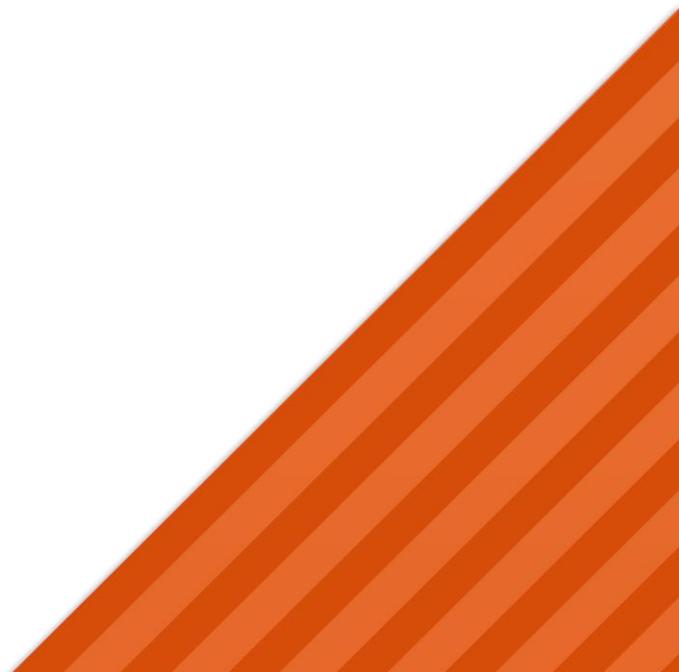




ESMART[®]

Настройка OpenVPN

на примере OpenVPN Community Edition



Содержание

1.	Общая информация.....	3
1.1	Принцип работы OpenVPN.....	4
1.2	Аутентификация OpenVPN по сертификатам.....	4
1.3	Преимущества использования смарт-карт.....	5
2.	Подготовка сертификатов.....	6
2.1	Сертификат пользователя.....	6
2.2	Получение сертификата OpenVPN-сервера.....	6
2.3	Подготовка сертификата в формате PFX.....	6
2.4	Извлечение ключа и сертификата из .pfx файла.....	8
2.5	Создание файла с параметрами Диффи-Хелмана.....	8
2.6	Список отозванных сертификатов.....	9
3.	Установка приложения OpenVPN на ОС Windows.....	10
3.1	Установка приложения OpenVPN.....	10
3.2	Основные директории, используемые OpenVPN.....	10
4.	Настройка сервера OpenVPN на базе ОС Windows.....	11
4.1	Файл конфигурации сервера OpenVPN.....	11
4.2	Запуск сервера OpenVPN.....	11
5.	Подготовка клиента OpenVPN на базе ОС Windows.....	13
5.1	Установка PKI Client.....	13
5.2	Получение идентификатора сертификата.....	13
5.3	Подготовка файла конфигурации для клиента.....	13
5.4	Подготовка компьютера клиента.....	14
5.5	Запуск клиента OpenVPN.....	16
5.6	Запуск клиента OpenVPN без прав администратора.....	17
6.	Установка OpenVPN в ОС Linux.....	18
6.1	Установка из репозитория для Ubuntu/Debian.....	18
6.2	Установка из репозитория для OpenSUSE/RedHat.....	18
6.3	Сборка из исходников для Ubuntu/Debian.....	18
6.4	Сборка из исходников для OpenSUSE/RedHat.....	18
6.5	Установка RPM-пакета.....	18
6.6	Проверка установленной версии OpenVPN.....	18
6.7	Основные директории, используемые OpenVPN.....	19
7.	Подготовка сервера OpenVPN на базе ОС Linux.....	20
7.1	Файл конфигурации сервера OpenVPN.....	20
7.2	Запуск сервера OpenVPN.....	20
8.	Подготовка клиента OpenVPN на базе ОС Linux.....	21
8.1	Установка PKI Client.....	21
8.2	Получение идентификатора сертификата.....	21
8.3	Подготовка файла конфигурации для клиентов.....	21
8.4	Подготовка компьютера клиента.....	22
8.5	Запуск клиента OpenVPN.....	23
9.	Возможные проблемы.....	24

1. Общая информация

Данное руководство предназначено для настройки OpenVPN – кроссплатформенного приложения с открытым исходным кодом для создания частных виртуальных сетей (Virtual Private Network). OpenVPN предназначен для создания защищенных шифрованных виртуальных соединений между отдельными машинами или сетями через сети общего пользования (как правило, сеть Интернет).

Все операции по настройке приведены на примере программного обеспечения OpenVPN Community Edition¹. Указанная версия является полнофункциональной, бесплатной и имеет открытый исходный код. Файлы для загрузки дистрибутивов и исходных кодов можно получить на официальном сайте сообщества OpenVPN. Рекомендуется использовать стабильные версии.

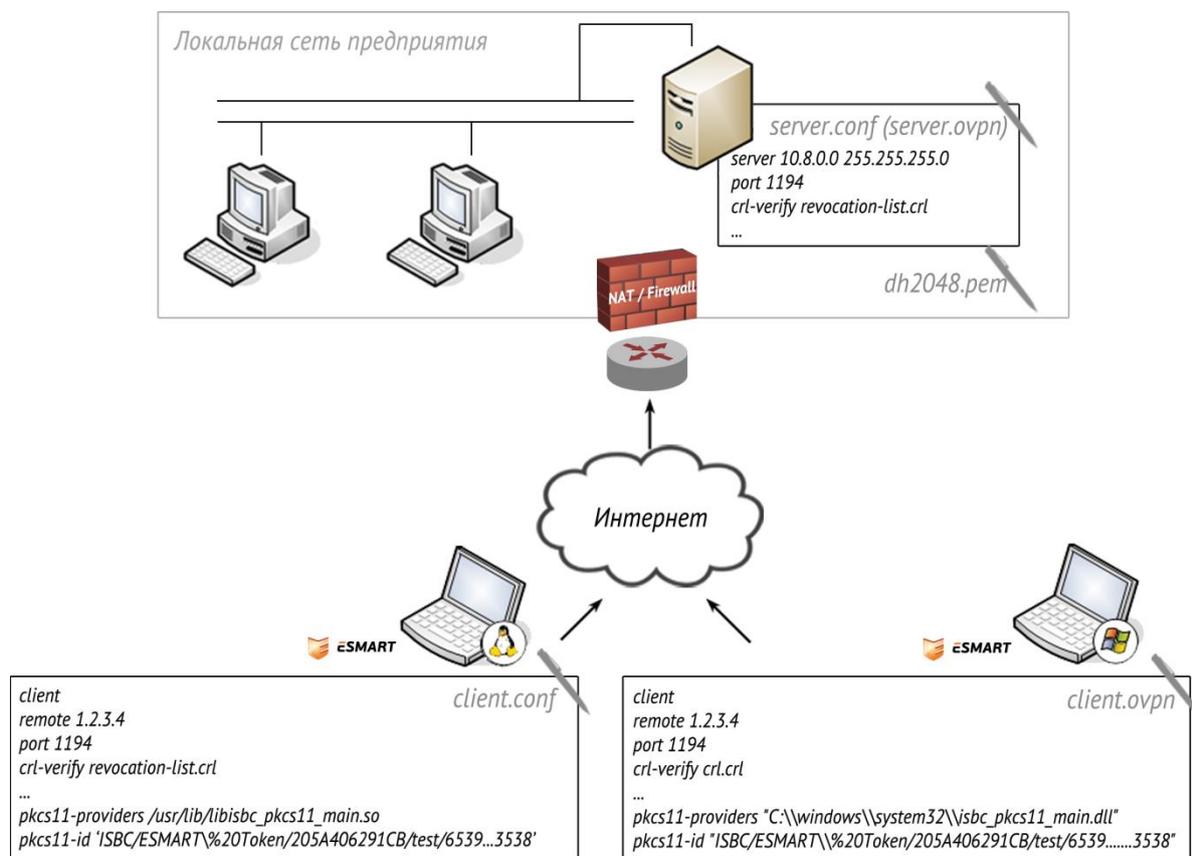
<https://openvpn.net/index.php/open-source/downloads.html>

OpenVPN успешно может применяться, даже если обе стороны (клиенты и сервер) находятся за NAT, несмотря на подмену заголовков пропускаемых пакетов. OpenVPN использует только один порт (по умолчанию 1194 UDP), который необходимо разрешить при настройке межсетевого экрана (файрвола).

