ESMART®

ESMART Token
Защищенное VPN-соединение

на примере Microsoft Windows Server 2003
и клиента Windows 7 Professional

Содержание

1. Установка VPN-соединений по сертификату

При настройке удаленного VPN-доступа к сетевым ресурсам нежелательно использовать параметры учетной записи, защищенной только паролем. Двухфакторная авторизация по смарт-карте является более защищенным вариантом. Требование предоставить смарт-карту с соответствующим сертификатом и ввести ПИН-код значительно уменьшает вероятность несанкционированного доступа к сети организации.

VPN обеспечивает безопасность благодаря защищенному туннельному подключению и шифрованию данных. Доступ к корпоративной сети предоставляется только пользователям, предоставившим верный сертификат на смарт-карте или USB-ключе и ПИН-код, подбор которого не возможен.

1.1 Требования к клиентским компьютерам

Для работы со смарт-картами требуется ОС Windows не ниже XP SP2. На каждом клиентском компьютере должен быть установлен криптопровайдер ESMART Token CSP. При использовании Windows XP также требуется установка пакета Microsoft Base CSP. Установка подробно описана в руководстве ***ESMART Token - CSP****.*

На клиентском ПК должен быть установлен драйвер для считывателя смарт-карт или драйвер USB-ключа ESMART Token.

1.2 Требования к оборудованию VPN-сервера

VPN-подключения увеличивают загрузку процессора на сервере удаленного доступа. Вход в систему с помощью смарт-карты или USB-ключа не вносит существенного вклада в эту загрузку. VPN-сервера удаленного доступа, обслуживающие большой объем входящих подключений, требуют использования быстрых процессоров (желательно в многопроцессорной конфигурации), а также поддержки высокой пропускной способности сети.

1.3 Требования к программному обеспечению VPN-сервера

Требования к программному обеспечению VPN-сервера для доступа на основе смарт-карт довольно просты. На серверах удаленного доступа может использоваться ОС Windows 2003 Server или более поздняя версия с включенной поддержкой маршрутизации и удаленного доступа и поддержкой EAP-TLS.

EAP-TLS представляет собой механизм взаимной проверки подлинности, разработанный для использования совместно с устройствами безопасности, например смарт-картами. EAP-TLS поддерживает подключения по протоколу PPP (Point-to-Point Protocol) и VPN и позволяет обмениваться общими секретными ключами для MPPE в дополнение к IPsec.

Основными преимуществами EAP-TLS являются устойчивость к атакам методом прямого подбора паролей и поддержка взаимной проверки подлинности. При взаимной проверке подлинности и клиент, и сервер должны подтвердить друг другу свои учетные данные. Если клиент или сервер не отправят сертификат для проверки своих учетных данных, подключение будет прервано.

Microsoft Windows Server 2003 и выше поддерживает EAP-TLS для коммутируемых и VPN-подключений, что позволяет удаленным пользователям использовать смарт-карты.

2. Подготовительные этапы

2.1 Установка центра сертификации

Установка и настройка корпоративного центра сертификации описана в руководствах по развертыванию центра сертификации Windows Server 2003 и Windows Server 2008.

2.2 *Выдача клиентских сертификатов*

Процедура выдачи клиентских сертификатов и записи сертификатов на смарт-карту или USB-ключ описана в руководствах по развертыванию центра сертификации Windows Server 2003 и Windows Server 2008 и выше.

