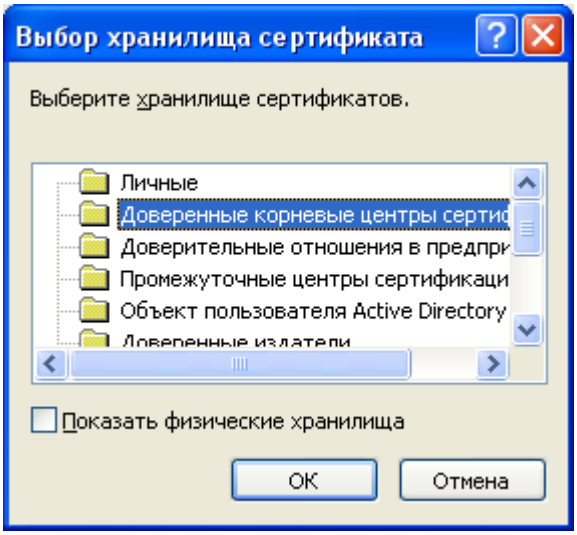
НАСТРОЙКА VPN СОЕДИНЕНИЯ

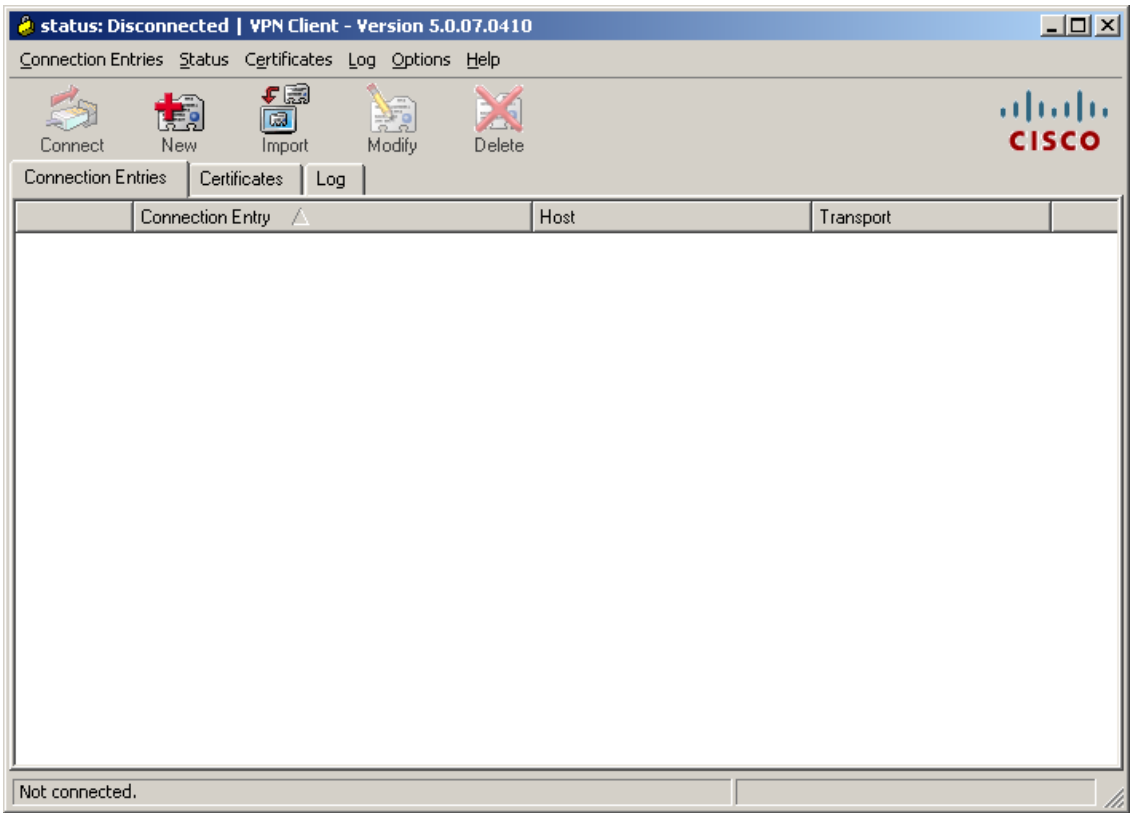
1. Скачайте и установите на личный компьютер следующие программы и файлы:
   - eToken PKI Client;
   - Cisco VPN Client:
     - для 32 разрядной операционной системы;
     - для 64 разрядной операционной системы;
2. В службе поддержки пользователей (СПП) запросите Сертификаты. Для этого напишите письмо в произвольной форме на адрес oos@qiwi.ru с просьбой выслать сертификаты для подключения к VPN, а так же Пароль и Имя учетной группы. В теме письма укажите «Сертификат для VPN».
3. Экспортируйте сертификаты CA01 и ROOT CA в систему двойным щелчком мыши.
   - Для сертификата CA01 выберете автоматический способ выбора хранилища.
   - Сертификат ROOT CA установите вручную в **Доверенные корневые центры сертификации** (Рис. 1).

