Поддержка ключа IEA 2048 битов CSR на примере конфигурации IEA

Содержание

Введение

Этот документ описывает, как генерировать ключевую поддержку на 2048 битов Запроса подписи сертификата (CSR) на устройстве шифрования IronPort (IEA) Cisco.

Настройка

Большинство Центров сертификации (CAs) сообщило явный запрос иметь все CSR, генерируемые с парой ключей длины 2048 битов. По умолчанию Версия 6.5 IEA использует длину ключа на 1024 бита для генерации пары ключей. Чтобы вынудить IEA генерировать пару ключей длины 2048, используйте keytool команду, как описано здесь.

Генерируйте сертификат

1. Войдите к CLI IEA

2. В главном меню, **тип x** для заскакивания в оболочку.

3. Изменение пользователю маршрута:
```
$ su -
```

4. Выполните keytool для создания нового keystore:
```
   # /usr/local/postx/server/jre/bin/keytool -genkey -alias <server alias>
-keyalg RSA -keysize 2048 -keystore <name the new keystore>
      *alias should be what the server is known as externally when customers
log into the device
      *When prompted for password use a easily remembered password
      *Enter in all requested information when prompted for the certificate
request, make special note of the next question:
      --- What is your first and last name?
      [Unknown]: server1.example.com
```

```
            *For this question enter in the fully qualified domain name
of the system
      *The name of the newkeystore should be in the format <name>.keystore
where name should include the current date
         Example: enterpriseks20130108.keystore
```

```
root@iea360 ~
# /usr/local/postx/server/jre/bin/keytool -genkey -alias stevesiea.cisco.com -keyalg RSA -keysize 2048 -keystore /usr/local/p
ostx/server/conf/2013_05_13.keystore
Enter keystore password:  password
What is your first and last name?
  [Unknown]:  stevesiea.cisco.com
What is the name of your organizational unit?
  [Unknown]:  TAC
What is the name of your organization?
  [Unknown]:  Cisco
What is the name of your City or Locality?
  [Unknown]:  Morrisville
What is the name of your State or Province?
  [Unknown]:  NC
What is the two-letter country code for this unit?
  [Unknown]:  US
Is CN=stevesiea.cisco.com, OU=TAC, O=Cisco, L=Morrisville, ST=NC, C=US correct?
  [no]:  yes

Enter key password for <stevesiea.cisco.com>
        (RETURN if same as keystore password):

root@iea360 ~
#
```

5. Выполните keytool для создания Файла CSR:
   # /usr/local/postx/server/jre/bin/keytool -certreq -keyalg RSA -alias <server alias> -file <servername>.csr -keystore <name of the new keystore>

```
root@iea360 ~
# /usr/local/postx/server/jre/bin/keytool -certreq -keyalg RSA -alias stevesiea.cisco.com -file /home/admin/stevesiea.csr -ke
ystore /usr/local/postx/server/conf/2013_05_13.keystore
Enter keystore password:  password

root@iea360 ~
#
```

6. Предоставьте файл CSR Центру сертификации для генерации сертификата. Гарантируйте отправку его как веба - сервера Apache Запрос подписи Certficate.
7. После того, как вы получаете .cer файл от CA, продолжаетесь к следующим шагам.

Импортируйте сертификат

Примечание: Пароль, используемый при генерации CSR**, должен** совпасть с keystore паролем для этих процедур для работы. Если бы CSR был создан отдельно, то введенный пароль **должен** совпасть с keystore паролем для этих процедур для работы.

