и экспорт.**
- 3 Нажмите **Настроить.**
- 4 Выберите папку пользователя.
- 5 Убедитесь, что в выбранной папке нет файла `pki_client_settings.json`.



Примечание. Подробнее об автоматическом получении настроек из файла см. «Руководство администратора».

Удаление ViPNet PKI Client

Удалите ViPNet PKI Client стандартными средствами Windows. Вы можете сохранить пользовательские данные:

- сертификаты и ключи ЭП;
- подписанные и зашифрованные файлы;
- настройки ЭП, зашифрования, туннелирования и другие.

Для этого в окне **Удаление ViPNet PKI Client** установите флажок **Сохранить пользовательские данные**.

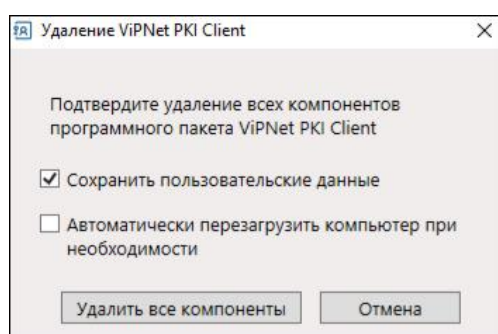


Рисунок 4. Удаление ViPNet PKI Client с сохранением пользовательских данных



Примечание. Вы можете удалить ViPNet PKI Client с помощью команды:

```
<путь к установочному файлу>\pki_client_installer.exe -q -uninstall
```

4

Управление сертификатами

Какие нужны сертификаты	27
Подготовка личного сертификата и ключа ЭП	28
Получение сертификата	29
Установка сертификатов и CRL	32
Смена и сброс пароля хранилища ключей	34
Просмотр сведений о сертификатах	35
Добавление точек распространения CRL	37
Экспорт сертификатов	39
Перенос сертификатов и ключей ЭП между устройствами	40
Перенос сертификатов и ключей ЭП в облачный сервис	42
Удаление сертификатов и ключей ЭП	43

Какие нужны сертификаты

- Личный сертификат — для подписи, расшифровки файлов, подключения к сайтам по TLS ГОСТ, и туннелируемым ресурсам с аутентификацией пользователя.
Получите его в УЦ [по запросу](#) и [установите](#), выбрав тип **Личный**.
- Сертификаты получателей — для зашифровки файлов.
Запросите их у получателей зашифрованных файлов и [установите](#), выбрав тип **Другой**.
- Сертификат УЦ — для подтверждения подлинности сертификатов, изданных этим УЦ: личного, сертификата получателя или сертификата другого УЦ.
Получите его в УЦ и [установите](#) в хранилище сертификатов.
- **CRL** или другое подтверждение действительности сертификатов в зависимости от того, что используется в УЦ:
 - Файлы CRL — получите файл в УЦ и [установите в хранилище сертификатов](#) вручную.
 - **Точки распространения CRL** — можно автоматически получать и устанавливать CRL путём опроса точек распространения. Вы можете просмотреть URL для опроса в [сведениях о сертификатах](#), изданных УЦ, в поле **Точки распространения списка аннулированных сертификатов**.
 - **Сервис онлайн-проверки статусов сертификатов по протоколу OCSP**. В этом случае CRL не используются. Информация о поддержке сервиса содержится в [сведениях о сертификатах](#), изданных УЦ, в поле **Публикация информации об издателе**.

Подготовка личного сертификата и ключа ЭП

Если нет сертификата и ключа ЭП

- 1 [Создайте запрос на сертификат.](#)
- 2 [Передайте запрос в УЦ.](#)
- 3 [Получите в УЦ:](#)
 - [личный сертификат;](#)
 - [корневой сертификат УЦ;](#)
 - [при наличии сертификаты всех УЦ из цепочки и соответствующие CRL.](#)
- 4 [Установите полученные сертификаты и CRL.](#)

Если есть сертификат и ключ ЭП в PFX-файле

- 1 [Импортируйте сертификат и ключ ЭП.](#)
- 2 [Установите корневой сертификат УЦ, а также при наличии сертификаты всех УЦ из цепочки и соответствующие CRL.](#)

Если есть сертификат на токене

- 1 [Подключите токен к компьютеру.](#)
- 2 Выберите  [Подключено устройств.](#)
- 3 В строке сертификата нажмите  > [Установить в хранилище.](#)
- 4 [Установите корневой сертификат УЦ, а также при наличии сертификаты всех УЦ из цепочки и соответствующие CRL.](#)

Если есть сертификат в облачном сервисе ЭП

- 1 [Настройте подключение к облачному сервису ЭП.](#)
- 2 Если у вас нет сертификата в облачном сервисе ЭП или вам нужно его обновить:
 - 2.1 [Создайте запрос на сертификат с сохранением ключа ЭП в облачном сервисе ЭП.](#)
 - 2.2 [Получите сертификат в УЦ.](#)
 - 2.3 [Для установки сертификата в облачный сервис ЭП обратитесь к вашему администратору.](#)

Получение сертификата

- 1 Чтобы сохранить ключ ЭП в облачном сервисе ЭП, [добавьте его и выберите используемым по умолчанию](#).
- 2 Создайте запрос на сертификат одним из способов:
 - [Перейдите в настройки ViPNet PKI Client](#) и в разделе  Сертификаты нажмите  **Создать запрос**.
 - В меню Пуск выберите ViPNet PKI Client >  **Создание запроса на сертификат**.



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

- 3 Выберите параметры и заполните личные данные.

Создание запроса на сертификат – ViPNet PKI Client

Копировать данные из сертификата
 Очистить форму

Шаблон сертификата

Физическое лицо

Параметры сертификата

Алгоритм ключа проверки ЭП: ГОСТ Р 34.10-2012 (512)

Параметры ключа проверки ЭП: Набор параметров А (ТК 26)

☒ Экспортируемый ключ ЭП

Поля сертификата:

* Фамилия: Иванов

* Имя и отчество: Иван Иванович

* Общее имя: Иванов Иван Иванович

* Страна: Российская Федерация (RU)

Регион: Регион

Населенный пункт: Населённый пункт

Улица, дом: Улица, дом

* СНИЛС: 12345678901

* ИНН физического лица: 123456789012

Электронная почта: ivan@ivanov.ru

☒ Добавить наименование средства ЭП владельца (ViPNet PKI Client)

Расширения

Срок действия ключа ЭП, мес: 36
От 1 до 360 месяцев.

Класс средства ЭП: Не указывать

Идентификация заявителя: Личное присутствие

Параметры сохранения файла запроса

Кодировка: ☒ PEM ☐ DER

Создать запрос Заккрыть

Рисунок 5. Создание запроса на сертификат

Примечание. С помощью шаблона сертификата **Специальный** вы можете:



- добавить другие значения расширений;
- изменить критичность расширений;
- изменить порядок атрибутов владельца.

4 Нажмите **Создать запрос**.

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

6 Укажите место хранения контейнера ключей ЭП:

- **Хранилище ViPNet PKI Client** — нажмите **Продолжить** и введите пароль.
Если хранилище еще не создано, задайте имя контейнера и нажмите **Продолжить**. Задайте и подтвердите пароль хранилища.
- **Токен** — задайте имя контейнера, **подключите токен** и выберите его в списке. Нажмите **Продолжить** и введите PIN-код от токена.
- **Облачный сервис** — задайте имя контейнера, нажмите **Продолжить** и подключитесь к облачному сервису ЭП.



Примечание. Если вы выбрали местом хранения контейнера ключей ЭП облачный сервис, может потребоваться подтверждение операции. Введите код подтверждения.

- 7 Нажмите **ОК**.
- 8 Передайте запрос в УЦ.
- 9 Получите личный сертификат и корневой сертификат УЦ, а также при наличии сертификаты всех УЦ из цепочки и соответствующие CRL.
- 10 **Установите полученные сертификаты**.

Установка сертификатов и CRL

Описанными ниже способами устанавливайте только те личные сертификаты, [запрос на которые был создан в ViPNet PKI Client](#). Если сертификат получен иным способом, см. [Подготовка личного сертификата и ключа ЭП](#).

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

Чтобы установить сертификаты и CRL:

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



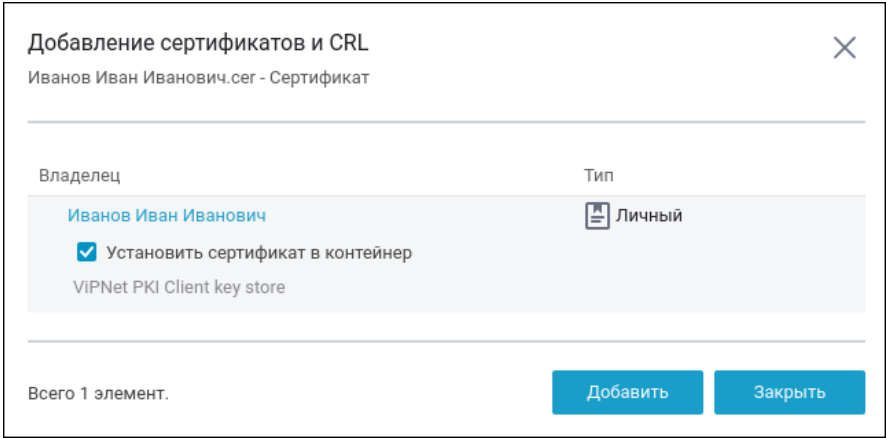
Примечание. Чтобы установить сертификаты УЦ и CRL в хранилище сертификатов локального компьютера, запустите настройки ViPNet PKI Client от имени администратора.

2 Выберите Сертификаты.

3 Нажмите **Добавить сертификат или CRL** и укажите путь к файлам сертификатов или CRL.

4 В окне **Добавление сертификатов и CRL** отображается список устанавливаемых сертификатов или CRL:

- Чтобы просмотреть подробную информацию об устанавливаемых сертификатах и CRL, нажмите имя владельца сертификата или CRL.
- Чтобы удалить сертификат или CRL из списка, нажмите  (появляется при наведении курсора на строку сертификата или CRL).
- Чтобы в контейнер ключей установить сертификат, запрос на который был создан в ViPNet PKI Client, установите соответствующий флажок.



Добавление сертификатов и CRL

Иванов Иван Иванович.сег - Сертификат

Владелец	Тип
Иванов Иван Иванович	 Личный
☒ Установить сертификат в контейнер ViPNet PKI Client key store	

Всего 1 элемент.

