



# ViPNet PKI Client

Общие сведения



© АО «ИнфоТеКС», 2022

ФРКЕ.00175-02 90 01

Версия продукта 1.7.0

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

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

VipNet® является зарегистрированным товарным знаком АО «ИнфоТеКС».

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

АО «ИнфоТеКС»

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

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

Сайт: [infotecs.ru](http://infotecs.ru)

Служба поддержки: [hotline@infotecs.ru](mailto:hotline@infotecs.ru)

# Содержание

<b>Введение</b> .....	<b>5</b>
О документе.....	5
Соглашения документа.....	5
О программе.....	6
Комплект поставки.....	6
Системные требования.....	6
Что нового в версии 1.7.0.....	7
Обратная связь.....	8
<b>Назначение и состав</b> .....	<b>9</b>
Назначение.....	9
Инфраструктура открытых ключей.....	10
Компоненты.....	11
Лицензирование.....	13
<b>Сценарии использования</b> .....	<b>14</b>
Получение сертификата.....	14
Получение и установка CRL.....	15
Подписание документа.....	16
Зашифрование файла.....	17
Использование ЭП в веб-приложениях.....	18
Подключение к веб-ресурсу по TLS.....	19
Подключение к туннелируемым ресурсам.....	20
<b>Начало работы</b> .....	<b>21</b>
Установка, обновление.....	21
Запуск и завершение работы.....	22
Активация лицензии.....	23
Обновление лицензии.....	24
<b>История версий</b> .....	<b>26</b>
Новые возможности версии 1.6.0.....	26
Новые возможности версии 1.5.1.....	26
Новые возможности версии 1.4.0.....	27
Новые возможности версии 1.3.1.....	28

Новые возможности версии 1.3.....	30
Новые возможности версии 1.2.....	31
Новые возможности версии 1.1.....	34
<b>Внешние устройства.....</b>	<b>35</b>
Общие сведения .....	35
Список поддерживаемых внешних устройств .....	35
Список поддерживаемых внешних устройств для подключения к сайтам, использующим TLS ГОСТ, и туннелируемым ресурсам .....	38
Алгоритмы и функции, поддерживаемые внешними устройствами.....	39
<b>Глоссарий.....</b>	<b>41</b>




# Введение

## О документе

Документ описывает назначение и состав программного комплекса ViPNet® PKI Client (далее — ViPNet PKI Client), сценарии его использования и начало работы с ним.

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

## Соглашения документа

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

# О программе

## Комплект поставки

- Установочный файл `pki_client_installer.exe`.
- Документация в формате PDF:
  - ViPNet PKI Client. Общие сведения.
  - ViPNet PKI Client. Руководство администратора.
  - ViPNet PKI Client File Unit. Руководство пользователя.
  - ViPNet CSP. Руководство пользователя.
  - ViPNet PKI Client. Руководство разработчика.

## Системные требования

- Процессор — Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более.
- Объем оперативной памяти — не менее 2 Гбайт.
- Свободное место на жестком диске — не менее 1 Гбайт.
- Операционная система с последними пакетами обновлений:
  - Windows 7 — 32/64-разрядная;
  - Windows Server 2012 — 64-разрядная;
  - Windows 8.1 — 32/64-разрядная;
  - Windows Server 2012 R2 — 64-разрядная;
  - Windows Server 2016 — 64-разрядная;
  - Windows Server 2019 — 64-разрядная;
  - Windows 10 — 32/64-разрядная следующих версий и сборок:
    - версия 1803, сборка 17134;
    - версия 1809, сборка 17763;
    - версия 1903, сборка 18362;
    - версия 1909, сборка 18363;
    - версия 2004, сборка 19041;
    - версия 20H2, сборка 19042;
  - Windows 11 — 64-разрядная версии 21H2, сборка 22000.

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

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

## Что нового в версии 1.7.0

- **Поддержка Windows 11 (версия 21H2, сборка 22000)**
- **Изменения в лицензировании TLS Unit**

Теперь возможности установления TLS-соединений с односторонней аутентификацией и двухсторонней аутентификацией с помощью TLS Unit лицензируются отдельно.

Лицензии с TLS Unit, приобретенные до выхода версии 1.7.0, будут по-прежнему разрешать TLS-соединения с односторонней аутентификацией и двухсторонней аутентификацией. Обновлять их не требуется.

- **Поддержка подключения к веб-ресурсам по протоколу TLS версии 1.3**
- **Выбор параметров ключа проверки ЭП при создании запроса на сертификат**

Теперь при создании запроса на сертификат вы можете выбрать параметры ключа проверки ЭП, рекомендованные техническим комитетом ТК 26 или компанией КриптоПро.

- **Совместимость с КриптоПро CSP**

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

Изменения в предыдущих версиях см. в приложении [История версий](#) (на стр. 26).

# 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](mailto:hotline@infotecs.ru).  
[Форма для обращения в службу поддержки через сайт.](#)  
Канал поддержки в Telegram: [t.me/vhd21](https://t.me/vhd21)  
Телефон для клиентов с расширенной поддержкой: +7 (495) 737-6196.
- Отдел продаж: [soft@infotecs.ru](mailto:soft@infotecs.ru).

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



# Назначение и состав

## Назначение

ViPNet PKI Client позволяет организовать взаимодействие с [PKI](#) (см. глоссарий, стр. 41) и защиту передаваемых данных с помощью шифрования и [электронной подписи](#) (см. глоссарий, стр. 43).

С помощью ViPNet PKI Client вы можете:

- Создать [запрос на сертификат](#) (см. глоссарий, стр. 41) и получить в [удостоверяющем центре](#) (см. глоссарий, стр. 42) сертификат, чтобы использовать его для защищенного обмена данными.
- Подтверждать свою личность и проверять личность других пользователей, от которых вы получаете файлы, с использованием электронной подписи (далее — ЭП) в соответствии с федеральным законом № 63-ФЗ «Об электронной подписи».
- Защищать файлы, которые вы отправляете другим пользователям, с помощью шифрования.
- Автоматически получать актуальные [списки аннулированных сертификатов \(CRL\)](#) (см. глоссарий, стр. 42) из [точек распространения](#) (см. глоссарий, стр. 42).
- Работать с облачным сервисом ЭП на базе ПАК ViPNet PKI Service.
- Подключаться к сайтам, использующим TLS ГОСТ.
- Устанавливать защищенные TLS-соединения с односторонней и двусторонней аутентификацией по алгоритмам ГОСТ с туннелируемыми ViPNet TLS Gateway ресурсами, использующими протоколы RDP, HTTP, SMTP, POP3, IMAP, WebDAV и SQL.

ViPNet PKI Client предоставляет дополнительные возможности администраторам и разработчикам информационных систем:

- Настройка на рабочих местах пользователей ViPNet PKI Client автоматического получения CRL из точек распространения.
- Разработка веб-приложений с поддержкой криптографических операций, которые смогут выполнять пользователи ViPNet PKI Client.

ViPNet PKI Client использует российские алгоритмы:

- Алгоритмы формирования и проверки ЭП ГОСТ Р 34.10-2001 с вычислением хэш-функции по ГОСТ Р 34.11-94 (только для проверки ЭП и расшифрования) и ГОСТ Р 34.10-2012 с вычислением хэш-функции по ГОСТ Р 34.11-2012.
- Алгоритм шифрования файлов ГОСТ 28147-89.
- Алгоритмы шифрования для TLS-соединений: ГОСТ 28147-89, ГОСТ Р 34.12-2015 «Магма» или «Кузнечик».

# Инфраструктура открытых ключей

При обмене данными между пользователями вне или внутри информационной системы бывает необходимо защитить данные от несанкционированного доступа или искажения.

Распространенный способ защиты электронных документов — использование асимметричных алгоритмов шифрования и ЭП. При этом каждый участник документооборота имеет пару связанных между собой ключей:

- [ключ ЭП](#) (см. глоссарий, стр. 41), который каждый участник документооборота хранит в секрете;
- [ключ проверки ЭП](#) (см. глоссарий, стр. 41), который свободно распространяется среди участников документооборота.

Пара ключей используется так:

- Отправитель зашифровывает документ с помощью ключа проверки ЭП получателя. Расшифровать этот документ может только получатель с помощью своего ключа ЭП.
- Отправитель заверяет документ ЭП с помощью своего ключа ЭП. Получатели могут убедиться, что документ действительно подписан отправителем и не искажен, с помощью ключа проверки ЭП отправителя.