Используемая технология SSL VPN позволяет объединять в сеть машины с разными операционными системами и архитектурой процессора.

В руководстве рассмотрен наиболее часто используемый сценарий использования VPN-соединения для удаленного подключения сотрудников к рабочему месту в офисе посредством RDP-соединения. Для аутентификации пользователи используют корпоративные сертификаты стандарта X.509 на смарт-карте или USB-ключе ESMART Token.

На рисунке представлена упрощенная схема использования OpenVPN в корпоративной сети.



¹ <https://openvpn.net/index.php/open-source/downloads.html>

В руководстве представлена краткая базовая информация по настройке OpenVPN соединения. Компаниям, уже использующим OpenVPN требуется внести только небольшие изменения в действующую систему.

Изменения файлов конфигурации клиентов для использования смарт-карт и USB-токенов ESMART Token вынесены в отдельные разделы **Подготовка клиента OpenVPN на базе ОС Windows** и **Подготовка клиента OpenVPN на базе ОС Linux**.

1.1 Принцип работы OpenVPN

OpenVPN позволяет создать защищенную виртуальную сеть между несколькими машинами.

Для обеспечения безопасности используются следующие механизмы:

- Аутентификация участников соединения;
- Целостность за счет механизма HMAC;
- Конфиденциальность за счет шифрования соединения.

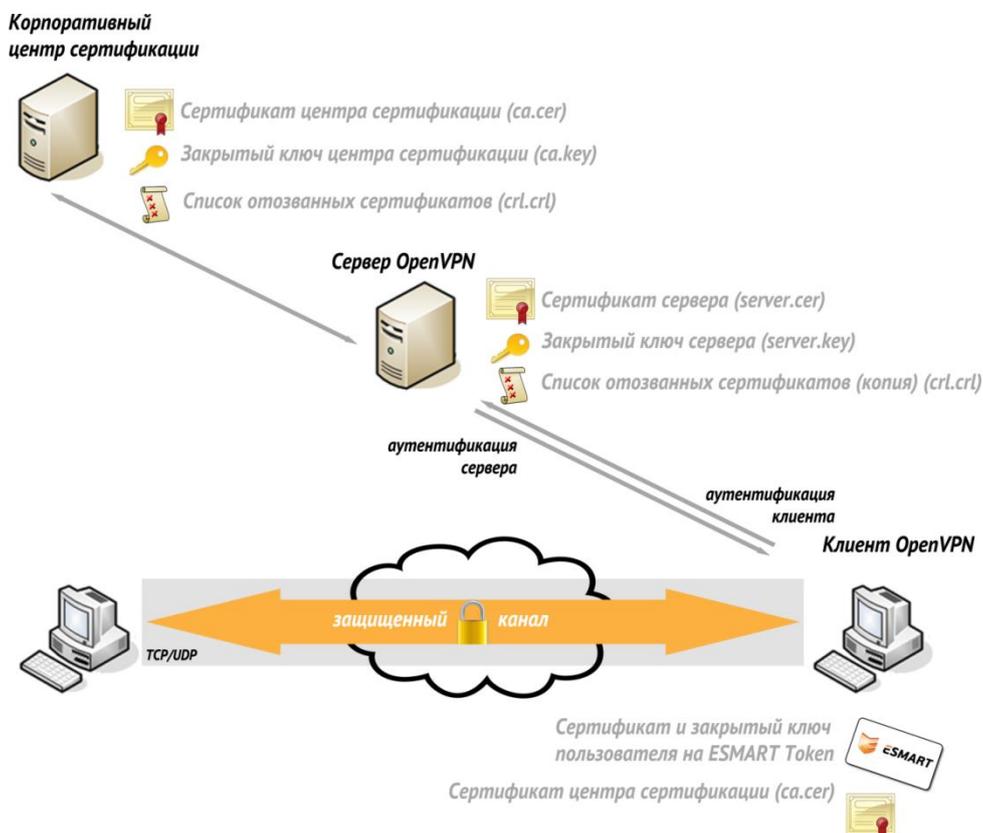
Участники соединения после успешной аутентификации вырабатывают сессионный ключ, который используется для шифрования пакетов. Для шифрования передаваемых данных используется протокол SSL/TLS. Криптографические операции выполняют библиотеки OpenSSL.

1.2 Аутентификация OpenVPN по сертификатам

OpenVPN предлагает три метода аутентификации:

- Аутентификация симметричным ключом;
- Аутентификация по логину и паролю;
- Аутентификация по сертификатам X.509.

Наиболее эффективным и надежным методом аутентификации является использование сертификатов стандарта X.509. Использование сертификатов позволяет успешно защитить соединение от атак типа MitM (Main-in-the-Middle).



При инициализации соединения происходит обмен сертификатами, на этом этапе проверяются:

- Подписаны ли сертификаты сторон доверенным корневым сертификатом (указанным в файле конфигурации сервера и клиента);
- Действительны ли сертификаты сторон (не истек ли срок действия сертификата);
- Не были ли сертификаты сторон отозваны (опционально);
- Верный ли тип сертификата используют стороны (опционально).

В случае успешной аутентификации стороны переходят к генерации сессионного ключа и установлению соединения.

1.3 Преимущества использования смарт-карт

Обычно пользователи хранят сертификат и закрытый ключ в файле формата PKCS#12 (файл с расширением .pfx в Windows и .p12 в Linux или MacOS). В этом случае доступ к закрытому ключу защищен паролем. Для повышения уровня безопасности и для удобства пользователей сертификаты клиента могут быть записаны на смарт-карту или USB-ключ.

Можно выделить следующие преимущества хранения сертификата пользователя на смарт-карте или USB-токене, а не в виде файлов .pfx:

- Все криптографические операции с закрытым ключом выполняются непосредственно на карте или USB-ключе ESMART Token, закрытый ключ с карты не извлекается;
- Применяется двухфакторная аутентификация: пользователь устанавливает соединение, предъявляя сертификат на смарт-карте или USB-ключе ESMART Token и вводит ПИН-код;
- ПИН-код карты защищен от взлома методом перебора, количество попыток задается при инициализации карты;
- После извлечения карты в системе остается только сертификат открытого ключа, не являющийся секретным;
- Дополнительно на смарт-карте может храниться корневой сертификат корпоративного центра сертификации;
- Дополнительно на смарт-карте может храниться пользовательский файл конфигурации OpenVPN в текстовом виде (в том числе в защищенном режиме, когда доступ к данным появляется только после предъявления ПИН-кода).

2. Подготовка сертификатов

Построение корпоративной сети рассмотрено на примере PKI с корпоративным центром сертификации на базе Windows Server.

В качестве альтернативных вариантов для создания сертификатов можно использовать консольные приложения OpenSSL, easy-RSA или графические приложения XCA, TinyCA или другие.

2.1 Сертификат пользователя

Клиентская часть OpenVPN может использовать сертификаты на базе стандартного шаблона **Пользователь со смарт-картой** (SmartCard User), записанные на смарт-карту или USB-ключ ESMART Token. Таким образом, пользователь может использовать смарт-карту с одним и тем же сертификатом для входа в операционную систему, для подписи/шифрования файлов и для аутентификации при создании защищенного VPN-соединения.

Использование одного сертификата позволяет упростить работу системных администраторов по управлению PKI (выдаче сертификатов пользователей, обновлению и отзыву сертификатов). В случае необходимости, на смарт-карту или USB-ключ ESMART Token можно поместить и дополнительный отдельный сертификат, предназначенный исключительно для установления VPN-соединения.

Процесс настройки центра сертификации, получения сертификатов пользователей на базе шаблона **Пользователь со смарт-картой** описаны в руководствах по развертыванию PKI на базе Windows Server 2003 и Windows Server 2008.

2.2 Получение сертификата OpenVPN-сервера

Для сертификата OpenVPN сервера может использоваться шаблон, содержащий параметр применения ключа **Проверка подлинности сервера** (Server authentication). Данному требованию соответствуют стандартные шаблоны **Компьютер** (Computer) и **Веб-сервер** (Web-Server).

При использовании центра сертификации на базе Windows Server Enterprise Edition возможно создание производных шаблонов сертификатов с требуемыми параметрами.