Рис. 1. Экспорт сертификатов



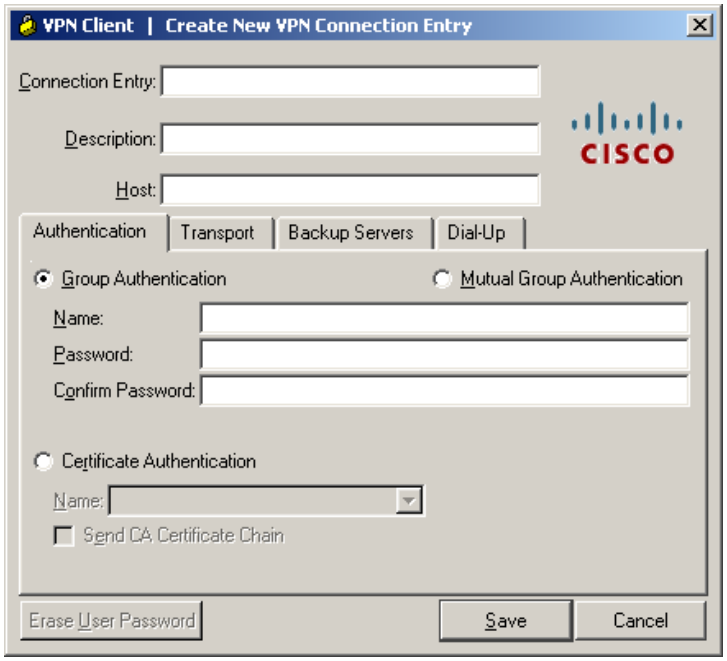
4. После успешной установки всех программ запустите *Cisco VPN Client* (Рис. 2).

Рис. 2. Программа Cisco VPN Client



5. Нажмите кнопку **NEW** и в появившемся окне заполните поля (Рис. 3):