Добавить Заккрыть

Рисунок 6. Установка сертификатов и CRL



Внимание! Сертификаты и CRL с истёкшим сроком действия или имеющие недействительную ЭП помечены значком  и не будут установлены.

- 5 Нажмите **Добавить**.
- 6 Если вы установили сертификат в контейнер ключей, введите пароль хранилища ViPNet PKI Client.
- 7 Нажмите **Заккрыть**.



Примечание. Если после установки сертификата в строке с именем владельца появится значок , см. [Проверка сертификатов](#).

Проверка сертификатов

Сертификаты, статус которых не удалось проверить, и недействительные сертификаты нельзя использовать для подписания и шифрования файлов в ViPNet PKI Client. Чтобы проверить [действительность](#) установленных сертификатов:

- 1 [Перейдите в настройки ViPNet PKI Client](#).
- 2 Выберите  **Сертификаты**.
- 3 Слева вверху нажмите .

В строке сертификата появится значок:

-  — если не удалось проверить статус сертификата;
-  — если сертификат недействителен.

Чтобы просмотреть причину, наведите курсор на значок:

Таблица 1. Статусы сертификатов

Статус	Действия
 - Не найден сертификат издателя - Ошибка построения цепочки сертификатов - Корневой сертификат не установлен в хранилище	Установите в хранилище все сертификаты цепочки
- Не найден действительный CRL - Срок действия CRL истёк - Срок действия CRL не наступил - В цепочке присутствует сертификат, который не удалось проверить	Получите в УЦ актуальный CRL и установите его в хранилище
 Сертификат недействителен	Если это личный сертификат, получите новый сертификат и установите его. Если это сертификат получателя, запросите у получателя новый сертификат

Смена и сброс пароля хранилища ключей

Смена пароля хранилища ключей

- 1 [Перейдите в настройки ViPNet PKI Client.](#)
- 2 Выберите  **Хранилище ключей.**
- 3 Нажмите **Сменить пароль.**
- 4 Введите текущий пароль, затем задайте и подтвердите новый.
- 5 Нажмите **Продолжить.**

Сброс пароля хранилища ключей

Вы можете сбросить пароль хранилища ключей без удаления приложения, например, если компьютером будет пользоваться другой пользователь и вам нужно удалить личную информацию.



Внимание! При сбросе пароля хранилища ключей будет удалена вся информация из хранилища.

Чтобы сбросить пароль:

- 1 [Перейдите в настройки ViPNet PKI Client.](#)
- 2 Выберите  **Хранилище ключей.**
- 3 Нажмите **Сбросить пароль.**
- 4 Нажмите **Продолжить.**
- 5 Задайте и подтвердите новый пароль хранилища ключей ViPNet PKI Client. Нажмите **Продолжить.**

Просмотр сведений о сертификатах

- 1 [Перейдите в настройки ViPNet PKI Client.](#)
- 2 Выберите  Сертификаты.
- 3 По умолчанию ViPNet PKI Client предупредит об истечении срока действия сертификата за 60 дней. Чтобы изменить это, справа вверху нажмите  и введите количество дней.
- 4 Вверху нажмите  и выберите, какие сертификаты вы хотите просмотреть:
 - Все сертификаты (по умолчанию);
 - Личные сертификаты;
 - Сертификаты других пользователей;
 - Сертификаты на внешних устройствах;
 - Сертификаты в облаке (требуется [подключение к облачному сервису ЭП](#)).



Совет. Чтобы изменить состав отображаемых столбцов, нажмите  и выберите столбцы с помощью флажков.

Чтобы отсортировать сертификаты по любому столбцу, щёлкните название столбца.

Чтобы найти сертификаты, в поле поиска введите часть имени владельца или издателя сертификата.

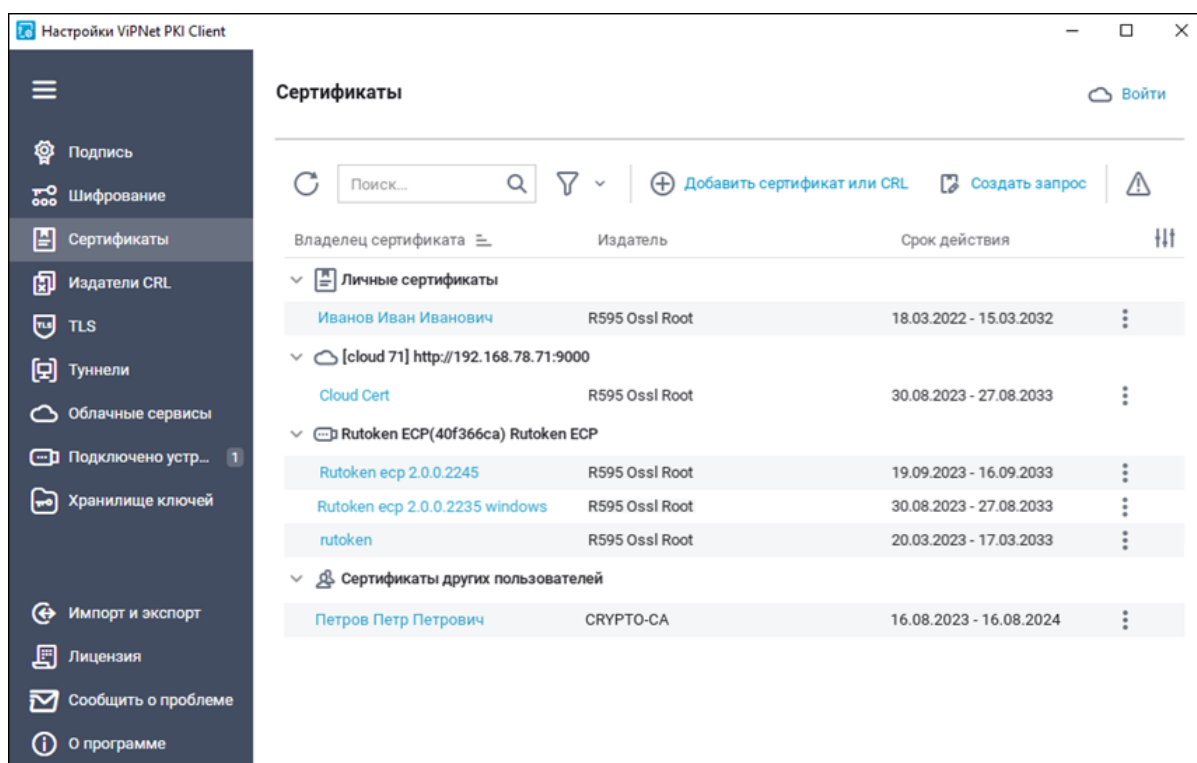


Рисунок 7. Просмотр сертификатов в ViPNet PKI Client

- 5 Чтобы просмотреть подробные сведения о сертификате, нажмите имя владельца сертификата.

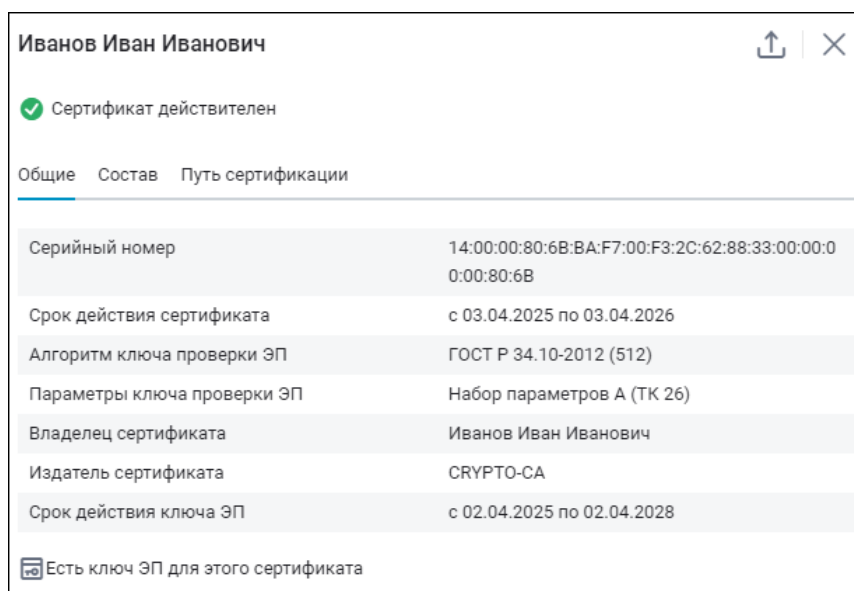


Рисунок 8. Сведения о сертификате



Внимание! Если при просмотре сведений о сертификате он отображается как недействительный или его статус не удалось проверить, см. [Проверка сертификатов](#).

Добавление точек распространения CRL

Если в УЦ есть точки распространения CRL и они доступны по сети, после установки сертификата УЦ CRL будут обновляться автоматически. Вы можете просмотреть URL точек распространения в свойствах сертификатов, изданных УЦ, в поле Точки распространения списка аннулированных сертификатов.

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



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

Добавьте точки распространения CRL для каждого сертификата из цепочки сертификатов УЦ.

- 1 У вашего администратора узнайте URL точки распространения CRL.
- 2 [Перейдите в настройки ViPNet PKI Client.](#)
- 3 Выберите  **Издатели CRL.**
- 4 Вверху нажмите  **Добавить.**
- 5 Выберите сертификат и нажмите **Выбрать.**
- 6 Нажмите на выбранный сертификат и на панели справа нажмите  **Добавить.**
- 7 Введите URL точки распространения CRL, период её опроса и нажмите .
- 8 Вы можете добавить URL и период опроса следующей точки.

