Средство криптографической защиты информации «Криптографический сетевой программный комплекс "КриптоПро NGate"».

Руководство пользователя

MS Windows

ЖТЯИ.00104-01 91 01

Общие сведения

ПО «КриптоПро NGate Клиент» является частью Средство криптографической защиты информации «Криптографический сетевой программный комплекс "КриптоПро NGate"» (далее – КСПК NGate), и должен эксплуатироваться в соответствии с требованиями Формуляра ЖТЯИ.00104-01 30 01. Данное руководство предназначено для пользователей, осуществляющих самостоятельную установку и настройку программы «КриптоПро NGate Клиент», защищённым посредством КСПК NGate. Для использования руководства требуются базовые навыки работы с операционной системой Microsoft Windows (ОС MS Windows). Поддерживаемые версии операционной системы для установки клиента:

- Windows 7/8/8.1/10/Server 2003/2008 (x86, x64);
- Windows Server 2008 R2/2012/2012 R2/2016 (x64).

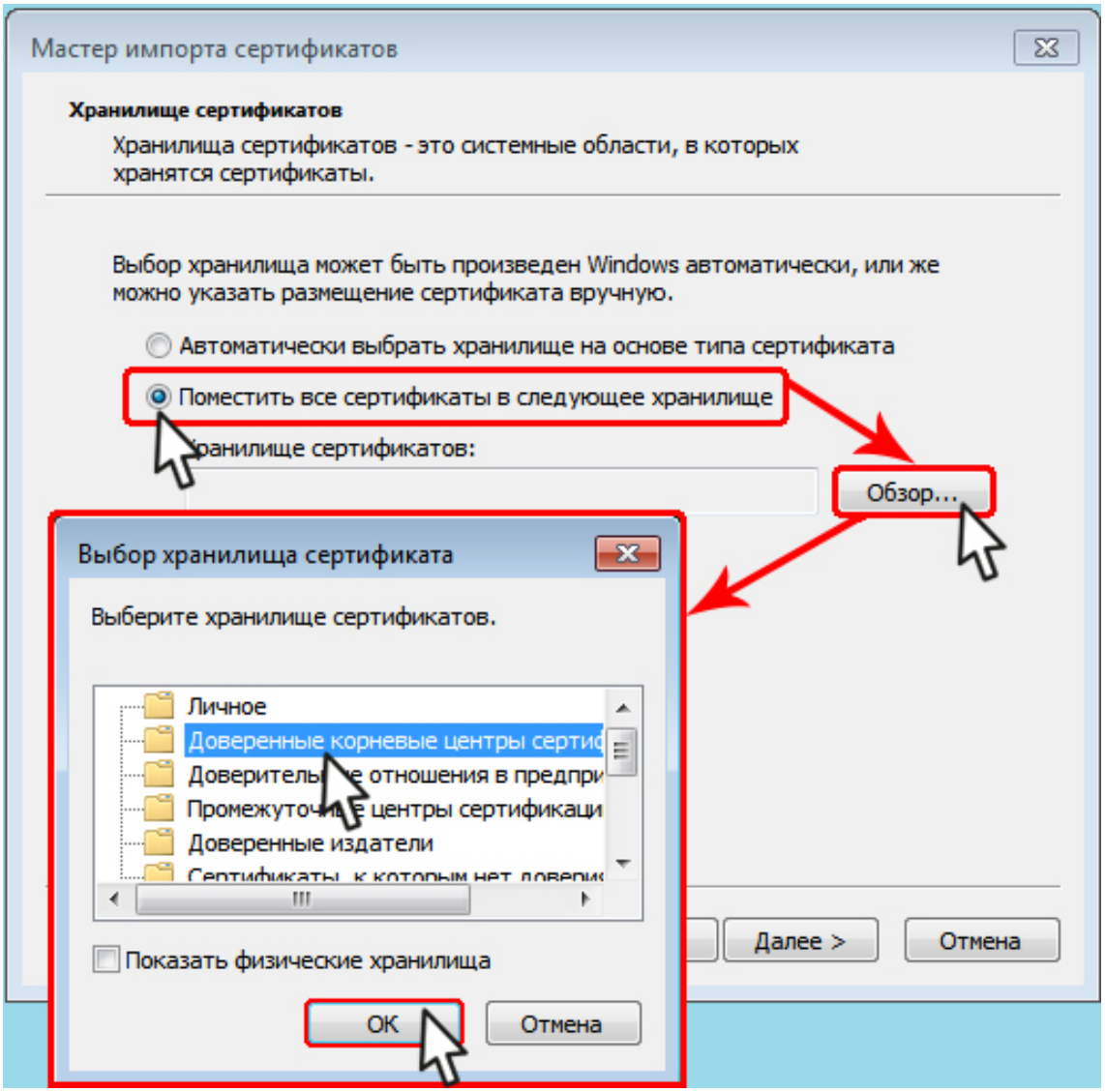
Руководство по подключению к порталу с использованием ПО «КриптоПро NGate Клиент»