Сертификат сервера можно получить одним из двух способов:

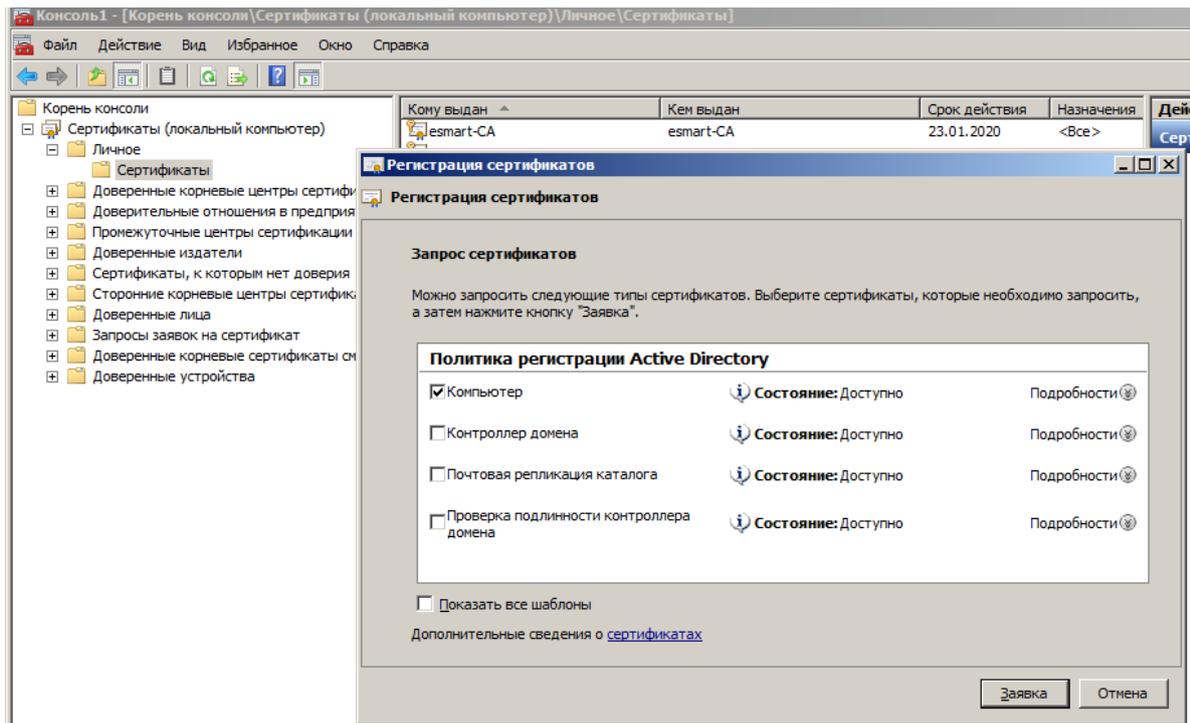
1. Запросить сертификат из консоли управления mmc (с оснасткой «Сертификаты для компьютера»). При этом данные компьютера в сертификате будут получены из Active Directory. Данный способ наилучшим образом подходит для компьютеров, входящих в домен.
2. Создать закрытый ключ сервера и запрос на сертификат посредством консольных приложений OpenSSL или Easy-RSA. Затем выпустить сертификат через веб-интерфейс центра сертификации. Подходит для машин не входящих в домен.

2.3 Подготовка сертификата в формате PFX

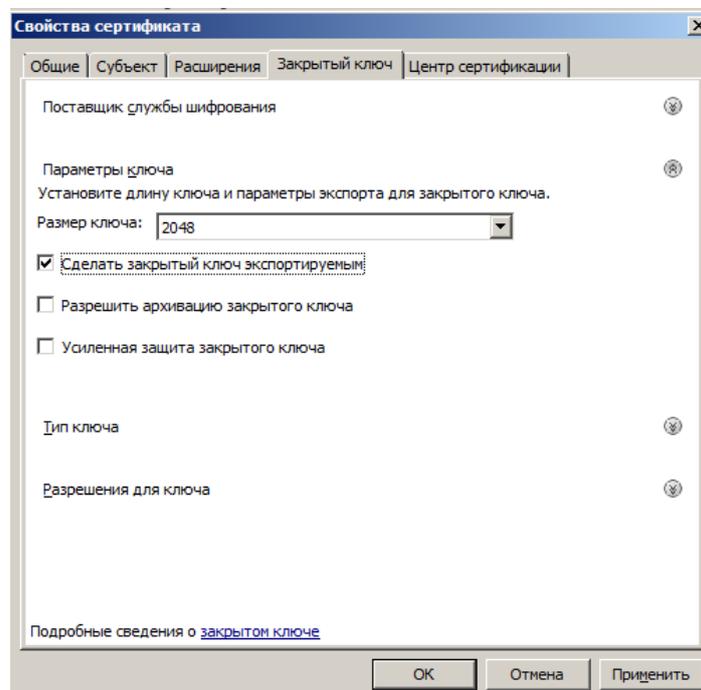
Центр сертификации на базе Windows Server позволяет получить сертификат и закрытый ключ в формате .pfx. Далее описан процесс получения ключа через консоль mmc с оснасткой «Сертификаты» для компьютера².

Для сервера выбран сертификат по стандартному шаблону **Компьютер** (Computer).

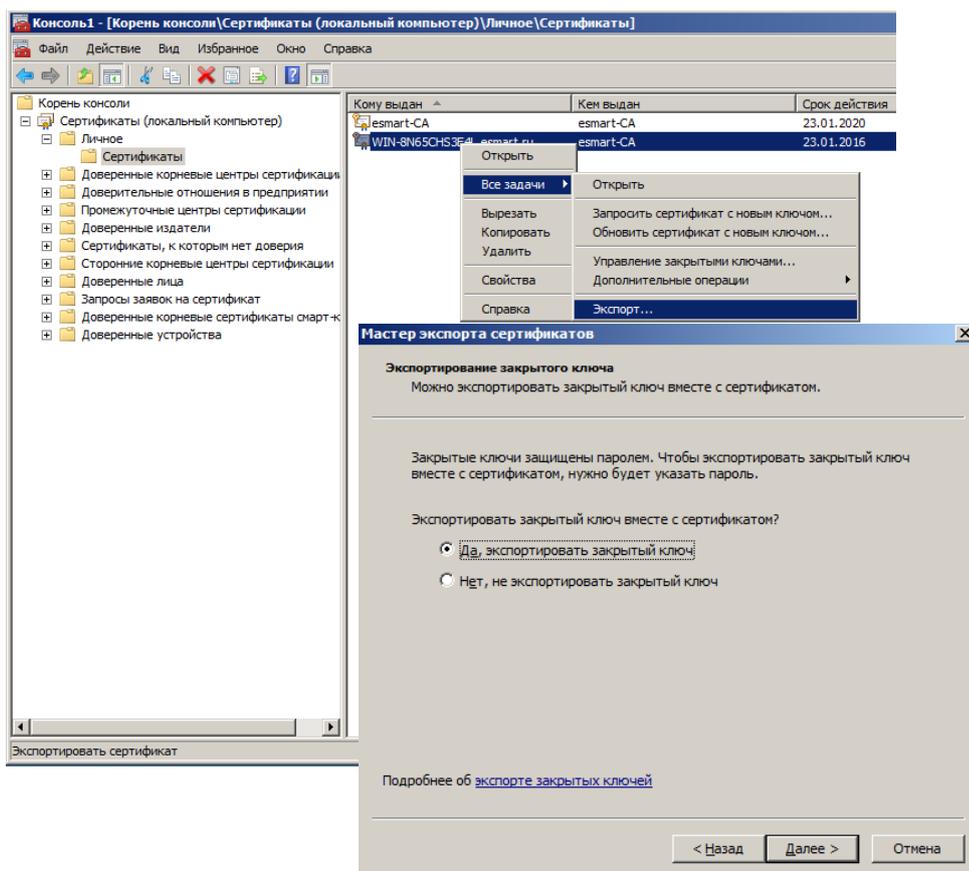
² Консоль certmgr.msc не может использоваться, т.к. позволяет получить сертификат только для текущего пользователя



При выдаче сертификата необходимо отметить опцию **Сделать закрытый ключ экспортируемым**. Для этого нужно развернуть вкладку **Подробности** (Details) и нажать кнопку **Свойства** (Properties). В окне свойств сертификата на вкладке **Закрытый ключ** (Private Key) следует отметить опцию **Сделать закрытый ключ экспортируемым** (Make Private key exportable).



Выданный сертификат необходимо экспортировать в файл .pfx, выбрав в контекстном меню **Все задачи > Экспорт...** (All tasks > Export).