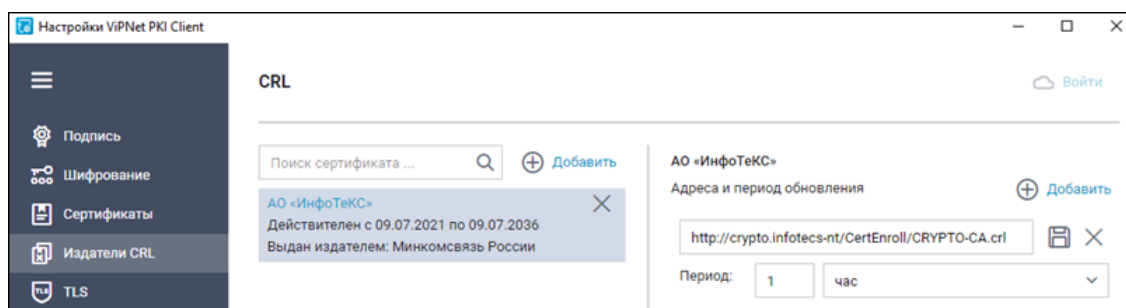


Рисунок 9. Добавление точки распространения CRL

- 9 Нажмите **Сохранить.**

Актуальные CRL будут автоматически скачиваться и устанавливаться в хранилище сертификатов **Промежуточные центры сертификации > Список отзыва сертификатов**. Подробнее о настройках и событиях при автообновлении CRL см. «Руководство администратора».



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

Экспорт сертификатов

Вы можете экспортировать личные сертификаты и сертификаты получателей, установленные в ViPNet PKI Client, в файлы формата X.509 (*.cer, *.pem). Это может потребоваться, например, для архивирования сертификатов или передачи сертификатов другим пользователям.



Примечание. Об экспорте сертификата с ключом ЭП см. [Перенос сертификатов и ключей ЭП между устройствами](#).

Чтобы экспортировать сертификат из ViPNet PKI Client:

- 1 [Перейдите в настройки ViPNet PKI Client](#).
- 2 Выберите  Сертификаты.
- 3 Напротив сертификата нажмите  > **Экспортировать**.
- 4 В окне **Экспорт сертификата** выберите формат файла экспорта и нажмите **Экспортировать**.
- 5 Укажите папку для сохранения файла и нажмите **Сохранить**.

Перенос сертификатов и ключей ЭП между устройствами

Экспорт сертификата и ключа ЭП в PFX-файл



Внимание! Вы можете экспортировать сертификат вместе с ключом ЭП, только если при создании запроса на этот сертификат ключ ЭП был помечен как экспортируемый.

- 1 [Перейдите в настройки ViPNet PKI Client.](#)
- 2 Выберите  Сертификаты.
- 3 Нажмите  и выберите **Личные сертификаты**.
- 4 Напротив сертификата нажмите  > **Экспортировать**.
- 5 В окне **Экспорт сертификата** выберите **PFX (с ключом ЭП)** и нажмите **Экспортировать**.
- 6 Укажите имя и путь для сохранения PFX-файла и нажмите **Сохранить**.
- 7 Задайте и подтвердите пароль PFX-файла.
- 8 Выберите алгоритм шифрования или оставьте значение по умолчанию.
- 9 Нажмите **Продолжить** и введите пароль хранилища ViPNet PKI Client.

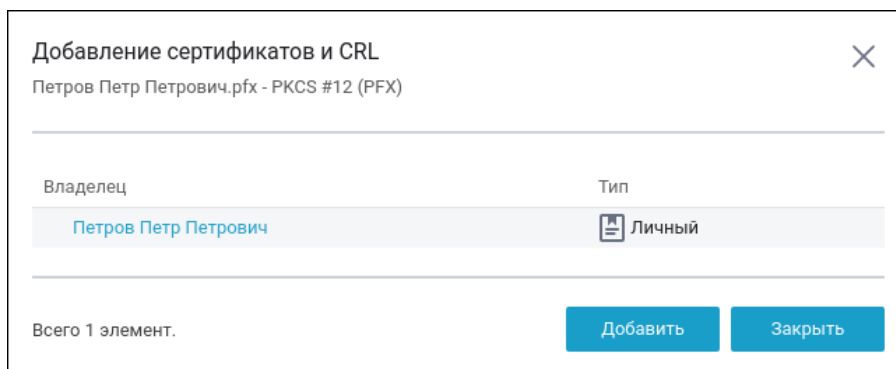
Сертификат и ключ ЭП будут сохранены в PFX-файл, который вы можете перенести на другое устройство.



Внимание! Файл с сертификатом и ключом ЭП переносите на другое устройство только доверенным способом. Например, используйте защищённый канал или внешнее устройство, но не используйте электронную почту или сетевые хранилища.

Импорт сертификата и ключа ЭП из PFX-файла

- 1 [Перейдите в настройки ViPNet PKI Client.](#)
- 2 Выберите  Сертификаты.
- 3 Нажмите  **Добавить сертификат или CRL** и укажите путь к PFX-файлу.
- 4 Введите пароль PFX-файла.
- 5 В окне **Добавление сертификатов и CRL** нажмите **Добавить**.



Добавление сертификатов и CRL

Петров Петр Петрович.pfx - PKCS #12 (PFX)

Владелец	Тип
Петров Петр Петрович	Личный

Всего 1 элемент.

Добавить Заккрыть

Рисунок 10. Импорт сертификата и ключа ЭП

6 Укажите место хранения контейнера ключей:

- **Хранилище ViPNet PKI Client** — нажмите **Продолжить** и введите пароль.

Если хранилище ещё не создано, задайте имя контейнера и нажмите **Продолжить**. Задайте и подтвердите пароль хранилища.

- **Токен** — задайте имя контейнера, **подключите токен** и выберите его в списке. Нажмите **Продолжить** и введите PIN-код от токена.

7 Нажмите **Заккрыть**.

Перенос сертификатов и ключей ЭП в облачный сервис

Если в вашей организации используется облачный сервис ViPNet PKI Service, вы можете перенести сертификат и ключ ЭП из хранилища сертификатов локального компьютера в облачный сервис напрямую из ViPNet PKI Client, без экспорта в PFX-файл.



Внимание! После переноса в облачный сервис сертификат и ключ ЭП будут удалены из хранилища сертификатов. Вы не сможете использовать их:

- для подписания и расшифровки файлов без подключения к облачному сервису;
- для подключения к туннелируемым ресурсам с аутентификацией пользователя.

Вы можете перенести сертификат и ключ ЭП, только если:

- при создании запроса на этот сертификат ключ ЭП был помечен как экспортируемый;
- сертификат не используется для подключения к туннелируемым ресурсам или к облачному сервису;
- перенос сертификатов и ключей ЭП включён администратором ViPNet PKI Service;
- используется ViPNet PKI Service версии 2.3.0 или выше.

Чтобы перенести сертификат и ключ ЭП в облачный сервис:

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

2 [Подключитесь к облачному сервису.](#)

3 Выберите  Сертификаты.

4 Нажмите  и выберите **Личные сертификаты**.

5 Напротив сертификата нажмите  > **Перенести в облачный сервис**.

6 Нажмите **Продолжить**.

7 Введите пароль хранилища ViPNet PKI Client.

8 Проверьте, что сертификат отображается в списке облачных сертификатов:

8.1 Слева вверху нажмите .

8.2 Нажмите  и выберите **Сертификаты в облаке**.

Удаление сертификатов и ключей ЭП

- 1 Перейдите в настройки ViPNet PKI Client.
- 2 Чтобы удалить сертификат и ключ ЭП, хранящиеся в облачном сервисе, [подключитесь к облачному сервису](#).
- 3 Выберите  Сертификаты.
- 4 Вверху нажмите  и в списке выберите [группу сертификатов](#).
- 5 Напротив сертификата нажмите  > Удалить.
- 6 Выберите Подтверждаю удаление <имя владельца сертификата>.
- 7 Чтобы удалить ключ ЭП, соответствующий сертификату, например, при аннулировании сертификата, установите соответствующий флажок и нажмите Удалить сертификат.

Внимание! Восстановить ключ ЭП нельзя.



Флажок Удалить ключ электронной подписи, соответствующий сертификату не отображается, если сертификат не содержит информацию о расположении ключа ЭП (например, при удалении сертификата получателя).

- 8 В зависимости от места хранения ключа ЭП:
 - **Хранилище ViPNet PKI Client** — введите пароль хранилища ViPNet PKI Client и нажмите Продолжить.
 - **Токен** — введите PIN-код от токена.



Примечание. Если вы удаляете сертификат из категории Сертификаты других пользователей, подтвердите удаление сертификата и нажмите Удалить сертификат.

5

Использование облачных сервисов ЭП

Об облачных сервисах ЭП	45
Перед подключением к сервису	46
Настройка подключения к сервису	47
Подключение к сервису	48
Смена пароля учётной записи пользователя	49

Об облачных сервисах ЭП

Облачные сервисы ЭП используются в корпоративных сетях для организации электронного документооборота. С помощью облачного сервиса ЭП можно подписывать и расшифровывать файлы, а также проверять ЭП файлов.

Если в вашей организации используется облачный сервис ViPNet PKI Service, вы можете работать с ним из интерфейса ViPNet PKI Client. В процессе установки сертификата ключ ЭП сохранится в облачном сервисе ЭП.

Перед подключением к сервису

1 Получите у вашего администратора:

- адрес ViPNet PKI Service;
- способ подключения и дополнительные данные (см. таблицу).

Таблица 2. Способы подключения и дополнительные данные

Способ подключения	Дополнительные данные
HTTP, имя и пароль	Имя и разовый пароль учётной записи
HTTPS (TLS ГОСТ), имя и пароль	• Имя и разовый пароль учетной записи; • Корневой сертификат УЦ, в котором издан сертификат ViPNet PKI Service, а также все сертификаты цепочки и соответствующие CRL
HTTPS (TLS ГОСТ), сертификат	• Корневой сертификат УЦ, в котором издан сертификат ViPNet PKI Service, а также все сертификаты цепочки и соответствующие CRL; • Список УЦ, в которых можно получить сертификат для подключения к облачному сервису ЭП

2 Если вы подключаетесь по протоколу HTTPS, [установите полученные сертификаты издателей и CRL](#).

3 Если вы подключаетесь с помощью сертификата:

3.1 Чтобы использовать ключ ЭП и сертификат на токене, [подключите его к компьютеру](#).

3.2 Получите сертификат в УЦ из списка, выданного администратором:

3.2.1 [Создайте запрос на сертификат](#).

3.2.2 [Передайте запрос в УЦ](#).

3.2.3 [Получите личный сертификат пользователя, а также при наличии сертификаты всех УЦ из цепочки и соответствующие CRL](#).

3.3 [Установите полученные сертификаты и CRL](#):

- Личный — в хранилище или в хранилище и на токен.
- Корневые и промежуточные сертификаты издателей и CRL — в хранилище.

3.4 [Передайте личный сертификат вашему администратору. После его добавления в вашу учётную запись вы сможете подключиться к облачному сервису ЭП](#).