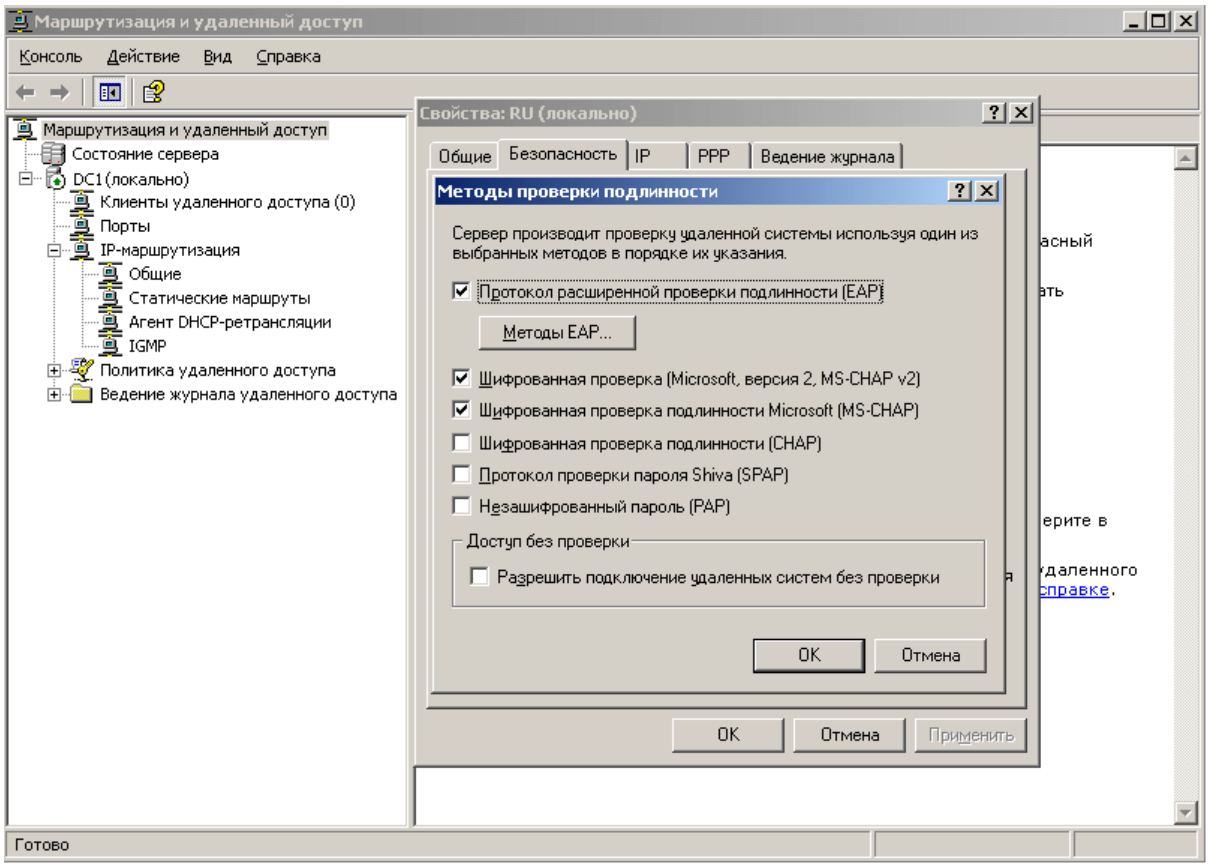
3. Настройка VPN-сервера

*Добавьте оснастку **Маршрутизация и удаленный доступ**.*

*В контекстном меню сервера выберите **Свойства,** перейдите на вкладку **Безопасность**.*

*Выберите пункт **Методы проверки подлинности**.*

*Установите флажок **Протокол расширенной проверки подлинности (EAP)** и нажмите кнопку **OK**.*