Чтобы использовать асимметричные ключи для шифрования и ЭП, пользователям нужна возможность проверять, кому принадлежит тот или иной ключ проверки ЭП (то есть между пользователями необходимо установить доверие). Для этого должна быть организована [инфраструктура открытых ключей \(PKI\)](#) (см. глоссарий, стр. 41).

Основной элемент PKI — удостоверяющий центр (далее — УЦ), который издает по запросам пользователей [сертификаты ключей проверки ЭП](#) (см. глоссарий, стр. 42). Каждый сертификат имеет срок действия и подтверждает, что его владельцу принадлежит ключ проверки ЭП и соответствующий ему ключ ЭП. Сертификат свободно распространяется среди участников документооборота.

Если по какой-либо причине доверие к сертификату утеряно (например, владелец сертификата потерял свой ключ ЭП, и он мог быть доступен посторонним лицам), УЦ аннулирует такой сертификат и вносит его в CRL. Актуальные CRL распространяются среди участников документооборота.

Таким образом, сертификат можно использовать для подписи и шифрования, если этот сертификат издан доверенным УЦ, срок действия сертификата не истек и сертификат отсутствует в CRL.

# Компоненты



## File Unit

С помощью File Unit вы можете:

- Проверять личность отправителя файла с помощью ЭП (см. [Подписание документа](#) на стр. 15).
- Защищать файлы путем шифрования и расшифровывать файлы, полученные от других пользователей (см. [Зашифрование файла](#) на стр. 16).

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



## Web Unit

С помощью Web Unit вы можете в веб-приложениях, совместимых с ViPNet PKI Client (см. [Использование ЭП в веб-приложениях](#) на стр. 17), выполнять следующее:

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



## SDK

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

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

На компьютерах пользователей веб-приложения потребуется установить Web Unit.

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



## CRL Unit

Служба CRL Unit обеспечивает автоматическое получение CRL из точек распространения и установку полученных CRL в хранилище (см. [Получение и установка CRL](#) на стр. 14).

Создает и управляет точками распространения CRL администратор корпоративной сети.



## Certificate Unit

С помощью Certificate Unit вы можете:

- Создавать запросы на сертификаты и сохранять их в файлы.
- Устанавливать сертификаты и CRL в хранилище.
- Экспортировать сертификаты.

- Просматривать установленные сертификаты.



### TLS Unit

С помощью TLS Unit вы можете установить между клиентом и веб-ресурсом защищенное TLS-соединение, поддерживающее российские алгоритмы ГОСТ 28147–89, ГОСТ Р 34.10-2012, ГОСТ Р 34.12-2015 «Магма» или «Кузнечик» (см. [Подключение к веб-ресурсу по TLS](#) на стр. 18).



### Tunnel Unit

С помощью Tunnel Unit вы можете устанавливать защищенные TLS-соединения с односторонней и двусторонней аутентификацией по алгоритмам ГОСТ с туннелируемыми ViPNet TLS Gateway ресурсами (см. [Подключение к туннелируемым ресурсам](#) на стр. 19).



### Cloud Unit

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

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



### ViPNet CSP

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

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

# Лицензирование

ViPNet PKI Client защищается от нелегального использования лицензией. Вы можете приобрести лицензию в [ИнфоТеКС](#) (на стр. 7).

Лицензия содержит:

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



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

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

---

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

Файл лицензии требуется указать при установке ViPNet PKI Client (см. [Установка, обновление](#) на стр. 21).

# Сценарии использования

## Получение сертификата

1 В ViPNet PKI Client создайте запрос на сертификат.

При создании запроса на сертификат формируются:

- ключ ЭП — помещается в **контейнер ключей** (см. глоссарий, стр. 41) на диске компьютера или внешнем устройстве;
- ключ проверки ЭП — помещается в файл запроса на сертификат.

2 Передайте созданный запрос в УЦ доверенным способом.

3 Администратор УЦ издаст по запросу сертификат.

4 Получите в УЦ свой сертификат, корневой сертификат издателя и CRL.

5 Установите полученные сертификаты и CRL в хранилище.

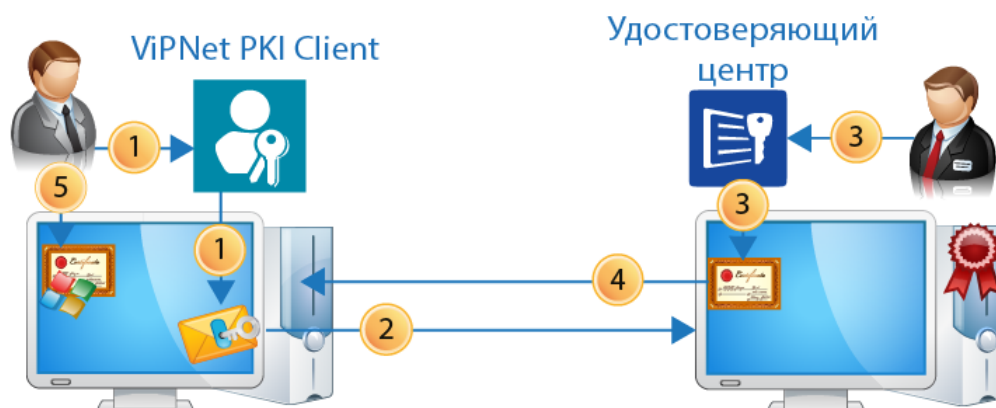


Рисунок 1. Передача запроса и получение сертификата

# Получение и установка CRL

- 1 В ViPNet PKI Client укажите URL точек распространения CRL и расписание их опроса.
- 2 ViPNet PKI Client будет по расписанию опрашивать указанные точки на предмет новых CRL.
- 3 При обнаружении новых CRL ViPNet PKI Client загрузит их на ваш компьютер.
- 4 ViPNet PKI Client установит загруженные CRL в хранилище.



Рисунок 2. Обновление CRL

# Подписание документа

Допустим, вам нужно отправить руководителю отчет в электронном виде, и по правилам вашей компании отчет должен быть заверен ЭП. Чтобы подписать отчет с помощью ViPNet PKI Client:

- 1 Убедитесь, что у вас есть сертификат и соответствующий ему ключ ЭП.

Если у вас нет сертификата, обратитесь в УЦ вашей компании (см. [Получение сертификата](#) на стр. 14).

- 2 В File Unit используйте функцию подписания: выберите файл отчета и сертификат, с помощью которого вы хотите его подписать. В результате File Unit создаст файл \*.sig, который в зависимости от выбранного типа подписи будет содержать исходный файл отчета и ЭП или только ЭП.



Рисунок 3. Подписание документа с помощью File Unit

- 3 Отправьте файл \*.sig руководителю (например, по электронной почте). Если при подписании вы использовали открепленную подпись, вместе с файлом \*.sig отправьте исходный файл отчета.
- 4 Руководитель с помощью File Unit и вашего сертификата проверит ЭП полученного отчета.



# Зашифрование файла

Допустим, вам нужно отправить по электронной почте документ, содержащий конфиденциальную информацию. Чтобы защитить документ от посторонних лиц, зашифруйте его с помощью ViPNet PKI Client:

- 1 Попросите получателя документа прислать вам его сертификат (например, по электронной почте).
- 2 Если издатели сертификата получателя и сертификата, который вы будете использовать для зашифрования, отличаются, запросите в УЦ получателя сертификат издателя и CRL и установите их в хранилище.
- 3 В File Unit используйте функцию шифрования: выберите файл документа для зашифрования и сертификат получателя. В результате File Unit создаст файл \*.enc, содержащий данные исходного документа в зашифрованном виде.

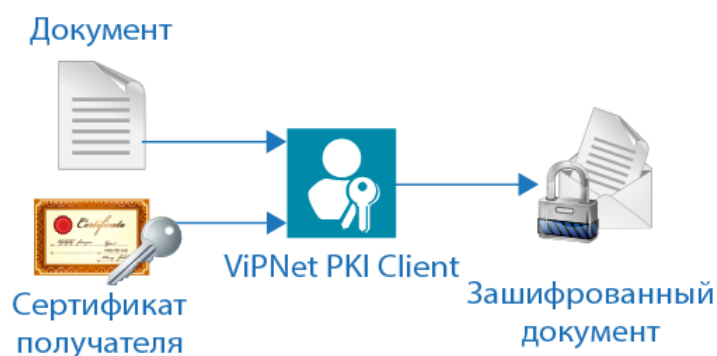


Рисунок 4. Шифрование документа с помощью File Unit

- 4 Отправьте файл \*.enc получателю (например, по электронной почте).
- 5 Получатель расшифрует полученный файл с помощью своего ключа ЭП.