4 [Настройте подключение к сервису](#).

Настройка подключения к сервису

- 1 Перейдите в настройки ViPNet PKI Client.
- 2 Выберите  **Облачные сервисы**.
- 3 Включите  **Использовать функции облачного сервиса**.
- 4 Нажмите  **Добавить** и укажите:
 - о название облачного сервиса;
 - о адрес и порт ViPNet PKI Service;
 - о режим аутентификации. При выборе режима аутентификации по сертификату выберите сертификат для подключения к сервису.
- 5 Нажмите .
- 6 Чтобы проверить соединение с сервисом, наведите на него курсор и нажмите .

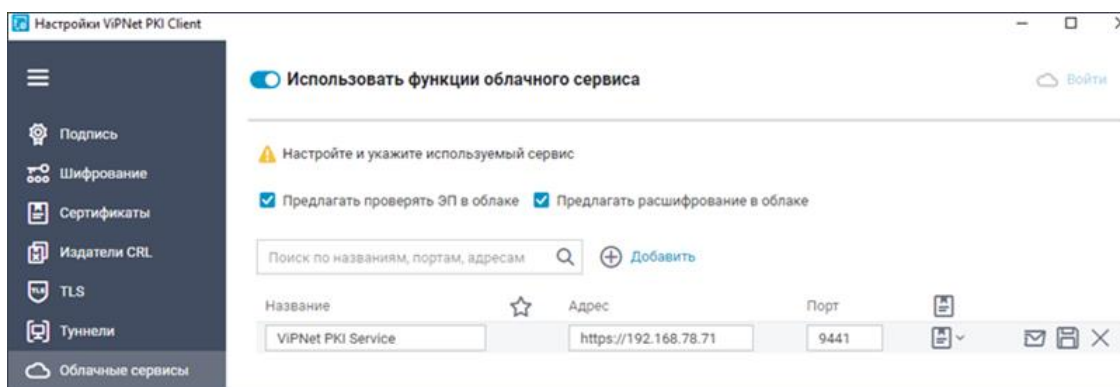


Рисунок 11. Настройка подключения к облачному сервису ЭП (на базе ViPNet PKI Service)

- 7 Чтобы отредактировать или удалить облачный сервис, наведите на него курсор и нажмите  или  соответственно.
- 8 Чтобы ViPNet PKI Client предлагал проверять подпись в облачном сервисе ЭП, если при проверке подписи не удалось проверить сертификат подписанта с помощью сертификатов, установленных в хранилище, выберите **Предлагать проверять ЭП в облаке**.
- 9 Чтобы ViPNet PKI Client предлагал расшифровывать файл в облачном сервисе ЭП, если подходящий для расшифрования сертификат не найден в хранилище, выберите **Предлагать расшифрование в облаке**.
- 10 Если вы добавили несколько сервисов, в списке **Используемый сервис** выберите тот, к которому будете подключаться по умолчанию.
- 11 Нажмите **Сохранить**.
- 12 Если вы добавляете облачный сервис впервые, закройте и заново [запустите настройки ViPNet PKI Client](#).
- 13 [Подключитесь к облачному сервису ЭП](#).

Подключение к сервису

ViPNet PKI Client будет подключаться к облачному сервису ЭП:

- при выполнении операций с использованием сертификатов и ключей ЭП, хранимых в облачном сервисе ЭП;
- просмотре и выборе сертификатов для подписи, хранимых в облачном сервисе ЭП;
- создании запроса на сертификат в облачном сервисе ЭП.

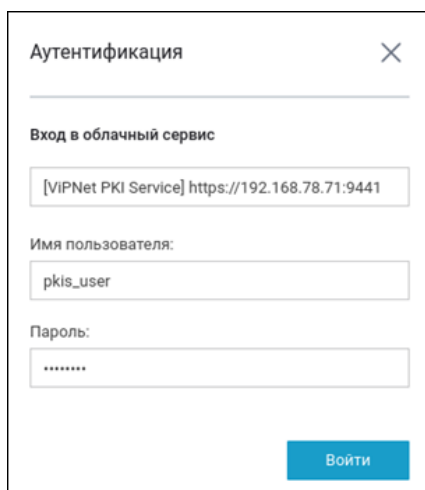
Продолжительность сессии — 1 час. После этого потребуется повторное подключение.

Подключение с помощью сертификата

- 1 [Перейдите в настройки ViPNet PKI Client.](#)
- 2 Выберите  **Облачные сервисы.**
- 3 В списке **Используемый сервис** выберите облачный сервис.
- 4 Справа сверху нажмите  **Войти.**
- 5 В зависимости от места хранения ключа ЭП:
 - **Хранилище ViPNet PKI Client** — введите пароль хранилища ViPNet PKI Client и нажмите **Продолжить**;
 - **Токен** — введите PIN-код от токена.

Подключение с помощью имени и пароля учетной записи

- 1 [Перейдите в настройки ViPNet PKI Client.](#)
- 2 Справа сверху нажмите  **Войти.**
- 3 Введите имя и пароль учётной записи и нажмите **Войти.**



Аутентификация

Вход в облачный сервис

[ViPNet PKI Service] https://192.168.78.71:9441

Имя пользователя:

pkis_user

Пароль:

Войти

Рисунок 12. Подключение к облачному сервису ЭП с помощью имени и пароля учетной записи

Смена пароля учётной записи пользователя

- 1 [Перейдите в настройки ViPNet PKI Client.](#)
- 2 Выберите  **Облачные сервисы.**
- 3 В списке **Используемый сервис** выберите облачный сервис и [подключитесь к нему.](#)
- 4 Справа сверху нажмите на имя пользователя и выберите **Сменить пароль.**
- 5 Задайте и подтвердите новый пароль и нажмите **Изменить.**



Совет. Если вы забыли свой пароль и хотите получить новый, обратитесь к вашему администратору и получите разовый пароль. При первом подключении смените его на постоянный.

6

Подпись и зашифрование файлов

Требования к сертификатам для подписи и зашифрования	51
Порядок подписания файла	52
Порядок зашифрования файла	55
Подписание и зашифрование файла	57

Требования к сертификатам для подписи и зашифрования

- Сертификат действителен.
- Личный сертификат, который используется для подписи:
 - установлен в одну из [категорий](#): **Личные сертификаты**, **Сертификаты в облаке** или **Сертификаты на внешних устройствах**;
 - содержит расширение **Использование ключа** со значением **Цифровая подпись**.
- Сертификат получателя, который используется для зашифрования:
 - установлен [в категорию](#) **Сертификаты других пользователей**;
 - содержит расширение **Использование ключа** со значением **Согласование ключей**.



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

Порядок подписания файла

- 1 Ознакомьтесь с [требованиями](#) к сертификату подписи.
- 2 Подготовьте личный сертификат и ключ ЭП.
- 3 Настройте параметры процесса подписи.
- 4 Подпишите файлы и передайте их получателям любым удобным способом.

Настройка параметров процесса подписи

- 1 Перейдите в настройки ViPNet PKI Client.
- 2 Выберите  Подпись.
- 3 Чтобы использовать сертификат подписи, хранящийся в облачном сервисе, [подключитесь к облачному сервису](#).
- 4 Нажмите  Выбрать сертификат.
- 5 Выберите сертификат и нажмите **Выбрать**.
- 6 Чтобы сохранить ЭП [отдельно от подписываемого файла](#), снимите флажок **Использовать прикрепленную подпись** (сохранить документ и подпись в одном файле *.sig).

По умолчанию ЭП [прикрепляется к подписываемому файлу](#).

- 7 Установите соответствующие флажки:
 - чтобы использовать подпись формата [XMLDSig](#);
 - сохранять файлы в кодировке Base64.
- 8 Чтобы добавить к ЭП подтверждение точного времени подписания файла:
 - 8.1 Установите флажок **Добавить в подпись штамп точного времени**.
 - 8.2 В поле **Адрес TSP-сервера** укажите URL-адрес сервера:
`http://<IP-адрес или доменное имя>:<порт>`
 - 8.3 Проверьте соединение с [сервером штампов времени](#).

Внимание! Чтобы использовать указанную TSP-службу при подписании с помощью сертификата и ключа ЭП, хранящегося в облачном сервисе ЭП:



- В облачном сервисе ЭП должен быть установлен сертификат УЦ, издавшего сертификат TSP-службы, а также при наличии сертификаты всех УЦ из цепочки и соответствующие CRL.
 - Облачный сервис ЭП должен иметь доступ к TSP-службе.
-

- 9 Чтобы изменить путь сохранения результатов подписи, нажмите **Обзор**.

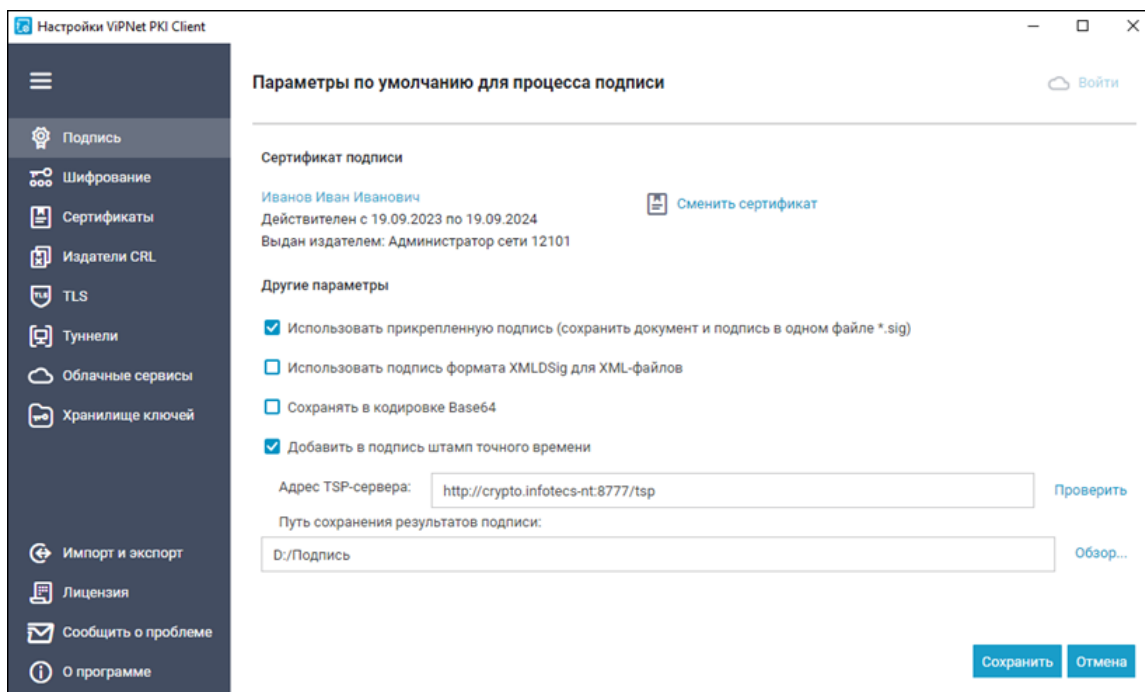


Рисунок 13. Настройка параметров ЭП

10 Нажмите **Сохранить**.