Рис. 3. Настройка параметров нового соединения

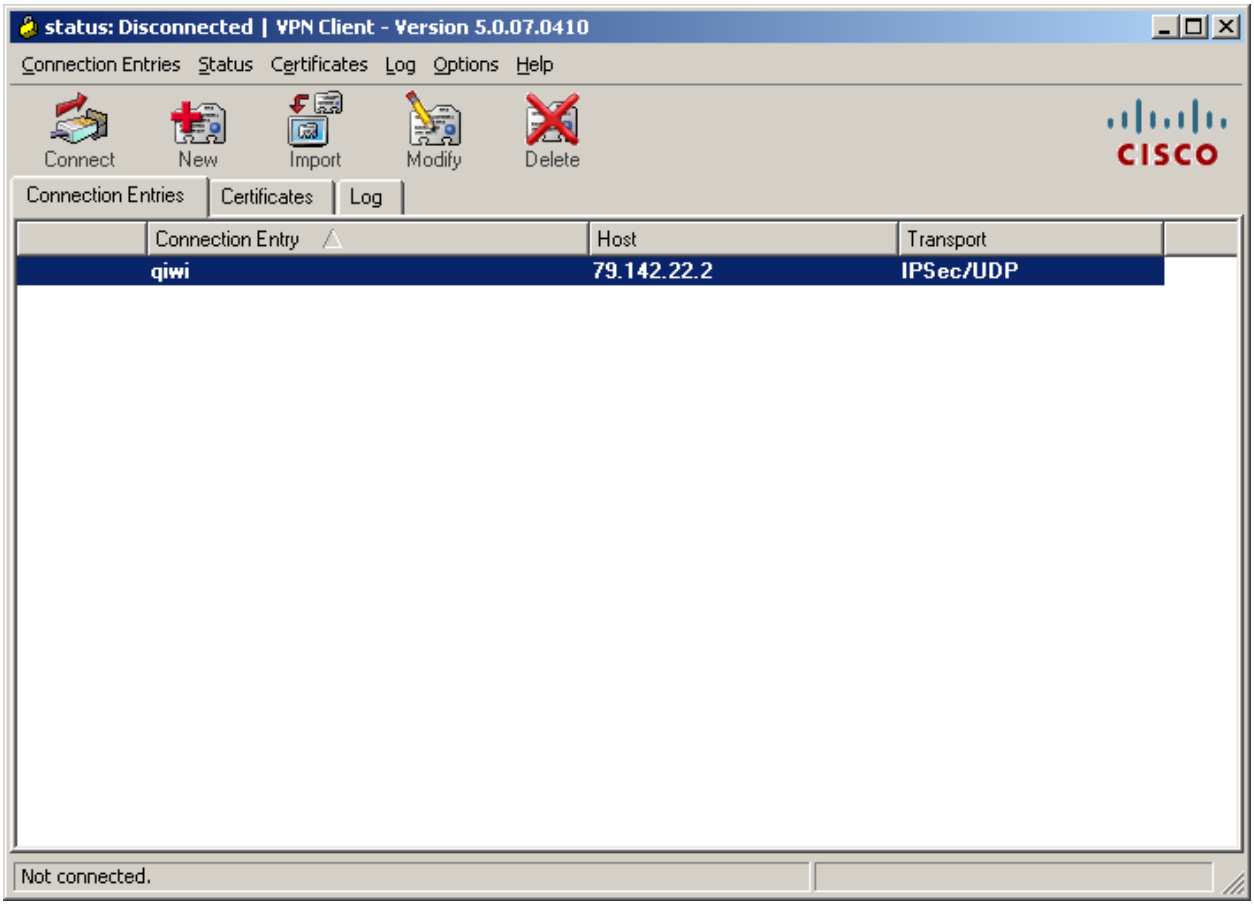


- **Connection Entry** и **Description** – введите любое название, например, QIWI.
- **Host** – укажите адрес сервера 79.142.22.2.

- **Name**, **Password** и **Confirm Password** – укажите Имя и Пароль группы высланные вам в письме от СПП (см. 1 пункт). запросите в Службе технической поддержки. Если вы это не делали ранее, тогда напишите в произвольной форме письмо по адресу oos@qiwi.ru, с просьбой выслать данные по указанным пунктам. В теме письма укажите «Сертификат для VPN».

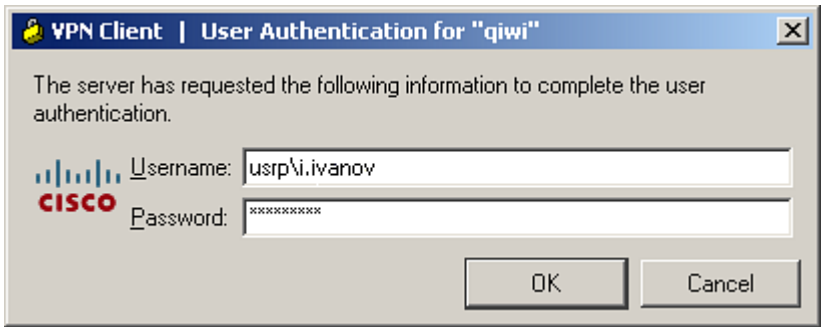
6. Нажмите кнопку **Save**.
7. В открытом окне *Cisco VPN Client* выберите только что созданную настройку и нажмите кнопку **Connect** (Рис. 4).

Рис. 4. Выбор соединения



8. После этого появиться окно, в котором необходимо ввести ваши учётные данные (Рис. 5):

Рис. 5. Ввод доменных авторизационных данных



- **Username** – имя пользователя, в формате *usrp\i.ivanov*;
- **Password** – доменный пароль.

9. Нажмите кнопку **OK**.

