ViPNet PKI Client File Unit

Руководство пользователя

infotecs

ФРКЕ.00175-02 34 01

Версия продукта 1.7.0

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 назначение и применение программы File Unit, которая входит в состав программного комплекса ViPNet® PKI Client (далее — ViPNet PKI Client).

Документ предназначен для пользователей ViPNet PKI Client, которые хотят безопасно обмениваться документами по открытым каналам связи или с использованием съемных носителей.

Соглашения документа

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

О программе

File Unit входит в состав ViPNet PKI Client и позволяет защитить файлы, передаваемые по открытым каналам связи или с помощью съемных носителей, с помощью шифрования (см. глоссарий, стр. 54) и электронной подписи (см. глоссарий, стр. 56).

Системные требования

- Процессор — Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более.
- Объем оперативной памяти — не менее 2 Гбайт.
- Свободное место на жестком диске — не менее 1 Гбайт.
- Операционная система с последними пакетами обновлений:
  - Windows 7 — 32/64-разрядная;
  - Windows Server 2012 — 64-разрядная;
  - Windows 8.1 — 32/64-разрядная;
  - Windows Server 2012 R2 — 64-разрядная;
  - Windows Server 2016 — 64-разрядная;
  - Windows Server 2019 — 64-разрядная;
  - Windows 10 — 32/64-разрядная следующих версий и сборок:
    - версия 1803, сборка 17134;
    - версия 1809, сборка 17763;
    - версия 1903, сборка 18362;
    - версия 1909, сборка 18363;
    - версия 2004, сборка 19041;
    - версия 20H2, сборка 19042.

    Работа ViPNet PKI Client на компьютерах с Windows 10 других версий и сборок не гарантируется.
- Браузер — Internet Explorer 11, Chromium с поддержкой ГОСТ 68.0.3440.84, КриптоПро Fox 24 или выше, а также Edge, Google Chrome, Mozilla Firefox, Opera, Яндекс.Браузер, Спутник последних версий.
- Программная платформа Microsoft .NET Framework 4.5.

Обратная связь

Дополнительная информация

Сведения о продуктах ViPNet, частые вопросы и полезная информация на сайте ИнфоТеКС:

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

Контактная информация

Если у вас есть вопросы, свяжитесь со специалистами ИнфоТеКС:

- Единый многоканальный телефон:

  +7 (495) 737-6192,

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

- Служба поддержки: hotline@infotecs.ru.

  Форма для обращения в службу поддержки через сайт.

  Канал поддержки в Telegram: t.me/vhd21

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

- Отдел продаж: soft@infotecs.ru.

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

1

Общая информация

Назначение

File Unit устанавливается на рабочие места пользователей вместе с другими компонентами ViPNet PKI Client. С File Unit можно работать через главное окно (см. Интерфейс на стр. 17) или контекстное меню Windows (см. Работа через контекстное меню Windows на стр. 18).

С помощью программы File Unit вы можете:

- Шифровать файлы (см. Зашифрование файла на стр. 38).

  Шифрование обеспечивает конфиденциальность данных в файле. Только получатель, с использованием сертификата которого зашифрован файл, может расшифровать и прочитать этот файл.

- Работать с зашифрованными файлами, полученными от других пользователей (см. Расшифрование файла на стр. 45).

  При получении файла, зашифрованного с использованием вашего сертификата с помощью File Unit или другой программы, поддерживающей асимметричное шифрование (см. глоссарий, стр. 54) и формат ENC (см. глоссарий, стр. 56), вы можете расшифровать его с помощью File Unit.

- Подписывать файлы (см. Подписание файла на стр. 35).

  ЭП удостоверяет личность подписавшего файл, а также гарантирует неизменность данных файла после подписания (то есть целостность файла).

- Проверять личность отправителя и целостность полученных файлов (см. Проверка ЭП файла на стр. 47).

  При получении файла, подписанного с помощью File Unit или другой программы, поддерживающей асимметричную ЭП (см. глоссарий, стр. 54) и формат `SIG` (см. глоссарий, стр. 56), вы можете проверить ЭП. В файле `*.sig` вместе с ЭП передается также сертификат пользователя, подписавшего файл, который требуется для проверки ЭП.

- Подтверждать время подписания файлов (см. Подписание файла на стр. 35).

  При подписании файла вы можете добавить к ЭП штамп времени. Штамп времени фиксирует точное время подписания файла и при возникновении спорных ситуаций позволяет доказать факт существования файла на момент его подписания.

Для выполнения криптографических операций в File Unit используются:

- Алгоритмы формирования и проверки ЭП данных ГОСТ Р 34.10-2001 с вычислением хэш-функции по ГОСТ Р 34.11-94 (только для проверки ЭП и расшифрования) и ГОСТ Р 34.10-2012 с вычислением хэш-функции по ГОСТ Р 34.11-2012.
- Алгоритм шифрования информации ГОСТ 28147-89.

Требования к сертификатам для подписи и шифрования

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

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

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

Принцип работы

File Unit формирует и проверяет ЭП, а также зашифровывает и расшифровывает файлы. Для выполнения криптографических операций File Unit обращается к криптопровайдеру ViPNet CSP из состава ViPNet PKI Client или ПАК ViPNet PKI Service (требуется лицензия на использование Cloud Unit). Подробно см. «ViPNet PKI Client. Руководство администратора».

File Unit работает на основе алгоритмов асимметричного шифрования и формирования электронной подписи, которые используют пару связанных между собой асимметричных ключей пользователя:

- Ключ ЭП — используется для формирования ЭП и расшифрования файлов. Ключ ЭП должен храниться в секрете.
- Ключ проверки ЭП — используется для проверки ЭП и шифрования файлов. Ключ проверки ЭП свободно распространяется среди других пользователей в составе сертификата (см. глоссарий, стр. 55).

Рассмотрим принцип работы File Unit совместно с ViPNet CSP на следующих примерах:

- Подписание файла (на стр. 12).
- Зашифрование файлов (на стр. 13).
- Подписание и зашифрование файлов (на стр. 14).

Подписание файла

1 Отправитель в File Unit инициирует подписание файла, который предназначен для отправки получателю.

2 File Unit подписывает файл:

2.1 File Unit обращается к ViPNet CSP для формирования ЭП с помощью ключа ЭП отправителя.

2.2 File Unit формирует файл `*.sig`, содержимое которого зависит от типа ЭП, который использует отправитель:

- Прикрепленная ЭП (см. глоссарий, стр. 55) — в этом случае в файл `<имя_файла>.sig` помещаются данные исходного файла, сформированная ЭП и служебная информация.

  Прикрепленная подпись упрощает обмен, копирование и шифрование подписанных файлов (например, в системах электронного документооборота). При этом прочитать файл смогут только пользователи, на компьютерах которых установлены средства работы с файлами `*.sig` (File Unit, ViPNet Деловая почта или программы сторонних производителей со схожими функциями, например КриптоАРМ).

- Открепленная ЭП (см. глоссарий, стр. 55) — в этом случае в файл `<имя_файла>.detached.sig` помещаются сформированная ЭП и служебная информация, а исходный файл передается получателю отдельно. Для проверки ЭП файла требуется и файл с открепленной подписью, и исходный файл.

  Открепленная подпись позволяет прочитать исходный файл пользователям, на компьютерах которых не установлены средства работы с файлами `*.sig`. Однако в этом случае передача, шифрование и другие операции с файлом подписи затрудняются, так как операции необходимо производить с двумя файлами: исходным файлом и файлом `<имя_файла>.detached.sig`.

Рисунок 1. Подписание документа с помощью File Unit

3 Отправитель передает получателю файл `*.sig`, а также исходный файл (если была выбрана открепленная подпись), например, с помощью электронной почты.

4 Получатель проверяет ЭП с использованием ключа проверки ЭП, который содержится в сертификате отправителя.

Зашифрование файлов

1 Отправитель в File Unit инициирует зашифрование файла, предназначенного для передачи получателям.

2 Отправитель выбирает сертификаты получателей, установленные в хранилище.

3 File Unit обращается к ViPNet CSP для зашифрования файла с помощью ключей проверки ЭП выбранных получателей и формирует зашифрованный файл `*.enc`.

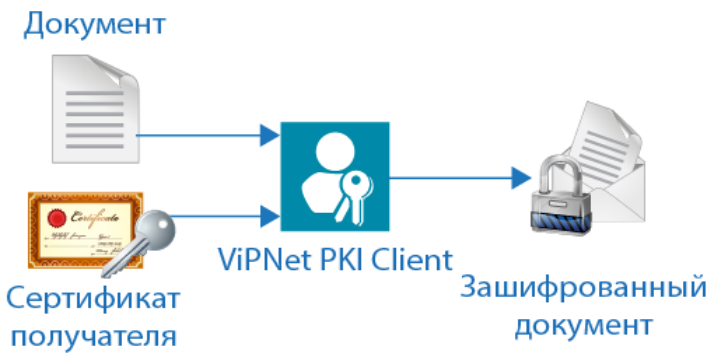

Рисунок 2. Шифрование документа с помощью File Unit

4 Отправитель передает получателям зашифрованный файл, например, с помощью электронной почты.

5 Получатели расшифровывают файл с использованием своих ключей ЭП.

Подписание и зашифрование файлов

1 Отправитель в File Unit инициирует подписание и зашифрование файла, предназначенного для передачи получателям.