# Использование ЭП в веб-приложениях

При получении некоторых электронных услуг (например, на портале государственных услуг или в интернет-банке) для защиты данных может требоваться использование ЭП или других криптографических функций.

Если веб-приложение, которое вы используете, совместимо с ViPNet PKI Client, для работы с ним используйте Web Unit:



**Примечание.** В некоторых веб-приложениях предусмотрена возможность скачивания и установки ViPNet PKI Client Web Unit.

- 1 В веб-приложении сформируйте заявление на получение услуги.
- 2 Если у вас еще нет сертификата, в Web Unit создайте запрос на сертификат.
- 3 Получите сертификат и установите его в хранилище.
- 4 Отправьте заявление. При этом потребуется подписать его ЭП, выбрав сертификат.
- 5 После подписания заявление будет отправлено.

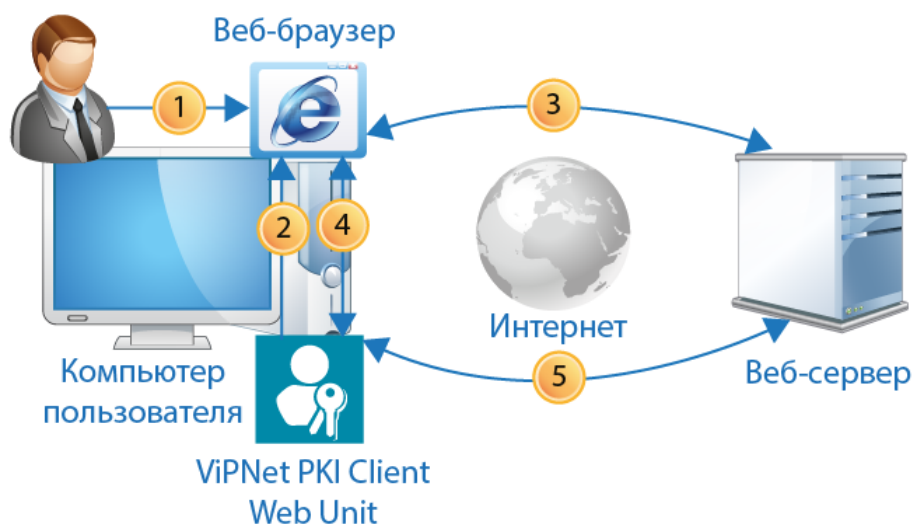


Рисунок 5. Использование ЭП в веб-приложениях

# Подключение к веб-ресурсу по TLS

Для подключения к некоторым веб-ресурсам (например, portalу государственных услуг или электронным торговым площадкам) требуется установить защищенное соединение по протоколу TLS, поддерживающему российские алгоритмы ГОСТ. По умолчанию браузеры не поддерживают алгоритмы ГОСТ для TLS-соединений. Чтобы решить эту проблему, используйте TLS Unit:

1 Пользователь с помощью браузера обращается к веб-ресурсу.

Если TLS Unit работает, он выполняет функцию локального прокси-сервера, все соединения с веб-ресурсами проходят через него и в соответствии с его настройками. Если TLS Unit выключен, для работы прокси-сервера используются настройки по умолчанию.

2 Веб-ресурс и TLS Unit согласовывают параметры соединения: протоколы, алгоритмы шифрования данных.

3 Если для установления TLS-соединения не требуется поддержка алгоритмов ГОСТ или требуется установить соединение не по протоколу TLS, используются стандартные средства браузера.

4 Если для установления TLS-соединения требуется поддержка алгоритмов ГОСТ Р 34.10-2012, ГОСТ 28147-89, ГОСТ Р 34.12-2015 «Магма» или «Кузнечик», используется TLS Unit:

4.1 TLS Unit проверяет цепочку сертификатов сервера.

4.2 Если для доступа к веб-ресурсу требуется аутентификация пользователя, TLS Unit предлагает пользователю выбрать сертификат из списка доступных.

После успешной проверки сертификатов устанавливается соединение.

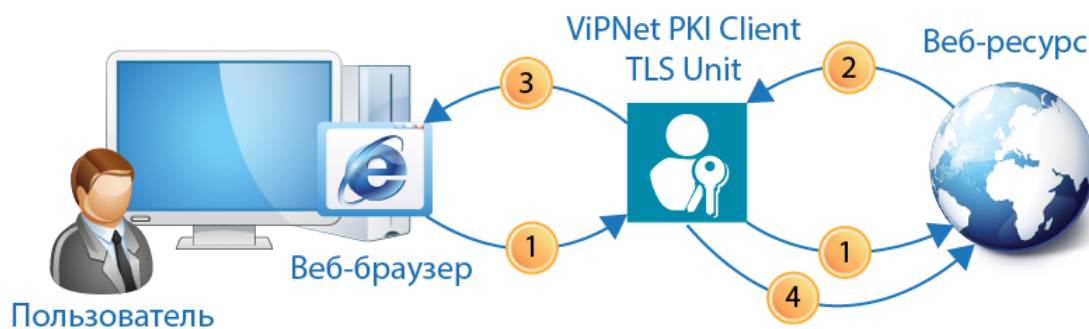


Рисунок 6. Установка TLS-соединения

# Подключение к туннелируемым ресурсам

При предоставлении удаленного доступа к корпоративным ресурсам (например, рабочему месту, файловому или почтовому серверу) может возникнуть необходимость в защищенном соединении между клиентом и сервером при передаче данных через Интернет. Если в вашей корпоративной сети для разграничения доступа к ресурсам используется ViPNet TLS Gateway версии не ниже 1.3, вы можете настроить туннелирование ресурсов, использующих протоколы RDP, HTTP, SMTP, POP3, IMAP, WebDAV и протоколы взаимодействия с базами данных (например, MSSQL, PostgreSQL, MySQL).

Tunnel Unit позволяет устанавливать TLS-соединения с односторонней и двусторонней аутентификацией по алгоритмам ГОСТ с этими ресурсами. Благодаря этому вы сможете получить защищенный доступ к нужным ресурсам и работать с ними.



Рисунок 7. Установка соединения с туннелируемыми ресурсами

Для установления TLS-соединения с туннелируемыми ресурсами должно быть выполнено следующее:

- На ПАК ViPNet TLS Gateway добавлены и настроены туннелируемые ресурсы.
- На компьютере пользователя установлены сертификаты УЦ из цепочки доверия транспортных сертификатов ViPNet TLS Gateway.

Подробнее см. «ViPNet TLS Gateway. Руководство администратора».

Соединение устанавливается следующим образом:

- В ViPNet PKI Client пользователь добавляет туннелируемый ресурс.
- С помощью соответствующего приложения пользователь подключается к туннелируемому ресурсу.

# Начало работы

## Установка, обновление

### Особенности установки, обновления

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



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

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

---

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

### Установка, обновление в обычном режиме

- 1 Запустите установочный файл и следуйте указаниям мастера.
- 2 Если на компьютере нет доступа в Интернет, активируйте лицензию (см. [Активация лицензии](#) на стр. 23).

## Установка, обновление с использованием командной строки

Таблица 1. Параметры установки

Параметр	Описание
/install	Установка в обычном режиме (см. выше)
/install /quiet	Тихий режим установки (без участия пользователя и демонстрации интерфейса)
-license=	Указание файла лицензии (обязательный параметр)
/ignore_os_check	Параметр, разрешающий установку ViPNet CSP, входящего в состав ViPNet PKI Client, на компьютер с операционной системой версии, которая не проверялась на совместимость



**Внимание!** Без параметра /ignore\_os\_check ViPNet PKI Client невозможно установить на компьютер с Windows 10 или Windows 11 версии, которая не проверялась на совместимость (см. [Системные требования](#) на стр. 6). Работа ViPNet PKI Client на этих версиях Windows не гарантируется.

Пример команды:

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

## Запуск и завершение работы

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

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

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

Для завершения работы компонентов ViPNet PKI Client:



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

# Активация лицензии

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

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

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

- 1 Перейдите в настройки ViPNet PKI Client (на стр. 22).
- 2 В разделе  Лицензия нажмите  Сохранить запрос на активацию.