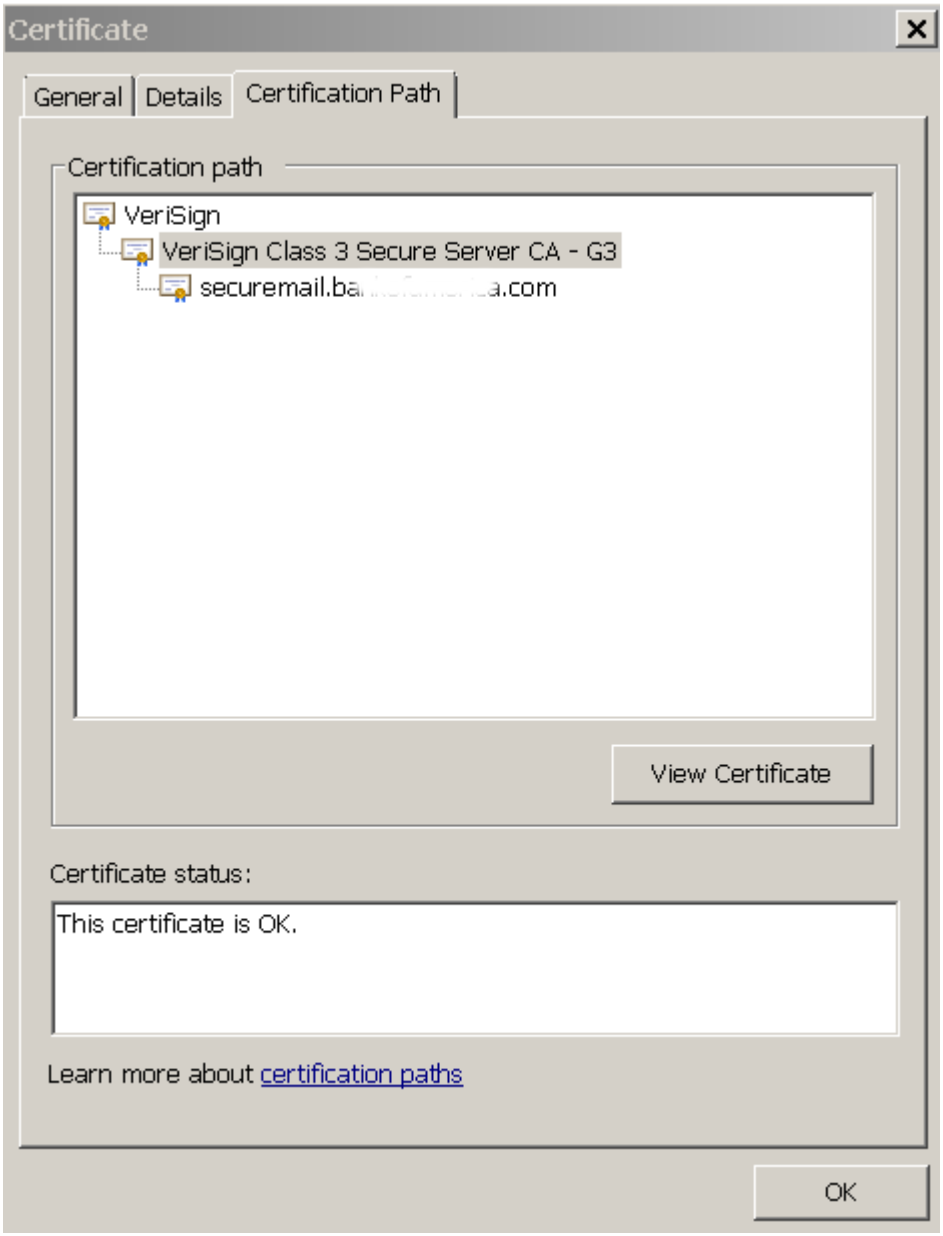
Необходимо объединить Сертификат в цепочку правильно

1. Каждый Сертификат CA должен быть извлечен из файла CER, полученного от CA, и затем объединился вместе в текстовом редакторе.

