ViPNet PKI Client Windows

Руководство пользователя

Версия продукта: 2.0.0

infotecs

ФРКЕ.00175-02 34 07

Версия продукта 2.0.0

АО «ИнфоТеКС»

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

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

Сайт: infotecs.ru

Служба поддержки: hotline@infotecs.ru

Содержание

Введение

О документе

Документ описывает установку, 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 ее, нажмите вторую
Меню > Команда	Последовательность элементов или действий
`Код`	Имя файла, путь, фрагмент кода или команда в командной строке

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

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`.
- Архив с описанием SDK `ViPNet PKI Client Web Unit SDK.zip`.
- Документация в формате PDF:
  - ViPNet PKI Client Windows. Руководство пользователя.
  - ViPNet PKI Client Windows. Руководство администратора.
  - ViPNet PKI Client. Руководство разработчика.

Системные требования

- Процессор — Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с 2 или более ядрами.
- Оперативная память — не менее 2 Гбайт.
- Свободное место на жестком диске — не менее 1 Гбайт.
- Операционная система с последними пакетами обновлений:
  - 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 1507, сборка 10240;
    - версия 1607, сборка 14393;
    - версия 1809, сборка 17763;
    - версия 20H2, сборка 19042;
    - версия 21H1, сборка 19043;
    - версия 21H2, сборка 19044;
  - Windows 11 — 64-разрядная версия 21H2, сборка 22000.

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

- Браузер — Atom, Chromium с поддержкой ГОСТ, Edge, Firefox, Google Chrome, Opera, Яндекс.Браузер последних версий.
- Облачный сервис 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 компании ИнфоТеКС регулируется политикой ответственного разглашения.

1

Назначение и состав

Назначение

ViPNet PKI Client — средство криптографической защиты информации и электронной подписи.

С помощью ViPNet PKI Client вы можете:

- Создать запрос на сертификат и, передав его в 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. «ViPNet PKI Client. Руководство разработчика»).

ViPNet PKI Client использует российские криптографические алгоритмы:

- Алгоритм проверки ЭП: ГОСТ Р 34.10-2001 с вычислением хэш-функции по ГОСТ Р 34.11-94 и ГОСТ Р 34.10-2012 с вычислением хэш-функции по ГОСТ Р 34.11-2012.
- Алгоритм 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, зашифрование файлов Проверка ЭП, расшифрование файлов
 TLS Unit	Подключение к сайтам, использующим TLS ГОСТ
 Tunnel Unit	Подключение к туннелируемым ViPNet TLS Gateway ресурсам (см. «ViPNet PKI Client Windows. 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 ее.

Лицензирование через ViPNet TLS Gateway

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

2

Начало работы

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. Если вам необходимо подключаться к сайтам по TLS ГОСТ, настройте подключение к ним.

Установка, 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 Примите условия лицензионного соглашения.

3 На шаге **Автоматическое получение настроек из файла** выберите папку пользователя.

Примечание. При необходимости, например, по указаниям вашего администратора, эту папку можно будет изменить после установки ViPNet PKI Client.

4 Следуйте указаниям мастера.

Запуск, 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 ее вручную.

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

Загрузка лицензии

1 Перейдите в настройки ViPNet PKI Client.

2 В разделе **Лицензия** нажмите **Выбрать способ** > **С использованием файла лицензии**.

3 Выберите файл лицензии и в окне **Загрузка лицензии** нажмите **Загрузить**.

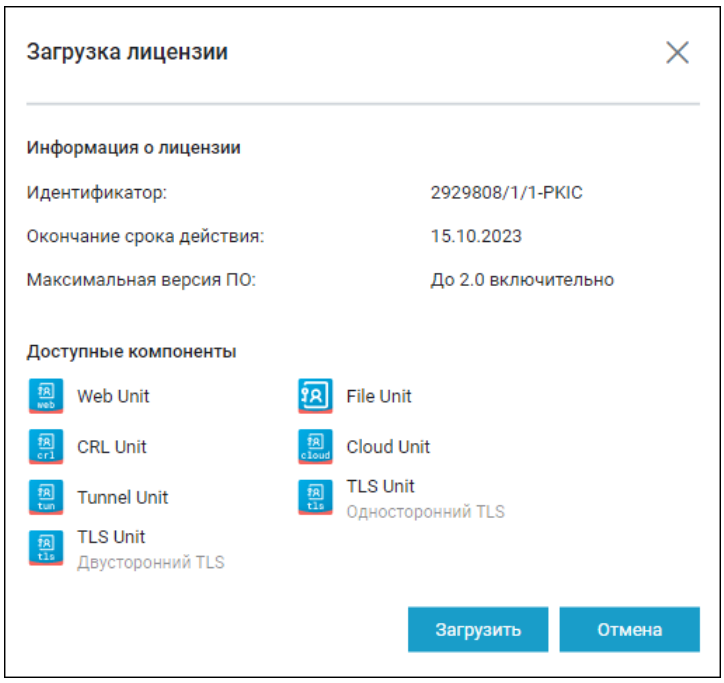

Рисунок 1. Просмотр информации о лицензии

Если связь с сервером регистрации ИнфоТеКС установлена, лицензия будет активирована автоматически. Если лицензия не была активирована, активируйте ее вручную.

Активация лицензии с использованием файла

1 Перейдите в настройки ViPNet PKI Client.

2 В разделе **Лицензия** нажмите **Активировать**.

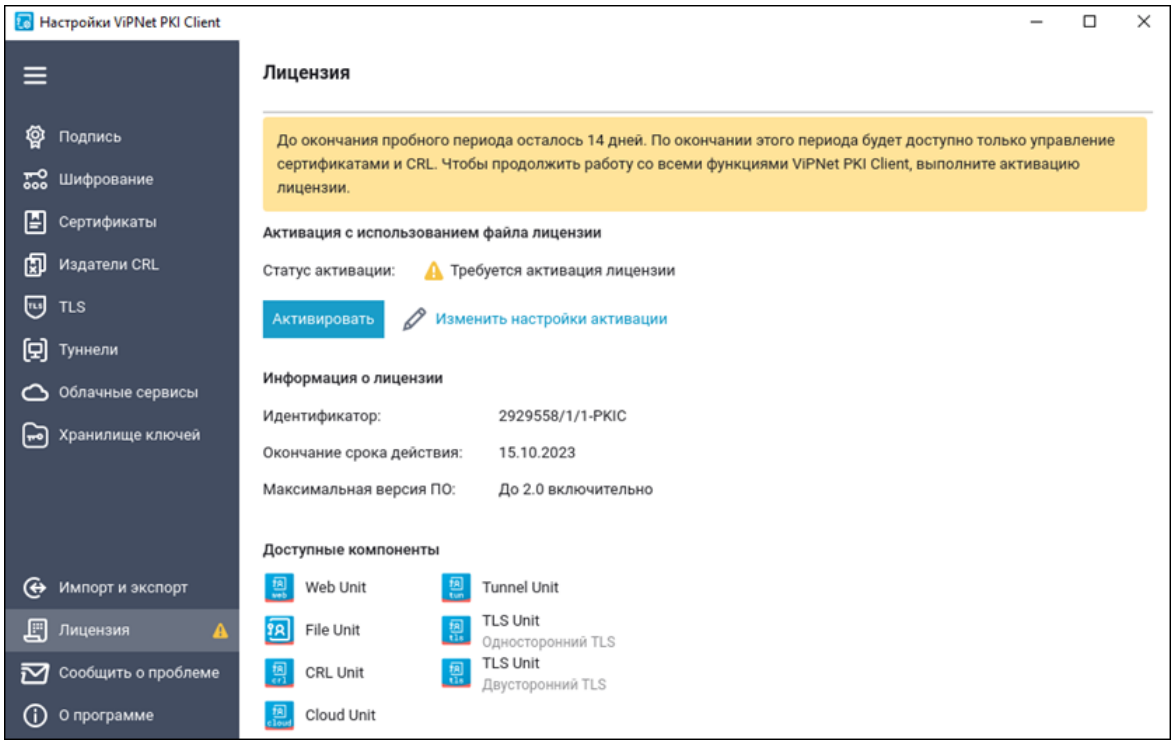

Рисунок 2. Просмотр информации о лицензии

3 Нажмите **Сохранить запрос**.

4 Укажите имя и путь для сохранения файла запроса.

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

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

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

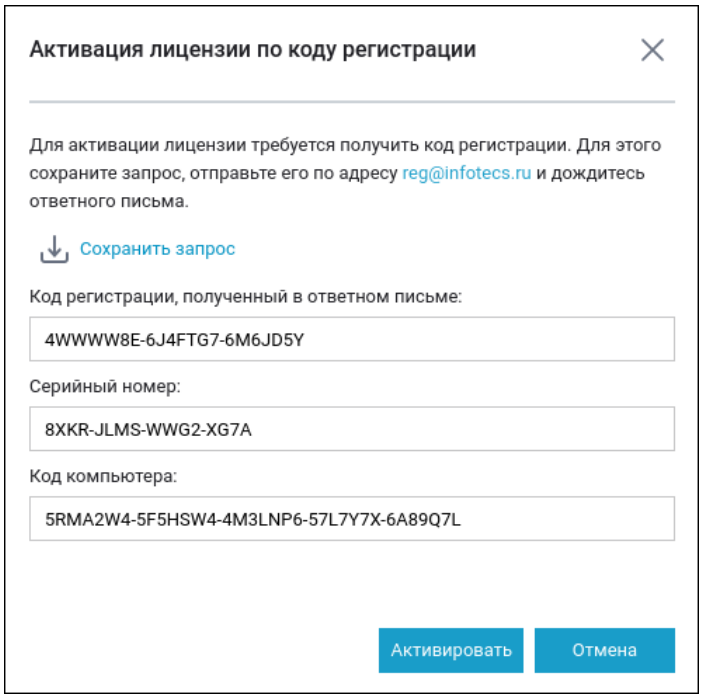

Рисунок 3. Ввод данных для активации ViPNet PKI Client

8 Нажмите **OK**.