1. **Установите «Крипто-Про CSP»:**
   a) Загрузите с официального сайта *https://www.cryptopro.ru/* программу криптопровайдер «Крипто-Про CSP 4.0», для доступа к загрузке необходима регистрация.
   b) Установите «Крипто-Про CSP», запустив установочный файл `CSPSetup.exe` с правами администратора.
   c) Следуйте указаниям установщика, рекомендуется установить программу с настройками по умолчанию.
2. **Установка клиента:**
   a) Запустить установочный файл программы `NGClientSetup.exe` с правами Администратора
   b) Установить ПО «КриптоПро NGate Клиент», следуя указаниям установщика, рекомендуется установка с настройками по умолчанию
3. **Установка корневого сертификата УЦ.**

   Для организации безопасного соединения с порталом на шлюзе NGate по *https* необходимо установить корневой сертификат удостоверяющего центра (УЦ) в хранилище сертификатов на вашем ПК. Сертификат на физическом носителе или ссылку на скачивание необходимо получить у сетевого администратора.

   Процесс установки корневого сертификата УЦ:

   a) Кликнуть правой кнопкой мыши по файлу сертификата (файл с расширением `.cer` или `.crt`) и выбрать в открывшемся меню **Установить сертификат**.
   b) Далее следовать указаниям **Мастера импорта сертификатов** до этапа выбора **Хранилища сертификата**.
   c) В данном окне произведите выбор хранилища вручную: установите переключатель в графе ◉ **Поместить все сертификаты в следующее хранилище** , затем нажмите кнопку **Обзор** и выберите папку хранилища сертификатов **Доверенные корневые центры сертификации**. Нажмите **ОК** > **Далее** для продолжения установки.

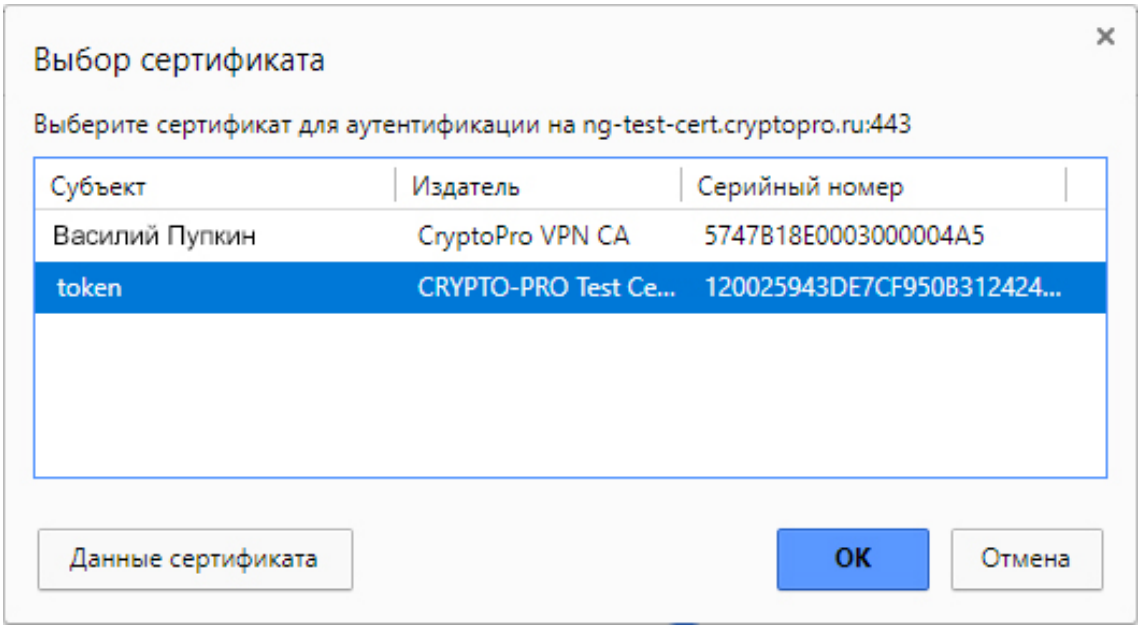


d) Продолжайте следовать указаниям установщика до завершения установки.

4. **Установка доверенного сертификата пльзователя:**

Примечание: Пропустите данный этап в случае доступа к порталу по логину и паролю.

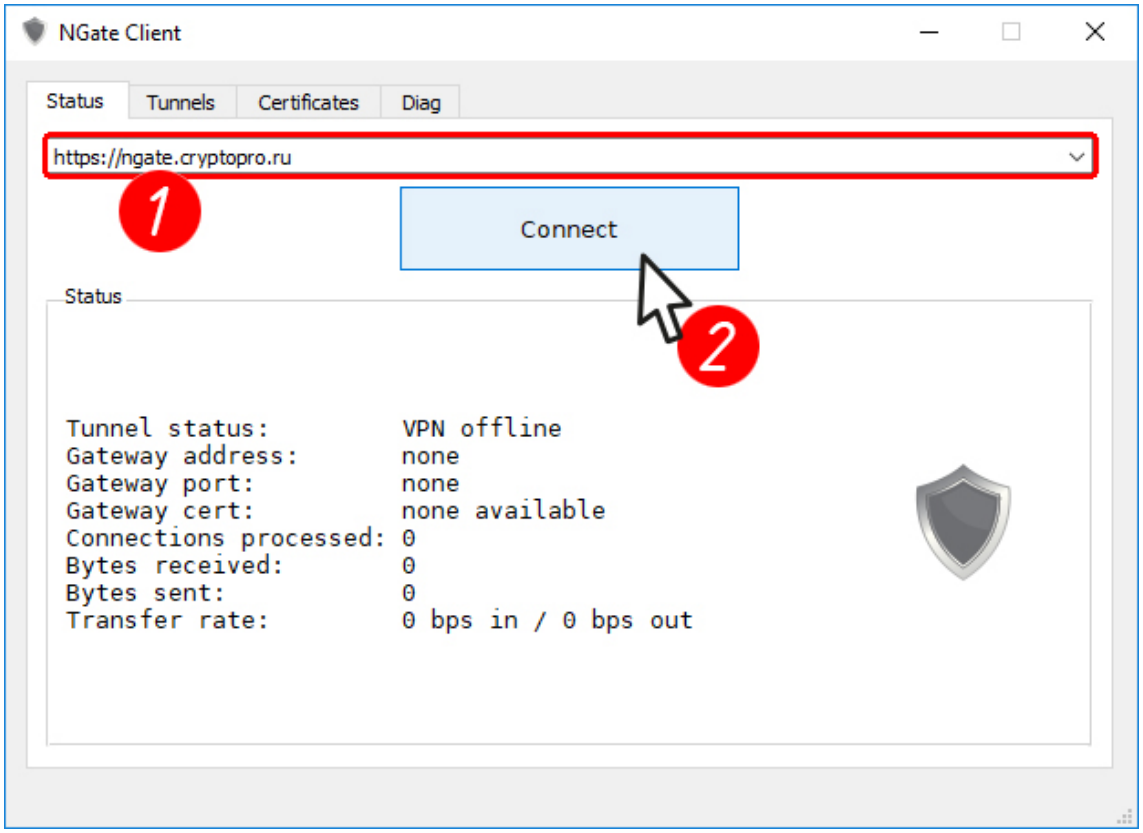
Способ установки доверенного сертификата пользователя определяется политиками безопасности Организации, к ресурсам которой необходим доступ. Инструкцию по получению и настройке необходимо получить у сетевого администратора. Как правило применяется ключевой носитель информации с интерфейсом подключения USB, которій необходимо подключить к ПК и затем выбрать из списка сертификатов.