2 File Unit обращается к ViPNet CSP для формирования ЭП с помощью ключа ЭП отправителя и формирует файл `*.sig`, содержимое которого зависит от типа ЭП (см. Подписание файла на стр. 12).

3 Отправитель выбирает сертификаты получателей, установленные в хранилище.

4 File Unit обращается к ViPNet CSP для зашифрования файла с помощью ключей проверки ЭП выбранных получателей и формирует зашифрованный файл `*.enc`.

5 Отправитель передает получателям подписанный и зашифрованный файл, например, с помощью электронной почты.

6 Получатели расшифровывают файл с использованием своих ключей ЭП.

7 Получатели проверяют ЭП с использованием ключа проверки ЭП, содержащегося в сертификате отправителя.

2

Начало работы

Установка и запуск

File Unit устанавливается в процессе развертывания ViPNet PKI Client (см. «ViPNet PKI Client. Руководство администратора»).

Чтобы запустить программу File Unit, в меню **Пуск** выберите **ViPNet** > **File Unit**.

Чтобы перейти к настройкам компонентов ViPNet PKI Client, выполните одно из действий:

- В основном окне File Unit нажмите  **Настройки**.
- В меню **Пуск** выберите **ViPNet** > **Настройки ViPNet PKI Client**.
- Дважды щелкните ярлык  на рабочем столе.

Интерфейс

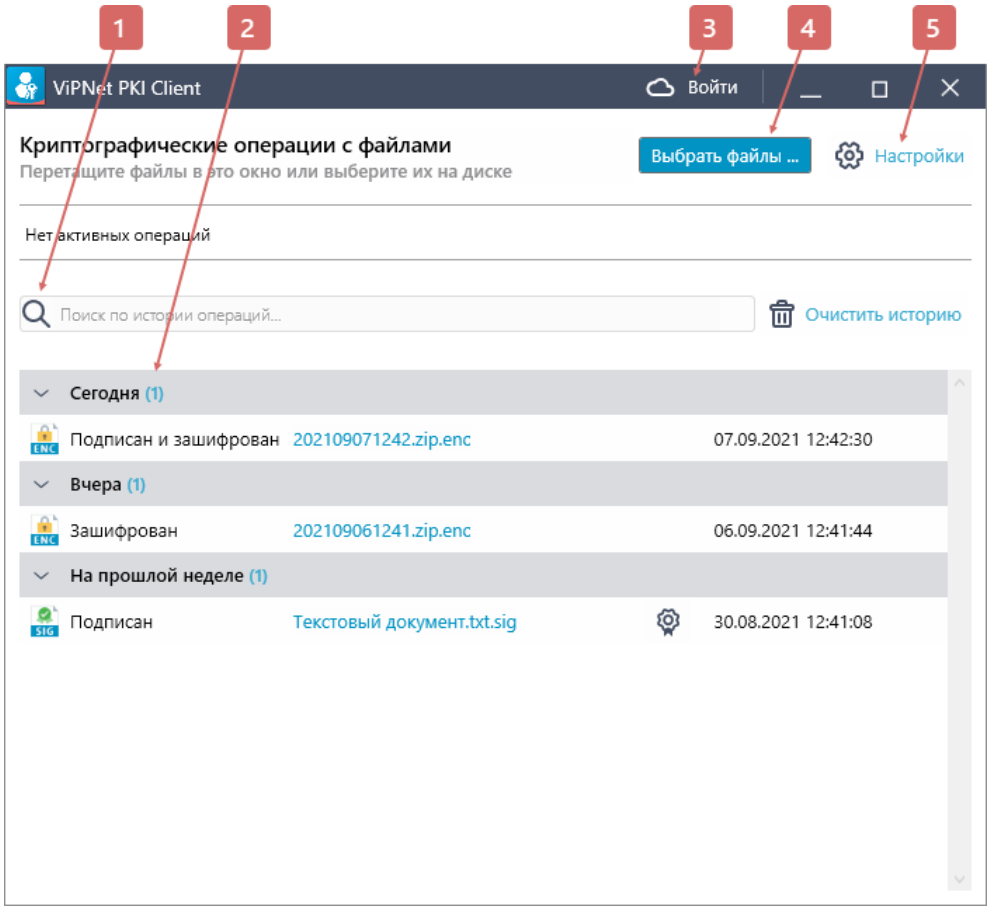

Рисунок 3. Главное окно File Unit

1 Строка поиска файлов.

2 Область истории операций с файлами.

3 Кнопка подключения к облачному сервису ЭП.

4 Кнопка выбора файлов для выполнения операций.

5 Кнопка настройки.

Работа через контекстное меню Windows

Работать с File Unit через контекстное меню Windows удобно, если вы находись в проводнике Windows и хотите зашифровать файл, не переключаясь в главное окно File Unit.

С помощью контекстного меню Windows вы можете выполнять:

- Зашифрование файла (на стр. 38).
- Подписание файла (на стр. 35).
- Подписание и зашифрование файла (на стр. 40).
- Расшифрование файл (на стр. 45).
- Проверка ЭП (см. Проверка ЭП файла на стр. 47).

Примечание. Прежде чем начать работать с File Unit через контекстное меню Windows, выполните подготовку (см. Подготовка к работе с файлами на стр. 19).

Чтобы выполнить одно из перечисленных выше действий с помощью контекстного меню Windows:

1 В проводнике Windows выберите один или несколько файлов и щелкните правой кнопкой мыши.

2 В контекстном меню выберите **ViPNet PKI Client** > **<Операция>**.

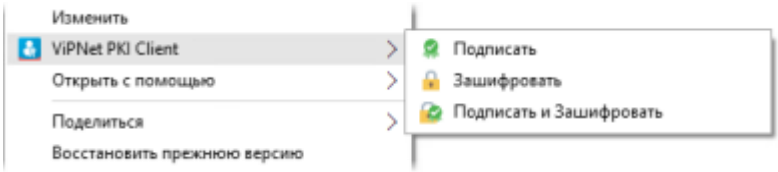

Рисунок 4. Работа через контекстное меню Windows

Во время выполнения операции следуйте указаниям:

- Защита файлов с помощью подписи и шифрования (на стр. 32).
- Работа с файлами, полученными от других пользователей (на стр. 43).

3

Подготовка к работе с файлами

Порядок подготовки к работе с файлами

	Действие и ссылка
1	Подготовьте личный сертификат и ключ ЭП (на стр. 21)
2	Установите сертификаты издателей и CRL в хранилище сертификатов (на стр. 27)
3	Настройте параметры ЭП (на стр. 33)
4	Настройте параметры шифрования файлов (на стр. 37)

Подготовка личного сертификата и ключа ЭП

У меня нет сертификата и ключа ЭП

1 Создайте запрос на сертификат (см. Получение сертификата на стр. 23).

2 Передайте запрос в УЦ и получите личный сертификат, сертификаты издателей из цепочки и соответствующие им CRL.

3 Установите личный сертификат в хранилище сертификатов Windows или на внешнее устройство (на стр. 27).

У меня есть сертификат и ключ ЭП в папке на диске

1 С помощью ViPNet CSP установите контейнер ключей (см. «ViPNet CSP. Руководство пользователя» > «Установка контейнера ключей из папки»).

2 Установите сертификат в хранилище сертификатов текущего пользователя **Личное** с указанием расположения контейнера ключей (см. в документе «ViPNet CSP. Руководство пользователя» > «Установка сертификата в системное хранилище Windows»).

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

1 Подключите внешнее устройство к компьютеру.

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

---

2 Выполните одно из действий:

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

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

1 Настройте подключение к ПАК ViPNet PKI Service.

2 Подключитесь к ПАК ViPNet PKI Service. Сертификат появится в списке сертификатов **Облачные**.

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

1. Создайте запрос на сертификат с помощью шаблона **Облачный** (см. Получение сертификата на стр. 23).
2. Установите его на ПАК ViPNet PKI Service (на стр. 27).

Получение сертификата

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

Чтобы создать запрос на сертификат:

1 Выполните одно из действий:

- Перейдите в настройки ViPNet PKI Client (на стр. 16), выберите раздел **Сертификаты** и нажмите **Создать запрос**.
- В меню **Пуск** выберите **ViPNet** > **Создание запроса на сертификат**.