После успешного ввода данных окно закроется и в области уведомлений появиться значок закрытого желтого замка (Рис. 6).

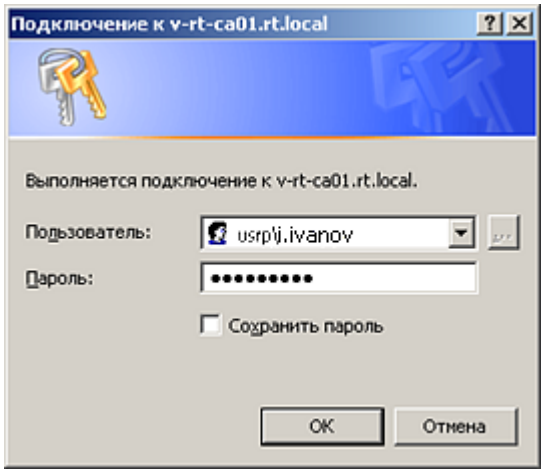
Рис. 6. Область уведомлений Windows

Теперь у вас есть доступ к внутреннему сайту для получения сертификата.

10. В браузере *Internet Explorer* откройте следующую страницу http://v-rt-ca01.rt.local/certsrv/.

    Система попросит вас ввести учётные данные от домена USRP (Рис. 7).

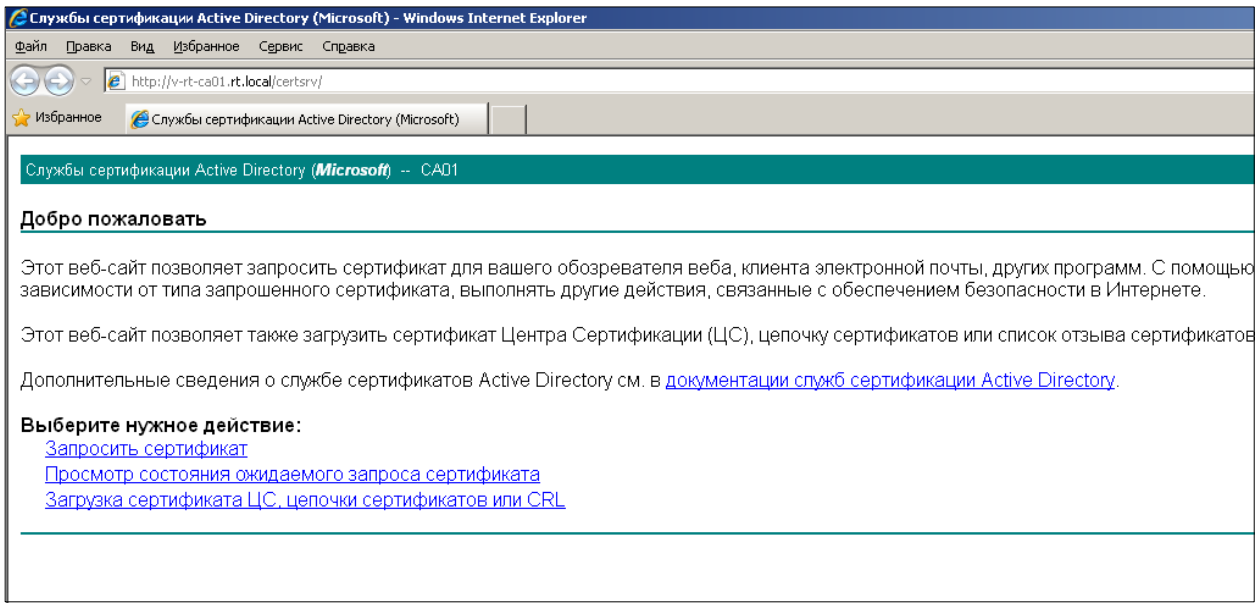
Рис. 7. Подключение к v-rt-ca01.rt.local



- **Пользователь** – имя пользователя, в формате *usrp\i.ivanov*;
- **Пароль** – доменный пароль.