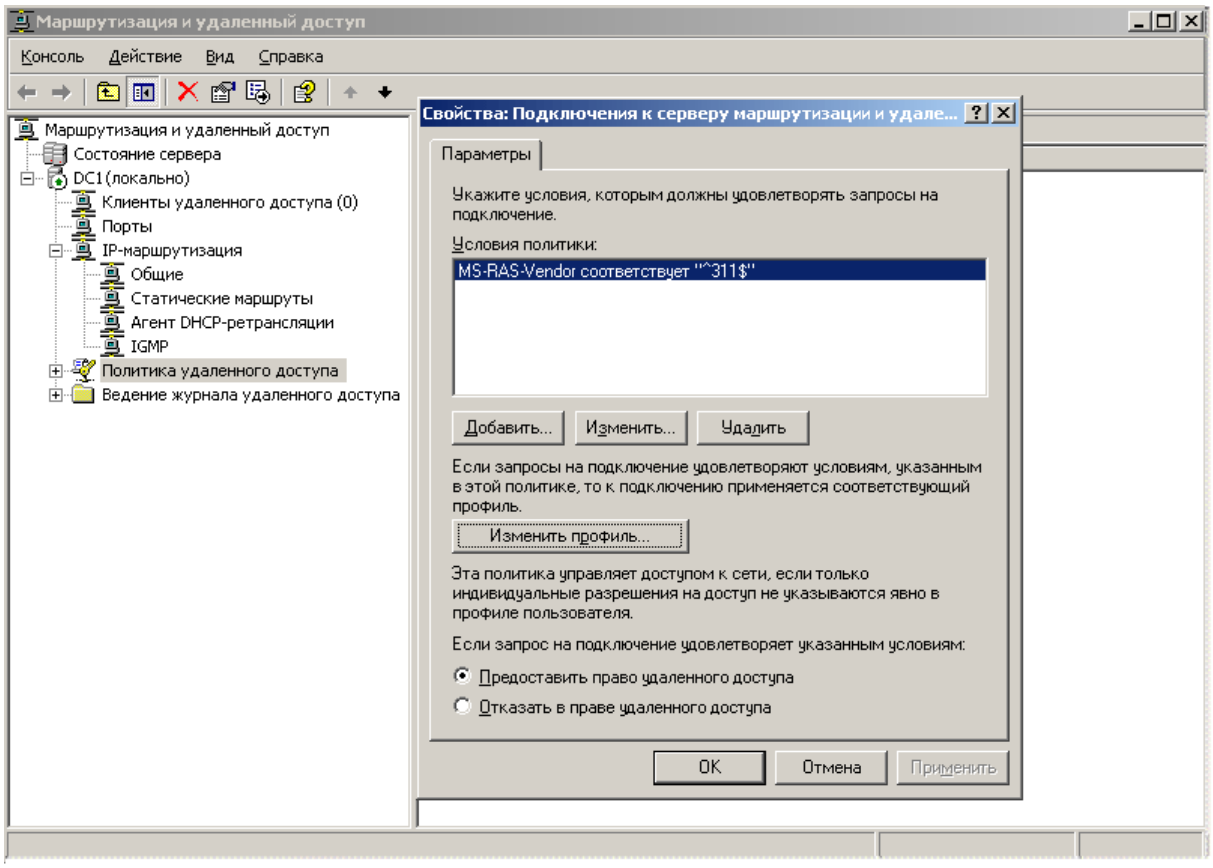
3.1 *Настройка политик удаленного доступа*