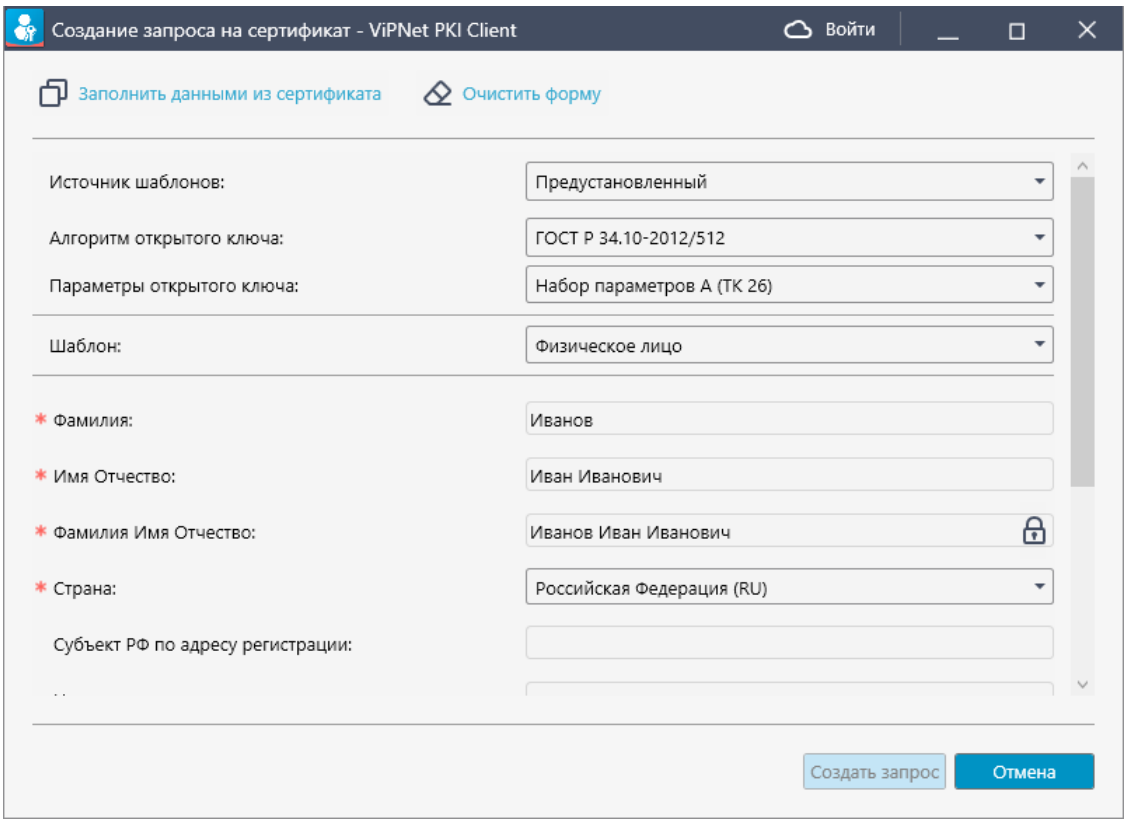

Рисунок 5. Создание запроса на сертификат

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

2 Выберите **Источник шаблонов**:

- **Предустановленный** — чтобы использовать добавленные по умолчанию шаблоны и сохранить контейнер ключей на диске или внешнем устройстве.
- **Пользовательский** — если в вашей организации требуется, чтобы в поле сертификата **Субъект (Subject)** присутствовали только определенные атрибуты:
  - Подготовьте файл в формате JSON (см. Подготовка файла шаблона в формате JSON на стр. 25) или XML (см. Подготовка файла шаблона в формате XML на стр. 25).
  - Задайте в подготовленном файле нужные атрибуты и загрузите в окно создания запроса на сертификат.

  При создании запроса контейнер ключей можно сохранить на диске или внешнем устройстве.
- **Облачный** — чтобы использовать шаблоны, добавленные на ViPNet PKI Service, и сохранить контейнер ключей на ПАК ViPNet PKI Service. В этом случае требуется настройка подключения к ПАК ViPNet PKI Service и авторизация на нем.

3 Выберите **алгоритм** и **параметры открытого ключа** или оставьте значение по умолчанию.

4 Выберите **Шаблон** сертификата и **Назначение сертификата** (если к качестве шаблона вы выбрали **Облачный**). **Шаблон** содержит разное количество и наименование атрибутов, которые попадут в поле сертификата **Субъект (Subject)**. **Назначение сертификата** содержит разное количество идентификаторов (OID), которые попадут в поле сертификата **Улучшенный ключ**.

5 Заполните личные данные.

6 В поле **Идентификация заявителя** выберите способ идентификации пользователя при получении сертификата. Например, чтобы получать лично, выберите **Личное присутствие**.

7 Нажмите **Создать запрос**.

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

9 Если контейнер ключей был сохранен не на ViPNet PKI Service (**Облачный**), в окне **ViPNet CSP — инициализация контейнера ключей:**
   - Укажите имя и место для сохранения контейнера ключей (см. глоссарий, стр. 55).
   - Задайте пароль для работы с контейнером ключей. Чтобы в дальнейшем не вводить пароль, установите флажок **Сохранить пароль**.

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

11 В окне сообщения об успешном создании файла запроса на сертификат выполните одно из действий:
   - Перейдите в папку с запросом.
   - Создайте еще один запрос.
   - Закройте окно.

12 Передайте запрос в УЦ и получите личный сертификат, сертификаты издателей и соответствующие CRL.

После получения сертификатов установите их в хранилище или на ПАК ViPNet PKI Service (см. Установка сертификатов и CRL на стр. 27).

Подготовка файла шаблона в формате JSON

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

Файл шаблона в формате JSON должен иметь вид:

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

Где:

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

Подготовка файла шаблона в формате XML

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

Файл шаблона должен иметь вид:

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

Где:

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

Установка сертификатов и CRL

Описанными ниже способами устанавливайте только те личные сертификаты, запрос на которые был создан в ViPNet PKI Client (см. Получение сертификата на стр. 23). Если вы получали сертификат иным способом, см. Подготовка личного сертификата (на стр. 21).

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

Установка с помощью ViPNet PKI Client

1 Перейдите в настройки ViPNet PKI Client (на стр. 16).

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

---

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

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

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

- Нажмите  **Добавить сертификат или CRL**, укажите путь к файлам сертификатов и (или) CRL.

3 В окне **Добавление сертификатов** отображается список устанавливаемых сертификатов и CRL. В этом списке:

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

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

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

При необходимости вы можете:

- Посмотреть подробную информацию об устанавливаемых сертификатах и CRL, для этого щелкните имя владельца сертификата или CRL.
- Удалить сертификат или CRL из списка, для этого щелкните значок (появляется при наведении курсора на строку сертификата или CRL).

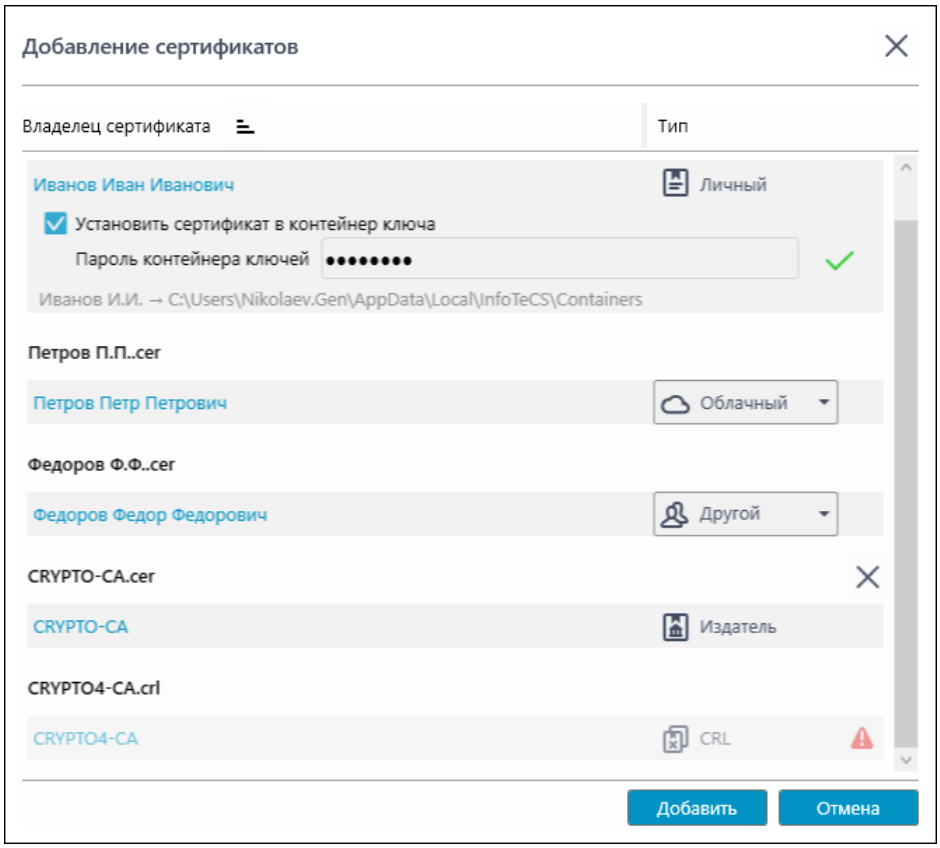

Рисунок 6. Установка сертификатов и CRL в ViPNet PKI Client

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

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

Результат установки отмечается значком напротив каждого установленного сертификата и CRL:

- — установка выполнена успешно;

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

Примечание. Если после установки сертификата в строке имени владельца сертификата появится предупреждающее сообщение, наведите курсор на значок , просмотрите подробные сведения об ошибках и устраните их (см. Проверка сертификатов на стр. 30).

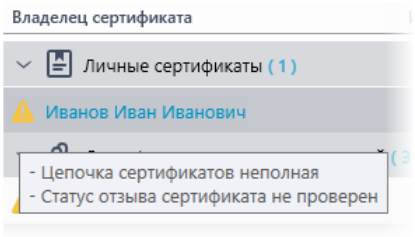

Рисунок 7. Просмотр предупреждающих сообщений

Установка с помощью контекстного меню Windows

Установка с помощью контекстного меню Windows

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

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

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

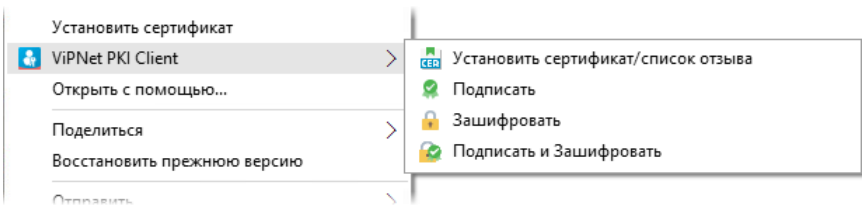

Рисунок 8. Установка сертификатов и CRL с помощью контекстного меню Windows

Проверка сертификатов

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

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

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

Вы можете выполнить проверку установленных сертификатов вручную. Для этого:

1 Перейдите в настройки ViPNet PKI Client (на стр. 16).