Обновление лицензии

Если лицензия была активирована с использованием файла и вам необходимо обновить ее 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. В разделе  **Лицензия** нажмите **Изменить настройки активации** > **С использованием файла лицензии**.
4. Выберите файл лицензии и в окне **Загрузка лицензии** нажмите **Загрузить**.
5. Если лицензия загрузилась, но не активировалась, активируйте ее.

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. «ViPNet PKI Client Windows. Руководство администратора».

Автоматическое получение настроек из файла

Выбор папки настроек

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

1 Перейдите в настройки ViPNet PKI Client.

2 В разделе  **Импорт и экспорт** нажмите **Настроить**.

3 Выберите папку, откуда вы будете получать настройки:

   - Папка пользователя — если файл с настройками помещен в вашу папку.
   - Общая папка — если файл с настройками помещен в общую папку, путь к которой вам передал администратор.

4 Нажмите **Сохранить**.

Отключить автоматическое получение настроек

1 Перейдите в настройки ViPNet PKI Client.

2 В разделе  **Импорт и экспорт** нажмите **Настроить**.

3 Выберите папку пользователя.

4 Убедитесь, что в выбранной папке нет файла `pki_client_settings.json`.

Примечание. Подробнее об автоматическом получении настроек из файла см. «ViPNet PKI Client Windows. Руководство администратора».

Смена и сброс пароля хранилища ключей

Если вы используете хранилище ключей ViPNet PKI Client, вы можете сменить или сбросить его пароль.

Смена пароля хранилища ключей

1. Перейдите в настройки ViPNet PKI Client.
2. В разделе  **Хранилище ключей** нажмите **Сменить пароль**.
3. Введите текущий пароль, затем задайте и подтвердите новый.
4. Нажмите **Продолжить**.

Сброс пароля хранилища ключей

Вам может потребоваться сбросить пароль хранилища ключей без удаления приложения в следующих случаях:

- Вы забыли пароль хранилища ключей ViPNet PKI Client. Вам нужно вернуть доступ к ключам.
- Компьютером будет пользоваться другой пользователь. 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. В разделе  **Хранилище ключей** нажмите **Сбросить пароль**.
3. Нажмите **Продолжить**.
4. Задайте и подтвердите новый пароль хранилища ключей ViPNet PKI Client. Нажмите **Продолжить**.

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**.

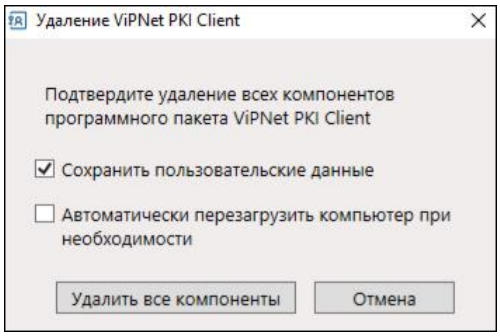

Рисунок 4. Удаление ViPNet PKI Client с сохранением пользовательских данных

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

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

3

Управление сертификатами

Какие нужны сертификаты

- Личный сертификат — для подписи, расшифрования файлов, подключения к сайтам, использующим TLS ГОСТ, и туннелируемым ресурсам с аутентификацией пользователя.

  Получите его в УЦ по запросу и установите в категорию **Личные сертификаты**.

- Сертификаты УЦ — для проверки личного сертификата.

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

- 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 путем опроса точек распространения. URL для опроса содержатся в сертификатах, изданных УЦ, в поле **Точки распространения списков отзыва (CRL)**.
  - Сервис онлайн-проверки статусов 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 файлов.

  Запросите их у получателей зашифрованных файлов и установите в категорию **Сертификаты других пользователей**.

Подготовка личного сертификата и ключа ЭП

Если нет сертификата и ключа ЭП

1. Создайте запрос на сертификат.
2. Передайте запрос в УЦ.
3. Получите личный сертификат и корневой сертификат УЦ, а также 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. Перейдите в раздел **Подключено устройств**, в строке сертификата нажмите и выберите **Установить в хранилище**.
3. 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 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. Если нужно, измените информацию в полях запроса вручную.

---

2 Чтобы сохранить ключ ЭП в облачном сервисе ЭП, добавьте его и выберите используемым по умолчанию.

3 Выберите необходимые параметры и заполните личные данные.

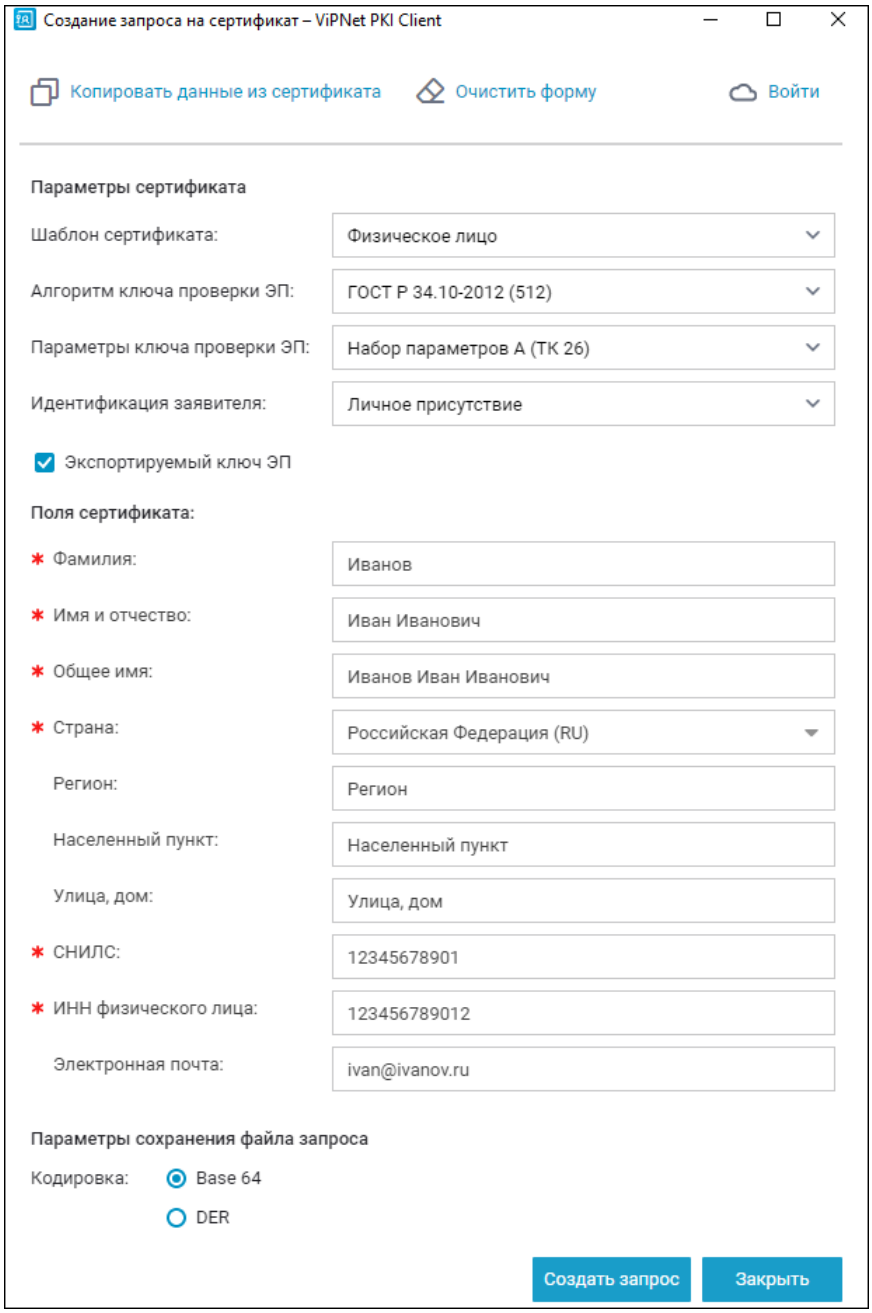

Рисунок 5. Создание запроса на сертификат

4 Нажмите **Создать запрос**.

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

6 Укажите место хранения контейнера ключей:

- 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 ПИН.

- Облачный сервис — задайте имя контейнера, нажмите **Продолжить** и подключитесь к облачному сервису ЭП.

7 Нажмите **OK**.

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 PKSC#7. Установка сертификатов из таких файлов выполняется аналогично. Если файл формата PKSC#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 В разделе **Сертификаты** выполните одно из действий:

- Нажмите **Добавить сертификат или CRL** и укажите путь к файлам сертификатов или CRL.
- Перетащите файлы сертификатов или CRL на панель просмотра (недоступно при запуске ViPNet PKI Client с правами администратора).

3 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.

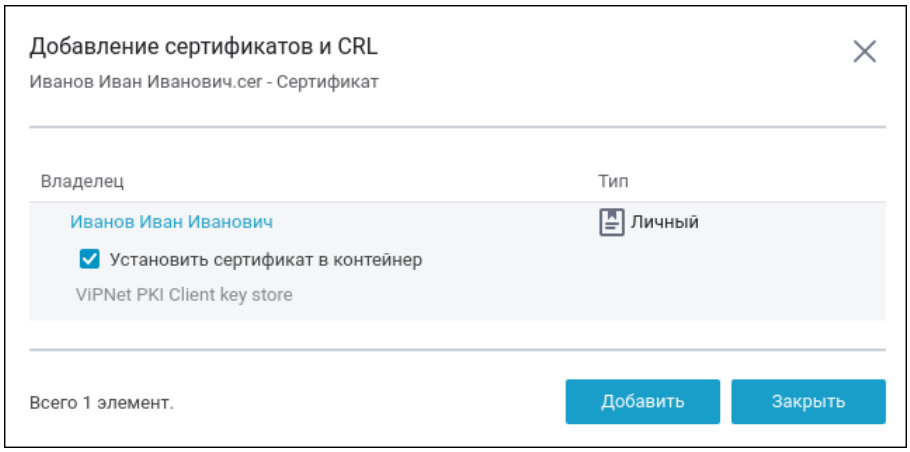

Рисунок 6. Установка сертификатов и CRL

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

4 Нажмите **Добавить**, затем **Закрыть**.

