Вопрос:

Эта статья Базы Знаний ссылается на программное обеспечение, которое не поддерживается Cisco. Информация предоставлена как любезность для вашего удобства. Для дальнейшей поддержки свяжитесь с поставщиком программного обеспечения.

Ниже приводятся инструкции для экспортирования корневого сертификата подписания CA и ключа от Microsoft CA server 2003. Существует несколько шагов в этот процесс. Крайне важно, чтобы было выполнено каждое действие.

Экспортирование Сертификата и секретного ключа от MS CA сервер
1. Перейдите **'Запускаются'-> 'Выполненный'-> MMC** 2. Щелкните **по 'File'-> 'Add / Remove Snap - in'** **3. Нажмите кнопку Add** 4. Выберите **'Certificates'**, тогда нажимают **'Add'** 5. Выберите **'Computer Account'-> 'Next'-> 'Local Computer'-> 'Finish'** 6. нажмите **'Close'-> 'OK'** ***MMC теперь загружен моментальным снимком Сертификатов - в.*** 7. Разверните **Сертификаты**-> и щелкните **по 'Personal'-> 'Certificates'** 8. Щелкните правой кнопкой по соответствующему свидетельству CA и выберите **'All Tasks'-> 'Export'** *Мастер Экспорта Сертификата запустит* 9. Нажмите **'Next'**-> Select **'да, Экспорт секретный ключ'-> 'Затем'** 10. ***Анчек все*** опции здесь. PKCS 12 должен быть единственной доступной опцией. **Нажмите кнопку Next** 11. Дайте секретному ключу пароль по Вашему выбору 12. Дайте имя файла, чтобы сохранить как и нажать **'Next'**, затем **'Конец'** ***У вас теперь есть свой сертификат подписания CA и root, экспортируемый как PKCS 12 (PFX) файл.***
Извлечение Открытого ключа (сертификат)

Вы должны будете обратиться к компьютеру к рабочему OpenSSL. Скопируйте свой файл PFX к этому компьютеру и выполните следующую команду:

pkcs12 openssl - в <filename.pfx>-clcerts-nokeys - certificate.cer

Это создает файл с открытым ключом, названный "certificate.cer"

Примечание: *Эти инструкции были проверены с помощью OpenSSL на Linux. Некоторый синтаксис может варьироваться на версии Win32.*

Извлечение и дешифрование Секретного ключа

WSA требует, чтобы был дешифрован секретный ключ. Используйте следующие команды OpenSSL:

pkcs12 openssl - в <filename.pfx>-nocerts - закрытый-ключ-encrypted.key

Вам предложат для, "**Вводят Пароль Импорта**". Это - пароль, созданный в ***шаге 11*** выше.
Вам также предложат для, "**Вводят Фраза - пропуск PEM**". Пароля шифрования (используемый ниже).

Это создаст файл зашифрованного закрытого ключа, названный "закрытым-ключом-encrypted.key"

Для создания дешифрованной версии этого ключа используйте следующую команду:

openssl rsa - в закрытом-ключе-encrypted.key - private.key

Общие и дешифрованные секретные ключи могут быть установлены на WSA от **'Сервисов безопасности'**-> **'Прокси HTTPS'**