Подписание файла

1 Запустите File Unit и выполните одно из действий:

- Перетащите файлы в главное окно File Unit.
- Нажмите **Выбрать файлы** и выберите один или несколько файлов.



Примечание. Чтобы просмотреть файл, выбранный для подписи, нажмите его имя в списке **Выбранные файлы**.

2 Чтобы использовать сертификат подписи, хранящийся в облачном сервисе:

2.1 Вверху нажмите  **Войти**.

2.2 Введите имя и пароль учётной записи и нажмите **Войти**.

3 На панели справа выберите **Подписать сертификатом**.

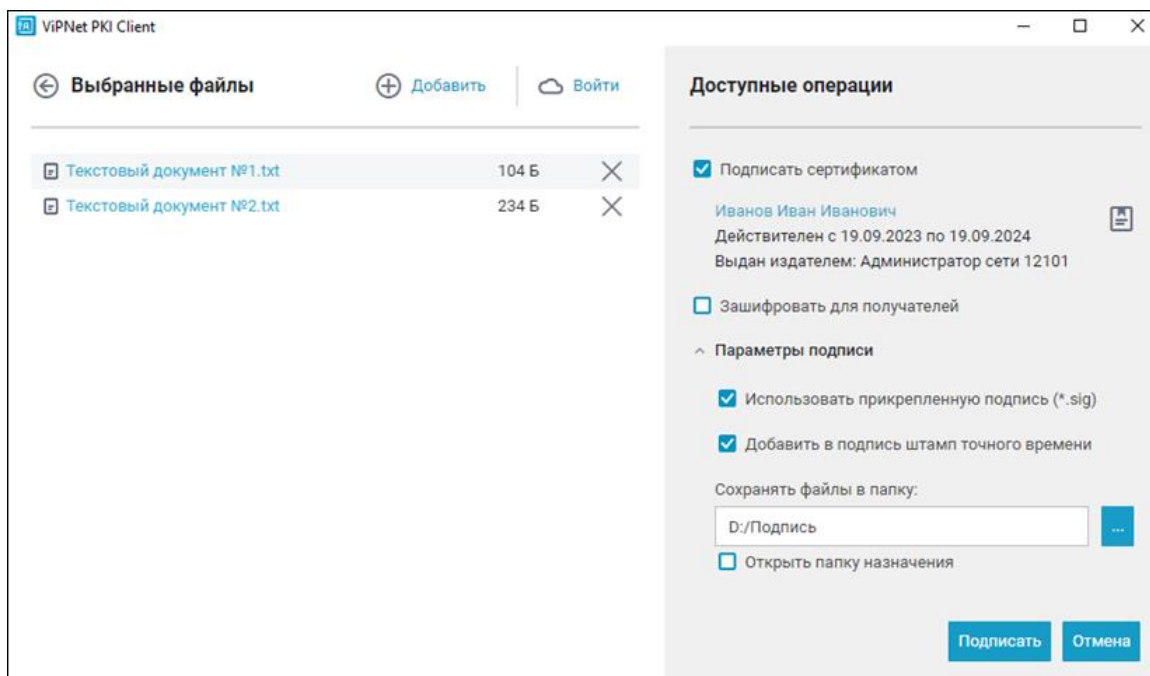


Рисунок 14. Подписание файла

- 4 Выберите параметры подписи.

Чтобы выбрать другой сертификат подписи, нажмите .

- 5 Нажмите **Подписать**.



Примечание. Если для подписания файла вы выбрали сертификат, хранящийся в облачном сервисе ЭП, может потребоваться подтверждение операции. Введите код подтверждения.

- 6 В зависимости от места хранения контейнера ключей:
 - **Хранилище ViPNet PKI Client** — введите пароль хранилища ViPNet PKI Client и нажмите **Продолжить**;
 - **Токен** — введите PIN-код от токена.



Внимание! После десяти неудачных попыток ввода пароля File Unit, Web Unit и настройки ViPNet PKI Client блокируются на 15 минут.

В выбранную папку будут помещены файлы:

- *.sig, если вы выбрали прикрепленную ЭП;
- *.detached.sig, если вы выбрали открепленную ЭП.

Порядок зашифрования файла

- 1 Ознакомьтесь с [требованиями](#) к сертификату получателя зашифрованных файлов.
- 2 Запросите у получателей зашифрованных файлов их сертификаты.
- 3 Установите полученные сертификаты: выберите тип **Другой**.
- 4 Настройте параметры шифрования.
- 5 Зашифруйте файлы и передайте их получателям любым удобным способом.

Настройка параметров зашифрования

- 1 Перейдите в настройки ViPNet PKI Client.
- 2 Выберите  **Шифрование**.
- 3 Чтобы повторно не выбирать сертификаты получателей при зашифровании файлов, создайте список получателей:
 - 3.1 В списке **Получатели зашифрованных файлов** нажмите  **Добавить**.
 - 3.2 Выберите сертификаты получателей и нажмите **Выбрать**.

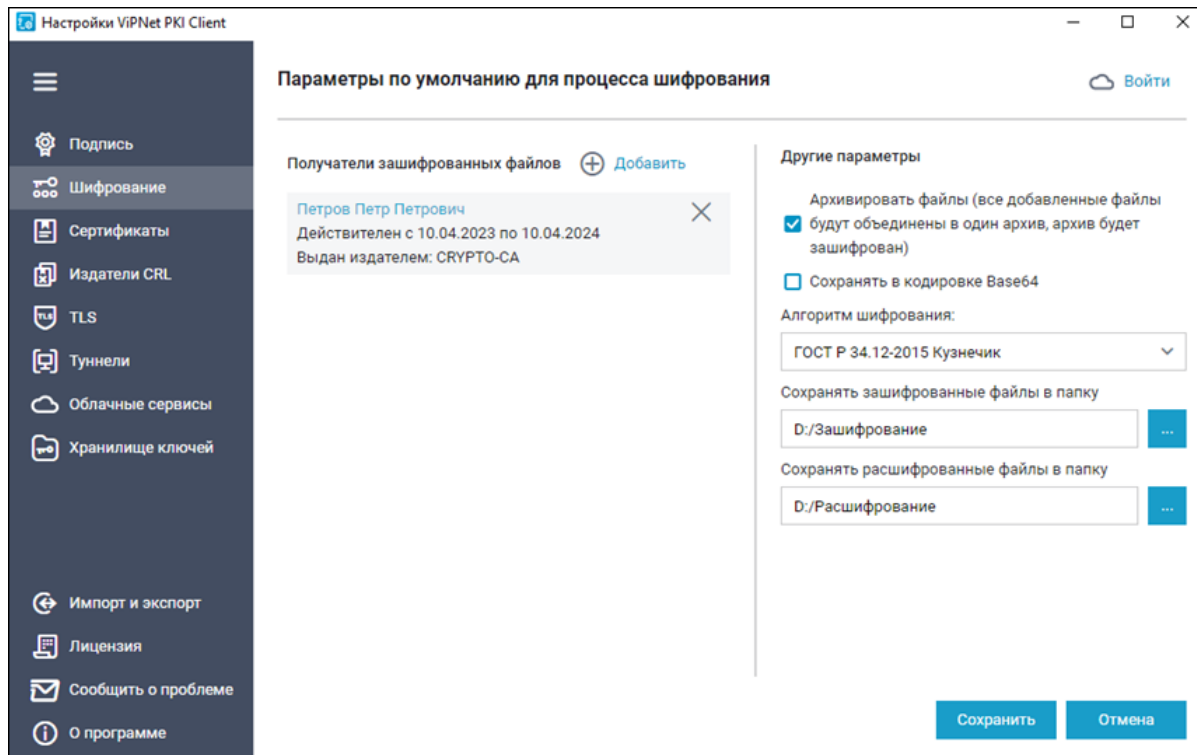


Рисунок 15. Настройка параметров шифрования



Примечание. Чтобы удалить сертификат получателя из списка, нажмите

- 4 Справа выберите параметры зашифрования и нажмите **Сохранить**.

Зашифрование файла

- 1 В File Unit выполните одно из действий:
 - Перетащите файлы в главное окно File Unit.
 - Нажмите **Выбрать файлы** и выберите один или несколько файлов.



Примечание. Чтобы просмотреть файл, выбранный для зашифрования, нажмите его имя в списке **Выбранные файлы**.

- 2 На панели справа выберите **Зашифровать для получателей**.