Примечание. Если после установки сертификата в строке с именем владельца появится значок , см. Проверка сертификатов.

Проверка сертификатов

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 раздел **Сертификаты** и слева вверху нажмите .

Если сертификат недействителен, в строке с именем владельца появится значок . Наведите курсор на значок, чтобы просмотреть причину:

- **Ошибка построения цепочки сертификатов**

  Установите в хранилище все сертификаты цепочки.

- **Сертификат отозван**

  Получите новый сертификат и установите его в хранилище.

- **Подпись неверна**

  Сертификат поврежден, получите новый сертификат.

- **Срок действия ключа ЭП истек**

  Выполните одно из действий:

- Если это личный сертификат, получите новый сертификат и установите его.
- Если это сертификат получателя, запросите у получателя новый сертификат.

- **Статус отзыва не определен**

  Получите в УЦ актуальный CRL и установите его в хранилище.

Добавление точек распространения CRL

Если в УЦ есть точки распространения CRL, и они доступны по сети, после установки сертификата УЦ 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 УЦ, установленных в локальное хранилище компьютера.

В случае цепочки сертификатов УЦ добавьте точки распространения CRL для каждого из сертификатов.

---

1 У вашего администратора узнайте URL точки распространения CRL.

2 Перейдите в настройки ViPNet PKI Client.

3 В разделе **Издатели CRL** вверху нажмите **Добавить.**

4 Выберите сертификат и нажмите **Выбрать**.

5 Нажмите на выбранный сертификат и на панели справа нажмите **Добавить**.

6 Введите URL точки распространения CRL, период ее опроса и нажмите .

7 Если необходимо, добавьте URL и период опроса следующей точки.

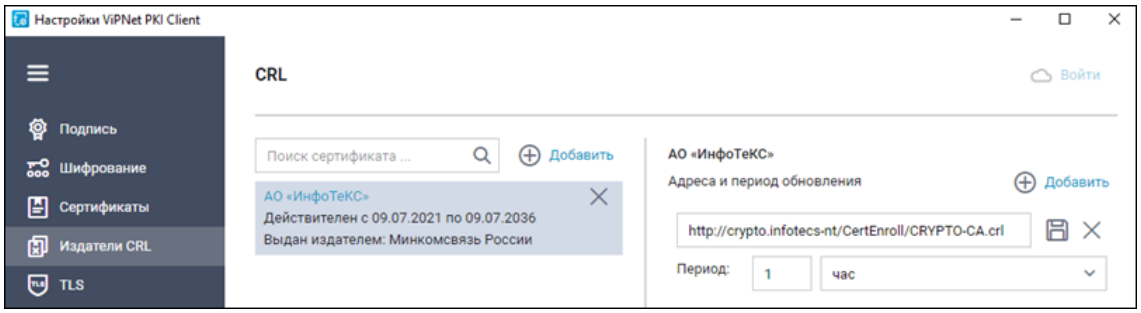

Рисунок 7. Добавление точки распространения CRL

8 Нажмите **Сохранить**.

Актуальные CRL будут автоматически скачиваться и устанавливаться в хранилище сертификатов **Промежуточные центры сертификации** > **Список отзыва сертификатов**. Подробнее о настройке автообновления CRL см. «ViPNet PKI Client Windows. Руководство администратора».

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

Чтобы экспортировать сертификат из ViPNet PKI Client:

1 Перейдите в настройки ViPNet PKI Client.

2 В разделе  **Сертификаты** напротив сертификата нажмите и выберите **Экспорт в CER-файл** или **Экспорт в PEM-файл**.

3 Укажите папку для сохранения файла и нажмите **Сохранить**.

Перенос сертификатов и ключей ЭП между устройствами

Экспорт сертификата и ключа ЭП в PFX-файл

1 Перейдите в настройки ViPNet PKI Client.

2 В разделе  **Сертификаты** нажмите  и выберите **Личные сертификаты**.

3 Напротив сертификата нажмите > **Экспорт 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.

4 Укажите имя и путь для PFX-файла и нажмите **Сохранить**.

5 Задайте и подтвердите пароль PFX-файла.

6 Выберите алгоритм шифрования или оставьте значение по умолчанию.

7 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, содержащий ключ ЭП, переносите на другое устройство только доверенным способом. Например, используйте защищенный 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 В разделе  **Сертификаты** нажмите  **Добавить сертификат или CRL** и укажите путь к PFX-файлу.

3 Введите пароль PFX-файла.

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

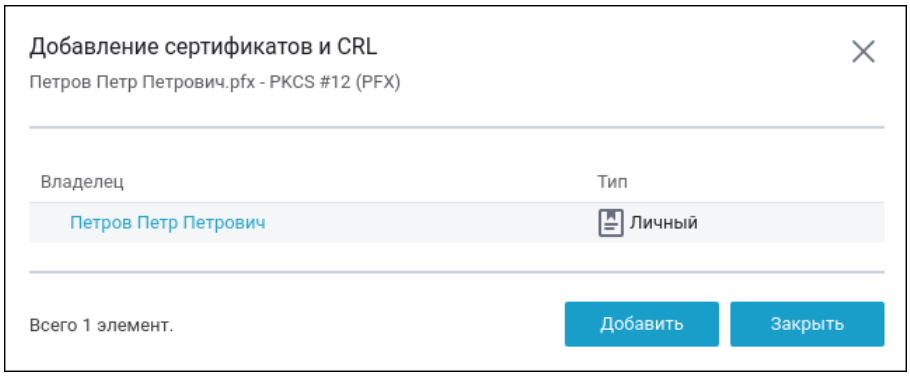

Рисунок 8. Импорт сертификата и ключа ЭП

5 Укажите место хранения контейнера ключей:

- 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 ПИН.

6 Нажмите **Закрыть**.

Просмотр сведений о сертификатах

Примечание. Просмотр сведений о сертификатах УЦ в ViPNet PKI Client не предусмотрен.

1 Перейдите в настройки ViPNet PKI Client.

2 Выберите раздел **Сертификаты**.

3 По умолчанию ViPNet PKI Client предупредит об истечении сроков действия сертификатов за 60 дней. Чтобы изменить это, справа вверху нажмите .

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, дважды щелкните название столбца.

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

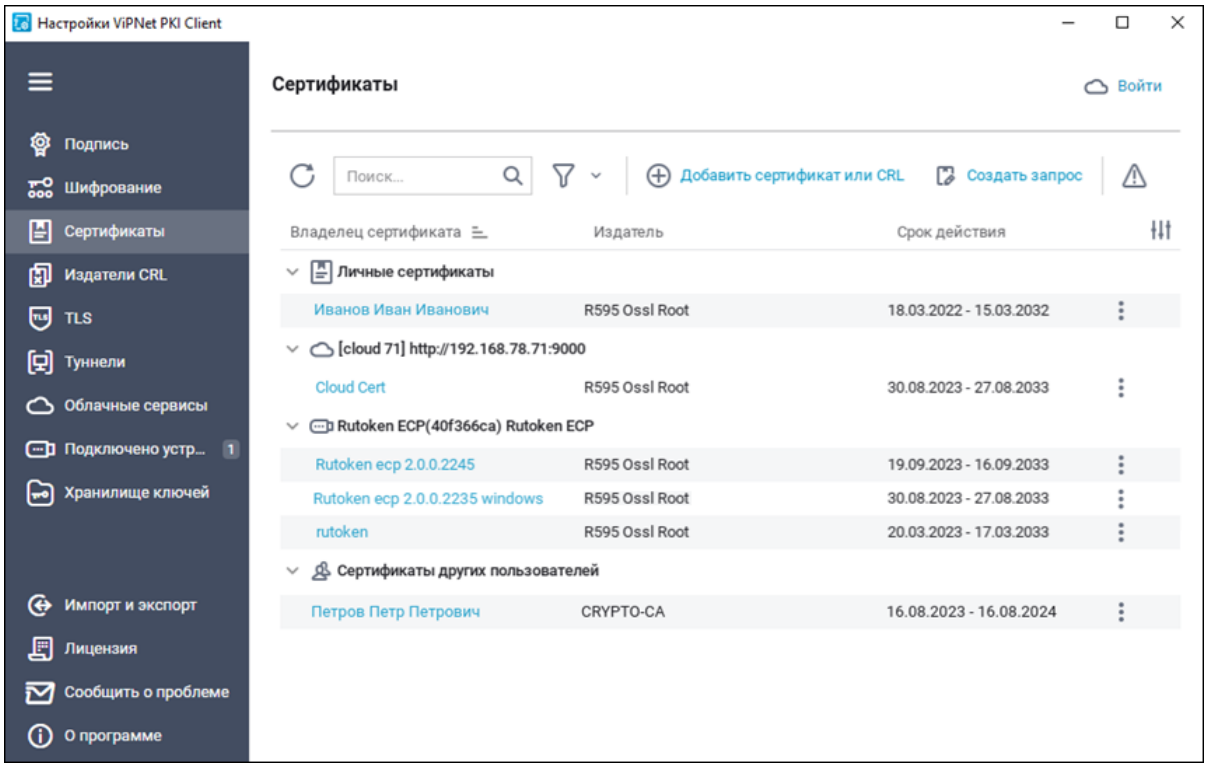

Рисунок 9. Просмотр сертификатов в ViPNet PKI Client

5 Нажмите имя владельца сертификата. Отобразятся подробные сведения о сертификате.