2 Выберите раздел  **Сертификаты**.

3 На панели инструментов нажмите  .

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

- **Цепочка сертификации неполная**

  В хранилище установлены не все сертификаты, образующие цепочку.

  Установите в хранилище недостающие сертификаты, чтобы образовалась полная цепочка (см. Установка сертификатов и CRL на стр. 27).

- **Сертификат отозван**

  Сертификат или один из сертификатов, образующих цепочку, аннулирован.

  Получите новый сертификат (см. Получение сертификата на стр. 23) и установите его в хранилище (см. Установка сертификатов и CRL на стр. 27).

- **Сертификат в цепочке содержит недействительную ЭП**

  Сертификат или один из сертификатов, образующих цепочку, искажен.

  Переустановите все сертификаты, образующие цепочку.

- **Срок действия ключа ЭП истек**

  Истек срок действия ключа ЭП.

  Выполните одно из действий:

  - Если вы устанавливаете личный сертификат, получите новый сертификат (см. Получение сертификата на стр. 23) и установите его в хранилище (см. Установка сертификатов и CRL на стр. 27).

- Если вы устанавливаете сертификат получателя, запросите у получателя новый сертификат.

- **Статус отзыва сертификата не проверен**

  Возможные причины:

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

  Установите актуальный CRL в хранилище (на стр. 27).

4

Защита файлов с помощью подписи и шифрования

Порядок подписания файла

	Действие и ссылка
1	Убедитесь, что у вас есть сертификат и соответствующий ключ ЭП (на стр. 21).
2	Если ваш сертификат установлен в хранилище сертификатов, проверьте, что в хранилище также установлены сертификаты издателей и соответствующие CRL (на стр. 27).
3	Настройте параметры ЭП (на стр. 33).
4	Подпишите файл (на стр. 35).
5	Передайте подписанный файл получателям любым удобным способом.

Настройка параметров ЭП

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

1 Перейдите в настройки ViPNet PKI Client (на стр. 16).

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

3 Выберите сертификат и нажмите **Выбрать**.

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

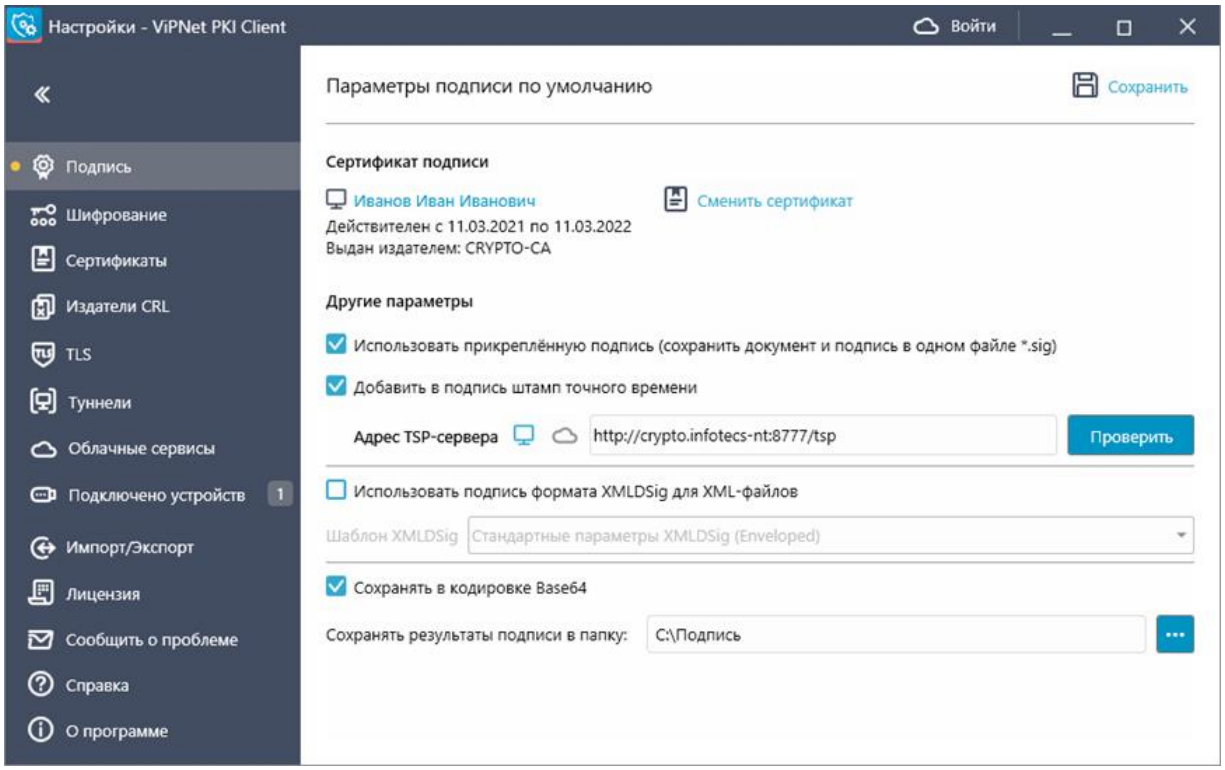

Рисунок 9. Настройка параметров ЭП

4 Чтобы сохранять подпись отдельно от подписываемого файла (см. глоссарий, стр. 55), снимите флажок **Использовать прикрепленную подпись (сохранить документ и подпись в одном файле *.sig)**. По умолчанию подпись прикрепляется к подписываемому файлу.

5 Чтобы использовать подпись формата XMLDSig (см. глоссарий, стр. 54) для XML-файлов, установите соответствующий флажок и выберите шаблон. По умолчанию в настройки добавлен шаблон с параметрами:

- Подписывается весь XML-документ, подпись помещается в корневой тег.
- Алгоритм каноникализации — `http://www.w3.org/TR/2001/REC-xml-c14n-20010315`.
- Алгоритм трансформации — `http://www.w3.org/2000/09/xmldsig#enveloped-signature`.

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

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

7 Чтобы добавлять к ЭП точное время подписания файла, настройте подключение к службе штампов времени (см. глоссарий, стр. 56):

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

7.2 Если вы не настраивали подключение к облачному сервису ЭП, в строке **Адрес TSP-сервера** укажите URL TSP-сервера (см. глоссарий, стр. 54) в формате `http://<IP-адрес или доменное имя>:<порт>/`. Поддерживаются протоколы HTTP и HTTPS. Для проверки соединения с указанным TSP-сервером нажмите **Проверить**.

7.3 Если вы настроили подключение к облачному сервису ЭП:

- Чтобы задать TSP-сервер вручную, в строке **Адрес TSP-сервера** щелкните значок  и укажите URL TSP-сервера (см. глоссарий, стр. 54) в формате `http://<IP-адрес или доменное имя>:<порт>/`. Поддерживаются протоколы HTTP и HTTPS. Для проверки соединения с указанным TSP-сервером нажмите **Проверить**.

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

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

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

8 Нажмите  и укажите папку для сохранения подписанных файлов.

9 Нажмите  **Сохранить**.

Подписание файла

Примечание. Вы можете подписывать файлы, используя контекстное меню Windows (см. Работа через контекстное меню Windows на стр. 18).

1 В главном окне File Unit выполните одно из действий:

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

Примечание. Чтобы открыть файл, который вы хотите подписать, щелкните его имя в разделе **Выбранные файлы**.

2 Справа выберите **Подписать сертификатом**.

Станут доступны настройки параметров ЭП.