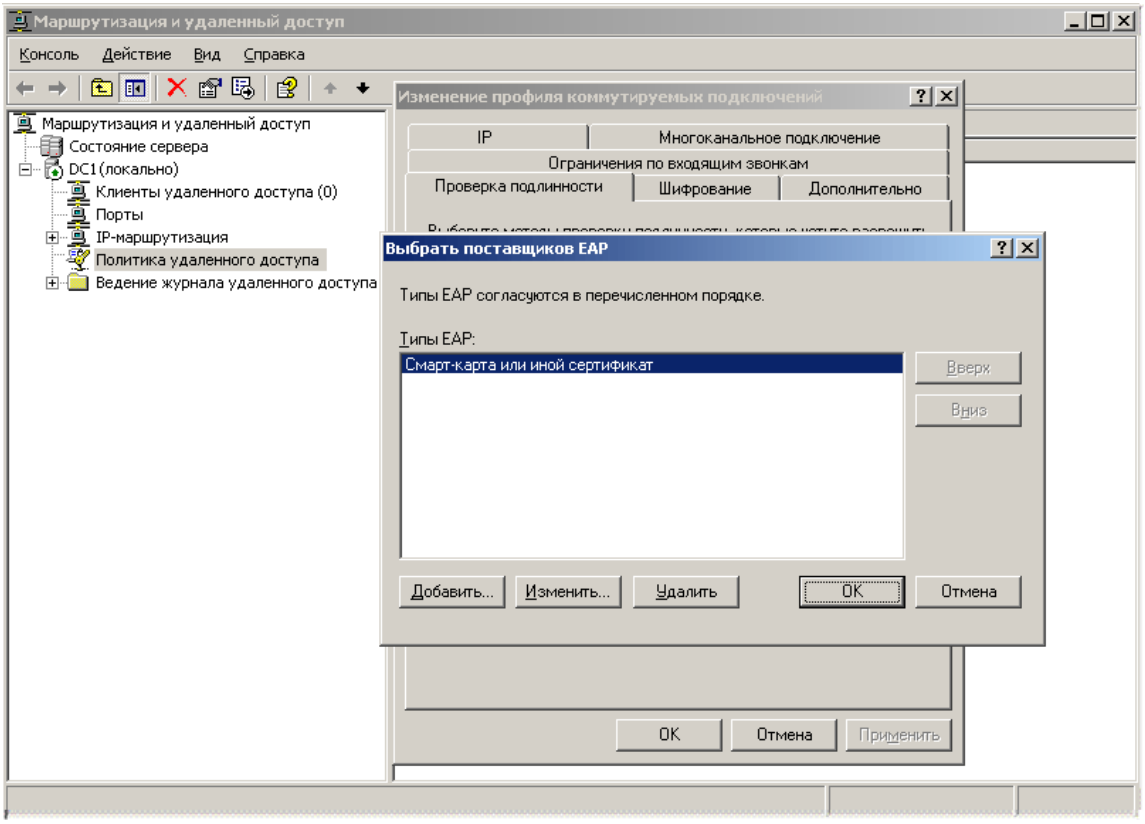
*В оснастке **Маршрутизация и удаленный доступ** выберите **Политики удаленного доступа › Подключения к серверу маршрутизации и удаленного доступа.***

*Нажмите **Изменить профиль**, выберите вкладку **Проверка подлинности** и нажмите **Методы EAP.***

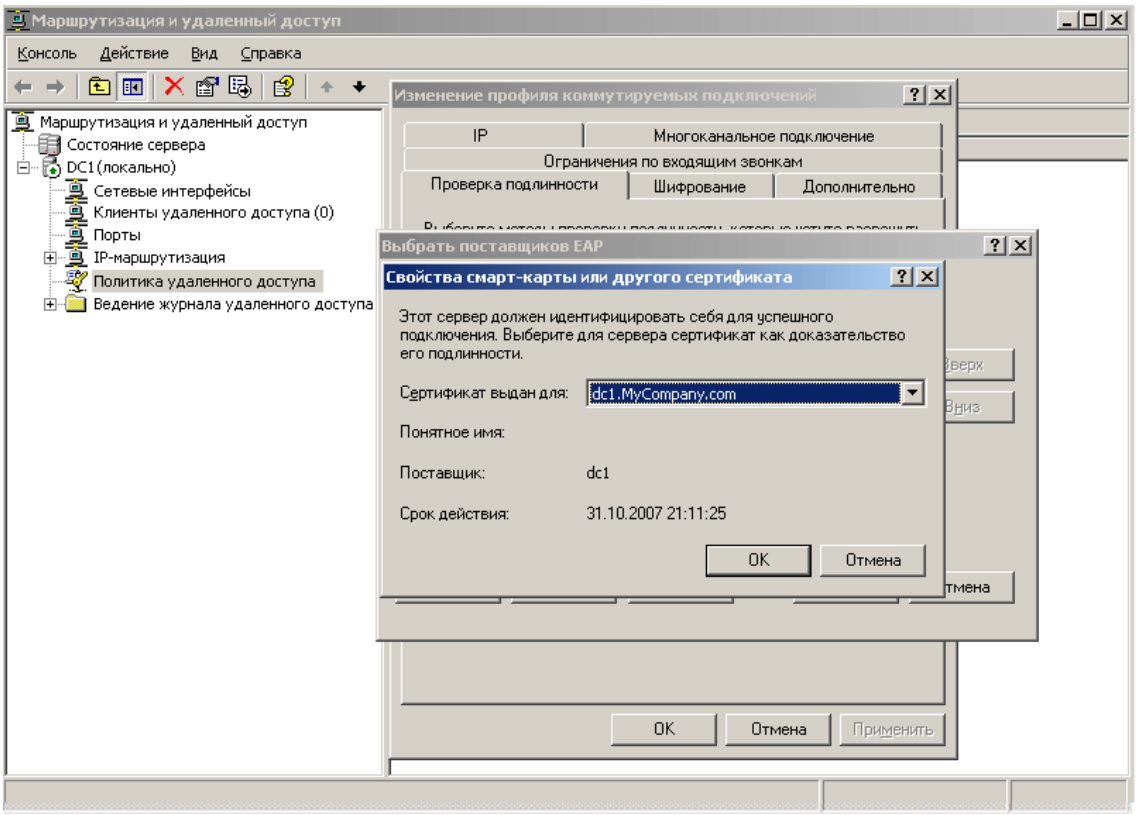
*Если в списке **Типы EAP** не появится элемент **Смарт-карта или иной сертификат**, нажмите кнопку **Добавить**, укажите **Смарт-карта или иной сертификат** и нажмите кнопку **OK**.*