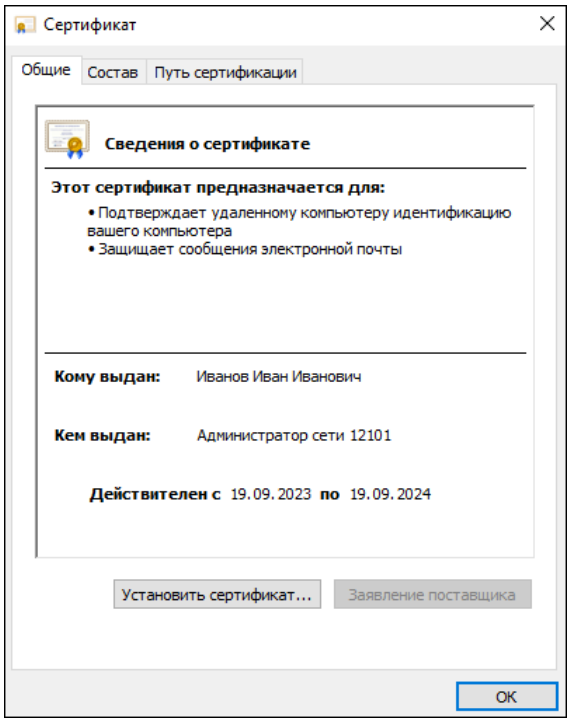

Рисунок 10. Сведения о сертификате

Внимание! Если при просмотре подробных сведений о сертификате он отображается как недействительный, проверьте его статус в ViPNet PKI Client. Если сертификат отображается как действительный, он может быть доступным для подписания и зашифрования.

Удаление сертификатов и ключей ЭП

1 Перейдите в настройки ViPNet PKI Client.

2 В разделе  **Сертификаты** вверху нажмите  и в списке выберите группу сертификатов.

3 В строке сертификата нажмите и выберите **Удалить**.

4 Выберите **Подтверждаю удаление <имя владельца сертификата>**.

5 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).

---

6 В зависимости от места хранения ключа ЭП:

- Хранилище ViPNet PKI Client — введите пароль хранилища ViPNet PKI Client и нажмите **Продолжить**.
- Токен — введите ПИН.
- Облачный сервис (если не подключались ранее) — введите имя и пароль учетной записи пользователя.

  Если для подключения к облачному сервису ЭП используется сертификат, который хранится на внешнем устройстве, введите ПИН внешнего устройства.

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

4

Использование облачных сервисов ЭП

Об облачных сервисах ЭП

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

Если в вашей организации используется облачный сервис ViPNet PKI Service, 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 сервису

1 Получите у вашего администратора:

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

Таблица 1. Способы подключения и дополнительные данные

Способ подключения	Дополнительные данные
HTTP, имя и пароля	Имя и разовый пароль учетной 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 Для подключения по протоколу HTTPS установите полученные сертификаты издателей и CRL.

3 Для подключения с помощью сертификата подготовьте его:

   3.1 Чтобы сохранить ключ ЭП и сертификат на токене, подключите его к компьютеру.

   3.2 Создайте запрос на сертификат.

   3.3 Передайте запрос в УЦ из полученного списка.

   3.4 Получите личный сертификат пользователя, а также при наличии сертификаты всех УЦ из цепочки и соответствующие CRL.

   3.5 Установите полученные сертификаты и CRL:

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

   3.6 Передайте личный сертификат вашему администратору. После его добавления в вашу учетную 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 В разделе **Облачные сервисы** включите **Использовать функции облачного сервиса**.

3 Нажмите **Добавить** и укажите:

- Название облачного сервиса.
- Адрес и порт ViPNet PKI Service.
- Способ аутентификации. При выборе способа аутентификации по сертификату выберите сертификат для подключения к сервису.

4 Нажмите .

5 Чтобы проверить соединение с сервисом, наведите на него курсор и нажмите .

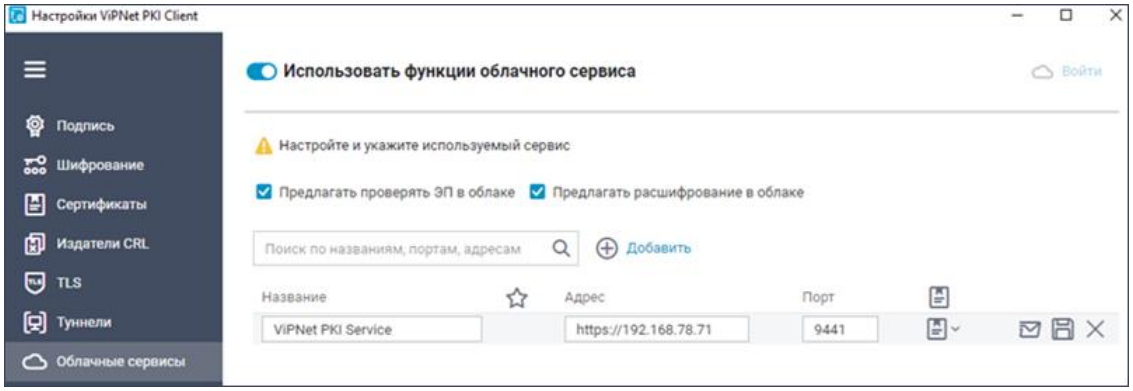

Рисунок 11. Настройка подключения к облачному сервису ЭП (на базе ViPNet PKI Service)

6 Чтобы отредактировать или удалить облачный сервис, наведите на него курсор и нажмите или соответственно.

7 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**.

8 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**.

9 Если вы добавили несколько сервисов, в списке **Используемый сервис** выберите тот, к которому будете подключаться по умолчанию.

10 Нажмите **Сохранить**.

11 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.
- При просмотре и выборе сертификатов для подписи, хранимых в облачном сервисе ЭП.
- При 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 В разделе **Облачные сервисы** выберите **Используемый сервис**.

3 Справа вверху нажмите Войти.

4 В зависимости от места хранения ключа ЭП:

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

Подключение с помощью имени и пароля учетной записи

1 Перейдите в настройки ViPNet PKI Client.

2 Справа вверху нажмите Войти.

3 Введите имя и пароль учетной записи и нажмите **Войти**.

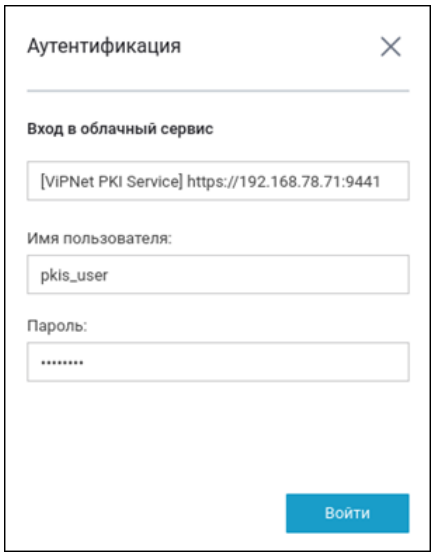

Рисунок 12. Подключение к облачному сервису ЭП с помощью имени и пароля учетной записи

Смена пароля учетной записи пользователя

1 Перейдите в настройки ViPNet PKI Client.

2 В разделе  **Облачные сервисы** выберите **Используемый сервис** и подключитесь к нему.

3 Справа вверху нажмите на имя пользователя и выберите **Сменить пароль**.

4 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.

5

Подпись, зашифрование файлов

Требования к сертификатам для подписи и зашифрования

- Сертификат действителен.
- Личный сертификат, который используется для подписи:
  - установлен в категорию **Личные сертификаты**;
  - в поле **Использование ключа** содержит хотя бы одно из назначений: **Цифровая подпись**, **Неотрекаемость**;
  - в поле **Расширенное использование ключа** содержит назначение **Защищенная электронная почта**.
- Сертификаты получателей, которые используются для зашифрования:
  - установлены в категорию **Сертификаты других пользователей**;
  - в поле **Использование ключа** содержат хотя бы одно из назначений: **Шифрование данных**, **Шифрование ключей**, **Согласование ключей**;
  - в поле **Расширенное использование ключа** содержат назначение **Защищенная электронная почта**.

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

Порядок подписания файла

	Действие и ссылка	Ссылка
1	Убедитесь, что у вас есть подходящий сертификат и соответствующий ключ ЭП. Если нет, подготовьте личный сертификат	Требования к сертификатам для подписи и зашифрования Просмотр сведений о сертификатах Проверка сертификатов Подготовка личного сертификата и ключа ЭП
2	Настройте параметры ЭП по умолчанию	Настройка параметров процесса подписи
3	Подпишите файлы и передайте их получателям любым удобным способом	Подписание файла

Настройка параметров процесса подписи

1 Перейдите в настройки ViPNet PKI Client.

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

3 Выберите сертификат и нажмите **Выбрать**.

Примечание. Если сертификат хранится на токене, установите его в локальное хранилище компьютера.

4 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.

5 Чтобы использовать подпись формата XMLDSig, установите соответствующий флажок.

6 Если необходимо, выберите сохранение файла в кодировке Base64.

7 Чтобы добавить к ЭП подтверждение точного времени подписания файла:

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

7.2 В поле **Адрес TSP-сервера** укажите URL-адрес сервера:

```
http://<IP-адрес или доменное имя>:<порт>
```

7.3 Проверьте соединение с сервером штампов времени.

Внимание! Чтобы использовать указанный TSP-сервер 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-сервера, а также при наличии сертификаты всех УЦ из цепочки и соответствующие CRL.
- Облачный сервис ЭП должен иметь доступ к TSP-серверу.

8 Если необходимо изменить путь сохранения результатов подписи, нажмите **Обзор**.