Выберите формат экспорта: *Файл обмена личной информацией – PKCS#12 (.PFX)*. Укажите путь к будущему файлу и пароль. В данном руководстве файл сертификата OpenVPN сервера имеет название **server.pfx**.

2.4 Извлечение ключа и сертификата из .pfx файла

OpenVPN необходимо предоставить ключи в виде текстовых файлов. Для извлечения закрытого ключа и сертификата из файла .pfx можно использовать консольное приложение OpenSSL, которое входит в состав пакета OpenVPN.

Извлечение закрытого ключа в текстовый файл (.key или .pem) без защиты паролем:

```
openssl pkcs12 -in server.pfx -out serverkey.key -nodes
```

Извлечение сертификата открытого ключа в текстовый файл (.cer или .crt):

```
openssl pkcs12 -in server.pfx -out serverkey.cer -clcerts
```

2.5 Создание файла с параметрами Диффи-Хеллмана

Для выработки совместного симметричного сессионного ключа получаем параметры Диффи-Хеллмана командой:

```
openssl dhparam -out dh2048.pem 2048
```

Путь к файлу с параметрами Диффи-Хеллмана указывается в файле конфигурации сервера OpenVPN. В настоящее время достаточный размер составляет 2048 байт (последний параметр команды). Генерация параметров более 4096 могут занять очень длительное время и значительно увеличить вычислительную нагрузку на обе стороны при установлении соединения.

2.6 Список отозванных сертификатов

Чтобы повысить безопасность системы, в файле конфигурации в директиве `crl-verify` можно указать путь к файлу списка отозванных сертификатов (Certificate Revocation List). Файл считывается заново при подключении каждого клиента. Кроме того, OpenVPN проверяет список отозванных сертификатов при каждом пересогласовании параметров SSL-соединения, по умолчанию раз в час. При необходимости отключить клиента можно вручную, используя интерфейс управления OpenVPN.

Использовать директиву `crl-verify` достаточно только в конфигурации сервера. В зависимости от используемого центра сертификации (Windows Server, XCA, OpenSSL и др.) доступ к файлу и процедура обновления списка может быть организована по разному.

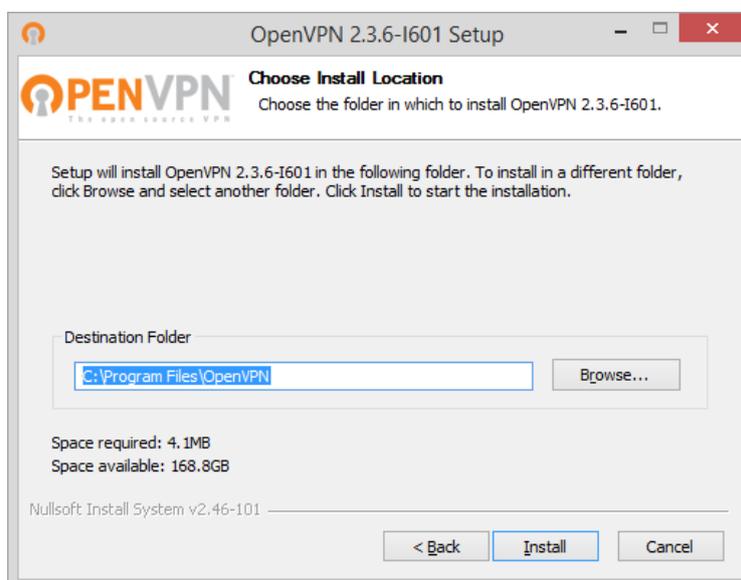
В файлах конфигурации клиентов `crl-verify` может присутствовать, например, если в компании используется несколько серверов OpenVPN. Если в файл конфигурации клиента включена директива `crl-verify`, файл списка отозванных сертификатов должен быть доступен через Интернет.

Файл списка отозванных сертификатов может иметь расширение `.crl` или `.pem`.

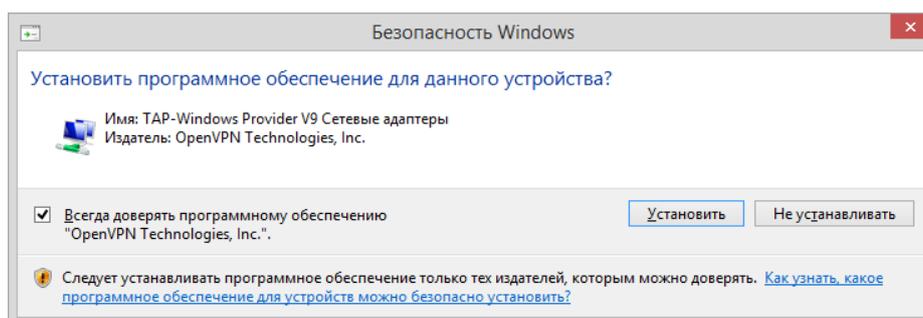
3. Установка приложения OpenVPN на ОС Windows

3.1 Установка приложения OpenVPN

Для установки OpenVPN в ОС Windows используется программа-инсталлятор с графическим интерфейсом, требуются права администратора.



Все пути в руководстве указаны в соответствии с директорией установки OpenVPN по умолчанию. OpenVPN использует виртуальный сетевой адаптер. В Windows по умолчанию данный тип адаптеров не предусмотрен. Установить виртуальный адаптер можно как при установке пакета OpenVPN, так и отдельно³.



3.2 Основные директории, используемые OpenVPN

При стандартной установке:

C:\Program Files\OpenVPN\bin\

Бинарные файлы

C:\Program Files\OpenVPN\bin\config

Файлы конфигурации

C:\Program Files\OpenVPN\sample-config

Примеры файлов конфигурации

³ <https://openvpn.net/index.php/open-source/downloads.html>

4. Настройка сервера OpenVPN на базе OS Windows

4.1 Файл конфигурации сервера OpenVPN

В данном разделе описаны только базовые принципы настройки сервера на базе OpenVPN и представлен минимальный файл конфигурации, необходимый для тестирования соединения.

Если OpenVPN уже настроен и используется в организации, можно перейти к разделу **Подготовка клиента OpenVPN на базе ОС Windows**. Вносить изменения в файл конфигурации сервера, как правило, не требуется.

Приведенные в данном руководстве файлы конфигурации построены на базе файлов-шаблонов из директории `C:\Program Files\OpenVPN\sample-config`.

Пример файла конфигурации **server.ovpn**:

```
port 1194 # Порт по умолчанию
proto udp # TCP или UDP-соединение, запись должна быть одинакова на клиенте и сервере
dev tun # Определяет тип интерфейса, запись должна быть одинакова на клиенте и сервере
ca ca.cer # Корневой сертификат центра сертификации
cert server.cer # Сертификат сервера
key server.key # Закрытый ключ сервера
dh dh2048.pem # Параметры Диффи-Хеллмана 2048 бит
server 10.8.0.0 # Директива выделить для сервера и подключающихся клиентов указанную подсеть
255.255.255.0
keepalive 10 120 # Параметры поддержания соединения: ping каждые 10 секунд, после 120 секунд неактивности соединение считается разорванным
comp-lzo # Компрессия, запись должна быть одинакова на клиенте и сервере
persist-key # Не запрашивать ключ заново при разрыве соединения, не перезапускать виртуальный адаптер
persist-tun
topology subnet # Рекомендованный параметр, если не требуется совместимость с OpenVPN 2.0.9 и ниже
crl-verify # Проверять, не был ли отозван сертификат пользователя по списку отозванных сертификатов
revocation_list.crl
client-to-client # Разрешить подключившимся клиентам видеть друг друга
```

Примечания:

При указании пути к любому файлу обратный слеш « \ » необходимо удвоить. Если путь к файлам содержит пробелы, следует поместить его в кавычки, например:

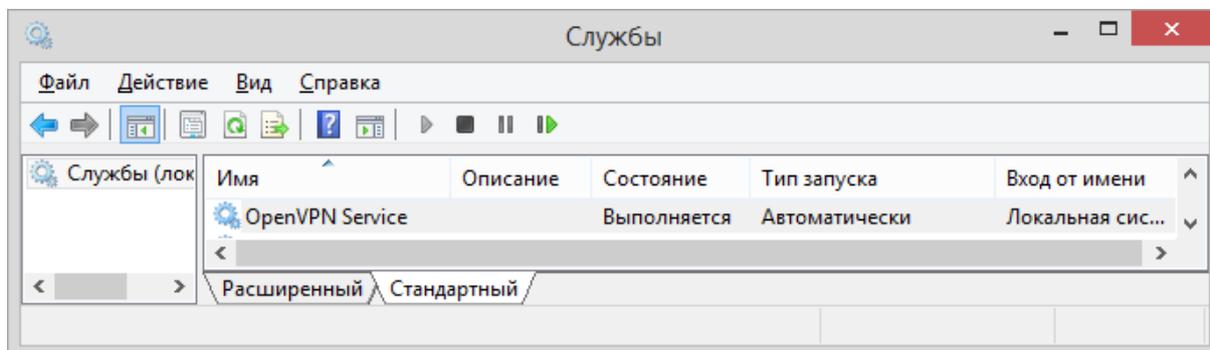
```
"C:\\Program Files\\OpenVPN\\config\\keys\\server.cer"
```

4.2 Запуск сервера OpenVPN

Сервер OpenVPN может запускаться как вручную, так и в качестве сервиса.