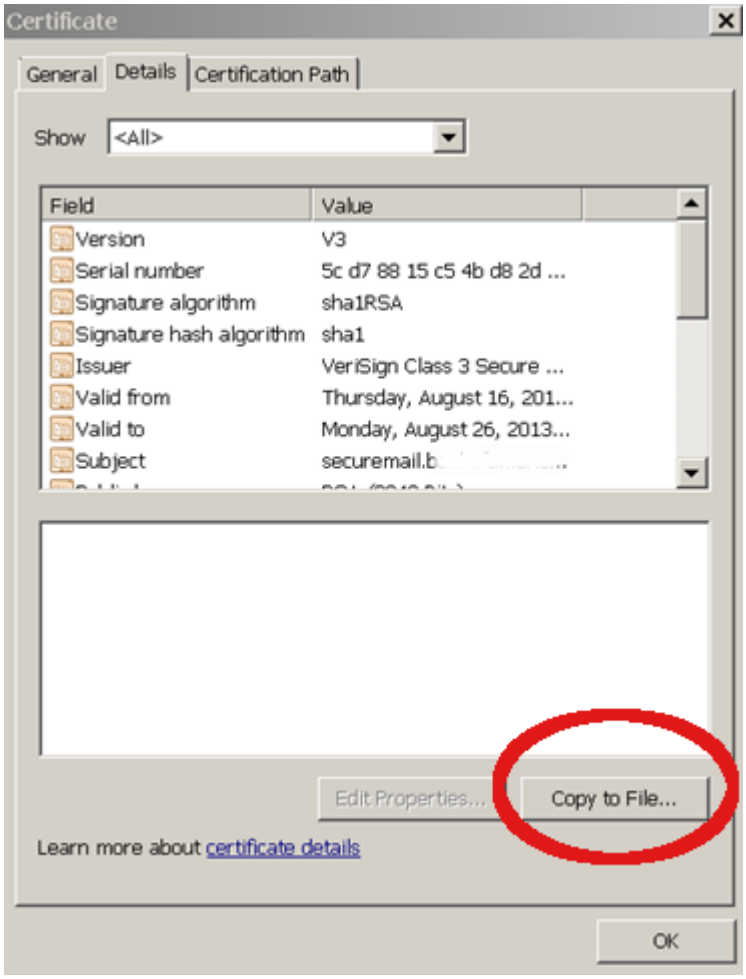
   Примечание: Это самым легким сделанный от машины Microsoft Windows. Другие операционные системы работают, но являются более трудными извлечь.
   Сертификаты должны быть объединены в цепочку в этом заказе :1. домен 2. Промежуточные 3. Root