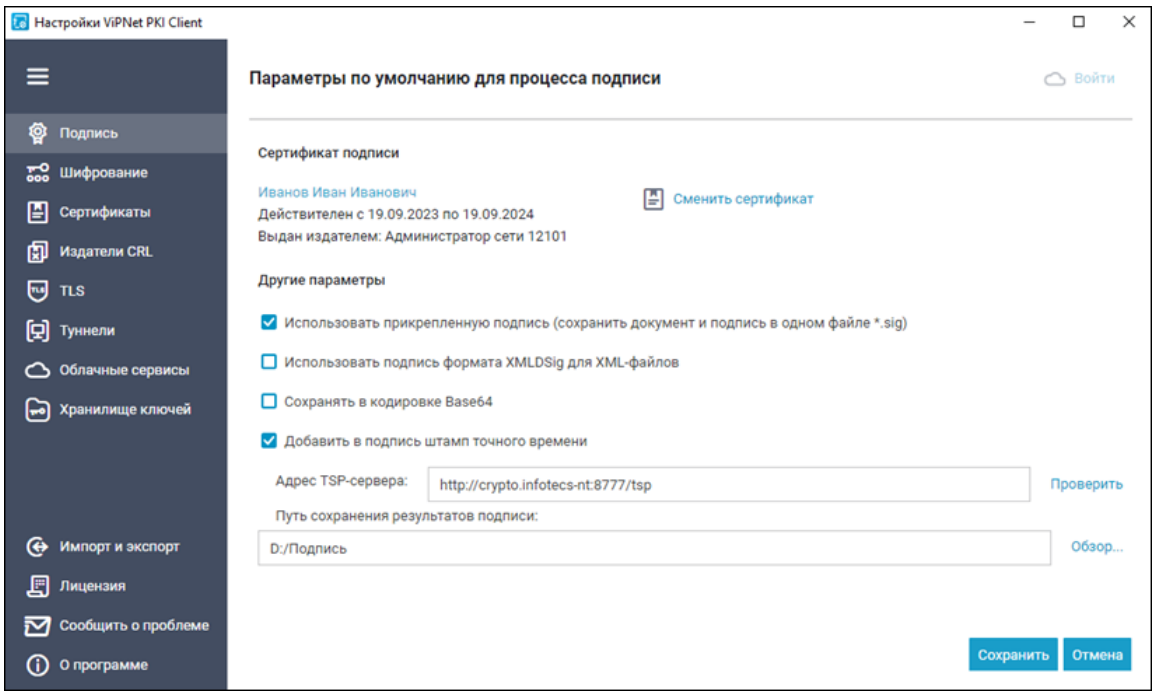

Рисунок 13. Настройка параметров ЭП

9 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 в списке **Выбранные файлы**.

2 Справа выберите **Подписать сертификатом**. Станут доступны настройки параметров ЭП.

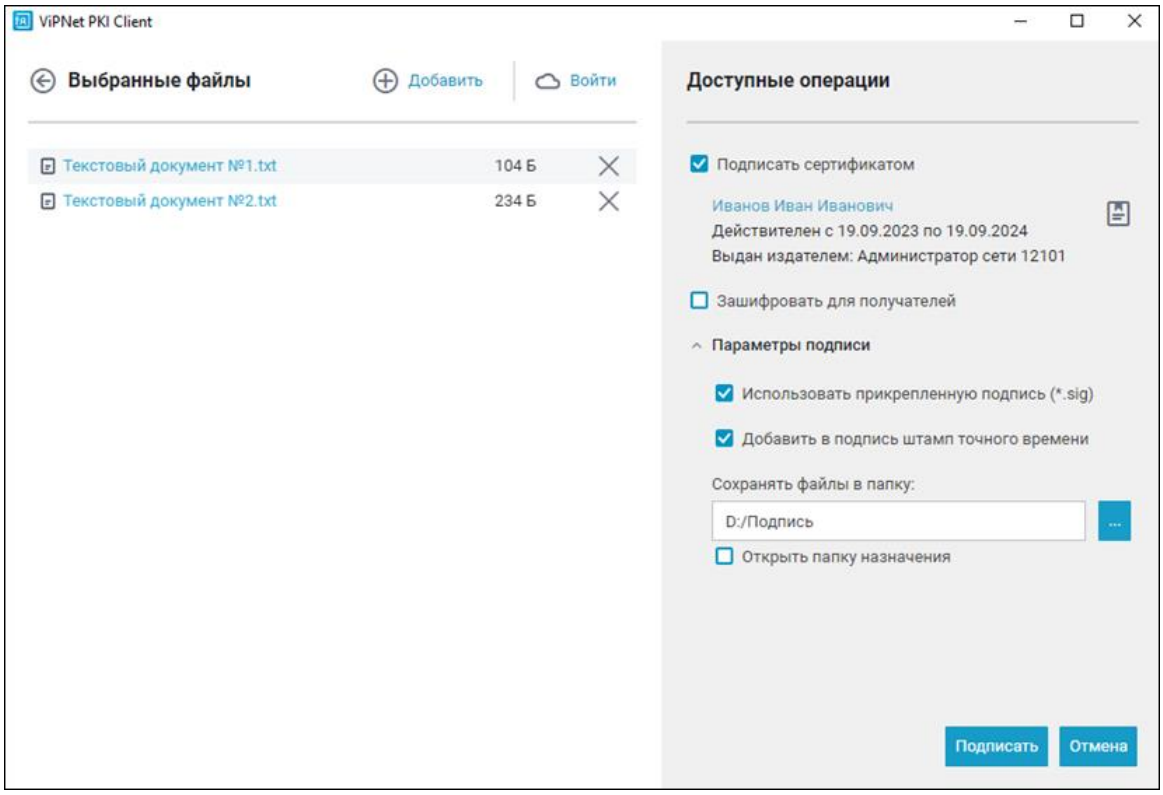

Рисунок 14. Подписание файла

3 Если необходимо, выберите другой сертификат с помощью , включите зашифрование и измените параметры ЭП.

Примечание. Если сертификат хранится на токене, установите его в локальное хранилище компьютера.

---

4 Нажмите **Подписать**.

5 В зависимости от места хранения контейнера ключей:

- Хранилище ViPNet PKI Client — введите пароль хранилища ViPNet PKI Client и нажмите **Продолжить**.
- Токен — введите ПИН.
- Облачный сервис ЭП (если не подключились ранее) — имя и пароль учетной записи пользователя.

  Если для подключения к облачному сервису ЭП используется сертификат, который хранится на внешнем устройстве, введите ПИН внешнего устройства.

Внимание! После 10 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

	Действие	Ссылка
1	Запросите у получателей зашифрованных файлов их сертификаты. Установите их и убедитесь, что они соответствуют требованиям	Установка сертификатов и CRL Требования к сертификатам для подписи и зашифрования Просмотр сведений о сертификатах Проверка сертификатов
2	Настройте параметры шифрования по умолчанию	Настройка параметров зашифрования
3	Зашифруйте файлы и передайте их получателям любым удобным способом	Зашифрование файла

Настройка параметров зашифрования

1 Перейдите в настройки ViPNet PKI Client.

2 Выберите раздел **Шифрование**.

3 Чтобы повторно не выбирать сертификаты получателей при зашифровании файлов, сформируйте список получателей:

3.1 В списке **Получатели зашифрованных файлов** нажмите **Добавить**.

3.2 Выберите сертификаты получателей и нажмите **Выбрать**.

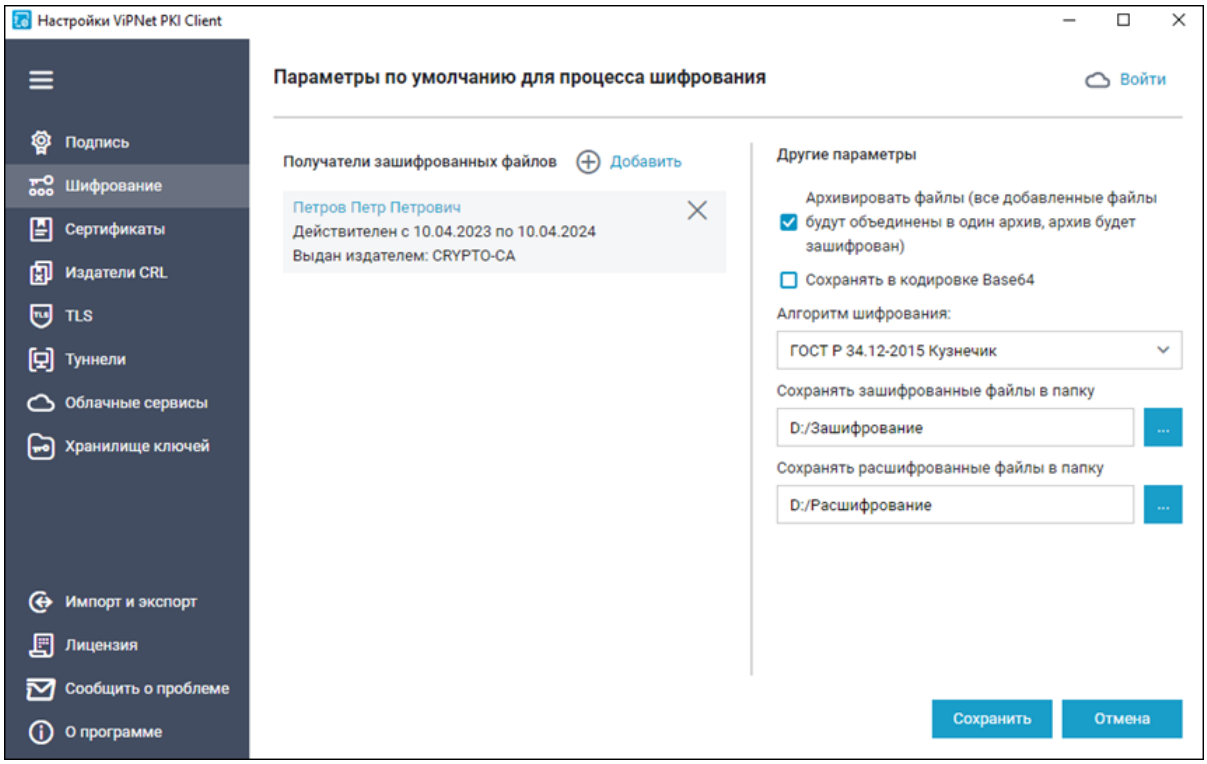

Рисунок 15. Настройка параметров шифрования

Примечание. Чтобы удалить сертификат получателя из списка, нажмите .

4 Выберите необходимые 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 в списке **Выбранные файлы**.

2 Справа выберите **Зашифровать для получателей**. Станут доступны настройки параметров зашифрования.