Для каждого файла конфигурации в директории `C:\Program Files\OpenVPN\config` будет запущен отдельный процесс OpenVPN. Файлы конфигурации для автоматического запуска должны иметь расширение `.ovrp`.

Для автоматического запуска требуется выставить способ запуска службы OpenVPN – Автоматически или Автоматически (отложенный запуск).



5. Подготовка клиента OpenVPN на базе ОС Windows

5.1 Установка PKI Client

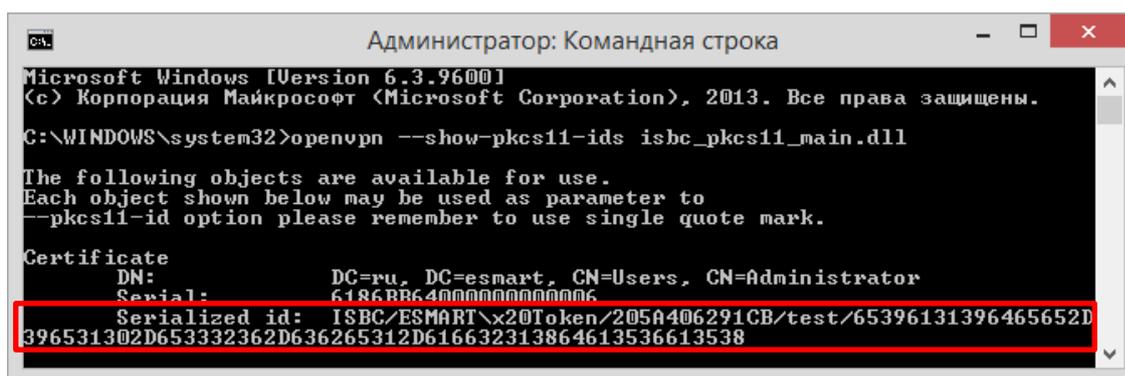
На клиентских компьютерах для работы OpenVPN со смарт-картами и USB-ключами ESMART Token в ОС Windows должны быть установлены библиотеки для работы по стандарту PKCS#11. Необходимые библиотеки входят в состав бесплатного приложения ESMART PKI Client. Установка приложения ESMART PKI Client описана в документе **ESMART PKI Client – Руководство администратора**.

Опытные пользователи могут установить библиотеки вручную, следуя указаниям в руководстве **ESMART Token – PKCS#11**.

5.2 Получение идентификатора сертификата

OpenVPN требуется явно указать, какой сертификат будет использоваться для конкретного соединения. Для этого в файле конфигурации указывается идентификатор сертификата (Serialized id) на носителе. Чтобы получить идентификатор, выполните следующую команду:

```
openvpn --show-pkcs11-ids "путь_к_библиотеке_isbc_pkcs11_main.dll"  
openvpn --show-pkcs11-ids "C:\Windows\System32\isbc_pkcs11_main.dll"
```



```
Администратор: Командная строка  
Microsoft Windows [Version 6.3.9600]  
(c) Корпорация Майкрософт (Microsoft Corporation), 2013. Все права защищены.  
C:\WINDOWS\system32>openvpn --show-pkcs11-ids isbc_pkcs11_main.dll  
The following objects are available for use.  
Each object shown below may be used as parameter to  
--pkcs11-id option please remember to use single quote mark.  
Certificate  
DN: DC=ru, DC=esmart, CN=Users, CN=Administrator  
Serial: 6186BB64000000000000000000000000  
Serialized id: ISBC/ESMART\x20Token/205A406291CB/test/65396131396465652D  
396531302D653332362D636265312D616632313864613536613538
```

Примечание:

ISBC – Имя производителя токена/карты

ESMART\%20Token – Наименование устройства (%20 замещает пробел)

205A406291CB – Серийный номер устройства

test – Название карты/токена, которое было указано при инициализации

65396131396465652D396531302D653332362D636265312D616632313864613536613538 – Идентификатор ключа

5.3 Подготовка файла конфигурации для клиента

Пример файла конфигурации:

```
client # Подключаться в качестве клиента  
proto udp # TCP или UDP-соединение, запись должна быть одинакова на клиенте и сервере  
dev tun # Определяет тип интерфейса, запись должна быть одинакова на клиенте и сервере
```

```

remote 1.2.3.4 1194      # IP-адреса или DNS-имена серверов с указанием портов
remote 2.3.4.5 1194      # remote-random – подключаться к произвольному из указанных серверов
remote-random           для распределения нагрузки

persist-key             # Не запрашивать ключ заново при разрыве соединения, не перезапускать
persist-tun            виртуальный адаптер

ca ca.crt              # Корневой сертификат центра сертификации

remote-cert-tls        # Проверка типа сертификата сервера, используется вместо устаревшей
server                 директивы ns-cert-type server

comp-lzo               # Компрессия, запись должна быть одинакова на клиенте и сервере

# cert client.crt      # Закрытый ключ и сертификат клиента в виде файлов необходимо за-
# key client.key        комментировать или удалить.

```

Замените параметры

```

cert client.crt
key client.key
на
pkcs11-providers "C:\windows\system32\isbc_pkcs11_main.dll"
pkcs11-id
"ISBC/ESMART\%20Token/205A406291CB/test/65396131396465652D396531302D653332362D6326
5312D616632313864613536613538"

```

Примечание:

Идентификатор ключа необходимо писать в одну строку и заключить в двойные кавычки.

Необходимо удвоить каждую обратную косую черту « \ » при указании пути к файлу библиотеки `isbc_pkcs11_main.dll` и в идентификаторе ключа «`ESMART\%20Token`».

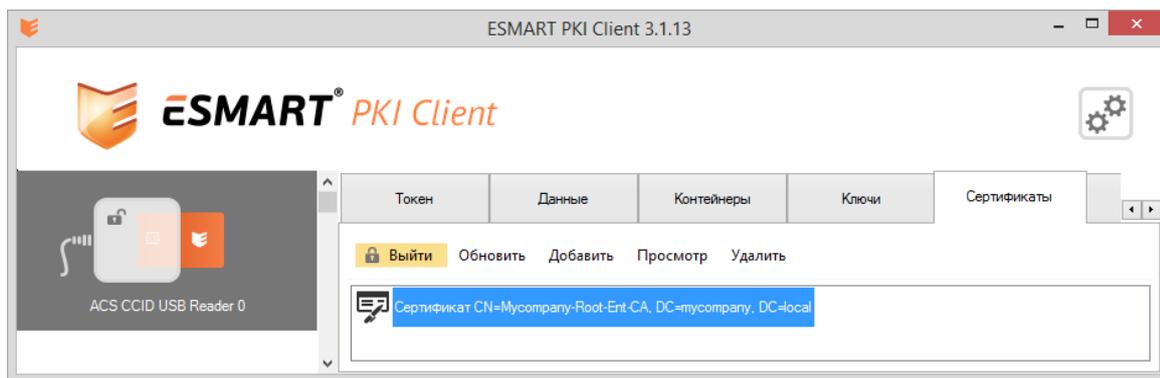
5.4 Подготовка компьютера клиента

При подготовке компьютера клиента потребуются текстовый файл конфигурации и файл корневого сертификата (в примере `ca.cer`). Оба файла можно записать на ESMART Token. В этом случае все необходимое для установления соединения будет храниться на одном носителе. Установочный файл OpenVPN при необходимости можно скачать с сайта openvpn.net.