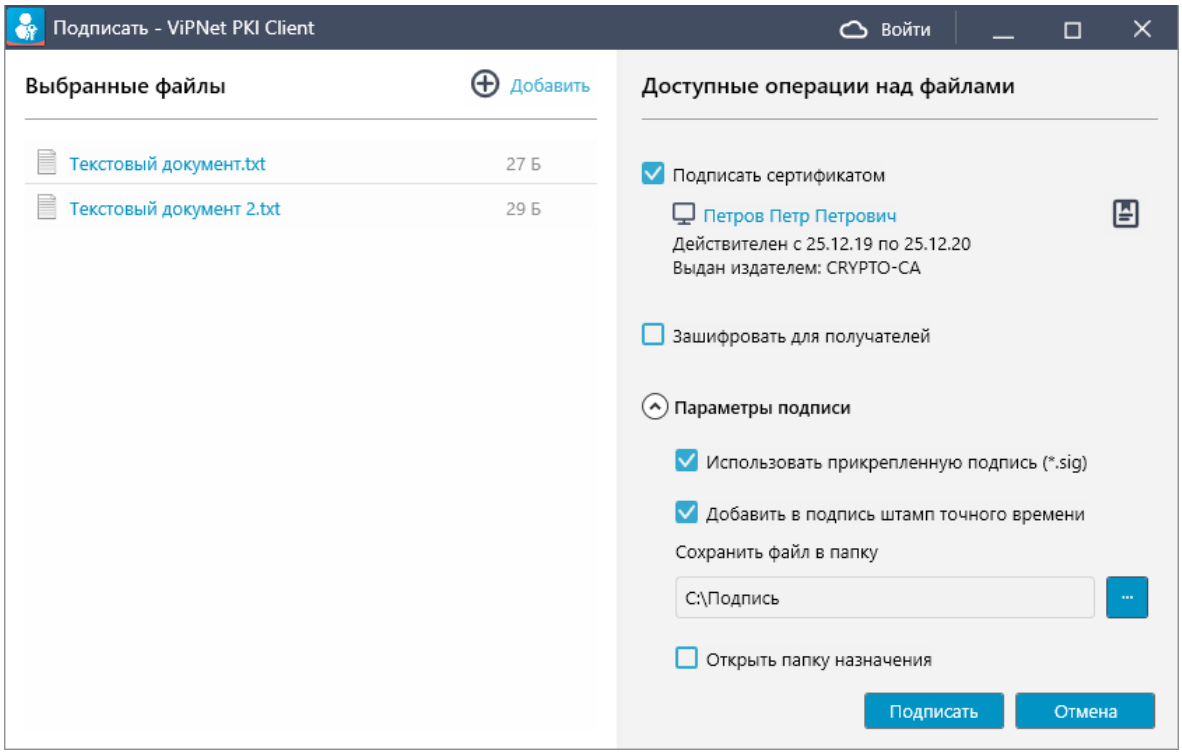

Рисунок 10. Подписание файла

Примечание. Штамп времени можно добавить только при подписании файлов размером не более 100 МБайт.

3 Если необходимо, измените параметры ЭП и нажмите **Подписать**.

4 В зависимости от места хранения вашего контейнера ключей, введите:

- Пароль контейнера ключей — папка на диске.
- ПИН внешнего устройства — внешнее устройство.
- Логин и пароль учетной записи пользователя — ПАК ViPNet PKI Service.

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

Количество неудачных попыток ввода пароля суммируется для всех файлов. То есть, если при попытке подписать 10 и более файлов вы ввели неверный пароль, указанные программы также будут заблокированы. При вводе верного пароля счетчик неудачных попыток обнуляется.

В результате будут сформированы и помещены в выбранную папку файлы:

- `<имя файла>.sig`, если вы использовали прикрепленную подпись;
- `<имя файла>.detached.sig`, если вы использовали открепленную подпись.

5 Чтобы открыть папку с файлом подписи (файл `*.sig`) или с исходным файлом, в главном окне программы в области истории операций с файлами щелкните имя файла и в контекстном меню выберите соответствующий пункт.

Порядок зашифрования файлов

	Действие и ссылка
1	Настройте параметры шифрования (на стр. 37).
2	Зашифруйте файл (на стр. 38).
3	Передайте файл получателям любым удобным способом.

Настройка параметров шифрования

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

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

2 Установите полученные сертификаты в хранилище (см. Установка сертификатов и CRL на стр. 27).

3 Перейдите в настройки ViPNet PKI Client (на стр. 16).

4 Выберите раздел **Шифрование**.

5 Чтобы каждый раз при шифровании файлов не приходилось выбирать сертификат получателя, сформируйте список получателей файлов:

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

5.2 Выберите один или несколько сертификатов и нажмите **Выбрать**.

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

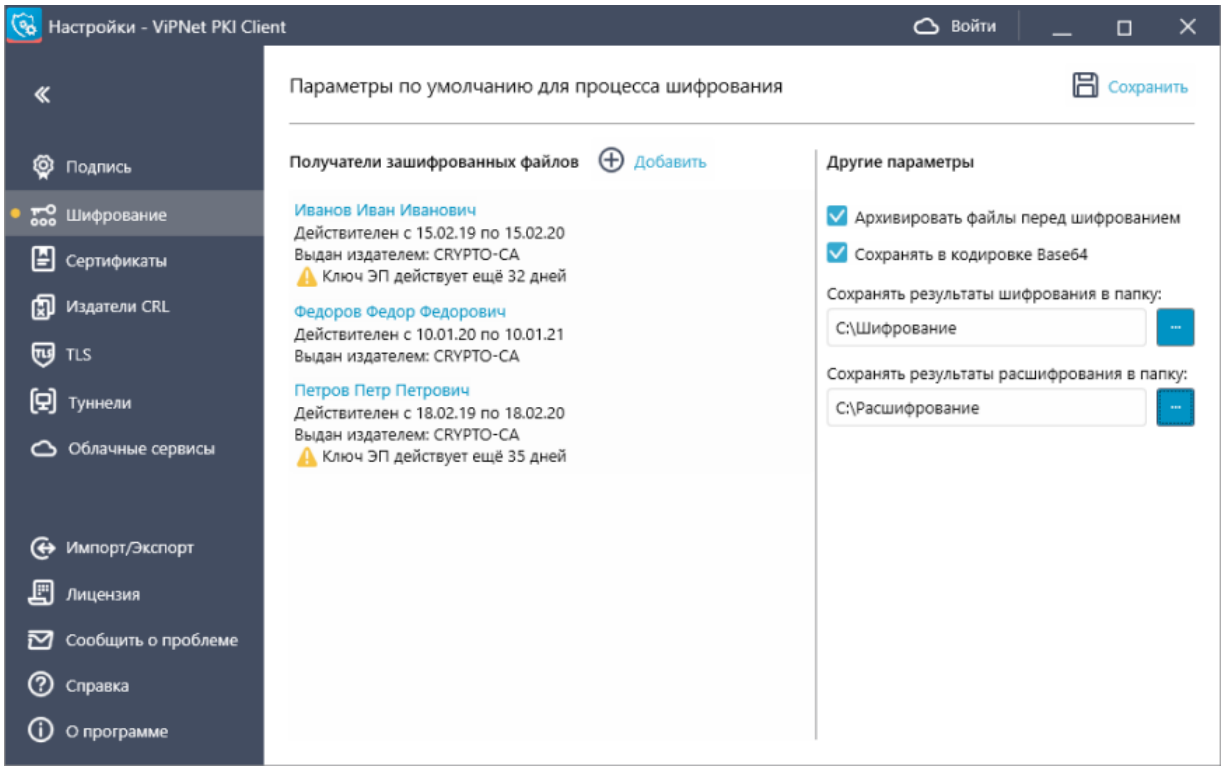

Рисунок 11. Настройка параметров шифрования

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

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

8 Нажмите ... и укажите папки для сохранения зашифрованных и расшифрованных файлов.

9 Нажмите **Сохранить**.

Зашифрование файла

Примечание. Вы можете зашифровывать файлы, используя контекстное меню Windows (см. Работа через контекстное меню Windows на стр. 18).

1 В главном окне File Unit выполните одно из действий:

- Нажмите **Выбрать файлы**. В открывшемся окне выберите один или несколько файлов и нажмите кнопку **Открыть**.
- Перетащите файлы в главное окно программы.

Примечание. Чтобы открыть файл, который вы хотите зашифровать, щелкните его имя в разделе **Выбранные файлы**.

2 В разделе **Доступные операции над файлами** выберите **Зашифровать для получателей**.

Станут доступны настройки параметров шифрования.

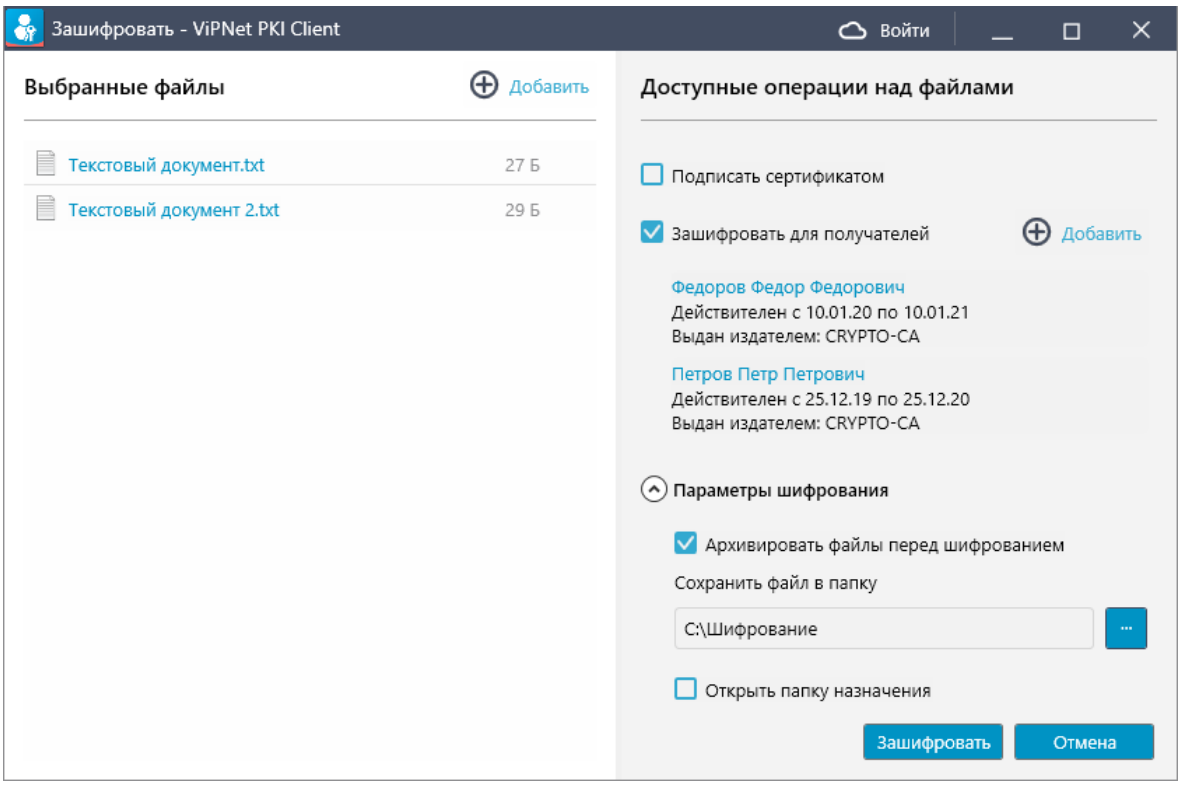

Рисунок 12. Зашифрование файла

3 Если необходимо, измените параметры шифрования и нажмите **Зашифровать**.