*Отметьте опцию **Предоставить право удаленного доступа**.*





Выберите пункт ***Смарт-карта или иной сертификат*** *и нажмите кнопку* ***Изменить***.

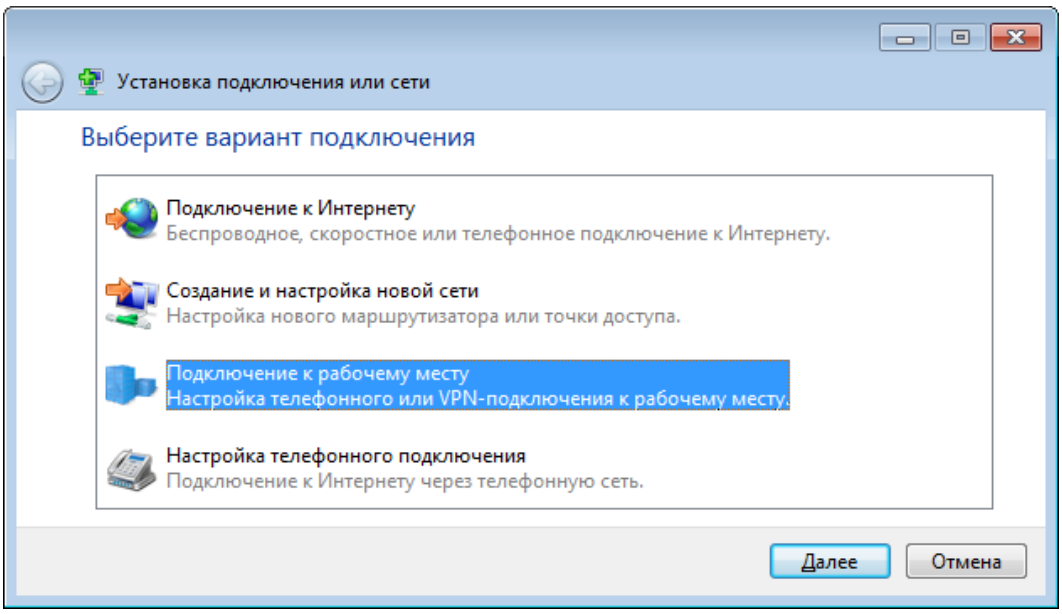


Укажите сертификат для проверки подлинности EAP и подтвердите изменения.