Для работы с сертификатами и данными рекомендуется установить бесплатное графическое приложение ESMART PKI Client. Также считать данные, которые хранятся на карте можно с помощью консольного приложения `pkcs11-tool`, входящего в пакет OpenSC.

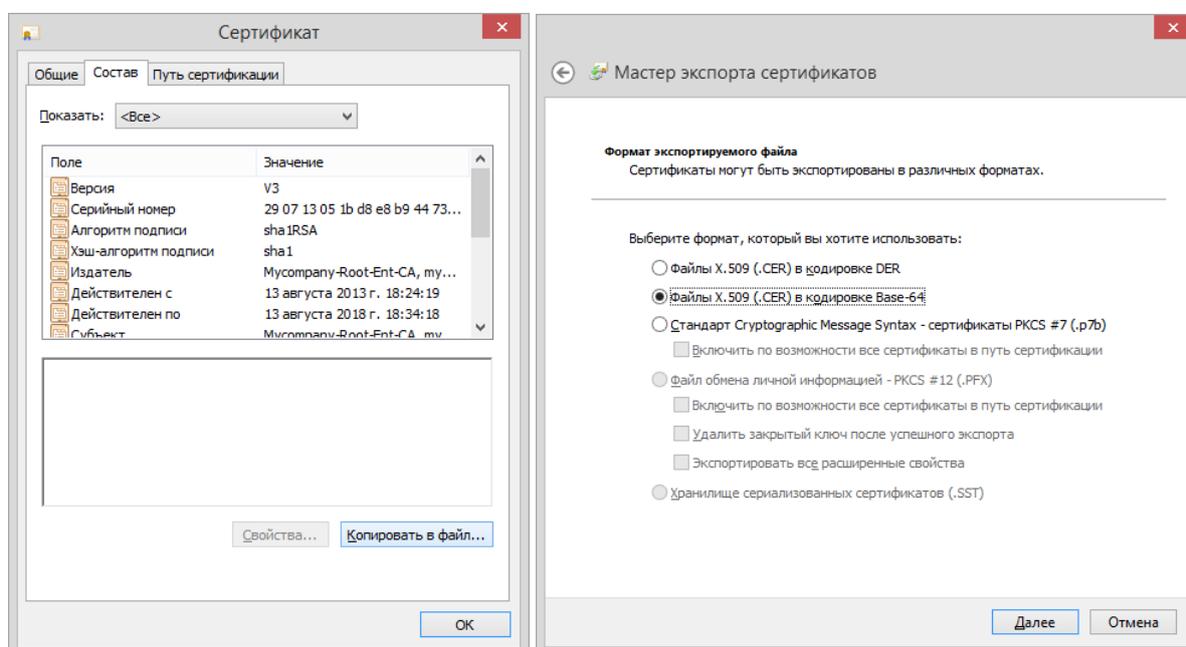
Запись корневого сертификата на ESMART Token

Авторизуйтесь на карте в ESMART PKI Client. Чтобы записать корневой сертификат на смарт-карту или USB-ключ ESMART Token, откройте вкладку «Сертификаты» и нажмите добавить. Откройте файл сертификата (в примере `ca.cer`).



Сохранение корневого сертификата в файл

Чтобы перенести сертификат с карты в файл, в ESMART PKI Client дважды нажмите левой кнопкой мыши на сертификате. В открывшемся окне на вкладке **Состав** выполните операцию **Копировать в файл**. Формат экспортируемого файла: **Файлы X.509 (.CER) в кодировке Base64**.



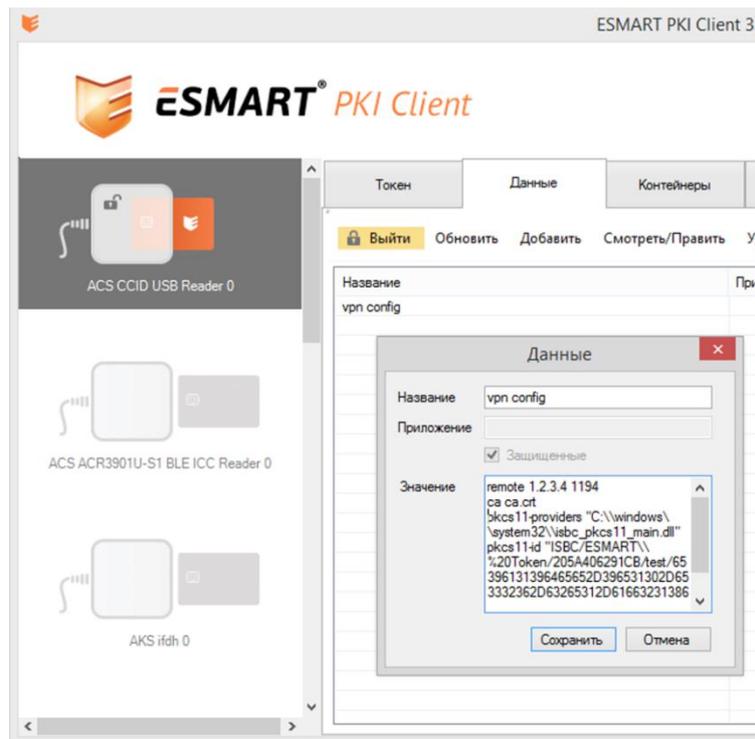
Путь к сохраненному файлу необходимо указать в файле конфигурации:

```
ca "C:\Program Files\OpenVPN\config\keys\ca.cer"
```

Запись файла конфигурации на ESMART Token

Текстовый файл конфигурации для клиента также может быть записан на смарт-карту или USB-ключ ESMART Token. Доступ к файлу (соответственно и информация об используемых IP-адресах и нестандартных портах OpenVPN сервера) может быть защищена ПИН-кодом.

Чтобы создать блок данных, который виден только после предъявления ПИН-кода, при создании блока через ESMART PKI Client отметьте галочкой параметр **Защищенные**. Скопируйте текст файла конфигурации в поле **Значение** и нажмите **Сохранить**.



Копирование файла конфигурации в файл

Откройте в ESMART PKI Client вкладку **Данные**. Откройте соответствующий блок данных и скопируйте содержимое из поля значение. Сохраните скопированный в файл с помощью любого текстового редактора. Рекомендуемый путь файла C:\Program Files\OpenVPN\config\ и рекомендуемое расширение .ovpn. При необходимости исправьте путь к файлу корневого сертификата, скопированного с карточки на предыдущем этапе.

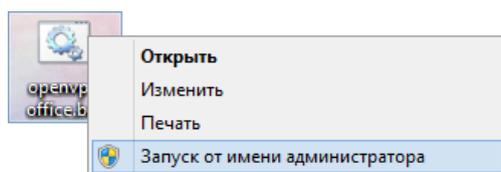
5.5 Запуск клиента OpenVPN

При запуске клиентской части в качестве сервиса, OpenVPN не имеет возможности получить ПИН-код пользователя для авторизации по смарт-карте. В графическом приложении OpenVPN для Windows также не предусмотрено графическое окно ввода ПИН-кода, поэтому приложение не может использоваться при подключении с авторизацией по смарт-картам.

Для удобства запуска OpenVPN вручную рекомендуется создать пакетный .bat файл следующего содержания:

```
openvpn "путь к файлу конфигурации"
openvpn "C:\Program Files\OpenVPN\config\client.ovpn"
```

Данный файл можно поместить на рабочий стол или в удобную для пользователя папку. Запускать .bat файл следует, выбрав в контекстном меню файла опцию **Запуск от имени администратора**. Права администратора требуются для того, чтобы были добавлены сетевые маршруты, полученные из файла конфигурации.



Запуск от имени администратора также можно выставить в свойствах .bat файла.

5.6 Запуск клиента OpenVPN без прав администратора

В ряде случаев может потребоваться запускать OpenVPN на корпоративном ПК без прав администратора.

При запуске OpenVPN без прав администратора в систему не будут внесены маршруты, заданные в файле конфигурации. Поэтому системному администратору необходимо заранее однократно прописать постоянные маршруты.

```
route -p add IP-address mask MASK GATEWAY
route -p add 1.2.3.4 mask 255.255.255.0 192.168.10.1
```

6. Установка OpenVPN в ОС Linux

Для сборки из исходников и установки OpenVPN в ОС Linux требуются права суперпользователя. Возможность использования смарт-карт предусмотрена в версии OpenVPN 2.1 и выше.