В результате зашифрованные файлы `*.enc` будут сформированы и помещены в выбранную папку.

4 Чтобы открыть папку с зашифрованным или исходным файлом, в области истории операций с файлами щелкните имя файла и в контекстном меню выберите соответствующий пункт.

Подписание и зашифрование файла

Примечание. Вы можете подписывать и зашифровывать файлы, используя контекстное меню Windows (см. Работа через контекстное меню Windows на стр. 18).

1 В главном окне File Unit выполните одно из действий:

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

Примечание. Чтобы открыть файл, который вы хотите подписать и зашифровать, щелкните его имя в разделе **Выбранные файлы**.

2 Справа выберите **Подписать сертификатом** и **Зашифровать для получателей**.

Станут доступны настройки параметров ЭП и шифрования.

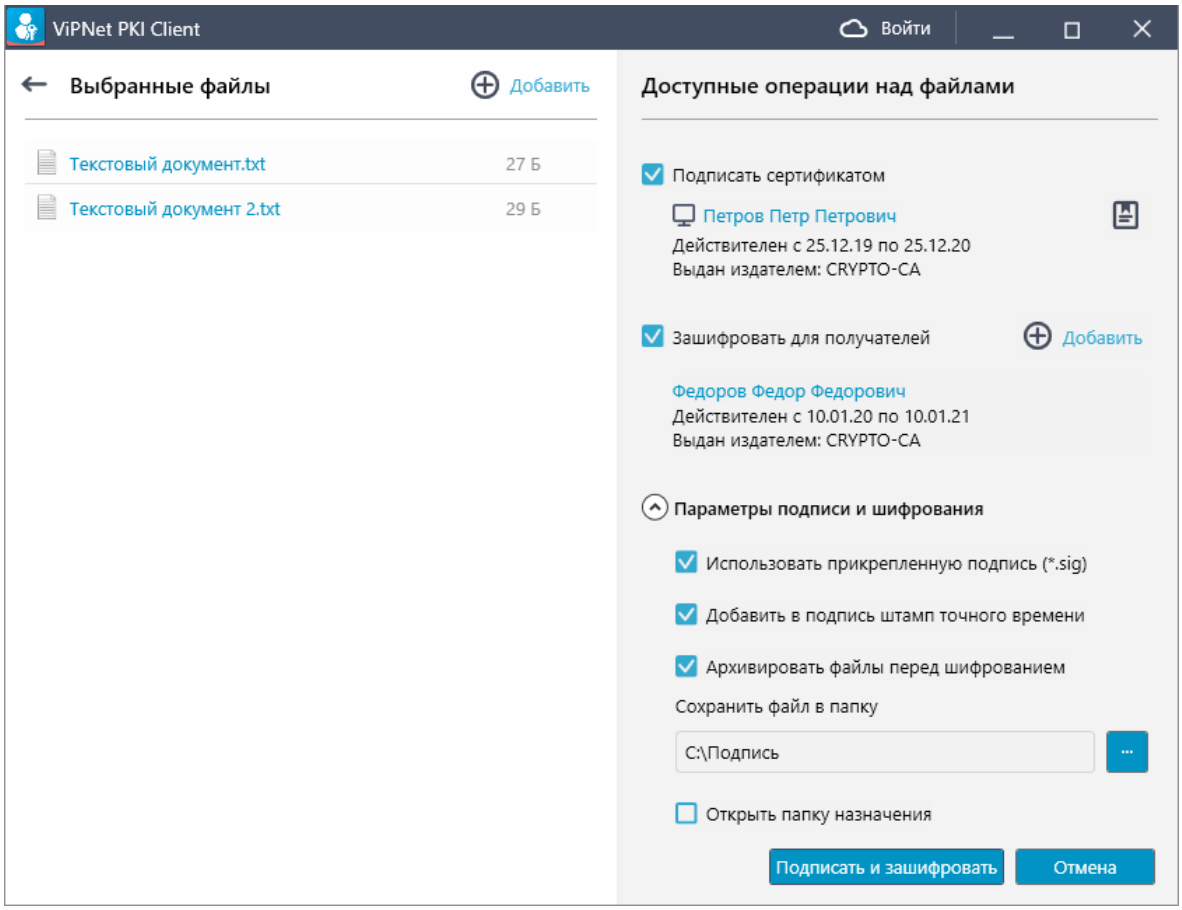

Рисунок 13. Одновременное подписание и шифрование файла

Примечание. Штамп времени можно добавить только при подписании файлов размером не более 100 МБайт.

---

3 Если необходимо, измените параметры ЭП и шифрования и нажмите **Подписать и зашифровать**.

4 В зависимости от места хранения вашего контейнера ключей, введите:

- Пароль контейнера ключей — папка на диске.
- ПИН внешнего устройства — внешнее устройство.
- Логин и пароль учетной записи пользователя — ПАК ViPNet PKI Service.

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

Количество неудачных попыток ввода пароля суммируется для всех файлов. То есть, если при попытке подписать и зашифровать 10 и более файлов вы ввели неверный пароль, указанные программы также будут заблокированы. При вводе верного пароля счетчик неудачных попыток обнуляется.

В результате будут сформированы и помещены в выбранную папку файлы:

- <имя файла>.sig.enc, если вы использовали прикрепленную подпись без архивирования перед зашифрованием.
- <ГГГГММДДччмм>.zip.enc, если вы использовали прикрепленную подпись с архивированием перед зашифрованием. Подписанный файл будет содержаться в архиве <ГГГГММДДччмм>.zip.
- <имя файла>.detached.sig и файл ЭП <имя файла>.enc, если вы использовали открепленную подпись без архивирования перед зашифрованием.
- <ГГГГММДДччмм>.zip.enc, если вы использовали открепленную подпись с архивированием файлов перед шифрованием. Файл ЭП и исходный файл будут содержаться в архиве <ГГГГММДДччмм>.zip.

5 Чтобы открыть папку с зашифрованным или исходным файлом, в области истории операций с файлами щелкните имя файла и в контекстном меню выберите соответствующий пункт.

5

Работа с файлами, полученными от других пользователей

Получение зашифрованных и подписанных файлов

При получении файлов `*.sig` и `*.enc` от других пользователей с помощью File Unit вы можете просмотреть их и удостоверить личности отправителей.

Чтобы прочитать файл, по расширению файла определите, какие операции были применены к нему перед отправкой: подписание, зашифрование или обе операции. От этого зависит операция, с помощью которой вы сможете прочитать файл:

- Если файл зашифрован (имеет вид `<имя файла>.enc`) — расшифруйте его (на стр. 45).
- Если файл подписан (имеет вид `<имя_файла>.sig`) — проверьте ЭП (см. Проверка ЭП файла на стр. 47).
- Если файл подписан и зашифрован, то есть имеет вид `<имя файла>.sig.enc`, то расшифруйте его (на стр. 45), а затем проверьте ЭП (см. Проверка ЭП файла на стр. 47).

Расшифрование файла

Примечание. Вы можете расшифровывать файлы с помощью контекстного меню Windows (см. Работа через контекстное меню Windows на стр. 18).

1 В главном окне File Unit выполните одно из действий:

- Нажмите **Выбрать файлы**. Выберите один или несколько файлов с расширением `*.enc`.
- Перетащите файлы с расширением `*.enc` в главное окно программы.

2 Щелкните имя файла в разделе **Выбранные файлы**.

3 Если файл зашифрован с помощью нескольких ваших личных сертификатов, в группе **Расшифровать используя сертификат** с помощью кнопки выберите сертификат для расшифрования.

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

Примечание. Если в хранилище сертификатов не найден сертификат для расшифрования и настроено подключение к ПАК ViPNet PKI Service (установлен флажок **Предлагать расшифрование в облаке**), щелкните ссылку **Расшифровать**. ViPNet PKI Client расшифрует файл на ПАК ViPNet PKI Service, если на нем установлен подходящий сертификат.