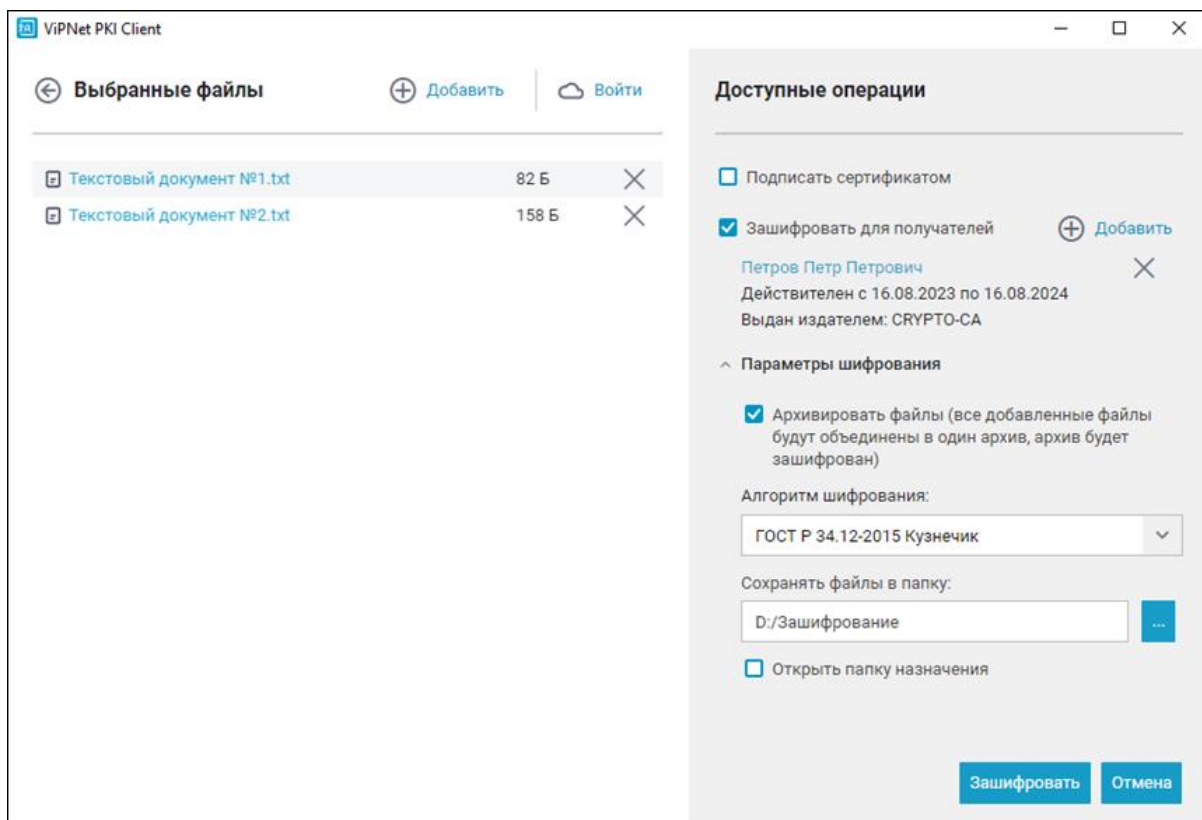


Рисунок 16. Зашифрование файла

- 3 Выберите параметры зашифрования.
- 4 Нажмите **Зашифровать**. В выбранную папку будут помещены зашифрованные файлы *.enc или *.zip.enc.

Подписание и зашифрование файла

1 В File Unit выполните одно из действий:

- Перетащите файлы в главное окно File Unit.
- Нажмите **Выбрать файлы** и выберите один или несколько файлов.



Примечание. Чтобы просмотреть файл, выбранный для подписи и зашифрования, нажмите его имя в списке **Выбранные файлы**.

2 Чтобы использовать сертификат подписи, хранящийся в облачном сервисе:

2.1 Вверху нажмите **Войти**.

2.2 Введите имя и пароль учётной записи и нажмите **Войти**.

3 На панели справа выберите **Подписать сертификатом** и **Зашифровать для получателей**.

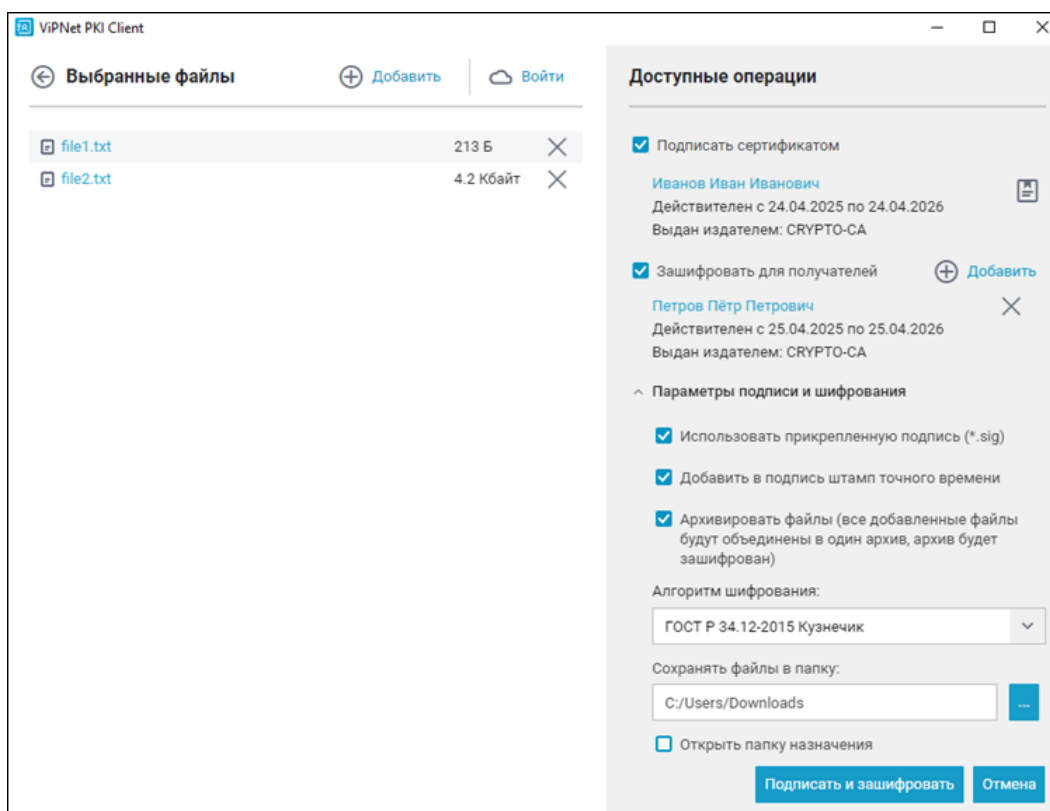


Рисунок 17. Одновременное подписание и зашифрование файла

4 Выберите параметры подписи и зашифрования.

5 Нажмите **Подписать и зашифровать**.

6 В зависимости от места хранения сертификата подписанта:

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



Внимание! После десяти неудачных попыток ввода пароля File Unit, Web Unit и настройки ViPNet PKI Client блокируются на 15 минут.

7

Работа с файлами, полученными от других пользователей

Получение подписанных и зашифрованных файлов	60
Проверка ЭП	61
Расшифрование файла	63

Получение подписанных и зашифрованных файлов

Если вы получили файл с расширением:

- *.sig — [проверьте ЭП](#);
- *.enc — [расшифруйте](#);
- *.sig.enc — [расшифруйте](#), а затем [проверьте ЭП](#).

Проверка ЭП

- 1 В главном окне File Unit выполните одно из действий:
 - Перетащите файлы *.sig в главное окно программы.
 - Нажмите **Выбрать файлы** и выберите один или несколько файлов *.sig.
- 2 Если вы выбрали несколько файлов, нажмите  напротив имени файла для проверки.
- 3 Для проверки ЭП по требованиям квалифицированной ЭП выберите **Проверить по требованиям КЭП**.
- 4 Чтобы проверить ЭП:
 - в ViPNet PKI Client — нажмите **Проверить ЭП**.
 - в облачном сервисе — нажмите **Проверить ЭП в облаке**.

Примечание. При проверке откреплённой ЭП может потребоваться выбрать исходный файл:



- если исходный файл и файл подписи имеют разные имена
- или они находятся в разных папках.

- 5 Просмотрите результат проверки ЭП:

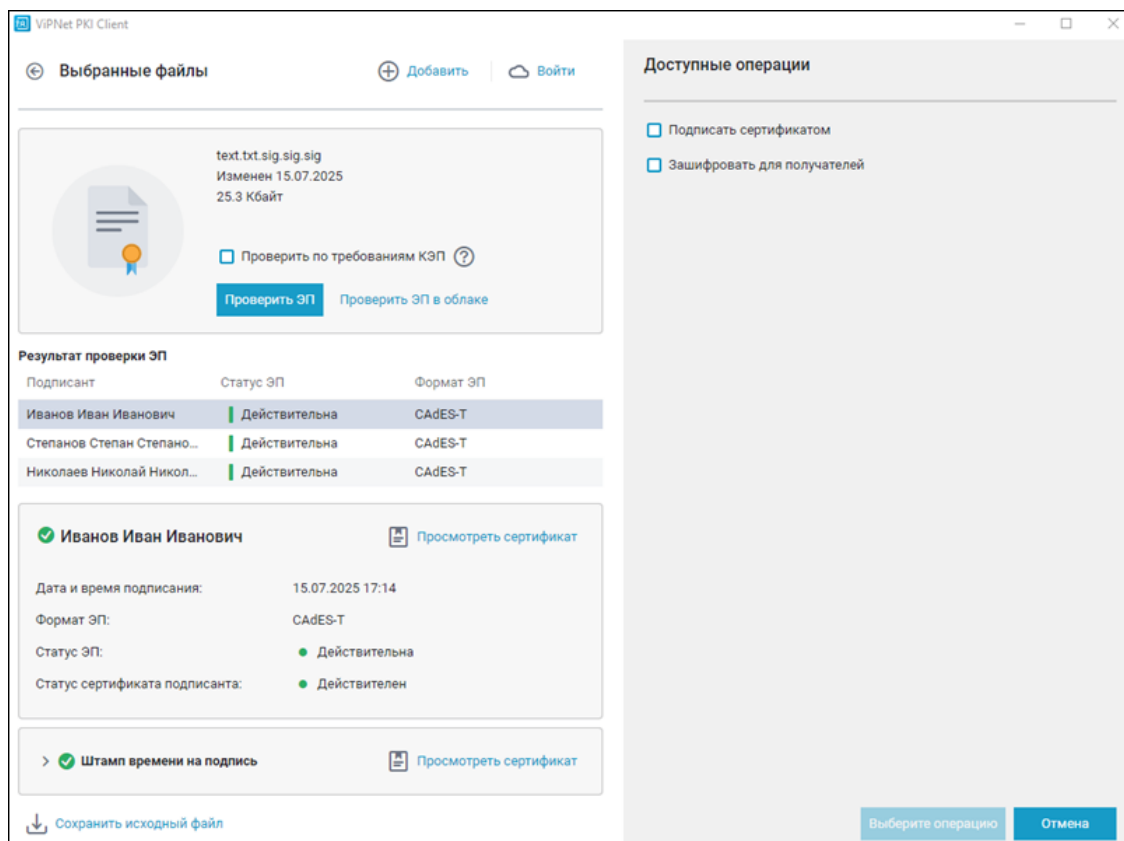


Рисунок 18. Результат проверки ЭП

- Если файл подписан несколькими пользователями, для просмотра подробной информации об ЭП владельца нажмите его имя в списке.
- Чтобы просмотреть сертификат владельца подписи, справа от его имени нажмите  **Просмотреть сертификат**.
- Если ЭП содержит штамп точного времени, вы можете:
 - просмотреть свойства штампа — слева от штампа нажмите ;
 - просмотреть сертификат TSP-службы — справа от штампа нажмите  **Просмотреть сертификат**.
- Чтобы просмотреть файл, извлечённый после проверки прикреплённой ЭП, нажмите  **Сохранить исходный файл** и укажите папку для сохранения файла.