6.1 Установка из репозитория для Ubuntu/Debian

Для установки OpenVPN из репозитория требуются права суперпользователя.

```
sudo apt-get install openvpn
```

6.2 Установка из репозитория для OpenSUSE/RedHat

Для установки OpenVPN из репозитория требуются права суперпользователя.

```
sudo zypper install openvpn
```

6.3 Сборка из исходников для Ubuntu/Debian

Для сборки OpenVPN из исходного кода необходимо удовлетворить следующие зависимости: `openssl-devel`, `lzo-devel`, `pat-devel`

Чтобы распаковать архив, используется команда:

```
tar xzf openvpn-[version].tar.gz
```

Затем в корневой директории распакованного архива выполняются команды:

```
./configure  
make  
make install
```

При установке должны быть удовлетворены следующие зависимости: `openssl`, `lzo`, `pat`

6.4 Сборка из исходников для OpenSUSE/RedHat

Для дистрибутивов Linux с системой управления пакетами RPM рекомендуется сначала собрать из исходников RPM-пакет, а затем установить его.

Для сборки необходимо удовлетворить следующие зависимости: `openssl-devel`, `lzo-devel`, `pat-devel`

Для сборки RPM-пакета используется утилита `rpmbuild`:

```
sudo rpmbuild -tb openvpn-[version].tar.gz
```

RPM-файл по умолчанию будет помещен в директорию

`/usr/src/packages/BUILD/` (OpenSUSE) или `/usr/src/redhat/BUILD` (RedHat).

6.5 Установка RPM-пакета

Для установки используется команда

```
rpm -ivh openvpn-[version].rpm
```

При установке должны быть удовлетворены следующие зависимости: `openssl`, `lzo`, `pat`

6.6 Проверка установленной версии OpenVPN

Для проверки версии OpenVPN в Ubuntu/Debian используется команда:

```
dpkg -l openvpn
```

Для проверки версии OpenVPN в OpenSUSE/RedHat используется команда:

```
rpm -q openvpn
```

6.7 Основные директории, используемые OpenVPN

`/etc/openvpn`

`/etc/init.d/openvpn`

`/usr/sbin/rcopenvpn`

`/usr/sbin/openvpn`

`/usr/share/doc/openvpn` или

`/usr/share/doc/package/openvpn`

`/usr/share/doc/openvpn/examples/
sample-config-files`

или `/usr/share/doc/package/openvpn/examples/
sample-config-files`

Файлы конфигурации и ключи

Скрипты для запуска/остановки

Бинарные файлы

Документация

Примеры конфигурационных файлов

7. Подготовка сервера OpenVPN на базе ОС Linux

7.1 Файл конфигурации сервера OpenVPN

В данном разделе описаны только базовые принципы настройки сервера на базе OpenVPN и представлен минимальный файл конфигурации, необходимый для тестирования соединения.

Если OpenVPN уже настроен и используется в организации можно перейти к разделу **Подготовка клиента OpenVPN на базе ОС Linux**. Вносить изменения в файл конфигурации сервера, как правило, не требуется.

Приведенные в данном руководстве файлы конфигурации построены на базе файлов-шаблонов из директории `/usr/share/doc/openvpn/examples/sample-config-files` или `/usr/share/doc/package/openvpn/examples/sample-config-files`

Пример файла конфигурации **server.conf**:

```
port 1194 # Порт по умолчанию
proto udp # TCP или UDP-соединение, запись должна быть одинакова на клиенте и сервере
dev tun # Определяет тип интерфейса, запись должна быть одинакова на клиенте и сервере
ca ca.cert # Корневой сертификат центра сертификации
cert server.cert # Сертификат сервера
key server.key # Закрытый ключ сервера
dh dh2048.pem # Параметры Диффи-Хеллмана 2048 бит
server 10.8.0.0 # Выделить для сервера и подключающихся клиентов указанную подсеть
255.255.255.0
keepalive 10 120 # Параметры поддержания соединения: ping каждые 10 секунд, после 120 секунд соединение считается разорванным
comp-lzo # Компрессия, запись должна быть одинакова на клиенте и сервере
persist-key # Не запрашивать ключ заново при разрыве соединения, не перезапускать виртуальный адаптер
persist-tun
topology subnet # Рекомендованный параметр, если не требуется совместимость с OpenVPN 2.0.9 и ниже
user nobody # Запускать демон от имени определенного пользователя с пониженными правами.
group nobody
crl-verify # Проверять, не был ли отозван сертификат пользователя по списку
revocation_list.crl отозванных сертификатов
client-to-client # Разрешить подключившимся клиентам видеть друг друга
```

7.2 Запуск сервера OpenVPN

Запускать сервер OpenVPN можно вручную или в фоновом режиме.

Если OpenVPN был установлен при помощи RPM или DEB пакета, в операционной системе будут созданы соответствующие скрипты запускаемых служб (`initscript`). При запуске в фоновом режиме новый процесс (демон) будет создаваться для каждого файла конфигурации в директории `/etc/openvpn`. Файл конфигурации должен иметь расширение `.conf` (в отличие от `.ovpn` для Windows).

8. Подготовка клиента OpenVPN на базе ОС Linux

8.1 Установка PKI Client

На клиентской машине должны присутствовать библиотеки для работы со смарт-картами и USB-ключами ESMART Token. Библиотеки могут быть установлены в составе графического приложения ESMART PKI Client (см. **ESMART PKI Client – Руководство администратора**) или отдельно (см. руководство **ESMART Token – PKCS#11**).

8.2 Получение идентификатора сертификата

OpenVPN требуется явно указать, какой сертификат будет использоваться для конкретного соединения. Для этого в файле конфигурации указывается идентификатор сертификата (Serialized id) на носителе. Чтобы получить идентификатор, выполните следующую команду:

```
openvpn --show-pkcs11-ids "путь к библиотеке libisbc_pkcs11_main.so"
openvpn --show-pkcs11-ids /usr/lib/libisbc_pkcs11_main.so
```

```
julia@julia-VirtualBox:~$ openvpn --show-pkcs11-ids /usr/lib/libisbc_pkcs11_main
.so
The following objects are available for use.
Each object shown below may be used as parameter to
--pkcs11-id option please remember to use single quote mark.
Certificate
c  DN: DC=ru, DC=esmart, CN=Users, CN=Administrator
   Serial: 6186BB64000000000006
   Serialized id: ISBC/ESMART\x20Token/205A406291CB/test/65396131396465652D
396531302D653332362D636265312D616632313864613536613538
```

Примечание:

ISBC – Имя производителя

ESMART\x20Token – Наименование устройства (последовательность \x20 замещает пробел)

205A406291CB – Серийный номер устройства

test – название карты/токена, которое было указано при инициализации

65396131396465652D396531302D653332362D636265312D616632313864613536613538 –
Идентификатор ключа

8.3 Подготовка файла конфигурации для клиентов

Пример файла конфигурации

```
client # Подключаться в качестве клиента
proto udp # TCP или UDP-соединение, запись должна быть одинакова на клиенте и сервере
dev tun # Определяет тип интерфейса, запись должна быть одинакова на клиенте и сервере
remote 1.2.3.4 1194 # IP-адреса или DNS-имена серверов с указанием портов
remote 2.3.4.5 1194 # remote-random – подключаться к произвольному из указанных серверов для распределения нагрузки
remote-random
persist-key # Не запрашивать ключ заново при разрыве соединения, не перезапускать виртуальный адаптер
persist-tun
```

```

ca ca.crt # Корневой сертификат центра сертификации
remote-cert-tls server # Проверка типа сертификата сервера, используется вместо устаревшей директивы ps-cert-type server
comp-lzo # Компрессия, запись должна быть одинакова на клиенте и сервере
# cert client.crt # Закрытый ключ и сертификат клиента в виде файлов необходимо за-
# key client.key комментировать или удалить.

```

Замените параметры

```

cert client.crt
key client.key

```

на

```

pkcs11-providers /usr/lib/libisbc_pkcs11_main.so
pkcs11-id 'ISBC/ESMART\%20Token/205A406291CB/test/65396131396465652D396531302D65333
2362D63265312D616632313864613536613538'

```

Идентификатор ключа следует записать в одну строку и поместить в одинарные кавычки.

