# JaCarta PKI и OpenVPN для Windows

## Краткое руководство draft

Листов: 9

Автор: S. Chelishev

# Аннотация

Настоящий документ описывает процесс конфигурирования OpenVPN для возможности использования носителей JaCarta PKI в качестве средства аутентификации.

.

# Оглавление

# Ход настройки

## Настройка сервера

Для возможности аутентификации в OpenVPN по цифровому сертификату, необходимо, чтобы клиент и сервер имели цифровые сертификаты, а сервер доверял издателю клиентского сертификата.

Рассмотрим выпуск ключей и сертификатов с использованием средств, предлагаемых самим OpenVPN.

Перейдите в каталог «easy-rsa», который находится в установочной директории и запустите init-config.bat. По необходимости, исправьте vars.bat для адаптации к вашему окружению, и создайте директорию, где будут храниться ключи.

Для работы, необходимо сгенерировать ключи для TLS:

Создайте пустые файлы для хранения индексов и серийных номеров (выполняется один раз). Запустите:

1. vars.bat
2. clean-all.bat

Сгенерируйте ключ Удостоверяющего Центра (выполняется один раз). Запустите:

1. vars.bat
2. build-ca.bat

В диалоге укажите имя вашего Удостоверяющего Центра.

Сгенерируйте файл для ключей Диффи-Хэллмана (только для сервера, выполняется один раз). Запустите:

1. vars.bat
2. build-dh.bat

Сгенерируйте приватный ключ и сертификат для сервера OpenVPN. Запустите

1. vars. bat
2. build-key-server .bat <имя машины>

В результате будут сгенерированы ключ и сертификат с именем машины.

Сгенерируйте файл PKCS #12 для каждой клиентской машины. Запустите

1. vars.bat
2. build-key-pkcs12.bat <имя машины>

В результате будет сгенерирован файл PKCS #12 с именем машины.

Отредактируйте ваш файл конфигурации сервера, задайте правильные сетевые настройки.

Обратите внимание, что необходимо правильно указать пути к файлам ключей и сертификатов. Выдержка из конфигурационного файла:

```
# Any X509 key management system can be used.
# OpenVPN can also use a PKCS #12 formatted key file
# (see "pkcs12" directive in man page).
ca C:\ПУТЬ К СЕРТИФИКАТУ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА\ca.crt
cert C:\ПУТЬ К СЕРТИФИКАТУ СЕРВЕРА\server.crt
key C:\ПУТЬ К КЛЮЧУ СЕРВЕРА\server.key

# Diffie hellman parameters.
# Generate your own with:
#   openssl dhparam -out dh2048.pem 2048
dh C:\ПУТЬ К ФАЙЛУ ДИФФИ-ХЭЛЛМАНА\dh1024.pem
```

# Настройка Клиента

Установите ПО «Единый Клиент JaCarta».

Инициализируйте JaCarta PKI. Затем с его помощью импортируйте файл PKCS#12, сгенерированный для клиента в ходе настройки сервера.

Установите сертификат с токена в личное хранилище компьютера.

Также потребуется сертификат Удостоверяющего Центра, полученный в ходе настройки сервера. Установите этот сертификат в хранилище доверенных корневых центров сертификации, а также сохраните локально.
Скопируйте sha1 отпечаток личного сертификата.

Отредактируйте ваш файл конфигурации клиента, задайте правильные сетевые настройки.

Обратите внимание, что необходимо правильно указать путь к сертификату Удостоверяющего Центра, а также правильно указать отпечаток сертификата клиента. Выдержка из конфигурационного файла:

```
# SSL/TLS parms.
# See the server config file for more
# description.  It's best to use
# a separate .crt/.key file pair
# for each client.  A single ca
# file can be used for all clients.
cryptoapicert "THUMB:9a dd 57 07 ee  ….  ОТПЕЧАТОК КЛИЕНТСКОГО СЕРТИФИКАТА"
ca  C:\ПУТЬ К СЕРТИФИКАТУ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА\ca.crt
```

# Проверка

Запустите OpenVPN на сервере и клиенте.
Если настройка выполнена правильно, появится запрос на введение ПИН-кода к карте, VPN-соединение успешно установится.

# Контакты, техническая поддержка

## Офис (общие вопросы)

Адрес: 129226, Москва, ул. Докукина, д. 16, стр. 1, компания «Аладдин Р. Д.».

Телефоны: +7 (495) 223-00-01 (многоканальный), +7 (495) 988-46-40.

Факс: +7 (495) 646-08-82.

E-mail: aladdin@aladdin-rd.ru (общий).

Web: www.aladdin-rd.ru

Время работы: ежедневно с 10:00 до 19:00, кроме выходных и праздничных дней.

## Техподдержка

Служба техподдержки принимает запросы только в письменном виде через веб-сайт:

**www.aladdin-rd.ru/support/index.php**

Для оперативного решения вашей проблемы укажите используемый Вами продукт, его версию, подробно опишите условия и сценарии применения, по возможности, снабдите сообщение снимками экрана, примерами исходного кода.

# Регистрация изменений

| Версия | Изменения |
|---|---|
| 0.1 | draft |
| | |
| | |

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 2874 от 18.05.12
Лицензии ФСБ России № 12632 Н от 20.12.12, № 24530 от 25.02.14
Система менеджмента качества компании соответствует требованиям стандарта ISO/ИСО 9001-2011
Сертификат СМК ГОСТ Р ИСО 9001-2011 № РОСС RU.ИС72.К00082 от 10.07.15
Microsoft Silver OEM Hardware Partner, Microsoft Silver Cloud Platform Partner, Apple Developer




Тел. +7 (495) 223-00-01 Email: aladdin@aladdin-rd.ru Web: www.aladdin-rd.ru