Расшифрование файла



Внимание! Использование сертификатов и ключей ЭП, созданных с помощью встроенного криптопровайдера токена, не поддерживается.

1 В главном окне File Unit выполните одно из действий:

- Перетащите файл *.enc в главное окно программы.
- Нажмите **Выбрать файлы**. Выберите файл *.enc и нажмите **Открыть**.

Файл появится в разделе **Выбранные файлы**.

2 Если файл зашифрован с помощью нескольких ваших личных сертификатов, справа нажмите  и выберите сертификат для расшифрования.

3 Чтобы изменить параметры расшифрования, в меню справа установите флажки около параметров.

4 Нажмите **Расшифровать**.



Примечание. Если в локальном хранилище компьютера нет сертификата для расшифрования и [настроено подключение к облачному сервису ЭП](#), вам будет предложено расшифровать файл с использованием сертификатов, хранимых в облачном сервисе ЭП.

При расшифровании файла с помощью сертификата из облачного сервиса ЭП может потребоваться подтверждение операции — введите код подтверждения.

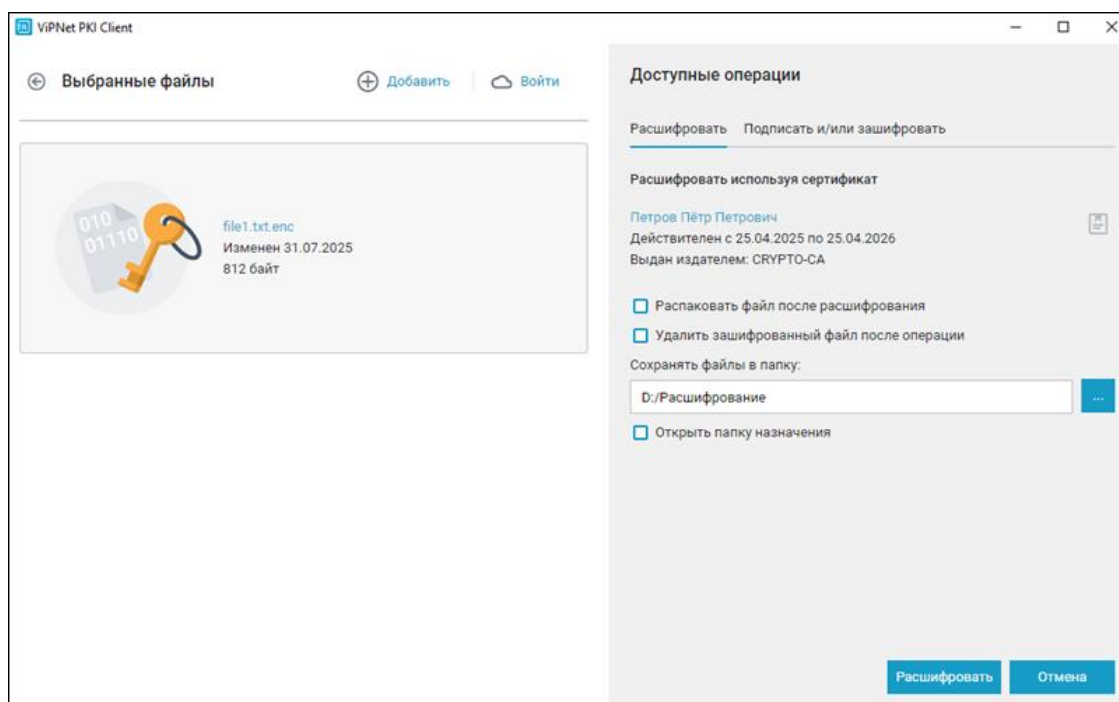


Рисунок 19. Расшифрование файла

5 В зависимости от места хранения контейнера ключей:

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



Внимание! После десяти неудачных попыток ввода пароля File Unit, Web Unit и настройки ViPNet PKI Client блокируются на 15 минут.

8

Подключение к сайтам, использующим TLS ГОСТ

Порядок настройки	66
Подключение к сайту	67
Просмотр информации о TLS-соединениях	68

Порядок настройки

- 1 Чтобы подключаться к сайтам с аутентификацией пользователя, убедитесь, что ваш личный сертификат, который вы будете использовать для подключения, соответствует требованиям:
 - сертификат действителен;
 - ЭП сертификата действительна;
 - срок действия ключа ЭП наступил и не истёк;
 - сертификат [содержит расширения](#):
 - **Расширенное использование ключа** со значением **Проверка подлинности клиента**;
 - **Использование ключа** со значением **Цифровая подпись** и (или) **Согласование ключей**.
- 2 [Запустите TLS Unit](#).
- 3 [Подключитесь к сайту](#).
- 4 Вы можете [просмотреть информацию о текущих TLS-соединениях](#).

Подключение к сайту

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

- Если для подключения не требуется аутентификация пользователя, соединение будет установлено.
- Если для подключения требуется аутентификация пользователя, выберите сертификат и в зависимости от места его хранения введите пароль хранилища ViPNet PKI Client или PIN-код от токена. Соединение будет установлено.

При первом подключении к сайту выбранный сертификат сохраняется в кеш, и при последующих подключениях к этому сайту в текущей сессии выбирать сертификат не требуется. Сертификат удаляется из кеша:

- автоматически при завершении работы TLS Unit;
- вручную, если необходимо выбрать другой сертификат для подключения. Для этого в области уведомлений щелкните правой кнопкой мыши значок TLS Unit и в контекстном меню выберите **Очистить кеш**.

Просмотр информации о TLS-соединениях

- 1 В области уведомлений щёлкните правой кнопкой мыши значок TLS Unit и в контекстном меню выберите **Последние соединения**.
- 2 Чтобы просмотреть подробную информацию об одном из соединений, слева от него нажмите значок ☒ и просмотрите:
 - версию протокола TLS;
 - алгоритмы согласования ключей, шифрования и контроля целостности данных.

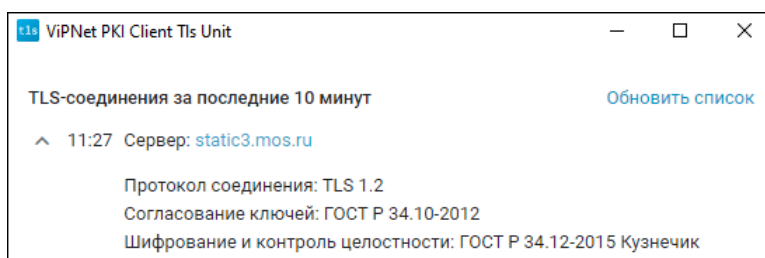


Рисунок 20. Просмотр информации о TLS-соединениях

9

Возможные неполадки

Обращение в техническую поддержку	70
Общие неполадки	71
File Unit	73

Обращение в техническую поддержку

1 Перейдите в настройки ViPNet PKI Client.

2 Выберите  Сообщить о проблеме.

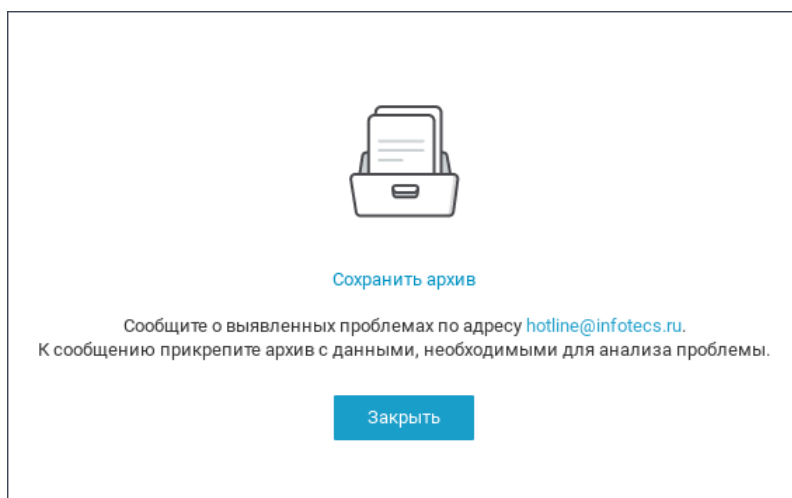


Рисунок 21. Сохранение архива с данными для отправки в ИнфоТеКС

3 Нажмите **Сохранить архив** и выберите папку для сохранения.

4 Выполните одно из действий:

- Если у вас установлен почтовый клиент, нажмите `hotline@infotecs.ru`. Откроется почтовый клиент с готовым письмом. Опишите неполадку, прикрепите архив и отправьте письмо в ИнфоТеКС.
- Если у вас не установлен почтовый клиент, создайте письмо вручную: укажите адрес получателя `hotline@infotecs.ru`, опишите неполадку и прикрепите архив. Отправьте письмо в ИнфоТеКС.



Примечание. ViPNet PKI Client не собирает вашу конфиденциальную информацию.

ИнфоТеКС ответственно подходит к защите вашей информации и принимает все меры для предотвращения несанкционированного доступа или разглашения информации, которую вы нам предоставляете.

Общие неполадки

Ошибка при удалении сертификата

Если возникла ошибка при [удалении сертификатов получателей с помощью ViPNet PKI Client](#), возможно, сертификат установлен в хранилище локального компьютера и у вас недостаточно прав для работы с этим хранилищем.

Удалите сертификат через консоль:

- 1 Откройте Microsoft Management Console:
 - 1.1 Нажмите сочетание клавиш **Win+R**.
 - 1.2 В поле **Открыть** введите `mmc` и нажмите **ОК**.
- 2 В меню **Файл** 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 > Готово**.
- 5 На панели навигации консоли нажмите **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 создания запроса на сертификат

Может возникнуть при попытке создать запрос на сертификат с сохранением ключа ЭП на токен с аппаратной поддержкой ГОСТ, если данный токен 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 токен с аппаратной поддержкой ГОСТ и поддержкой выбранного набора параметров ключа проверки ЭП или токен с программной поддержкой ГОСТ;
- выберите другой набор параметров ключа проверки ЭП.