   Двойное нажатие, чтобы открыть Файл сертификата (.CER файл), и затем нажать

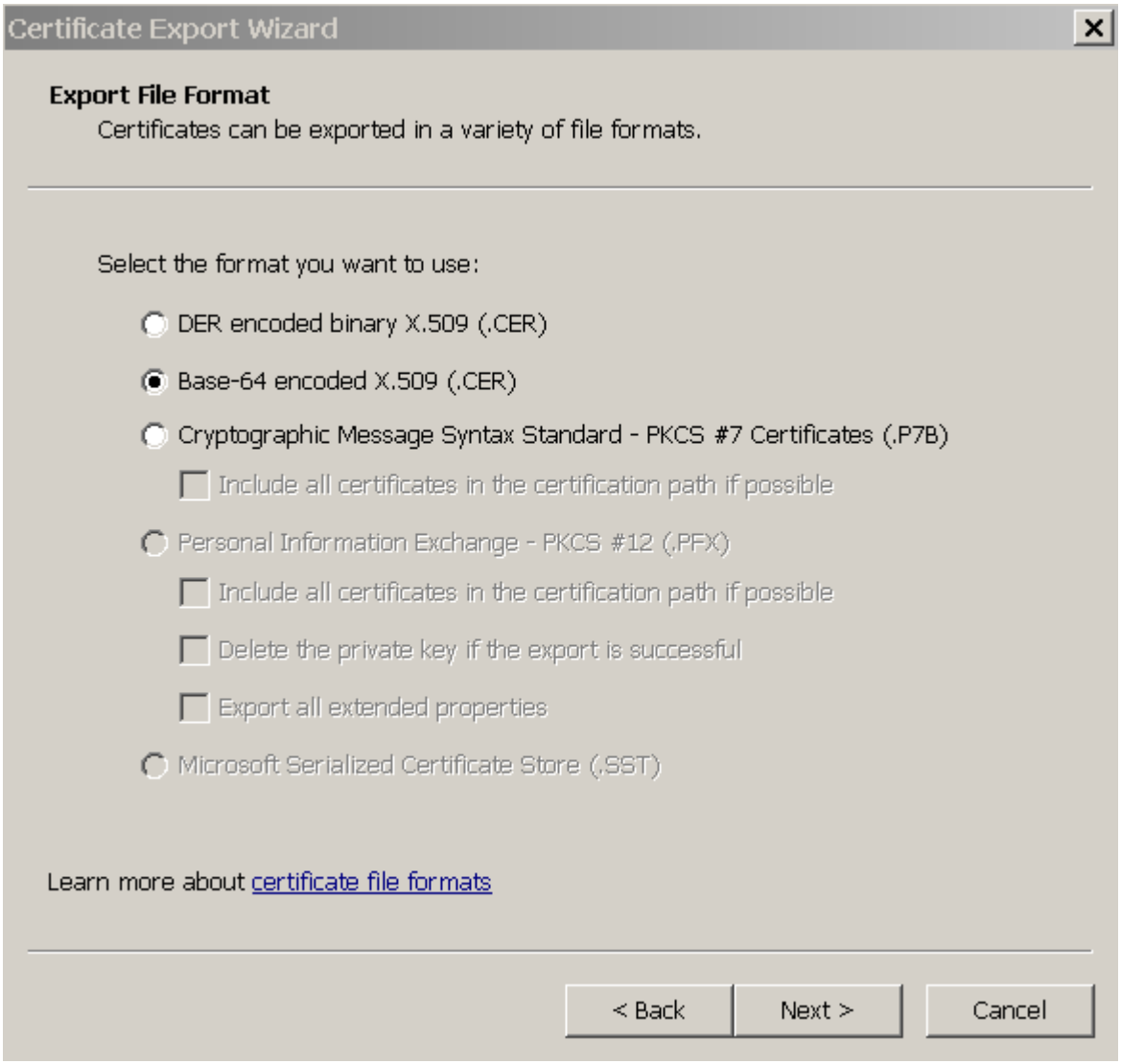
вкладку **Certification Path**:



Запустите со среднего уровня из Пути сертификации, нажмите вкладку **Details**, нажмите **Copy to File**, и затем назовите его **1. CER**.