8.4 Подготовка компьютера клиента

При подготовке компьютера клиента потребуются текстовый файл конфигурации и файл корневого сертификата (в примере *ca.cer*). Оба файла можно записать на ESMART Token. В этом случае все необходимое для установления соединения будет храниться на одном носителе. Установить OpenVPN можно будет из репозитория.

Для работы с сертификатами и данными рекомендуется установить бесплатное графическое приложение ESMART PKI Client. Также считать данные, которые хранятся на карте можно с помощью консольного приложения *pkcs11-tool*, входящего в пакет *OpenSC*.

Запись файлов на ESMART Token

В отличие от Windows в Linux сохранять корневой сертификат на карту необходимо в текстовом виде.

Доступ к файлу (соответственно и информация об используемых IP-адресах и нестандартных портах OpenVPN сервера) может быть защищена ПИН-кодом.

Авторизуйтесь на карте. Во вкладке «Данные» создайте новый блок и в поле «Значение» скопируйте содержимое файла корневого сертификата в кодировке Base64. Содержимое имеет следующий вид:

```

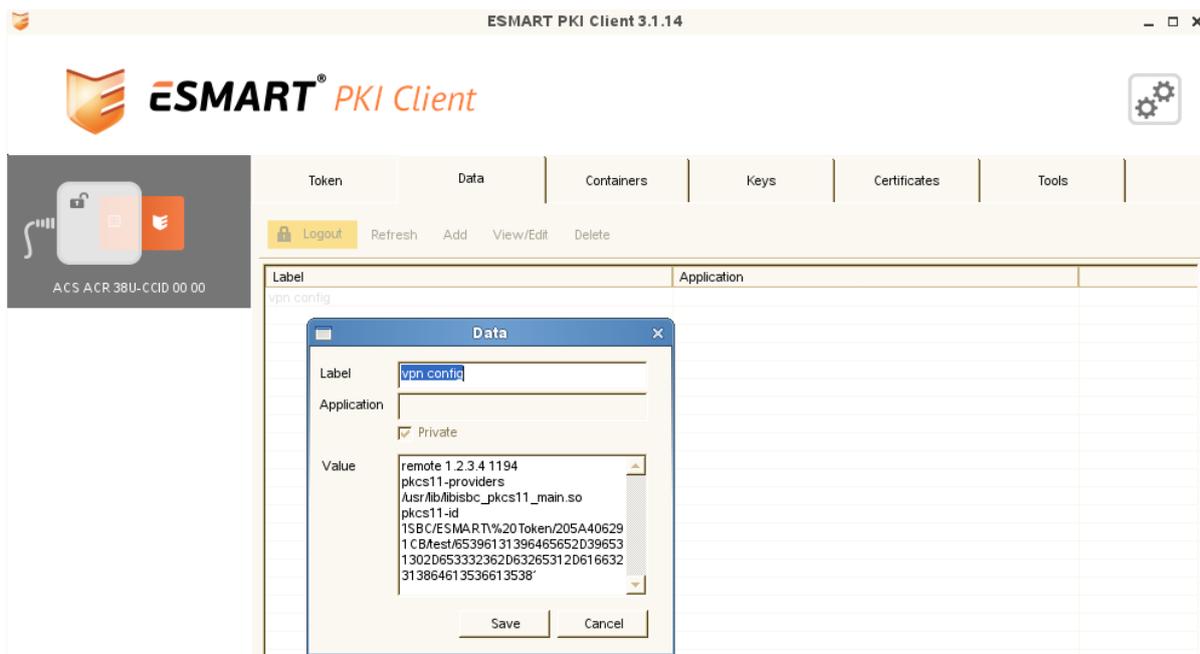
-----BEGIN CERTIFICATE-----
MIIDdzCCA1+gAwIBAgIQCyvzMWLNgpde++vpQ/4HJTANBgkqhkiG9w0BAQUFADBO
tVj4c9cASR2DnOzILwVFFC6zK2HuAh9KNBwX0+u2NK4JB00tdB3dZq+9lCB3dJW8
MGRtgo6DiaMYWKCzjBlmmNM+0rbMXqfbTCGE
-----END CERTIFICATE-----

```

Первую и последнюю строки (BEGIN CERTIFICATE и END CERTIFICATE) также необходимо скопировать.

Создайте новый блок данных и скопируйте в него содержимое файла сертификации. Если при добавлении блока отметить опцию **Защищенные**, блоки будут видны только авторизации на карте.

Ниже показан пример блока данных с файлом конфигурации.



Сохранение данных с ESMART Token в файл

Чтобы сохранить данные, хранящиеся на ESMART Token в файл, авторизуйтесь на ESMART Token. Откройте блок данных, скопируйте его содержимое и сохраните в файл любым текстовым редактором. Файл конфигурации с расширением `.conf`, как правило, помещают в директорию `/etc/openvpn`. Файл корневого сертификата с расширением `.cer` или `.crt` также может быть помещен в директорию `/etc/openvpn`. При необходимости скорректируйте путь к сохраненному файлу корневого сертификата, указанный в файле конфигурации.

8.5 Запуск клиента OpenVPN

Запуск клиента OpenVPN выполняется командой

```
openvpn "путь к файлу конфигурации"
openvpn openvpn-client.conf
```

9. Возможные проблемы

<p>OpenVPN не запрашивает PIN-код карты</p>	<p>Использование смарт-карт поддерживается с версии OpenVPN 2.1. Рекомендуется использовать версию 2.3 и выше.</p> <p>Проверить текущую версию в ОС Linux можно следующими командами:</p> <p>OpenSUSE/RedHat: <code>sudo rpm -q openvpn</code> Debian/Ubuntu: <code>sudo dpkg -l openvpn</code></p> <p>В ОС Windows версия указана в свойствах исполняемого файла <code>openvpn.exe</code></p>
<p>Использую приложение с графическим приложением для работы с OpenVPN, но окно ввода ПИН-кода не появляется</p>	<p>Графические оболочки OpenVPN пока не имеют возможности обрабатывать ввод пользователем ПИН-кода. Следует использовать консольную версию. Для удобства запуска соединения рекомендуется создать исполняемый текстовый <code>.bat</code> файл</p> <pre>openvpn "Путь к файлу конфигурации"</pre> <p>и запускать <code>.bat</code> файл из контекстного меню с правами администратора.</p>
<p>Соединение обрывается через некоторое время после подключения и не подключается автоматически</p>	<p>Возможно, в файл конфигурации на стороне клиента добавлена опция кэширования ПИН-кода карты. По умолчанию ПИН-код кэшируется до момента извлечения карты. Если в файле конфигурации присутствует строка</p> <pre>pkcs11-pin-cache 300</pre> <p>через 300 секунд ПИН-код будет удален из кэша и при следующем обращении к карте для пересогласования параметров соединения OpenVPN не получит доступ к закрытому ключу на карте. Текущая версия OpenVPN не может повторно запросить ПИН-код пользователя, поэтому соединение будет прервано. Использовать директиву <code>pkcs11-pin-cache</code> следует только при крайней необходимости.</p>
<p>На ПК клиента отсутствуют права администратора</p>	<p>При запуске OpenVPN без прав администратора не будут внесены требуемые маршруты. Поэтому необходимо заранее прописать постоянные маршруты:</p> <pre>route -p add IP-ADDRESS mask MASK GATEWAY</pre>
<p>Один и тот же сертификат загружен на две карты (токена), одна работает, а другая нет</p>	<p>Поскольку идентификатор содержит в себе серийный номер смарт-карты или ключа, а также ее произвольное название, даже если один и тот же контейнер будет импортирован на другую карту. Необходимо запросить идентификатор сертификата для каждой карты и создать два разных файла конфигурации.</p>
<p>После замены файла <code>.pfx</code> на сертификат на ESMART Token по шаблону Smart Card User маршрутизация работает некорректно.</p>	<p>Маршрутизация пользователей с помощью механизма CCD (<code>client-config-dir</code>) использует параметр <code>Common name</code> из сертификата. В сертификате в файле <code>.pfx</code> и новом сертификате на смарт-карте имя <code>Common Name</code> может строиться по-разному.</p>
<p>При соединении появляется ошибка</p> <pre>VERIFY nsCertType ERROR: /CN=server require nsCertType=SERVER</pre>	<p>В файле конфигурации клиента используется директива <code>ns-cert-type server</code>.</p> <p>Данный параметр является устаревшим и используется только для совместимости с версиями OpenVPN 2.0 и ниже. Следует использовать директиву</p> <pre>remote-cert-tls server</pre>