Невозможно просмотреть созданный контейнер ключей на токене

На токенах **без аппаратной поддержки алгоритмов ГОСТ** нельзя просмотреть созданный контейнер ключей с помощью собственных утилит.

Чтобы просмотреть контейнер:

1 Запустите командную строку Windows.

2 Перейдите в папку с исполняемыми файлами ViPNet PKI Client командой:

```
cd "C:\Program Files (x86)\Infotecs\ViPNet PKI Client\bin"
```

3 С помощью утилиты `ossl_manager` из состава OSSL просмотрите созданный контейнер:

```
ossl_manager.exe pkey --list --p11-lib=<библиотека>.dll --p11-init-flags=2  
--engine-dir="C:\Program Files (x86)\InfoTeCS\ViPNet PKI Client\bin"  
--p11-pin=<пароль>, где:
```

o <библиотека> — библиотека стандарта PKCS#11 для используемого токена:

- `softtoken_ngost_rutoken` — Рутокен;
- `softtoken_ngost_jacarta` — JaCarta;
- `softtoken_ngost_esmart` — ESMART Token.

o <пароль> — пароль контейнера ключей.

Вы получите список ключей в контейнере.

File Unit

Нет сертификата в списке сертификатов для подписи

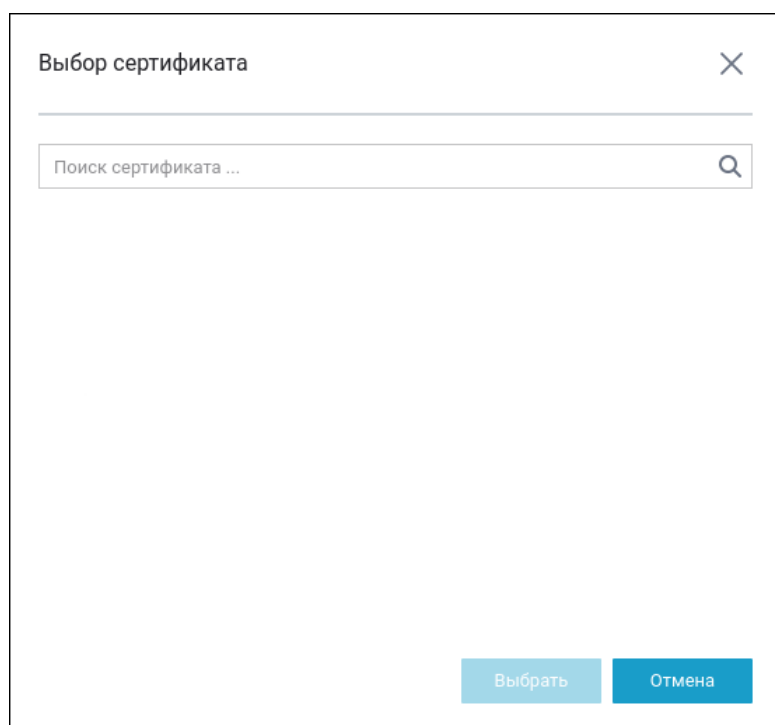


Рисунок 22. Сертификат не отображается в списке сертификатов

Проверьте, что [сертификат](#) соответствует требованиям.

Ошибка при расшифровании

Возможно, 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.](#)
- 2 Выберите  Сертификаты.
- 3 Нажмите имя владельца сертификата.
- 4 На вкладке **Состав** найдите поле **Средство ЭП владельца**.



Поддерживаемые токены

Список поддерживаемых токенов

Ниже приведены токены, которые можно использовать в ViPNet PKI Client. Для каждого токена указаны условия работы с ним.

Таблица 3. Поддерживаемые токены

Полные названия токенов	Модификация	Необходимые условия для работы с токеном
Рутокен Lite	64КБ, 1010	На компьютере должны быть установлены драйверы Рутокен
Рутокен ЭЦП 2.0	2000, 2100, 2100 micro, 2100 Type-C, 2100 смарт-карта, 3000, 4500 Flash	
Рутокен ЭЦП 3.0	3100, 3100 NFC, 3220, 3220 micro	
Рутокен S	64КБ, 64КБ micro	На компьютере должны быть установлены драйверы Рутокен . Чтобы установить сертификат на токен, используйте приложение «Панель управления Рутокен». Чтобы удалить сертификат с ключом ЭП, выберите его в категории Личные сертификаты , удалите в ViPNet PKI Client и удалите в приложении «Панель управления Рутокен» .
JaCarta	LT, PKI, PKI/BIO	На компьютере должен быть установлен

Полные названия токенов	Модификация	Необходимые условия для работы с токеном
JaCarta-2	SE, ГОСТ, PRO/ГОСТ, PKI/ГОСТ, PKI/BIO/ГОСТ	ПК «Единый Клиент JaCarta» компании «Аладдин Р.Д.» (рекомендуемая минимальная версия — 3.0)
ESMART Token «MS_KEY К» - «АНГАРА»	ГОСТ, 192K Исполнение 8.1.1	На компьютере должно быть установлено ПО ESMART PKI Client для Windows (рекомендуемая версия — 4.17)

Аппаратная поддержка алгоритмов ГОСТ токенами

Таблица 4. Поддерживаемые российские криптографические алгоритмы

Название токена	Модификации	Аппаратная поддержка алгоритмов ГОСТ
Рутокен Lite	64КБ, 1010	отсутствует
Рутокен S	64КБ, 64КБ micro	отсутствует
Рутокен ЭЦП 2.0	2000, 2100, 2100 micro, 2100 Type-C, 2100 смарт-карта, 3000, 4500 Flash	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012
Рутокен ЭЦП 3.0	3100, 3100 NFC, 3220, 3220 micro	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018), ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018) «Магма» и «Кузнечик»
JaCarta	LT, PKI, PKI/BIO	отсутствует
JaCarta-2	SE	ГОСТ Р 34.10-2012
	ГОСТ, PRO/ГОСТ, PKI/ГОСТ, PKI/BIO/ГОСТ	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012
ESMART Token	ГОСТ	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012
	192K	отсутствует
«MS_KEY К» - «АНГАРА» (АНГАРА+)	Исполнение 8.1.1 с неизвлекаемым ключом	отсутствует



Внимание! Если вы сменили или хотите сменить PIN-код от токена, на котором отсутствует аппаратная поддержка алгоритмов ГОСТ, см. «Руководство администратора».



Термины и сокращения

Infotecs Software Token

Программное устройство для хранения ключей с интерфейсом PKCS#11.

OCSP-сервер

Сервер в составе доверенного субъекта инфраструктуры открытых ключей, предоставляющего информацию о статусах сертификатов по запросам в режиме онлайн.

TLS (Transport Layer Security)

Криптографический протокол транспортного уровня для защищённой передачи данных между узлами в интернете. Использует асимметричные ключи, симметричное шифрование данных и коды аутентичности сообщений.

TSP-сервер

Сервер, работающий по протоколу TSP (Time Stamp Protocol), обладающий точным и надёжным источником времени, и предоставляющий штампы времени по запросам.

ViPNet PKI Service

Программно-аппаратный комплекс для выполнения криптографических операций по запросам пользователей, а также для создания и защищенного хранения ключей пользователей. Является средством криптографической защиты информации класса KB и средством электронной подписи класса KB2.

XMLDSig

Формат электронной подписи для подписания документа целиком или части документа. При этом подписанты разных частей одного документа могут различаться.

Аутентификация

Процесс односторонней или двусторонней (взаимной) проверки подлинности между клиентом (пользователем) и системой (сервером), например, с использованием учётных данных или сертификатов ключей проверки электронной подписи.

Действительность сертификата

Сертификат, для которого выполняются условия:

- срок действия сертификата наступил и не истёк;
- сертификат не аннулирован;
- цепочка сертификатов полна, и все сертификаты цепочки действительны.

Запрос на сертификат

Документ с информацией, которая требуется для издания сертификата ключа проверки электронной подписи в удостоверяющем центре (владелец, срок действия, назначение сертификата и прочее).

Ключ проверки электронной подписи (ключ проверки ЭП)

Несекретный (открытый) ключ из пары асимметричных ключей, который представляет собой уникальную последовательность символов, однозначно связанную с секретным ключом (ключом электронной подписи или закрытым ключом) и предназначенную для проверки подлинности электронной подписи.

Ключ электронной подписи (ключ ЭП)

Секретный (закрытый) ключ из пары асимметричных ключей, который 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 TLS Unit при издании служебных сертификатов для подключения к сайтам.

Открепленная подпись

Тип электронной подписи, при использовании которой электронная подпись файла помещается в отдельный контейнер. Для проверки такой электронной подписи требуется контейнер с электронной подписью и исходный файл.

Прикрепленная подпись

Тип электронной подписи, при использовании которой исходный файл и электронная подпись помещаются в один контейнер. Для проверки электронной подписи требуется только этот контейнер.

Сертификат издателя

Сертификат ключа проверки электронной подписи, принадлежащий удостоверяющему центру и служащий для подписи сертификатов, издаваемых удостоверяющим центром.

Сертификат ключа проверки электронной подписи

Документ, изданный удостоверяющим центром 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 списков аннулированных сертификатов (CDP)

Хранилище, в которое удостоверяющий центр публикует актуальные списки аннулированных сертификатов. URL таких точек указываются в соответствующем расширении сертификатов, издаваемых удостоверяющим центром.

Удостоверяющий центр (УЦ)

Организация, уполномоченная издавать сертификаты ключа проверки электронной подписи для физических и юридических лиц, а также управлять жизненным циклом этих сертификатов.

Файл *.enc

Файл, содержащий информацию, зашифрованную с использованием ключа проверки электронной подписи получателя (или нескольких получателей).

Файл *.pfx

Файл для переноса ключей и сертификатов между устройствами и приложениями. Является расширением стандарта PKCS#12.

Файл *.sig

Файл, содержащий 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).

Шаблон сертификата

Структура, которая определяет набор полей для информации о владельце сертификата и позволяет упростить создание запросов на сертификаты.

Штамп времени

Реквизит электронного документа, подтверждающий точное время создания документа. Также может подтверждать время получения или отправки документа.

Электронная подпись (ЭП)

Созданная криптографической операцией дополнительная информация, с помощью которой можно подтвердить авторство и неизменность основной информации.

Электронная рулетка

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