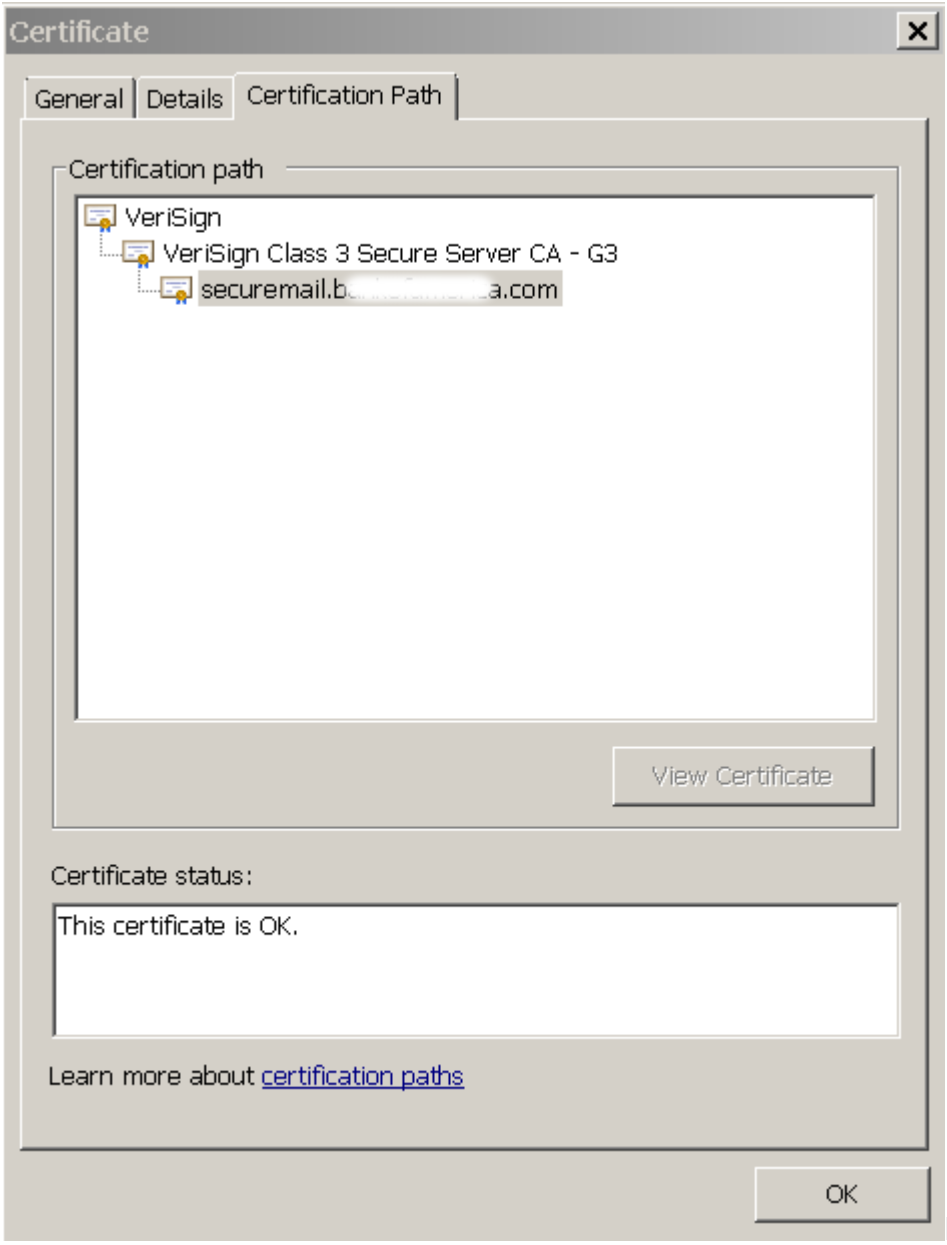


Выберите **закодированный X.509 Base-64 (.CER)**.

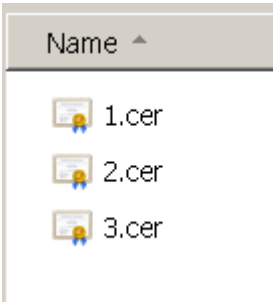


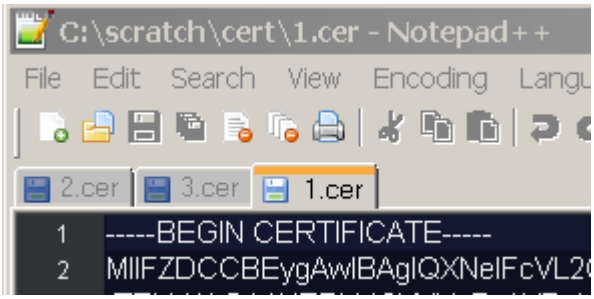
Повторитесь для Верхнего уровня CA и назовите его **2. CER**.

Повторитесь для серверного сертификата и **назовите его 3. CER**.



Используйте текстовый редактор (**не**, блокнот, но блокнот ++ работает хорошо), чтобы открыть все три файла **X.CER** и объединить их в заказе (1 наверху, и 3 в нижней части):





Примечание: Не должно быть никаких пустых линий между сертификатами и никакой пустой линии в нижней части.

Сохраните как **<servername>.CER**.

Загрузите **<servername>.CER** файл к IEA в**/home/admin / <servername.cer>** с FTP или SCP.