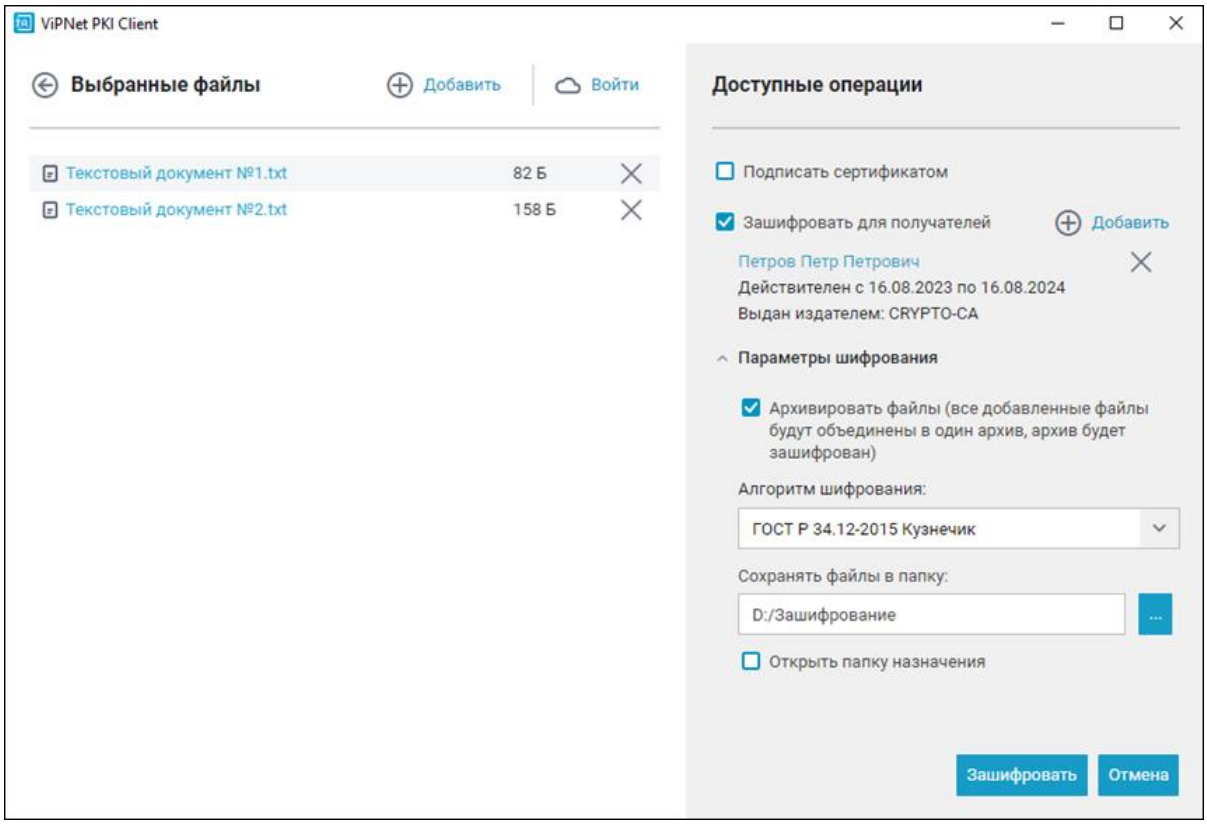

Рисунок 16. Зашифрование файла

3 Если необходимо, измените список получателей и 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 в списке **Выбранные файлы**.

---

2 Справа выберите **Подписать сертификатом** и **Зашифровать для получателей**. Станут доступны настройки параметров ЭП и зашифрования.

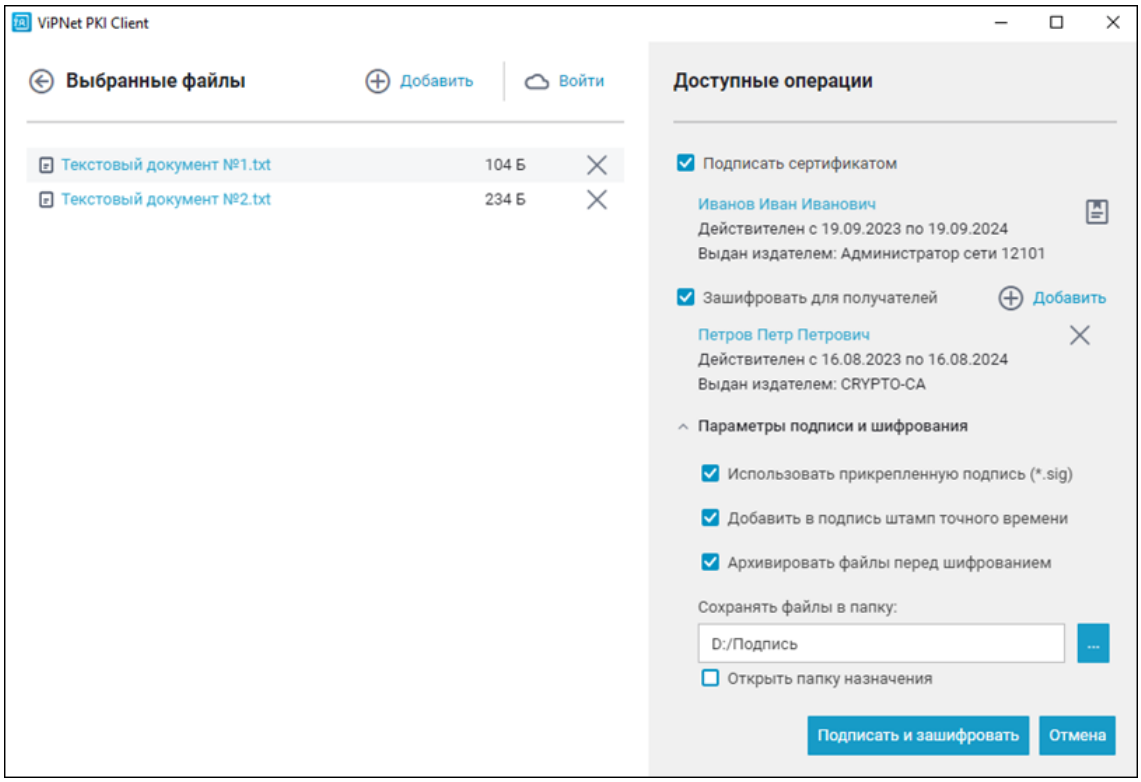

Рисунок 17. Одновременное подписание и зашифрование файла

3 Если необходимо, измените параметры ЭП и зашифрования.

4 Нажмите **Подписать и зашифровать**.

5 В зависимости от места хранения сертификата подписанта:

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

- Токен — введите ПИН.
- Облачный сервис ЭП (если не подключились ранее) — имя и пароль учетной записи пользователя.

  Если для подключения к облачному сервису ЭП используется сертификат, который хранится на внешнем устройстве, введите ПИН внешнего устройства.

Внимание! После 10 неудачных попыток ввода пароля File Unit, Web Unit и настройки ViPNet PKI Client блокируются на 15 минут.

6

Работа с файлами, полученными от других пользователей

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

Примечание. При выборе нескольких файлов проверка открепленной ЭП возможна только если исходный файл расположен в той же папке, что и файл `*.detached.sig`.

1 В главном окне File Unit выполните одно из действий:

- Перетащите нужные файлы `*.sig` в главное окно программы.
- Нажмите **Выбрать файлы** и выберите один или несколько файлов `*.sig`.

2 В зависимости от количества выбранных файлов и типа ЭП:

- Если вы выбрали один файл с прикрепленной ЭП, результат проверки ЭП отобразится в разделе **Выбранные файлы**.

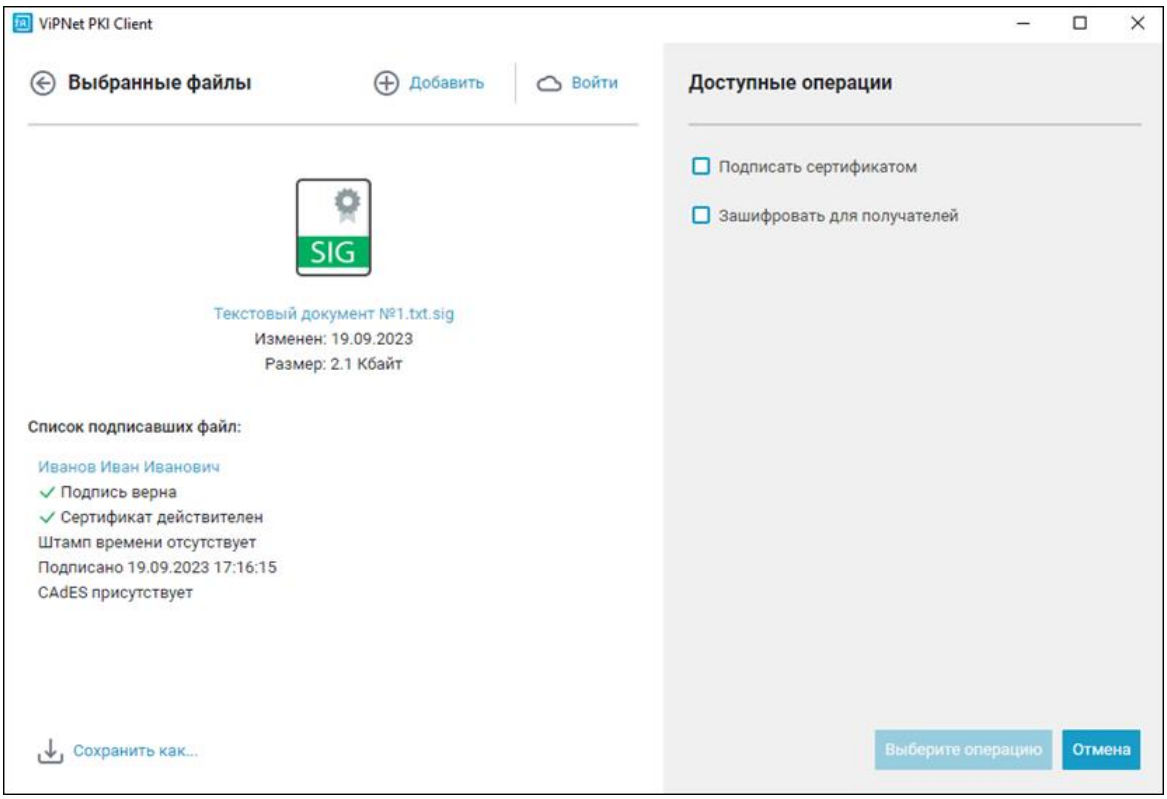

Рисунок 18. Проверка прикрепленной ЭП

- Если вы выбрали один файл с открепленной ЭП, напротив имени файла нажмите . Укажите исходный файл и нажмите **Открыть**.
- Если исходный файл и файл ЭП расположены в одной папке, проверка ЭП выполнится автоматически. Результат проверки ЭП отобразится в отдельном окне.