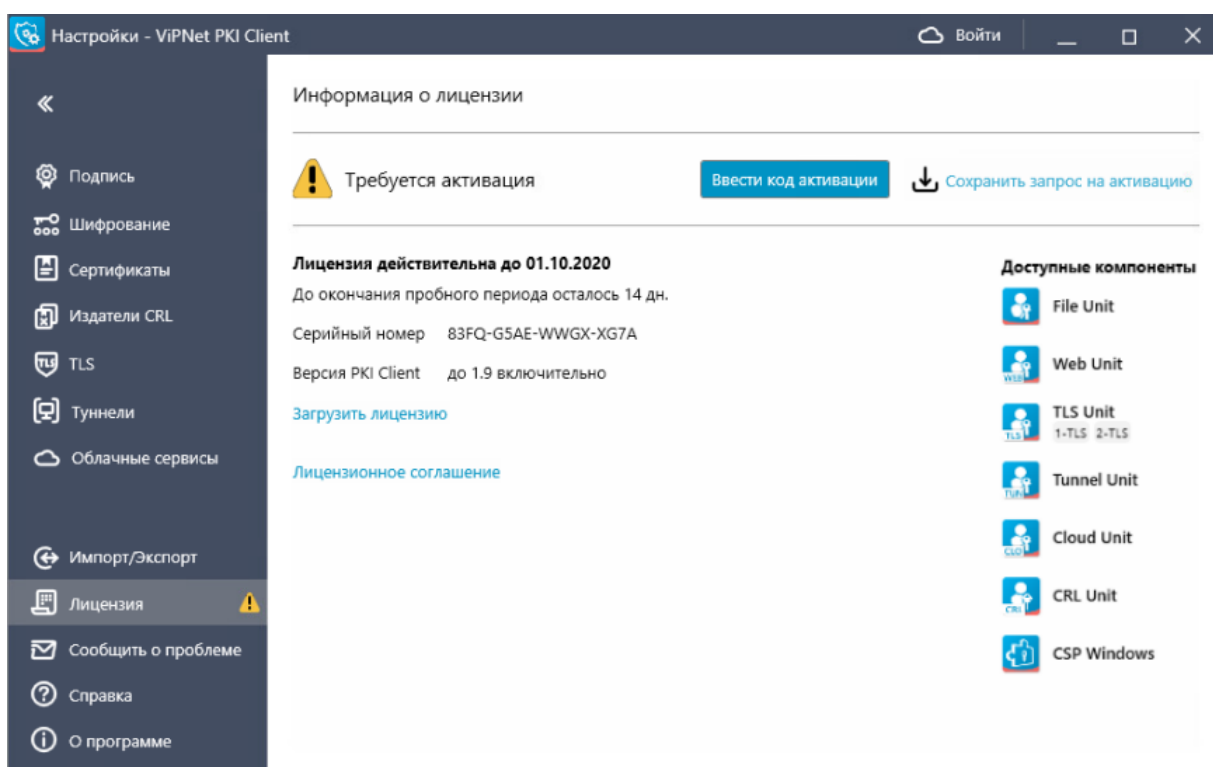
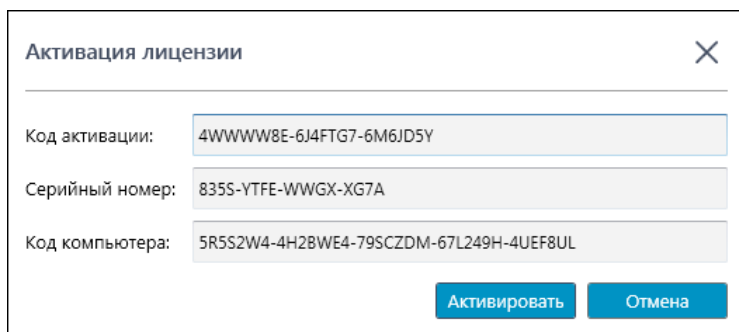


Рисунок 8. Просмотр информации о лицензии

- 3 Выполните одно из действий:
  - Если у вас установлен почтовый клиент, нажмите `Reg@infotecs.ru`. Откроется окно почтового клиента с уже сформированным письмом. Перетащите файл запроса в окно с письмом и отправьте его в ИнфоТеКС.
  - Если у вас не установлен почтовый клиент, сохраните файл запроса и создайте письмо вручную. Укажите адрес получателя письма `Reg@infotecs.ru` и прикрепите к письму файл запроса. Тема и оформление письма могут быть любыми.
- 4 Дождитесь получения ответного письма, в котором будут указаны данные для активации.

- 5 Нажмите **Ввести код активации**.
- 6 В поле **Код активации** введите полученный регистрационный код и нажмите **Активировать**.



Активация лицензии

Код активации: 4WWW8E-6J4FTG7-6M6JD5Y

Серийный номер: 8355-YTFE-WWGX-XG7A


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

Активировать Отмена

Рисунок 9. Ввод данных для активации ViPNet PKI Client


- 7 Нажмите **ОК**.

Чтобы убедиться, что лицензия активирована:

- 1 Перейдите в настройки ViPNet PKI Client (на стр. 22) и выберите раздел  **Лицензия**.
- 2 Проверьте, что на странице информации о лицензии нет надписи **Требуется активация**.

## Обновление лицензии

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

- 1 Отправьте запрос на получение лицензии через [веб-форму на сайте ИнфоТекС](#) и получите новый файл лицензии.
- 2 Перейдите в настройки ViPNet PKI Client (на стр. 22).
- 3 В разделе  **Лицензия** выполните одно из действий:
  - Нажмите **Загрузить лицензию** и укажите путь к новому файлу лицензии.
  - Перетащите новый файл лицензии в окно настроек.
- 4 Ознакомьтесь с информацией о лицензии и нажмите **Загрузить**.



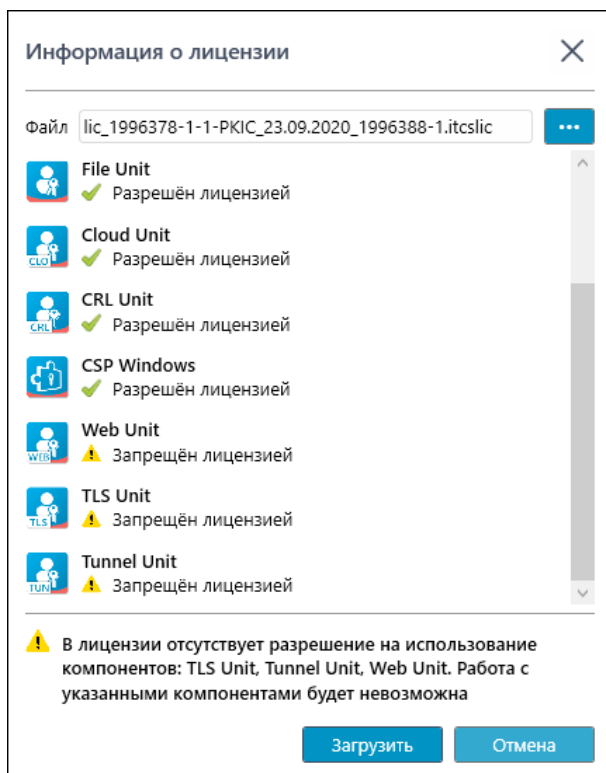


Рисунок 10. Информация о лицензии

# История версий

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

## Новые возможности версии 1.6.0

Обзор изменений в версии 1.6.0 по сравнению с 1.5.1.

- **Поддержка работы с новой версией ПАК ViPNet PKI Service**

Теперь вы можете подключаться к облачным сервисам на базе ПАК ViPNet PKI Service 2.0. Поддержка работы с ПАК ViPNet PKI Service 1.0.4 прекращена.

- **Поддержка внешних устройств для подключения к туннелируемым ресурсам**

Теперь для подключения к туннелируемым ресурсам с аутентификацией пользователя могут использоваться сертификаты и ключи ЭП, хранящиеся на внешних устройствах (см. [Список поддерживаемых внешних устройств для подключения к сайтам, использующим TLS ГОСТ, и туннелируемым ресурсам](#) на стр. 38).

- **Новое поле при создании запроса на сертификат — Идентификация заявителя**

В запросы на сертификаты добавлено поле **Идентификация заявителя**. Реализовано в соответствии с приказом ФСБ РФ 27.12.2011 №795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи».

- **Изменение поддержки сертификатов ГОСТ Р 34.10–2001**

Сертификаты ГОСТ Р 34.10–2001 больше нельзя использовать для подписания и зашифрования файлов, а также для подключения к сайтам, использующим TLS ГОСТ, и туннелируемым ресурсам. Теперь эти сертификаты можно использовать только для проверки ЭП и расшифрования файлов. Реализовано в соответствии с документом ФСБ России №149/7/1/3-58 от 31.01.2014 «О порядке перехода к использованию новых стандартов ЭЦП и функции хэширования».