Скопируйте**/home/admin / <servername.cer> к/usr/local/postx/server/conf**:

```
root@iea360 /home/admin
# cp /home/admin/stevesiea.cer /usr/local/postx/server/conf

root@iea360 /home/admin
#
```

2. Используйте GUI IEA для импорта сертификата [Ключи и Сертификаты | Настройка SSL].

   Примечание: Keystore = **[Каталог Установки]/conf/enterprisenamestore.keystore** или текущее название вашего keystore файла.

   Сертификат =**/usr/local/postx/server/conf/NEWCERT.CER**.

   Проверьте **доверие CA Certs**.

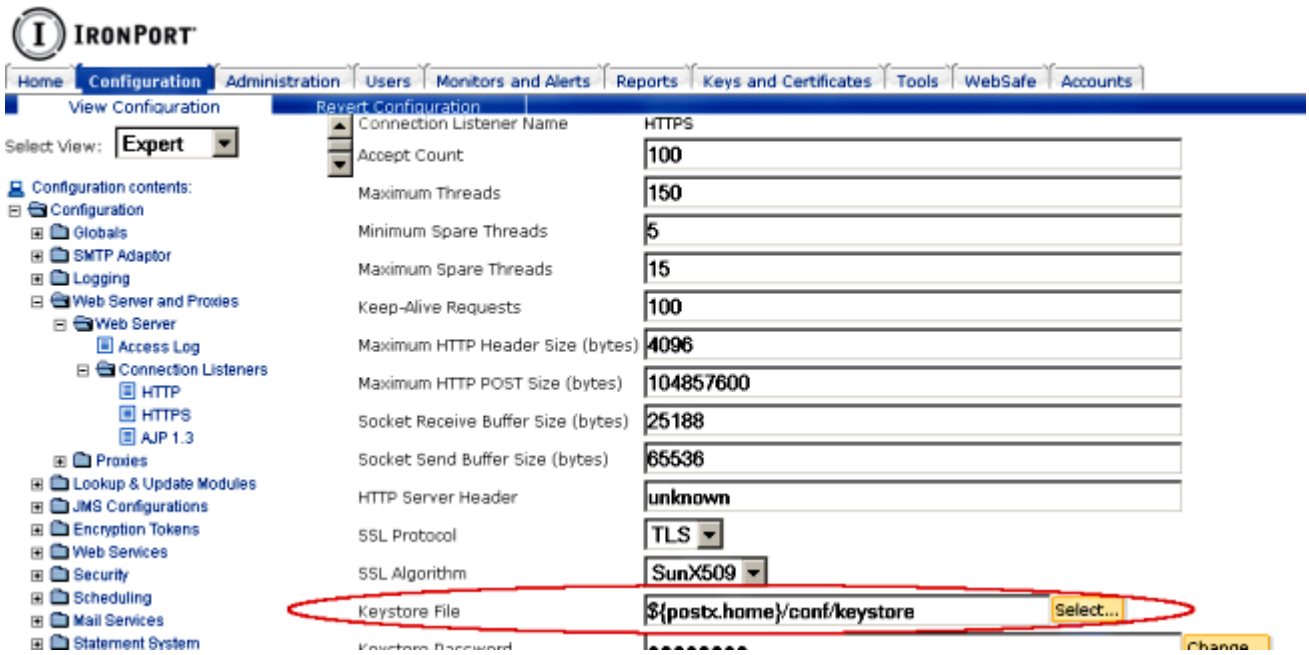
   Нажмите **Import Certificate**

3. (Дополнительный - Если новый keystore должен быть создан). От GUI IEA скажите IEA использовать новый keystore:

   Выберите Configuration | Web-сервер и прокси | Web-сервер | слушатели соединения | HTTPS

Введите в пути к новому keystore файлу:

Пример: $ **{postx.home}/conf/2013_5_13.keystore**



4. Разверните Изменения и перезапустите Адаптер SMTP.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.