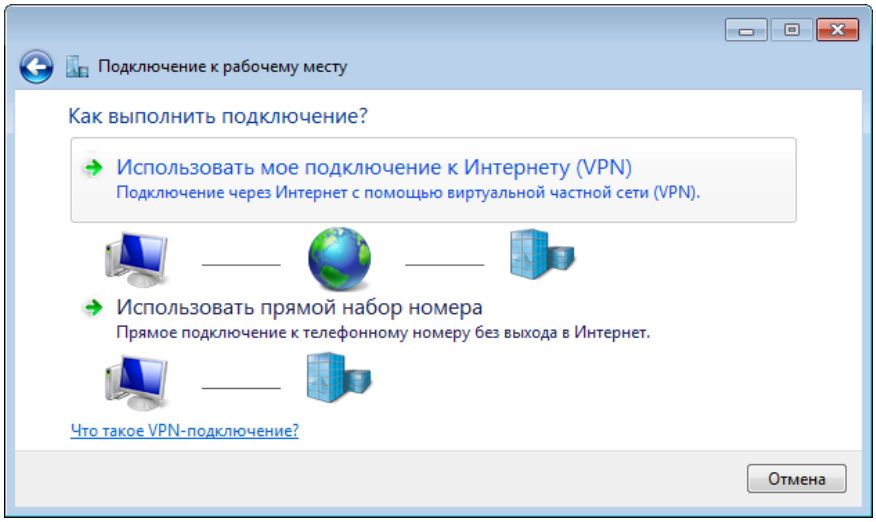
4. Настройка VPN-клиента

Процедура настройки клиентов для проверки подлинности с использованием смарт-карт может отличаться в зависимости от установленной операционной системы. Далее показана настройка VPN-соединения для Windows 7 Professional.

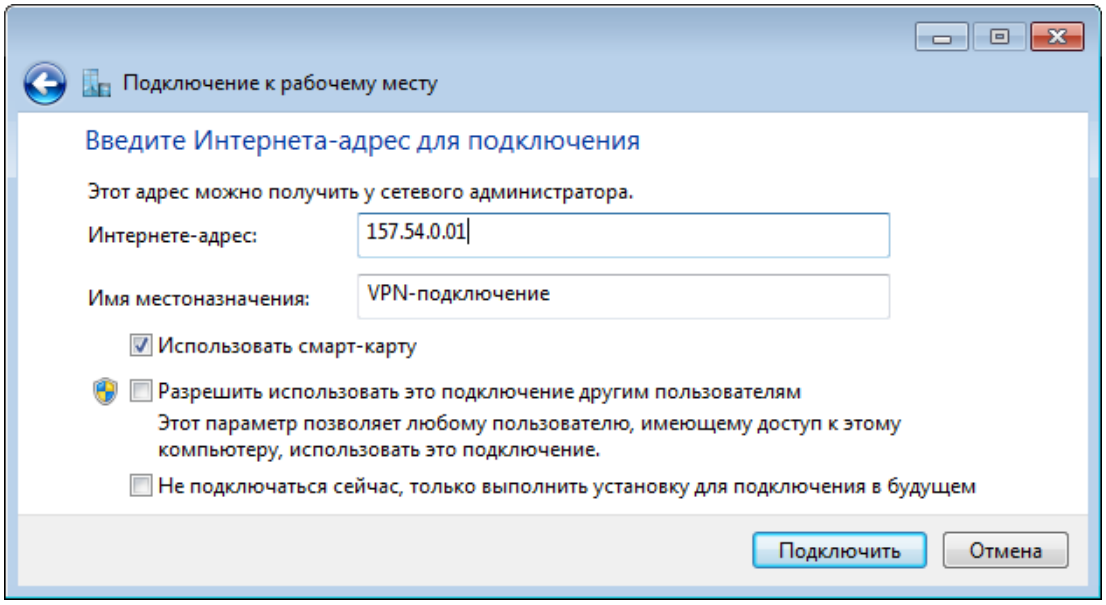
Откройте Панель управления. Выберите ***Сеть и Интернет › Центр управления сетями и общим доступом****. В разделе* ***Изменение сетевых параметров*** *выберите* ***Настройка нового подключения или сети****.*