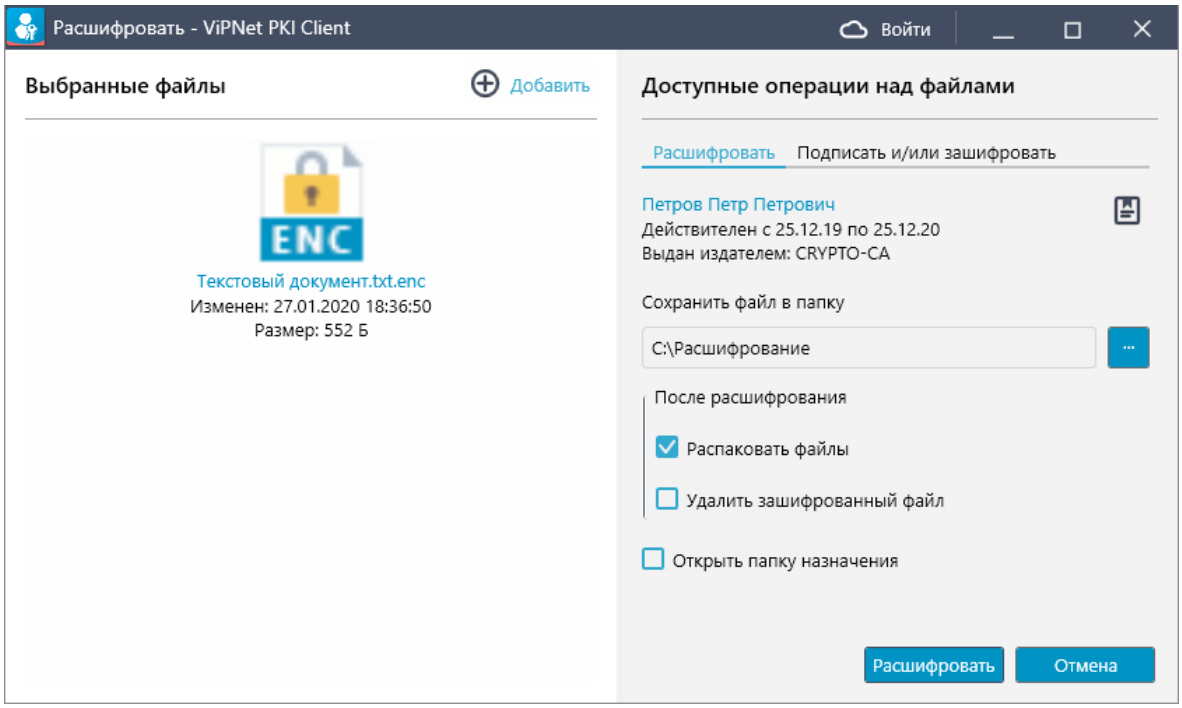

Рисунок 14. Расшифрование файла

5 В окне ввода пароля, в зависимости от места хранения вашего контейнера ключей, введите:

- Пароль контейнера ключей — папка на диске.
- ПИН внешнего устройства — внешнее устройство.
- Логин и пароль учетной записи пользователя — ПАК ViPNet PKI Service, если не подключились ранее.

  Если подключение к ПАК ViPNet PKI Service осуществляется по сертификату, а сертификат и ключ ЭП хранятся на внешнем устройстве, введите ПИН-код внешнего устройства.

Внимание! После десяти неудачных попыток ввода пароля программы File Unit, Web Unit и настройки ViPNet PKI Client блокируются на 15 минут. Количество неудачных попыток ввода пароля считается суммарно для всех файлов. То есть, если при попытке расшифровать 10 и более файлов вы ввели неверный пароль, указанные программы также будут заблокированы. При вводе верного пароля счетчик неудачных попыток обнуляется.

---

6 Выполните шаги 2-5 для остальных зашифрованных файлов.

7 Чтобы открыть папку с расшифрованным или исходным файлом, в области истории операций с файлами щелкните имя файла и в контекстном меню выберите соответствующий пункт.

Проверка ЭП файла

Примечание. Вы можете проверять ЭП, используя контекстное меню Windows (см. Работа через контекстное меню Windows на стр. 18).

1 В главном окне File Unit выполните одно из действий:

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

2 В зависимости от количества выбранных файлов и типа ЭП:

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

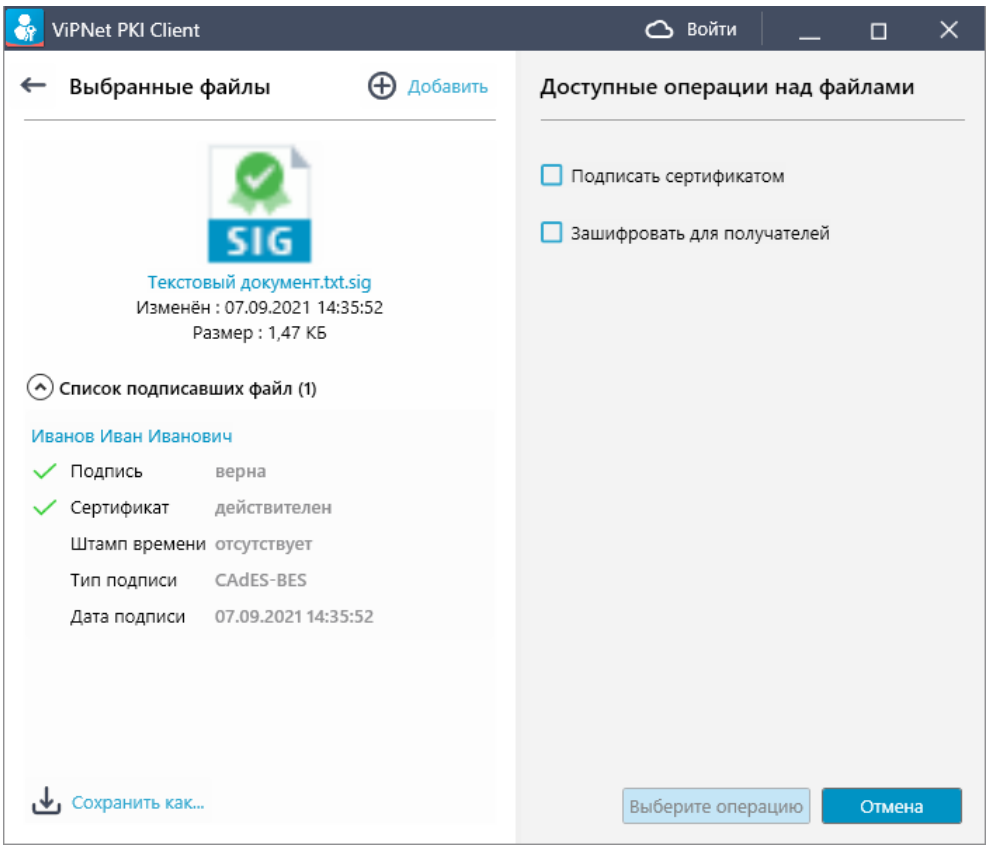

Рисунок 15. Проверка прикрепленной ЭП

- Если вы выбрали один файл с открепленной ЭП (то есть исходный файл не был помещен совместно с ЭП в файл `*.sig`), укажите исходный файл с помощью соответствующей кнопки или перетащите его в выделенную область. Если исходный файл и файл подписи расположены в одной папке, проверка ЭП произойдет автоматически.

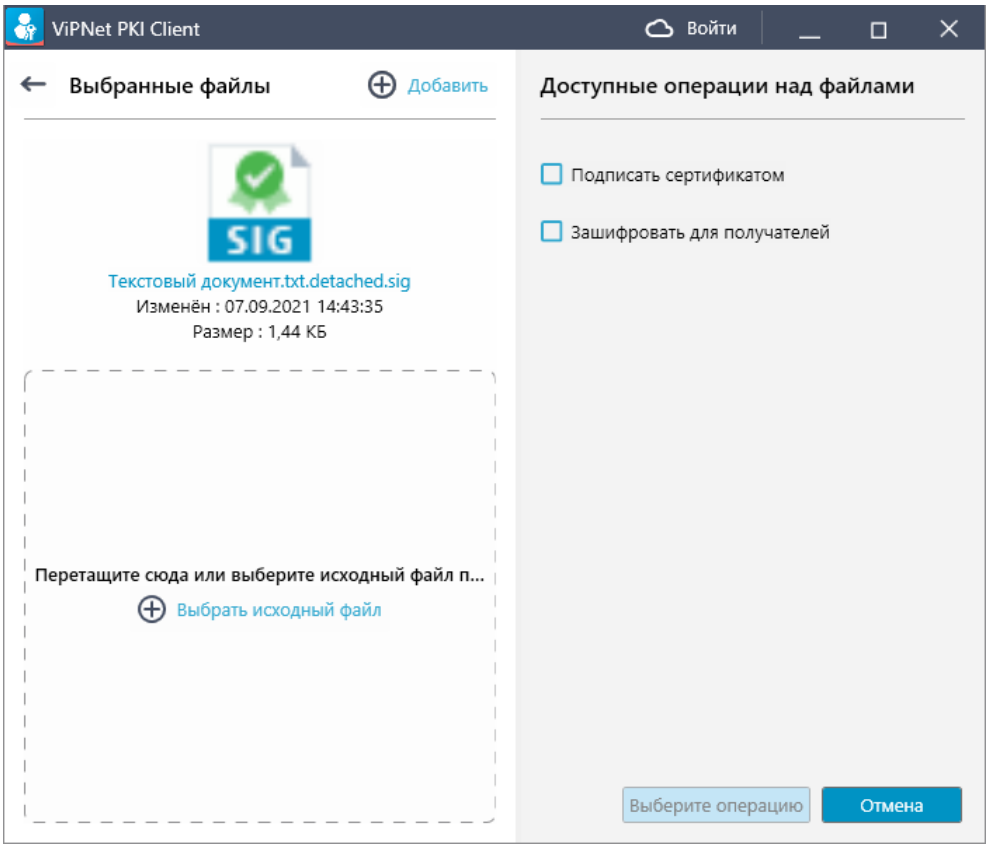

Рисунок 16. Проверка открепленной ЭП

- Если вы выбрали несколько файлов, то для проверки ЭП щелкните значок напротив имени файла:
  - Если при подписании использовалась прикрепленная ЭП, результат проверки подписи будет отображен в отдельном окне.
  - Если при подписании использовалась открепленная ЭП, в открывшемся окне укажите исходный файл и нажмите **Открыть**. Если исходный файл и файл подписи расположены в одной папке, проверка ЭП произойдет автоматически. Результат проверки подписи также будет отображен в отдельном окне.