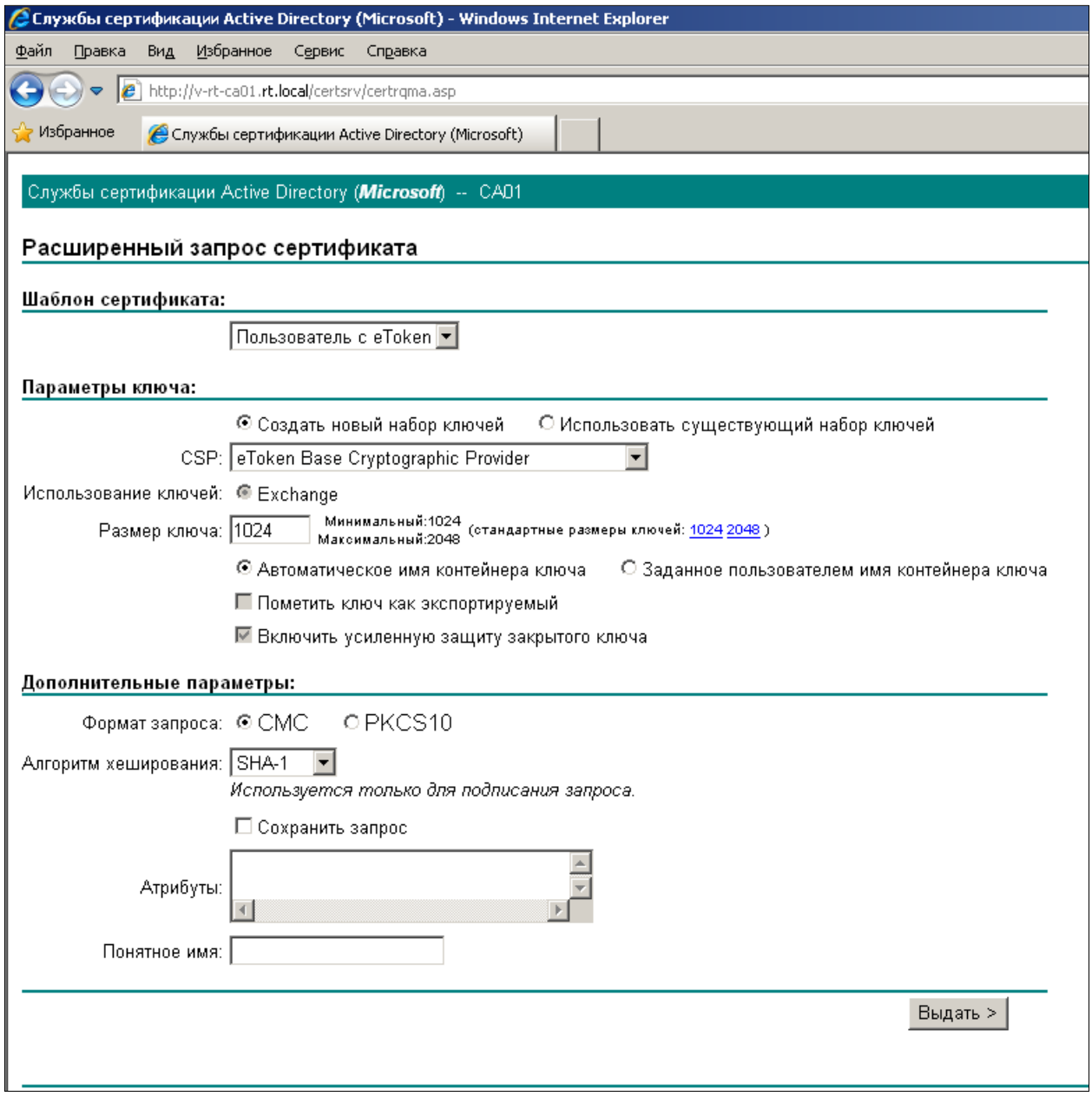
11. После успешного ввода данных откроется следующая страничка:

Рис. 8. Главная страница службы сертификации Active Directory



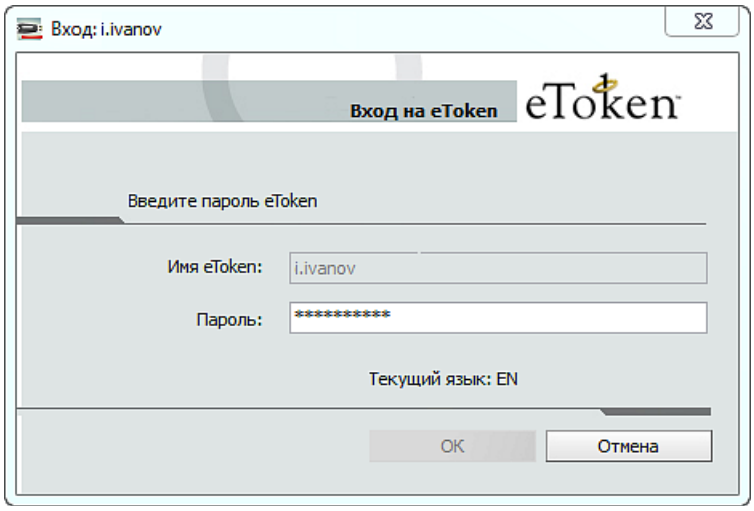
12. Последовательно нажмите ссылки: **Запросить сертификат** → **Создать и выдать запрос к этому ЦС**.
13. На новой странице в поле **Шаблон сертификата** выберите **Пользователь с eToken**, в поле **Размер ключа** выберите размер **1024** (Рис. 9).

Рис. 9. Настройка параметров сертификата в службе сертификации Active Directory



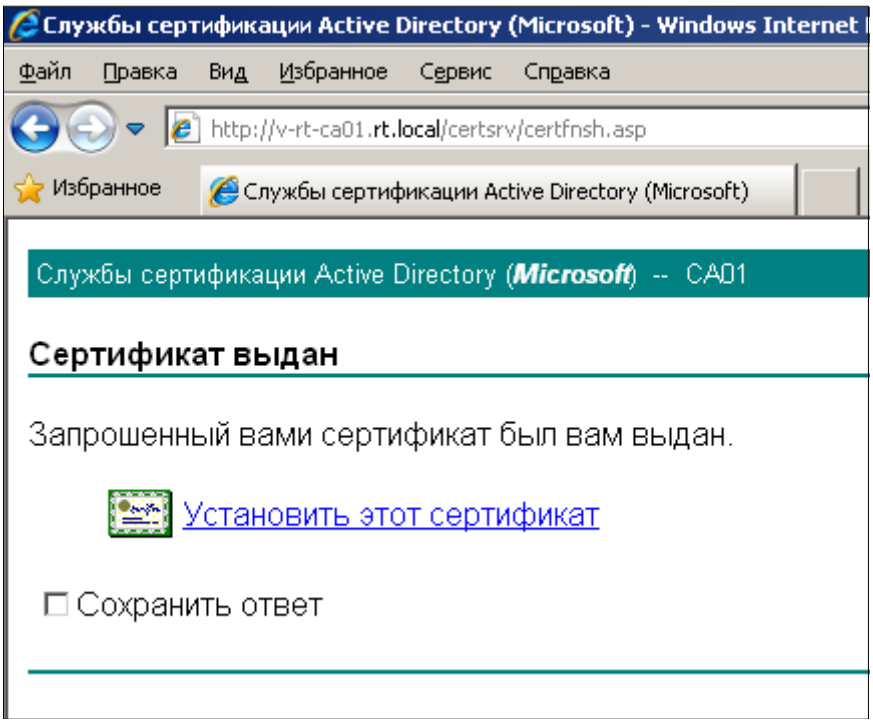
14. Нажмите кнопку **Выдать**, и введите пароль от eToken (Рис. 10).

Рис. 10. Ввод пароля eToken



15. Далее нажмите ссылку **Установить этот сертификат** (Рис. 11).