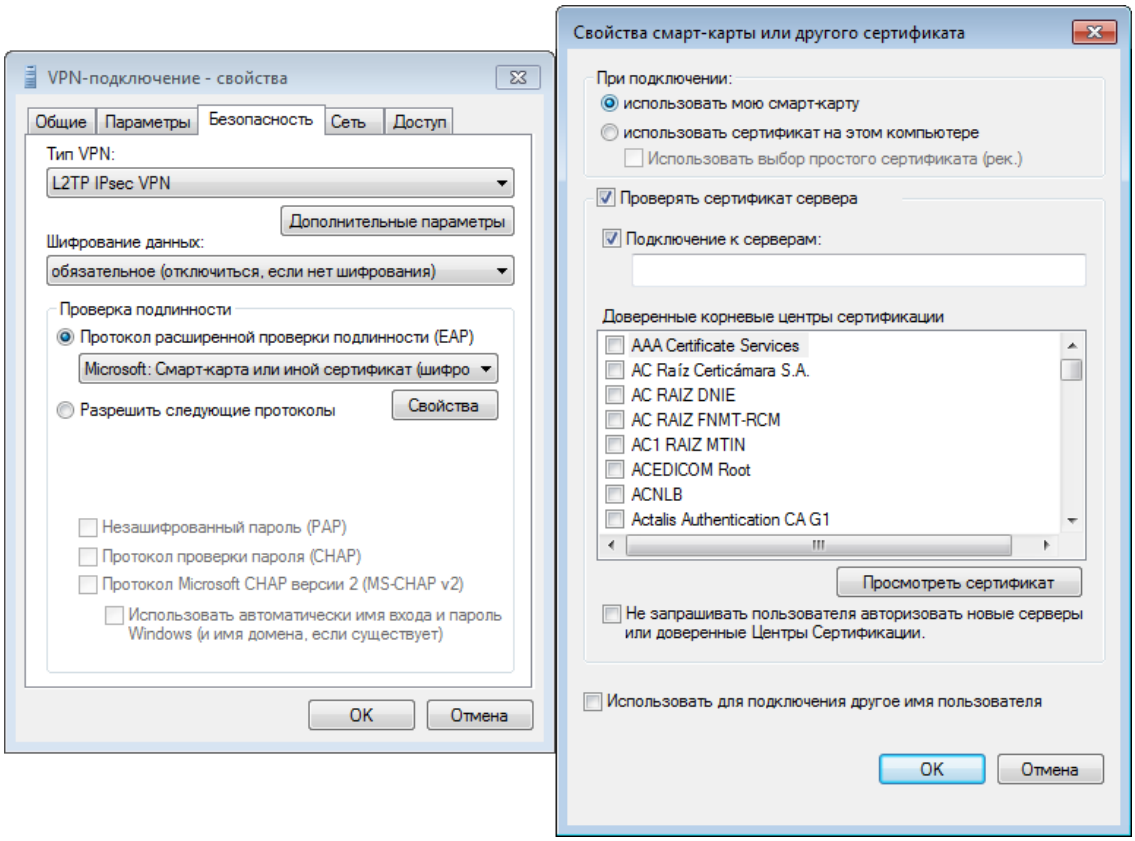
Выберите ***Подключение к рабочему месту › Использовать мое подключение к Интернету (VPN)***.



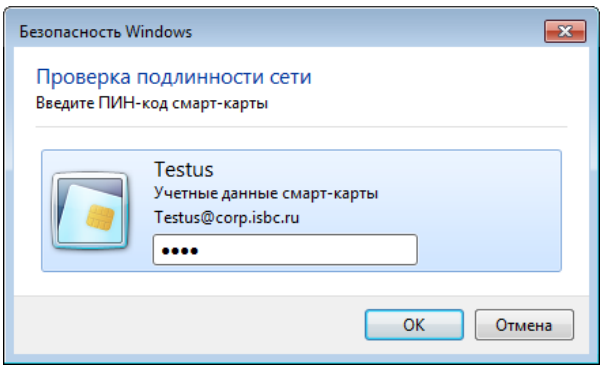
Задайте параметры подключения и отметьте ***Использовать смарт-карту***.



Выберите в списке созданное подключение и откройте в контекстном меню ***Свойства***.



При установлении VPN-соединения откроется окно ввода ПИН-кода.



Если смарт-карта не вставлена, соединение не будет установлено: