

Работа с защищёнными DST

Быстрый старт

Версия продукта 4.5.5 hotfix 9

Файл дистрибутива (DST) содержит ключи и справочники для первоначального развёртывания узла ViPNet. Поэтому запрещено передавать его в открытом виде по незащищённым сетям. Для безопасной передачи файла DST зашифруйте его с использованием сертификата того пользователя, для которого предназначен файл DST. Воспользоваться ключами сможет только этот пользователь сети ViPNet.

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



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

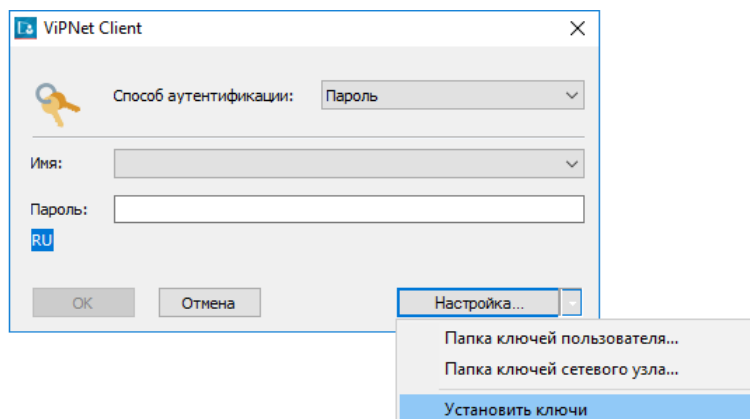
Порядок действий администратора

- 1 В программе ViPNet Administrator сформируйте файлы DST.
См. документ «ViPNet Удостоверяющий и ключевой центр. Руководство администратора», раздел «Создание дистрибутивов ключей».
- 2 Установите программу ViPNet PKI Client.
См. документ «ViPNet PKI Client. Общие сведения», раздел «Установка, обновление».
- 3 Установите в хранилище «Другие пользователи» сертификаты пользователей, для которых были сформированы DST-файлы.
- 4 Настройте ViPNet PKI Client для шифрования.
См. документ «ViPNet PKI Client File Unit. Руководство пользователя», раздел «Настройка параметров шифрования».
- 5 Поочерёдно зашифруйте все файлы DST на сертификатах соответствующих пользователей.
См. документ «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 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.

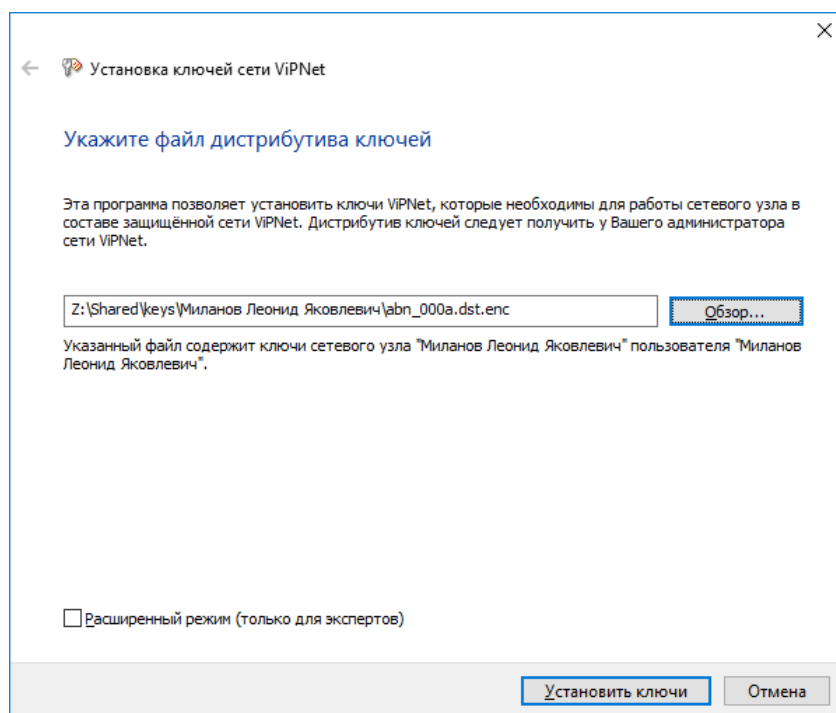
Если вы отказались от установки справочников и ключей, вы можете выполнить её позднее. Для этого запустите программу и в окне ввода пароля щёлкните значок , справа от кнопки **Настройка**, и выберите **Установить ключи**.



Откроется мастер установки ключей.

3 Укажите путь к файлу *.enc.

Убедитесь, что выбран дистрибутив ключей, предназначенный для вашего сетевого узла.



По умолчанию справочники и ключи устанавливаются в папку

C:\ProgramData\Infotecs\ID_Узла\.

Чтобы указать другую папку, перейдите в расширенный режим установки.

После установки ключей вы можете запустить ViPNet Client. Для входа введите пароль либо подключите устройство аутентификации и введите ПИН.



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, телеграм-канал поддержки: t.me/vhd21

ФРКЕ.00116-05 34 09, версия продукта 4.5.5 hotfix 9

© АО «ИнфоТеКС», 2025. ViPNet® является зарегистрированным товарным знаком АО «ИнфоТеКС».

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