5. Подключение к порталу посредством клиента:

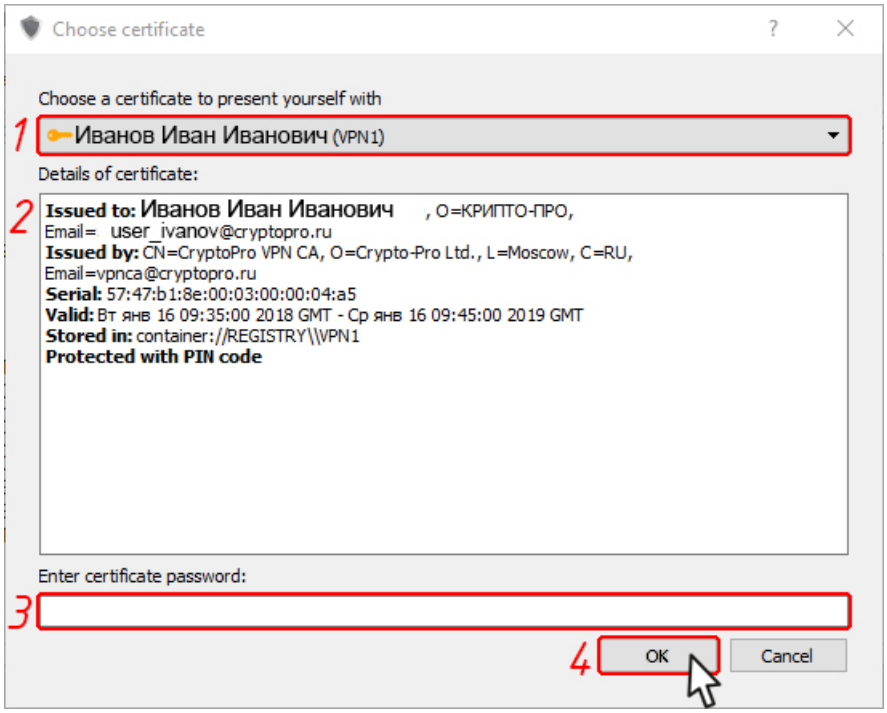
a) Запустите ПО «КриптоПро NGate Клиент», по умолчанию при запуске должна открыться вкладка **Status**.

b) На вкладке **Status** ведите в адресную строку URL адрес портала (поз. 1) и нажмите **Connect** (поз. 2):

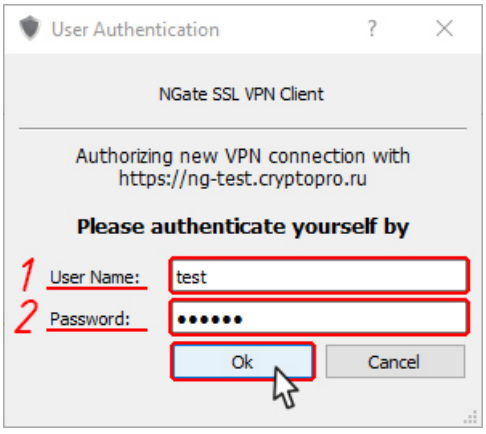


c) Выберите сертификат пользователя для доступа к порталу из выпадающего меню (поз. 1). В поле подробной информации о сертификате (поз. 2) отобразятся данные выбранного сертификата. В поле

поз. 3 введите пароль от контейнера, в котором хранится сертификат (если пароль задан), нажмите **ОК** (поз. 4):



d) В случае, если доступ к порталу осуществляется по *логину* и *паролю* (LDAP), то (если все предыдущие этапы выполнены верно) должна открыться страница аутентификации на портале. Введите логин *User Name* (поз. 1) и пароль *Password* (поз. 2), нажмите **ОК**



e) Если всё выполнено верно, то доступ к сконфигурированным сетевым ресурсам Организации должен быть открыт.