- **Изменения в шаблонах XML-подписи**

- Добавлена поддержка подписи формата [WS-Security](#).
- Добавлена поддержка трансформации СМЭВ 3 (<urn://smev-gov-ru/xmlsig/transform>).

- **Смена ПИНа Infotecs Software Token**

Теперь вы можете сменить ПИН Infotecs Software Token.

## Новые возможности версии 1.5.1

Обзор изменений в версии 1.5.1 по сравнению с 1.4.0.

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

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

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

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

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

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

- **Добавлен английский язык**

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

## Новые возможности версии 1.4.0

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

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

Если в вашей организации для хранения сертификатов и ключей ЭП используется [ПАК ViPNet PKI Service](#) (см. глоссарий, стр. 42), вы можете подключиться к нему для выполнения криптографических операций из интерфейса ViPNet PKI Client.

- **Установка личного сертификата в контейнер ключей**

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

- **Работа с файлами в кодировке Base64**

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

- **Изменения в программе TLS Unit**

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

Раньше поддерживались только устройства Infotecs Software Token и Rutoken Lite. В новой версии для подключения вы можете использовать устройства семейств Rutoken, JaCarta и

ESMART Token с аппаратной поддержкой российских криптографических алгоритмов (см. [Список поддерживаемых внешних устройств для подключения к сайтам, использующим TLS ГОСТ, и туннелируемым ресурсам](#) на стр. 38).

- Добавлены новые алгоритмы шифрования.

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

- **Новая версия криптопровайдера ViPNet CSP**

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


## Новые возможности версии 1.3.1

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

- **Добавлена возможность экспорта и импорта настроек**

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

- **Изменения в программе Tunnel Unit**

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

- **Изменения в интерфейсе**
  - Раздел CRL переименован в **Издатели CRL**.
  - Добавлен раздел **Импорт/Экспорт**.

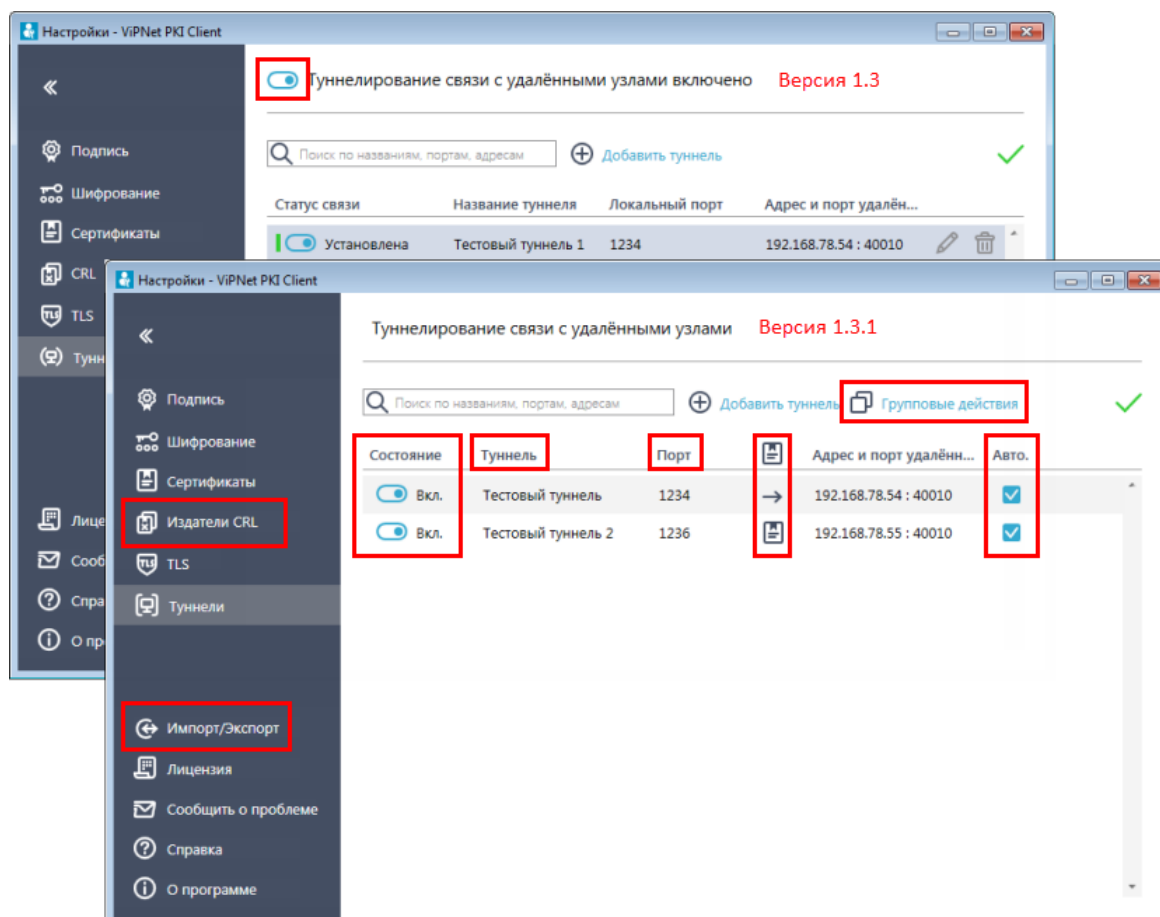


Рисунок 11. Изменения интерфейса в разделе Туннели

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

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

- **Изменен список поддерживаемых операционных систем**

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

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

## Новые возможности версии 1.3

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet PKI Client версии 1.3 по сравнению с версией 1.2. Информация об изменениях в предыдущих версиях приведена в приложении [История версий](#) (на стр. 26).

- **Добавлен новый компонент Tunnel Unit**

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

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

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

- **Обновлен интерфейс ViPNet PKI Client**

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

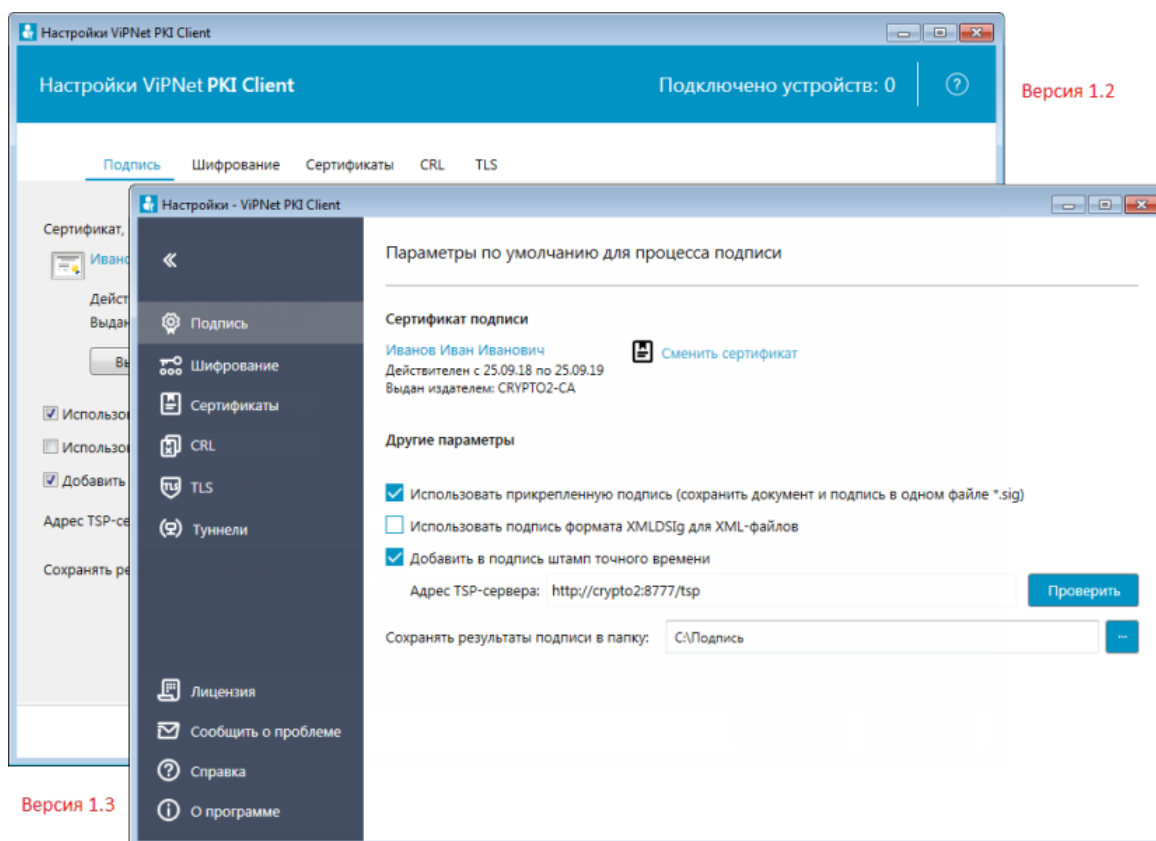



Рисунок 12. Интерфейс ViPNet PKI Client 1.3

- **Улучшена работа с сертификатами и CRL**

- Вы можете устанавливать несколько сертификатов и CRL одновременно.