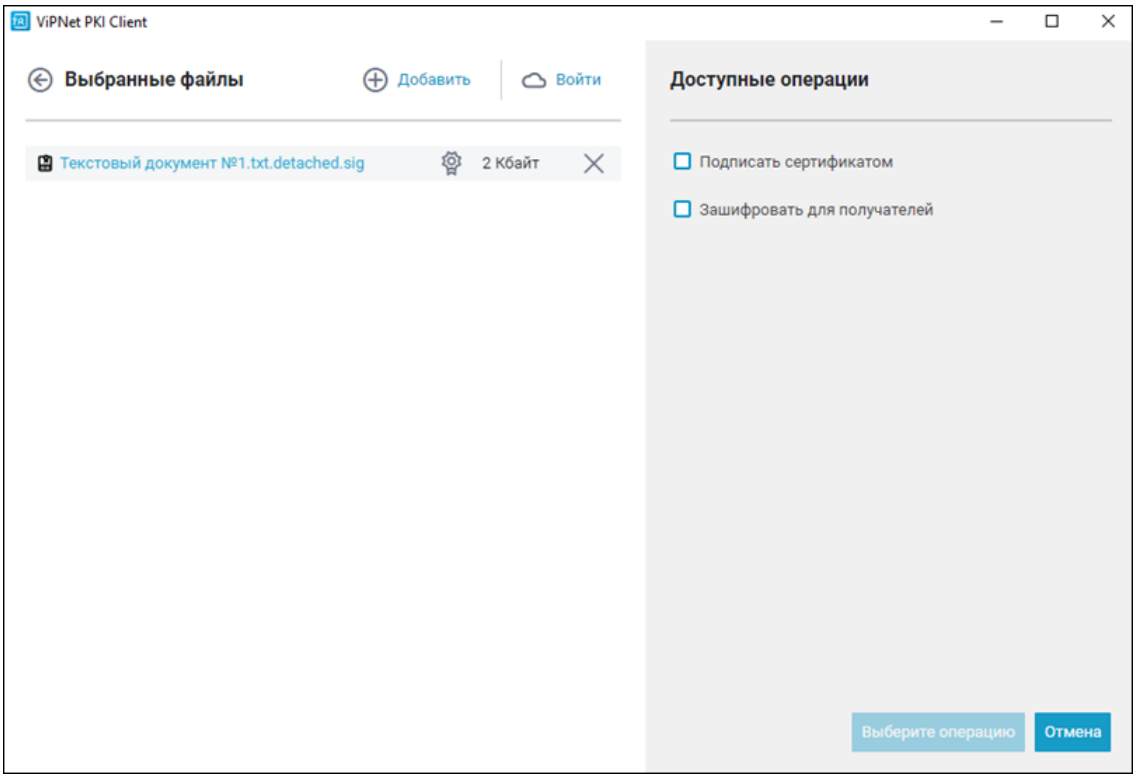

Рисунок 19. Проверка откреплённой ЭП

- Если вы выбрали несколько файлов, для проверки ЭП нажмите напротив имени файла:
  - Если использовалась прикрепленная ЭП, результат проверки ЭП отобразится в отдельном окне.
  - Если использовалась откреплённая ЭП, укажите исходный файл и нажмите **Открыть**.
  - Если исходный файл и файл подписи расположены в одной папке, проверка ЭП произойдет автоматически. Результат проверки подписи отобразится в отдельном окне.

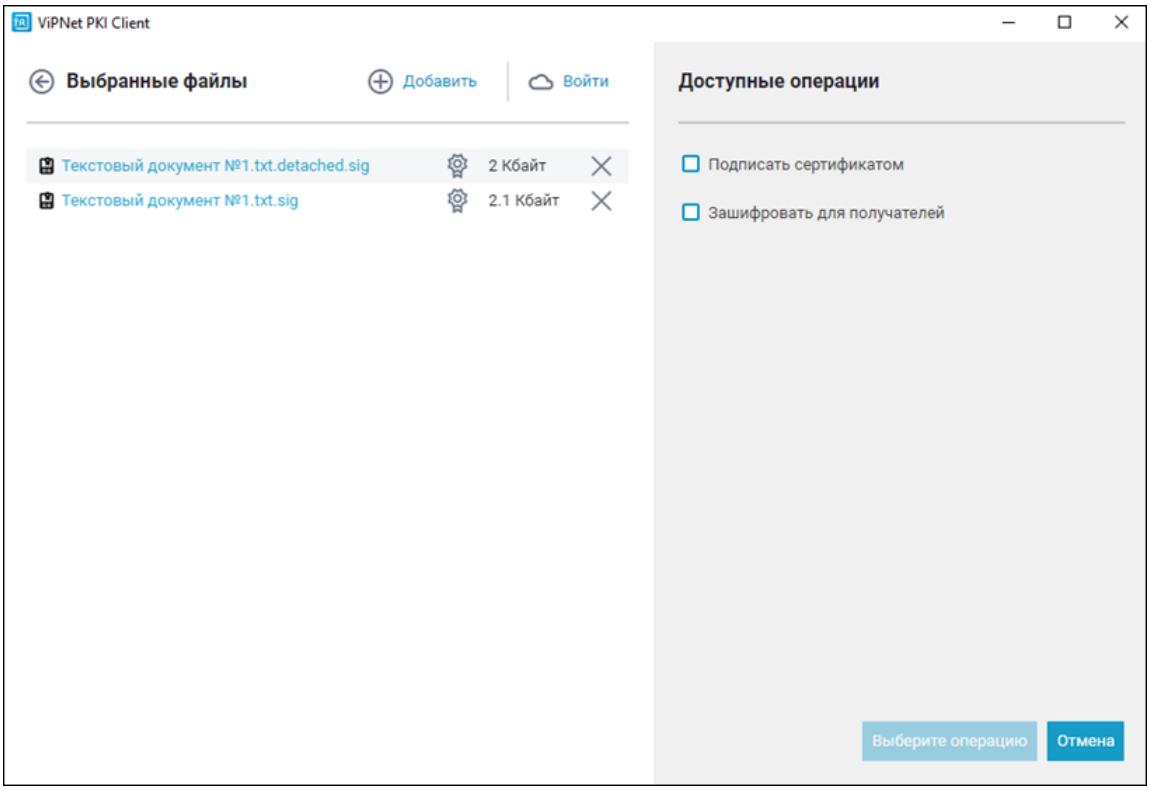

Рисунок 20. Проверка ЭП нескольких файлов

3 Просмотрите результат проверки ЭП:

- чтобы открыть сертификат владельца подписи, нажмите его имя;
- чтобы открыть штамп времени, нажмите **присутствует**;
- если необходимо, сохраните исходный файл.

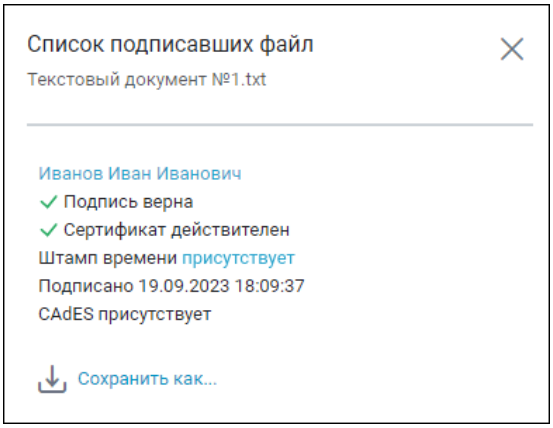

Рисунок 21. Результаты проверки подписи

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 При необходимости измените параметры расшифрования и нажмите **Расшифровать**.

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

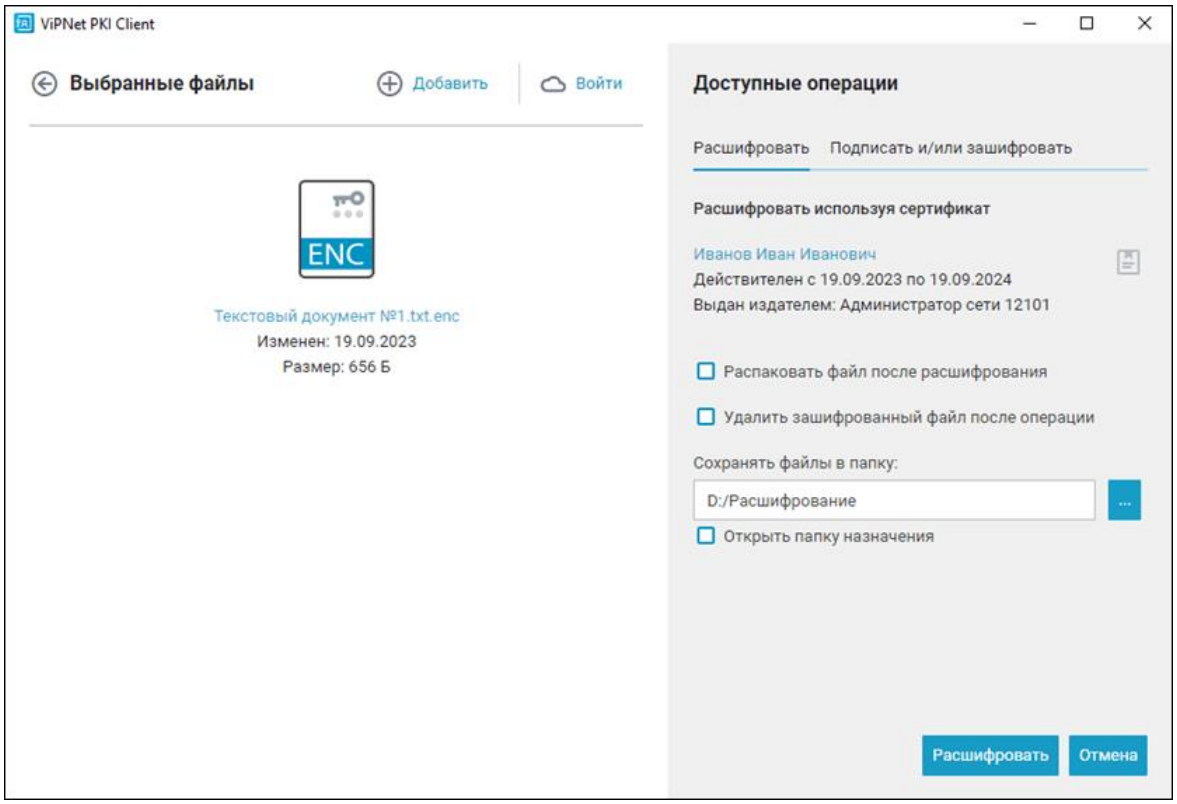

Рисунок 22. Расшифрование файла

4 В зависимости от места хранения контейнера ключей:

- Хранилище ViPNet PKI Client — введите пароль хранилища ViPNet PKI Client и нажмите **Продолжить**.
- Токен — введите ПИН.
- Облачный сервис ЭП (если не подключились ранее) — имя и пароль учетной записи пользователя.