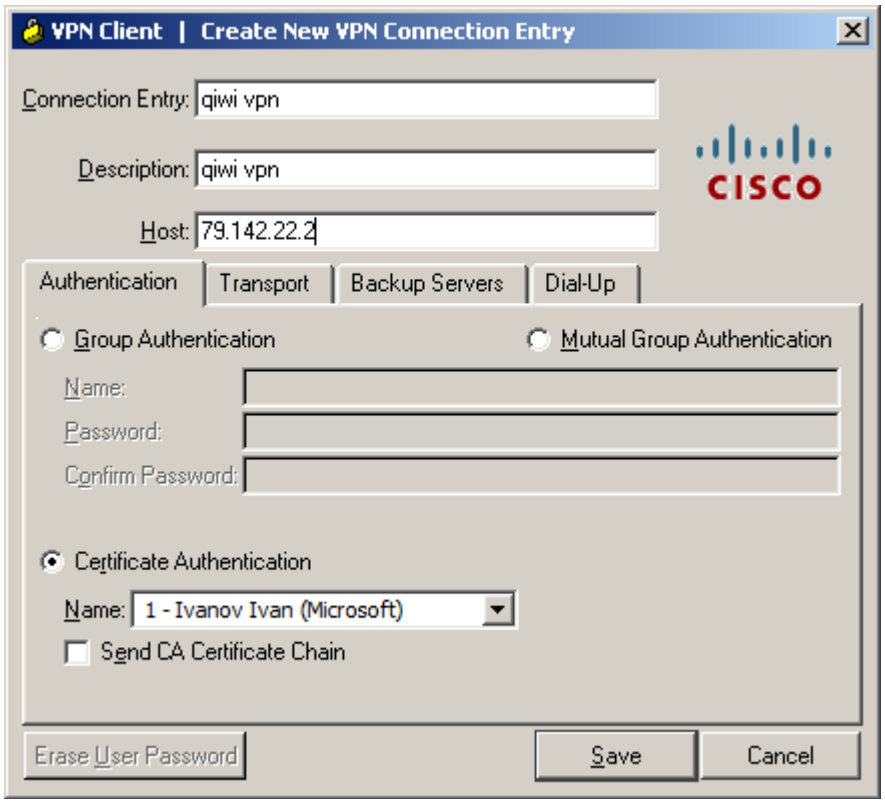
Рис. 11. Установка сертификата



Теперь на eToken записан сертификат, который необходим для настройки полноценного VPN.

16. Снова откройте *Cisco VPN Client* и нажмите кнопку **NEW** (Рис. 12). Настройте параметры в соответствии с описанием:

Рис. 12. Ввод параметров для vpn соединения

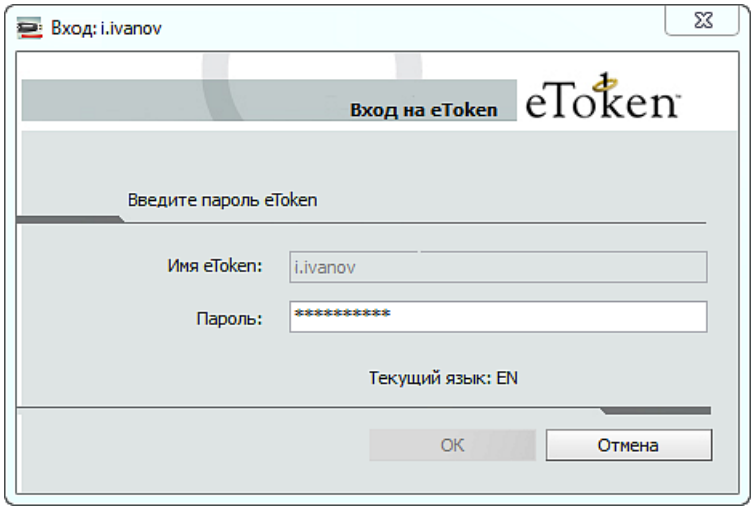


- **Connection Entry** и **Description -** укажите любое название, например, QIWI VPN.
- **Host -** укажите адрес нашего сервера 79.142.22.2.
- Установите флаг **Certificate Authentication** и выберите ваш доменный сертификат.

17. Нажмите кнопку **Save**.
18. В открытом окне Cisco VPN Client выберите вновь созданную конфигурацию подключения и нажмите кнопку **Connect**.

    После нажатия кнопки появиться запрос на ввод пароля от eToken (Рис. 13).

Рис. 13. Ввод пароля eToken



19. Введите пароль и нажмите кнопку **OK**.

Пароль желательно ввести в течение 20 секунд.

В случае успеха в области уведомлений снова появиться желтый закрытый замок (Рис. 14).

Рис. 14. Область уведомлений

Теперь вы имеете доступ ко всем внутренним ресурсам компании.