- Вы можете устанавливать сертификаты и CRL, перетащив их в окно **Настройки - ViPNet PKI Client** в раздел  **Сертификаты**.
- **Изменения в программе File Unit**
  - Вы можете выполнять криптографические операции для нескольких файлов одновременно.
  - Вы можете добавлять файлы для выполнения криптографических операций, перетащив их в главное окно программы File Unit.

## Новые возможности версии 1.2

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

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

Добавлена возможность организации защищенного [TLS-соединения](#) (см. глоссарий, стр. 41) с использованием внешних устройств, поддерживающих хранение ключей, созданных по алгоритму ГОСТ Р 34.10-2012.

- **Изменения в интерфейсе**

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

- Вкладка **Менеджер сертификатов** заменена на вкладку **Сертификаты**.
- Добавлена вкладка **CRL**. Информация о сертификатах издателей и [точках распространения CRL](#) (см. глоссарий, стр. 42) теперь отображается здесь.
- Добавлена вкладка **TLS** для настройки TLS-соединений.

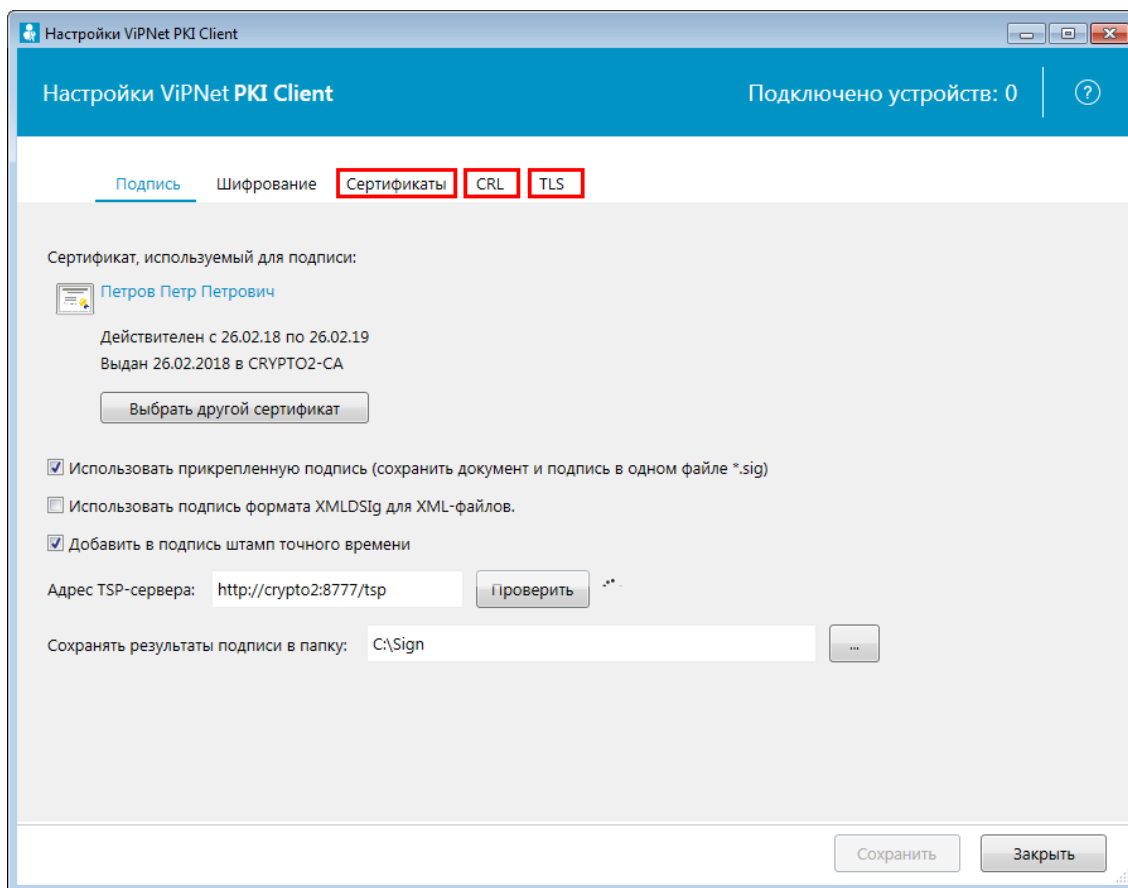


Рисунок 13. Изменения в интерфейсе окна с настройками ViPNet PKI Client

- **Работа с сертификатами и CRL**

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

В новой версии ViPNet PKI Client в работе с сертификатами и CRL произошли следующие изменения:

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



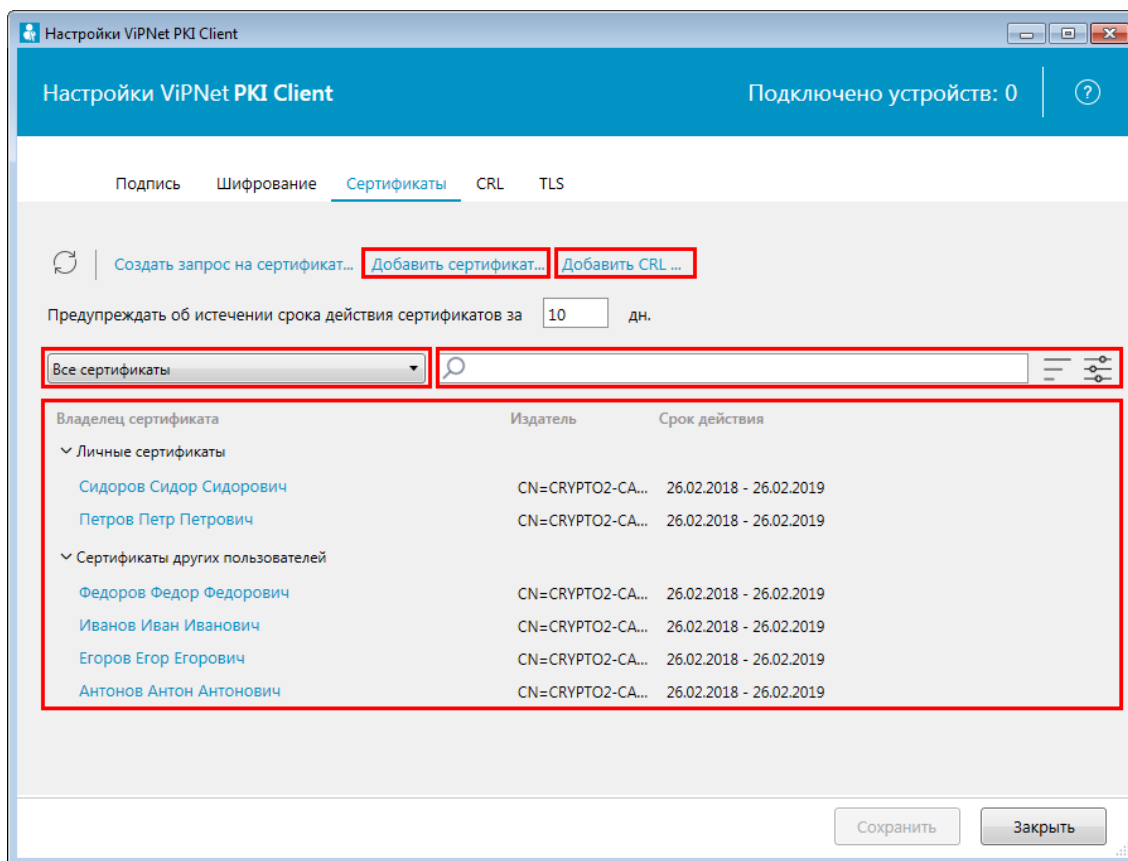


Рисунок 14. Изменения в работе с сертификатами и CRL

- **Настройка TLS-соединений**

В некоторых случаях может возникнуть необходимость подключения к веб-ресурсам, у которых либо истек срок действия сертификата, либо цепочка сертификации неполная, либо ее невозможно проверить. В новой версии вы можете устанавливать TLS-соединение с такими веб-ресурсами (подробнее см. документ «ViPNet PKI Client. Руководство администратора», главу «Настройка подключения к веб-ресурсу по протоколу TLS», раздел «Требования к сертификату сервера для установки TLS-соединения»).