  Если для подключения к облачному сервису ЭП используется сертификат, который хранится на внешнем устройстве, введите ПИН внешнего устройства.

Внимание! После 10 неудачных попыток ввода пароля File Unit, Web Unit и настройки ViPNet PKI Client блокируются на 15 минут.

7

Настройка подключения к сайтам, использующим TLS ГОСТ

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 верна;
   - сертификат в поле **Расширенное использование ключа** содержит назначение **Проверка подлинности клиента**;
   - сертификат в поле **Использование ключа** содержит назначение **Цифровая подпись** и (или) **Согласование ключей**.
2 Запустите TLS Unit.
3 Подключитесь к сайту.
4 При необходимости просмотрите информацию о текущих TLS-соединениях.

Примечание. Подробнее о настройке подключения к сайтам по TLS ГОСТ см. «ViPNet PKI Client Windows. Руководство администратора».

Подключение к сайту

Совет. Если вы используете браузер Firefox, необходимо настроить его совместную работу с TLS Unit. Подробнее см. «ViPNet PKI Client Windows. Руководство администратора».

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 ПИН 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 щелкните 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.

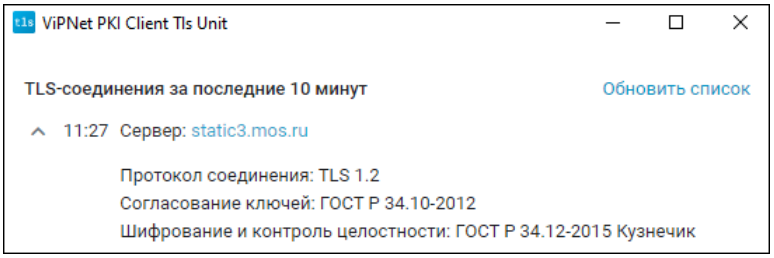

Рисунок 23. Просмотр информации о TLS-соединениях

8

Возможные неполадки

Обращение в техническую поддержку

1 Перейдите в настройки ViPNet PKI Client.

2 На панели слева нажмите **Сообщить о проблеме**.

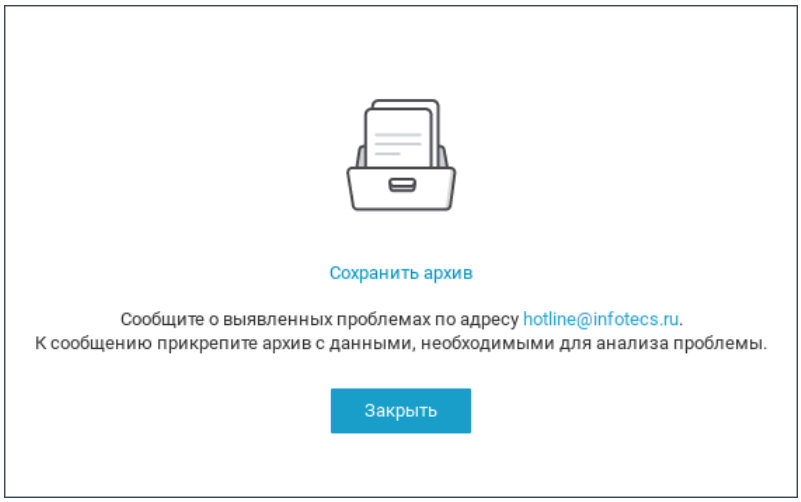

Рисунок 24. Сохранение архива с данными для отправки в ИнфоТеКС

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.

Попробуйте удалить сертификат через консоль:

1. Откройте Microsoft Management Console:
   1.1. Нажмите сочетание клавиш **Win+R**.
   1.2. В поле **Открыть** введите `mmc` и нажмите **OK**.
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 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.

File Unit

Нет сертификата в списке сертификатов для подписи

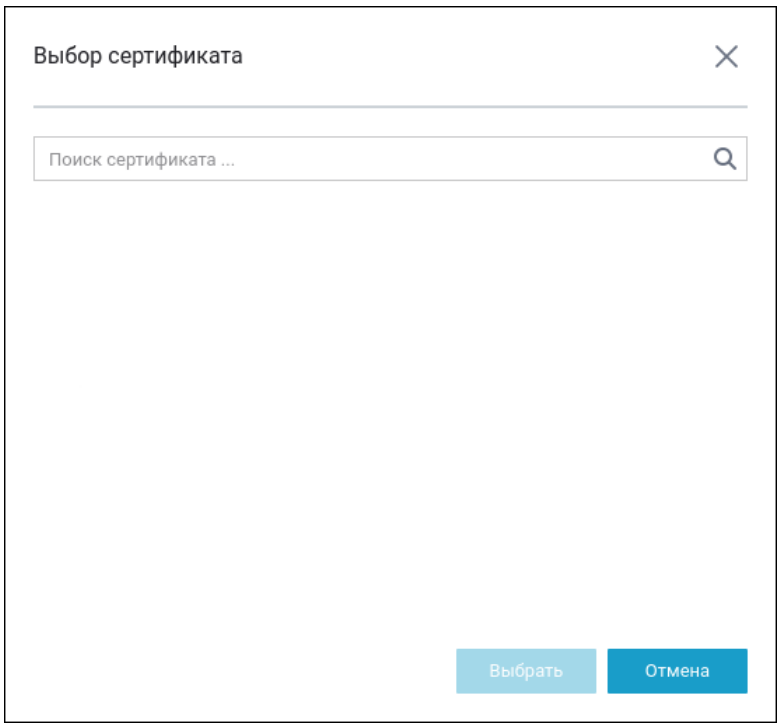

Рисунок 25. Сертификат не отображается в списке сертификатов

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 В разделе **Сертификаты** откройте сертификат.

3 На вкладке **Состав** найдите поле **Средство электронной подписи владельца**.

A

Внешние устройства

Список поддерживаемых внешних устройств

В следующей таблице перечислены внешние устройства, которые можно использовать в ViPNet PKI Client. Для каждого внешнего устройства в таблице указаны необходимые условия для работы с ним.

Таблица 2. Поддерживаемые внешние устройства

Полные названия устройств	Необходимые условия для работы с внешним устройством
Рутокен Lite **Рутокен ЭЦП 2.0** **Рутокен ЭЦП 2.0 Flash** **Рутокен ЭЦП 3.0** **Рутокен ЭЦП 3.0 NFC**	На компьютере должны быть установлены драйверы Рутокен.
Рутокен S	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».

Полные названия устройств	Необходимые условия для работы с внешним устройством
JaCarta LT **JaCarta PRO** **JaCarta PKI** **JaCarta ГОСТ** **JaCarta-2 SE** **JaCarta-2 ГОСТ** **JaCarta-2 PRO/ГОСТ** **JaCarta-2 PKI/ГОСТ**	На компьютере должен быть установлен ПК «Единый Клиент JaCarta» компании «Аладдин Р.Д.» (рекомендуемая минимальная версия — 3.0).
ESMART Token ГОСТ **«MS_KEY K» - «АНГАРА»**	На компьютере должно быть установлено ПО ESMART PKI Client для Windows (рекомендуемая версия — 4.13).

Внешние устройства, поддерживающие алгоритмы ГОСТ

В следующей таблице перечислены внешние устройства, поддерживающие российские криптографические алгоритмы.

Таблица 3. Внешние устройства, поддерживающие алгоритмы ГОСТ

Полные названия устройств	Аппаратная поддержка алгоритмов ГОСТ на устройстве
Рутокен Lite **Рутокен S**	отсутствует
Рутокен ЭЦП 2.0 **Рутокен ЭЦП 2.0 Flash**	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012
Рутокен ЭЦП 3.0 **Рутокен ЭЦП 3.0 NFC**	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018) «Магма» и «Кузнечик»
JaCarta LT **JaCarta PRO** **JaCarta PKI**	отсутствует
JaCarta-2 SE	ГОСТ Р 34.10-2012
JaCarta-2 ГОСТ **JaCarta-2 PRO/ГОСТ** **JaCarta-2 PKI/ГОСТ**	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012

Полные названия устройств	Аппаратная поддержка алгоритмов ГОСТ на устройстве
ESMART Token ГОСТ	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012
«MS_KEY K» - «АНГАРА»	ГОСТ Р 34.10-2012, ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018) «Магма» и «Кузнечик»

Внимание! Если вы сменили или хотите сменить ПИН токена, на котором отсутствует аппаратная поддержка алгоритмов ГОСТ, см. «ViPNet PKI Client Windows. Руководство администратора».

B

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 в составе доверенного субъекта инфраструктуры открытых ключей, обладающего точным и надёжным источником времени и предоставляющего 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 КВ и средством электронной подписи класса КВ2.

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.