

Работа с защищенным DST

Быстрый старт

Файл дистрибутива (DST) содержит ключи и справочники для первоначального развертывания узла ViPNet. Поэтому его передача в открытом виде по незащищенным сетям не разрешена. Для безопасной передачи файла DST зашифруйте его с использованием сертификата того пользователя, для которого предназначен файл DST. После этого воспользоваться ключами сможет только определенный пользователь сети ViPNet.

Ниже описан порядок действий администратора сети и пользователя по работе с защищенным файлом DST с помощью ПО ViPNet PKI Client и ViPNet Client.




Внимание! Данный сценарий предполагает, что в вашей организации развернута инфраструктура открытых ключей (PKI). Также у пользователей вашей сети есть действующие ключи подписи и сертификаты, с помощью которых можно зашифровать файлы DST.

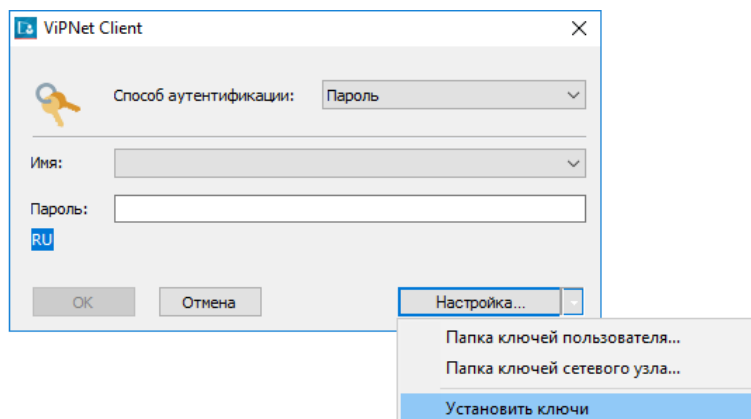
Порядок действий администратора

- 1 В программе ViPNet Administrator сформируйте файлы DST согласно документу «ViPNet Удостоверяющий и ключевой центр. Руководство администратора», раздел «Создание дистрибутивов ключей».
- 2 Установите программу ViPNet PKI Client согласно документу «Программный комплекс ViPNet PKI Client. Общие сведения», раздел «Установка компонентов ПК ViPNet PKI Client».
- 3 Установите в хранилище «Другие пользователи» сертификаты пользователей, для которых были сформированы DST-файлы.
- 4 Настройте ViPNet PKI Client для шифрования согласно документу «ViPNet PKI Client File Unit. Руководство пользователя», раздел «Настройка параметров шифрования».
- 5 Поочередно зашифруйте все файлы DST на сертификатах соответствующих пользователей согласно документу «ViPNet PKI Client File Unit. Руководство пользователя», раздел «Шифрование файла».
- 6 Передайте зашифрованные дистрибутивы (*.enc) пользователям любым способом.

Порядок действий пользователя

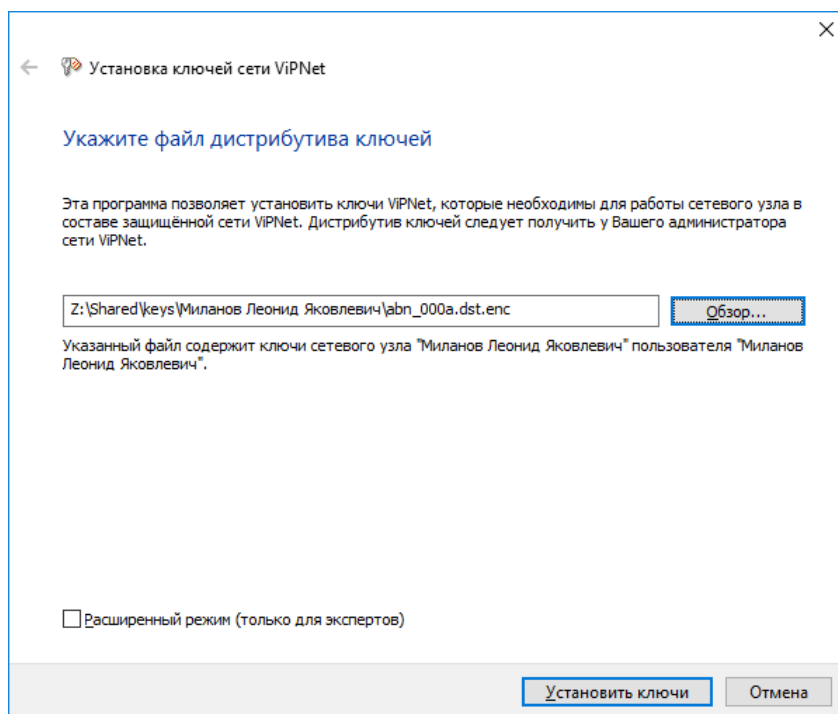
- 1 Получите у администратора сети файл для установки ПО ViPNet Client, дистрибутив ключей (файл *.enc) и пароль или внешнее устройство для аутентификации.
- 2 Установите программу ViPNet Client или ViPNet Coordinator (установка ViPNet PKI Client не требуется), после установки появится предложение установить справочники и ключи для вашего узла.

Если вы отказались от установки справочников и ключей, вы можете выполнить ее позднее. Для этого запустите программу ViPNet и в окне ввода пароля щелкните значок  справа от кнопки **Настройка** и в меню выберите пункт **Установить ключи**.



- 3 На первой странице мастера установки ключей укажите путь к файлу дистрибутива (*.enc).

Убедитесь, что выбран дистрибутив ключей, предназначенный для вашего сетевого узла. Имя сетевого узла и имя пользователя отображаются ниже поля для указания пути к файлу дистрибутива.



По умолчанию справочники и ключи устанавливаются в одну папку
C:\ProgramData\Infotecs\<папка с идентификатором узла>.

Чтобы указать другую папку, перейдите в расширенный режим установки.

- 4 Если установка ключей прошла успешно, появится соответствующее сообщение.

Если выполнить установку ключей не удалось, ознакомьтесь с сообщением о возникших ошибках и обратитесь к администратору сети для их устранения.

После успешной установки ключей можно запустить программу ViPNet Client, указав полученный ранее пароль или подключив внешнее устройство для аутентификации.



АО «ИнфоТеКС», 127083, Москва, улица Мишина, д. 56, стр. 2, этаж 2, помещение IX, комната 29

Телефон: +7 (495) 737-6162, 8-800-250-0260 — бесплатный звонок из России (кроме Москвы)

Веб-сайт: infotecs.ru

Служба поддержки: hotline@infotecs.ru

ФРКЕ., версия продукта 4.5.5

© АО «ИнфоТеКС», 2020. ViPNet® является зарегистрированным товарным знаком АО «ИнфоТеКС».

Все названия компаний и продуктов, являющиеся зарегистрированными товарными знаками, принадлежат соответствующим владельцам.