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

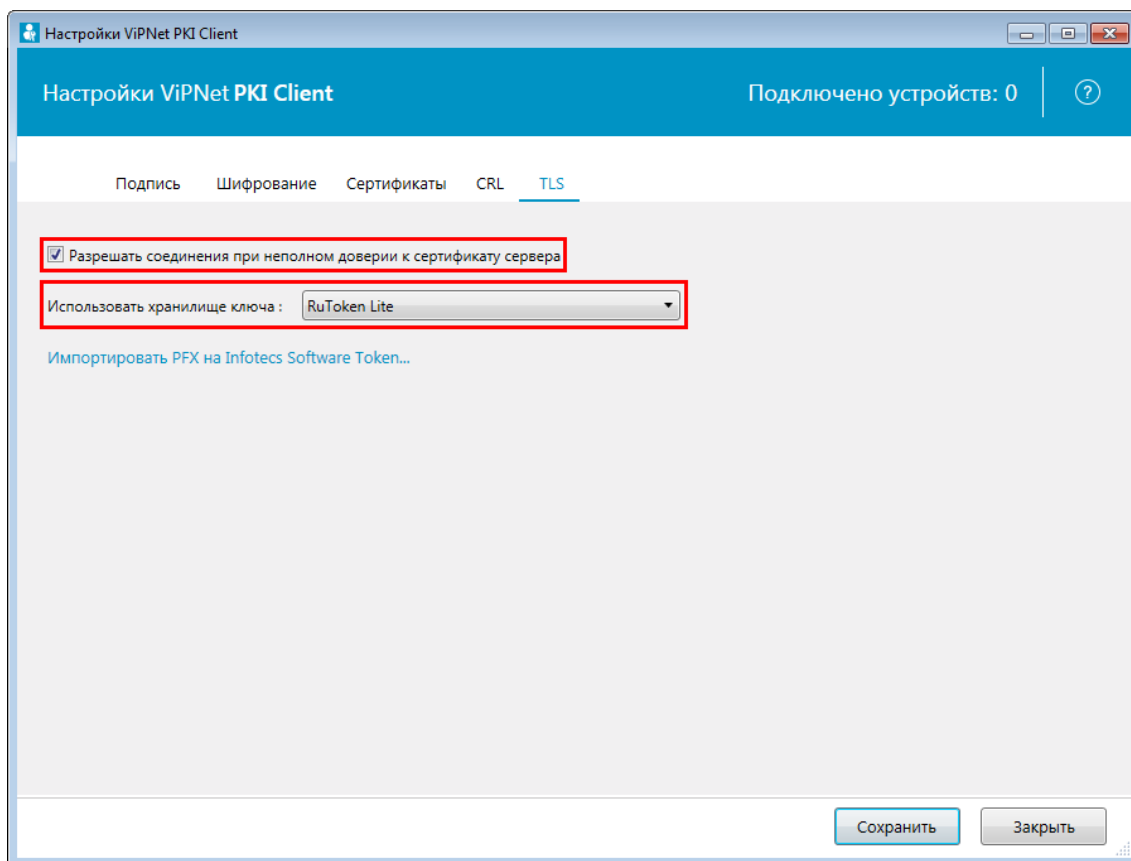


Рисунок 15. Настройка TLS-соединения

## Новые возможности версии 1.1

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

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

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

# Внешние устройства

## Общие сведения

Внешние устройства предназначены для хранения **контейнеров ключей** (см. глоссарий, стр. 41), которые вы можете использовать для аутентификации, формирования **электронной подписи** (см. глоссарий, стр. 43) или для других целей.

На внешнем устройстве могут храниться ключи, созданные по различным алгоритмам в программном обеспечении ViPNet или в сторонних программах. Максимальное количество контейнеров ключей, которое может храниться на одном внешнем устройстве, зависит от объема памяти устройства.

Все операции с контейнерами ключей и внешними устройствами вы можете выполнить в программе ViPNet CSP. Чтобы использовать какое-либо внешнее устройство, на компьютер необходимо установить драйверы этого устройства. Перед записью ключей на устройство убедитесь, что оно отформатировано.

## Список поддерживаемых внешних устройств

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

Таблица 2. Поддерживаемые внешние устройства

Название семейства устройств в ViPNet CSP	Полные названия и типы устройств	Необходимые и рекомендуемые условия работы с семейством устройств
ESMART Token	Смарт-карты и токены типов ESMART Token, ESMART Token ГОСТ	На компьютере должно быть установлено ПО ESMART PKI Client для Windows (рекомендуемая версия — 4.5 RC). Устройства типа ESMART Token необходимо отформатировать с помощью ПО ESMART PKI Client для Windows с профилем ViPNet2. Перенос ключей подписи с устройства и на устройство ESMART Token ГОСТ невозможен, так как на устройстве используется аппаратная криптография с неизвлекаемым ключом.

Название семейства устройств в ViPNet CSP	Полные названия и типы устройств	Необходимые и рекомендуемые условия работы с семейством устройств
Infotecs Software Token	ViPNet SoftToken — программная реализация стандарта PKCS#11	<p>Необходимо установить компонент ViPNet SoftToken (входит в состав ПО ViPNet OpenSSL). С помощью программы <code>token_manager.exe</code> на компьютере должен быть создан программный токен.</p> <p>Подробную информацию о работе с программным токеном см. в документе «ViPNet SoftToken. Руководство разработчика», раздел «Использование утилиты <code>token_manager</code> для работы с программными токенами».</p>
aKey	Смарт-карты aKey S1000, aKey S1003, aKey S1004 производства компании Ak Kamal Security	<p>На компьютере должна быть установлена библиотека <code>akpkcs11.dll</code>, предоставленная компанией Ak Kamal Security.</p> <p>Устройство имеет два ПИН-кода: администратора и пользователя. Значение этих ПИН-кодов по умолчанию — 12345678.</p> <p>Перенос ключей подписи с устройств и на устройства данного семейства невозможен, так как на устройствах используется аппаратная криптография с неизвлекаемым ключом.</p>
ViPNet HSM	Программно-аппаратный комплекс ViPNet HSM производства АО «ИнфоТеКС»	<p>На компьютере должно быть установлено ПО ViPNet HSM SDK.</p> <p>В ViPNet CSP необходимо задать параметры подключения к серверу ViPNet HSM.</p>
JaCarta	Персональные электронные ключи и смарт-карты eToken ГОСТ, eToken PRO (Java), JaCarta PKI, JaCarta LT, JaCarta SE, JaCarta PKI/ГОСТ, JaCarta PRO, JaCarta-2 PKI/ГОСТ, JaCarta-2 ГОСТ, JaCarta-2 PRO/ГОСТ производства компании «Аладдин Р.Д.»	<p>На компьютере должно быть установлено ПО «Единый Клиент JaCarta» компании «Аладдин Р.Д.» (рекомендуемая минимальная версия — 2.12).</p> <p>Перенос ключей подписи с апплетов «Криптотокен» и «Криптотокен 2 ЭП» (модели JaCarta со словом «ГОСТ» в названии) и на эти апплеты невозможен, так как на устройствах используется аппаратная криптография с неизвлекаемым ключом.</p> <p>Работа с апплетом PRO через ПО «Единый Клиент JaCarta» версии 2.12 не поддерживается. Необходимо установить последнее обновление ПО «Единый Клиент JaCarta» с сайта производителя либо обратиться в службу поддержки компании «Аладдин Р.Д.».</p>
Rutoken	Электронные идентификаторы Рутокен ЭЦП 2.0 и Рутокен Lite производства компании «Актив»	<p>На компьютере должны быть установлены драйверы Rutoken (рекомендуемая версия — 4.8.5.0).</p> <p>Перенос ключей подписи с устройств, а также на устройства Рутокен ЭЦП 2.0 невозможен, так как на устройствах используется аппаратная криптография с неизвлекаемым ключом.</p>