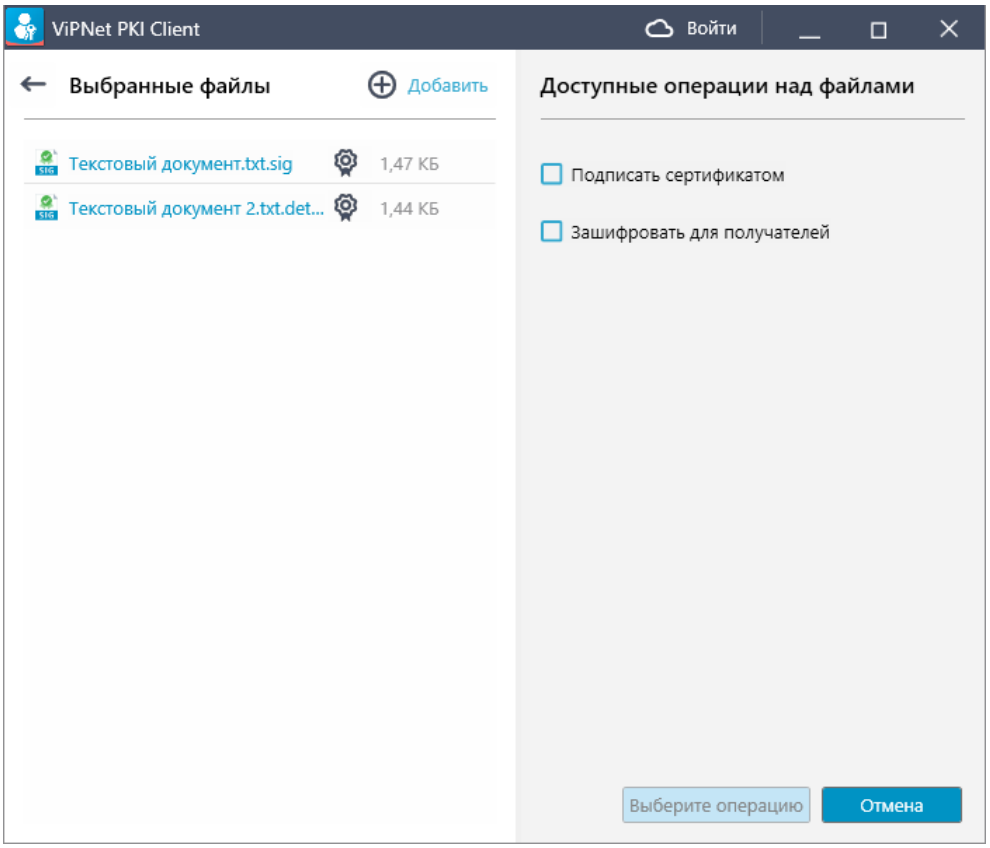

Рисунок 17. Проверка ЭП нескольких файлов

3 В окне с результатами проверки подписи:

- Щелкните имя владельца подписи, чтобы просмотреть информацию о его сертификате.
- Если к подписи был добавлен штамп времени, щелкните ссылку **присутствует**, чтобы просмотреть информацию о нем.
- Сохраните исходный файл.
- Если при проверке подписи не удалось проверить сертификат подписанта с помощью сертификатов, установленных в хранилище сертификатов Windows (например, истек CRL издателя), и настроено подключение к ПАК ViPNet PKI Service (установлен флажок **Предлагать проверять ЭП в облаке**), нажмите **Проверить**. ViPNet PKI Client проверит подпись на ПАК ViPNet PKI Service.

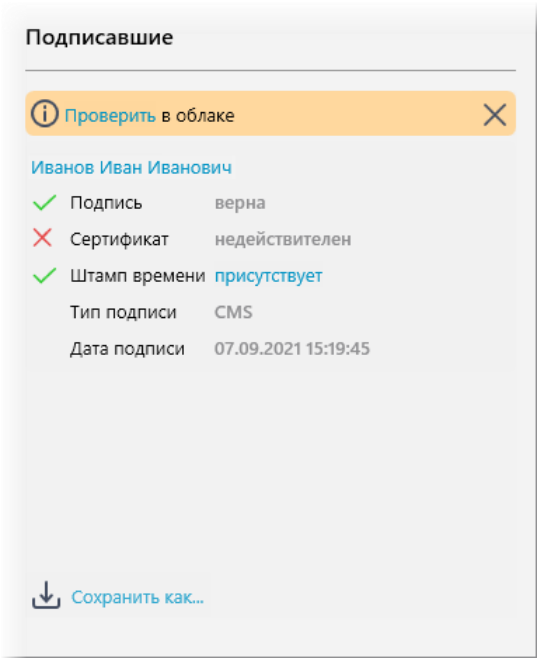

Рисунок 18. Результаты проверки подписи

6

Возможные неполадки и способы их устранения

Требуемый сертификат не отображается в списке сертификатов для подписания

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

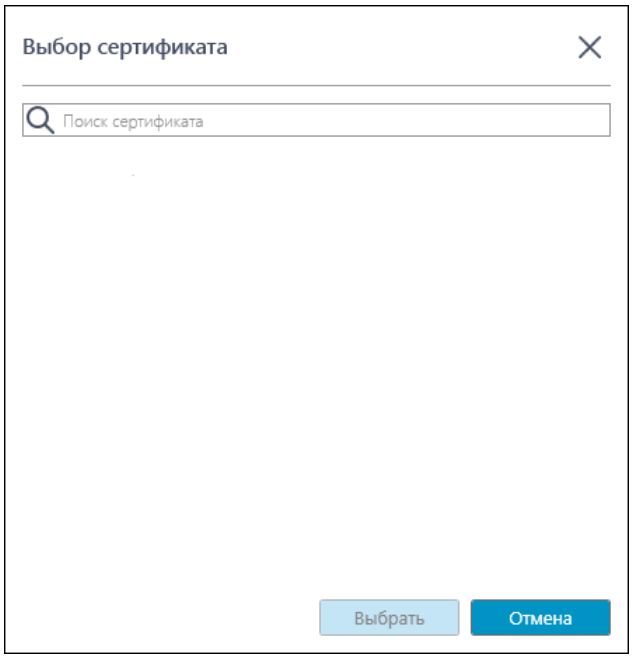

Рисунок 19. Сертификат не отображается в списке сертификатов для подписи

Проверьте, что сертификат соответствует требованиям (см. Требования к сертификатам для подписи и шифрования на стр. 11).

Ошибка при расшифровании

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

Чтобы узнать в каком ПО был создан ключ ЭП:

1. Перейдите в настройки ViPNet PKI Client (на стр. 16).
2. В разделе  **Сертификаты** откройте сертификат.
3. На вкладке **Состав** найдите поле **Средство электронной подписи владельца**.

A

Глоссарий

TSP-сервер (служба штампов времени)

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

XMLDSig

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

Асимметричное подписание

Система подписания, при которой алгоритмы используют два математически связанных ключа. Закрытый ключ используется для подписи файла, а с помощью открытого ключа и сертификата пользователя подпись подтверждается.

Асимметричное шифрование

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

Ключ проверки электронной подписи (ключ проверки ЭП)

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

Ключ электронной подписи (ключ ЭП)

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

Контейнер ключей

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

Открепленная подпись

Тип электронной подписи, при использовании которой электронная подпись и служебная информация помещаются в файл с расширением `*.sig` отдельно от исходного файла.

Например, при подписании `file.txt` открепленная электронная подпись помещается в контейнер `file.txt.detached.sig`. Далее для проверки электронной подписи требуется не только данный контейнер, но и исходный файл, который в контейнер `file.txt.detached.sig` не входит.

Прикрепленная подпись

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

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

Сертификат издателя

Сертификат удостоверяющего центра, которым заверяются издаваемые сертификаты.

Сертификат ключа проверки электронной подписи

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

Список аннулированных сертификатов (CRL)

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

Удостоверяющий центр

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

Файл *.enc

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

Файл *.sig

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

Штамп времени

Реквизит электронного документа, которым служба штампов времени удостоверяет, что в указанный момент времени ей было предоставлено значение хэш-функции данного документа. Штамп времени подтверждает точное время создания документа. Также может подтверждать время получения или отправления документа.

В штампе времени указывается следующее: значение хэш-функции документа, на который выдан штамп; идентификатор политики (OID), в соответствии с которой был выдан штамп; время выдачи штампа; точность времени и другие параметры.

Электронная подпись (ЭП)

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