Название семейства устройств в ViPNet CSP	Полные названия и типы устройств	Необходимые и рекомендуемые условия работы с семейством устройств
Rutoken S	Электронные идентификаторы <b>Рутокен S</b> производства компании «Актив»	На компьютере должны быть установлены драйверы Rutoken (рекомендуемая версия — 4.8.5.0).
R301 Foros	Смарт-карты и токены <b>R301 Форос PKCS</b> производства компании «СмартПарк»	На компьютере должна быть установлена библиотека <code>foros_pkcs11.dll</code> (для 32-разрядной либо 64-разрядной архитектуры процессора), предоставленная компанией «СмартПарк».  Перенос ключей подписи с устройств и на устройства данного семейства невозможен, так как на устройствах используется аппаратная криптография с неизвлекаемым ключом.
SafeNet eToken (eToken Aladdin)	Персональные электронные ключи <b>Gemalto SafeNet eToken 5100/5105, 5200/5205, 5110, 7300</b> , смарт-карта <b>Gemalto SafeNet eToken 4100</b> производства компании Gemalto (SafeNet)  Персональные электронные ключи <b>eToken PRO</b> , смарт-карты <b>eToken PRO</b> производства компании «Аладдин Р.Д.»	Если компьютер работает под управлением ОС Windows 10, на нем должно быть установлено ПО SafeNet Authentication Client (рекомендуемая версия — 10.6.146).  Если компьютер работает под управлением другой ОС, на нем должно быть установлено либо ПО PKI Client версии 5.1 SP1, либо ПО SafeNet Authentication Client (рекомендуемая версия — 10.6.146).  Смарт-карта <b>eToken PRO</b> может использоваться с любым стандартным PC/SC-совместимым устройством считывания карт.  <b>Примечание.</b> Если вам необходимо работать с устройством из семейства <b>SafeNet eToken (eToken Aladdin)</b> , то во избежание появления ошибок при выполнении криптографических операций не устанавливайте на компьютер одновременно ПО «Единый Клиент JaCarta» и ПО SafeNet Authentication Client. Работа с устройствами JaCarta PRO с помощью драйверов SafeNet возможна, но не рекомендуется производителем.



**Примечание.** Список поддерживаемых операционных систем для каждого из приведенных устройств вы найдете на официальном веб-сайте производителя этого устройства.

# Список поддерживаемых внешних устройств для подключения к сайтам, использующим TLS ГОСТ, и туннелируемым ресурсам

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

Таблица 3. Поддерживаемые внешние устройства для подключения к сайтам, использующим TLS ГОСТ, и туннелируемым ресурсам

Название семейства устройств в программе ViPNet CSP	Полные названия и типы устройств	Необходимые и рекомендуемые условия работы с семейством устройств
Infotecs Software Token	Infotecs Software Token — программная реализация стандарта PKCS#11	Входит в поставку ViPNet PKI Client. По умолчанию создан программный токен 8888. С помощью утилиты token_manager.exe на компьютере может быть создан другой программный токен.
ESMART Token	Смарт-карты и токены типов ESMART Token, ESMART Token ГОСТ	На компьютере должно быть установлено ПО ESMART PKI Client для Windows (рекомендуемая версия — 4.5 RC). Перенос ключей подписи с устройства и на устройство ESMART Token ГОСТ невозможен, так как на устройстве используется аппаратная криптография с неизвлекаемым ключом.
JaCarta	Персональные электронные ключи и смарт-карты JaCarta PKI, eToken ГОСТ, JaCarta ГОСТ, JaCarta SE, JaCarta PKI/ГОСТ и JaCarta-2 PKI/ГОСТ с апплетом ГОСТ, JaCarta-2 ГОСТ производства компании «Аладдин Р.Д.»	На компьютере должно быть установлено ПО «Единый Клиент JaCarta» компании «Аладдин Р.Д.» (рекомендуемая версия — 2.12). Перенос ключей подписи с устройств eToken ГОСТ, JaCarta ГОСТ, JaCarta PKI/ГОСТ и JaCarta-2 PKI/ГОСТ на эти устройства невозможен, так как на устройствах используется аппаратная криптография с неизвлекаемым ключом.
Rutoken	Электронные идентификаторы Рутокен ЭЦП, Рутокен ЭЦП 2.0 и Рутокен Lite производства компании «Актив»	Необходимо загрузить и установить библиотеку PKCS#11 (загружается с сайта Rutoken). Перенос ключей подписи на данный тип устройств невозможен.

Название семейства устройств в программе ViPNet CSP	Полные названия и типы устройств	Необходимые и рекомендуемые условия работы с семейством устройств
Rutoken S	Электронные идентификаторы <b>Рутокен S</b> производства компании «Актив»	На компьютере должны быть установлены драйверы Rutoken (рекомендуемая версия — 4.8.5.0).

## Алгоритмы и функции, поддерживаемые внешними устройствами

В следующей таблице перечислены криптографические алгоритмы, поддерживаемые внешними устройствами, приведена информация о возможности использования устройств в качестве датчиков случайных чисел, а также информация о поддержке стандарта PKCS#11.



**Примечание.** Стандарт PKCS#11 (также известный как Cryptoki) — один из стандартов семейства PKCS (Public Key Cryptography Standards — криптографические стандарты ключа проверки электронной подписи), разработанных компанией RSA Laboratories. Стандарт определяет независимый от платформы интерфейс API для работы с криптографическими устройствами идентификации и хранения данных.

Таблица 4. Алгоритмы и функции, поддерживаемые внешними устройствами

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

Название семейства устройств в ViPNet CSP	Аппаратная поддержка российских криптографических алгоритмов (на устройстве)	Программная поддержка российских криптографических алгоритмов (в ViPNet CSP)	Использование ДСЧ в ViPNet CSP	Поддержка PKCS#11
aKey	aKey S1000, aKey S1003, aKey S1004 — ГОСТ Р 34.10-2012; aKey S1000, aKey S1003 — ГОСТ Р 34.10-2001	отсутствует	Нет	Да
ViPNet HSM	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	отсутствует	Нет	Да
JaCarta (устройства JaCarta PKI, JaCarta SE, JaCarta LT, JaCarta PKI/ГОСТ и JaCarta-2 PKI/ГОСТ с апплетом Laser)	отсутствует	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	Нет	Да
JaCarta (устройства JaCarta PKI/ГОСТ и JaCarta-2 PKI/ГОСТ с апплетом ГОСТ, JaCarta-2 ГОСТ)	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 (короткий ключ 256 бит)	отсутствует	Да	Да
Rutoken	Рутокен ЭЦП 2.0 — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012; Рутокен Lite — отсутствует	Рутокен ЭЦП 2.0 — отсутствует; Рутокен Lite — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	ЭЦП 2.0 — да; Lite — нет	Да
Rutoken S	отсутствует	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	Нет	Да
SafeNet eToken (eToken Aladdin)	отсутствует	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	Нет	Да



**Примечание.** Выработка ключей шифрования (функция `C_DeriveKey` интерфейса PKCS#11) поддерживается не всеми перечисленными устройствами. Для получения более подробной информации см. документацию по необходимому устройству.



# Глоссарий

## PKI (Public Key Infrastructure)

Инфраструктура открытых ключей — комплекс аппаратных и программных средств, политик и процедур, обеспечивающих распространение доверительного отношения к открытым ключам (в том числе ключам проверки электронной подписи) в распределенных системах через создание сертификатов ключей проверки электронной подписи и поддержание их жизненного цикла.

## TLS (Transport Layer Security)

Криптографический протокол, обеспечивающий защищенную передачу данных между узлами в Интернете. Использует асимметричную криптографию для обмена ключами, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений.

## Запрос на сертификат

Защищенное электронной подписью сообщение, содержащее имя пользователя, ключ проверки электронной подписи и его параметры, желаемый срок действия сертификата, предполагаемые назначения сертификата и другие параметры (полный набор параметров зависит от формата запроса и программного обеспечения, в котором он был сформирован).

## Ключ проверки электронной подписи (ключ проверки ЭП)

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

## Ключ электронной подписи (ключ ЭП)

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

## Контейнер ключей

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

## ПАК ViPNet PKI Service

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

### Сертификат издателя

Сертификат удостоверяющего центра, которым заверяются издаваемые сертификаты.

### Сертификат ключа проверки электронной подписи

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

### Список аннулированных сертификатов (CRL)

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

### Точка распространения данных

Источник, доступный по общеизвестным протоколам (например, HTTP или LDAP), используемый для размещения сформированной в удостоверяющем центре информации (сертификатов издателей и списков аннулированных сертификатов).

### Удостоверяющий центр (УЦ)

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

### Файл \*.enc

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

### Файл \*.sig

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

## Электронная подпись (ЭП)

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