Содержание

Введение

Этот документ описывает, как определить, совпадает ли подписанный сертификат Центра сертификации (CA) с Запросом подписи существующего сертификата (CSR) для Cisco Unified Application Server.

Предварительные условия

Требования

Cisco рекомендует иметь знание X.509/CSR.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения

Запрос сертификации состоит из составного имени, открытого ключа и дополнительного набора атрибутов, коллективно подписанных сертификацией запроса объекта. Запросы сертификации отправлены к центру сертификации, который преобразовывает запрос в сертификат общего ключа X.509. В какой форме центр сертификации возвращается недавно, подписанный сертификат выходит за рамки этого документа. PKCS #7 сообщение является одной возможностью. (RFC:2986)

Диспетчер связи Cisco управление сертификатами

Намерение включать ряд атрибутов является двукратным:

- Предоставить другую информацию о данном объекте или пароль вызова, которым объект может позже запросить аннулирование сертификата.
- Предоставить атрибуты для включения в сертификаты X.509. Текущие серверы UC не поддерживают пароль вызова.

Текущая Cisco серверы UC требует этих атрибутов в CSR как показано в этой таблице:

Информация	Описание
orgunit	подразделение
orgname	организационное название
местность	местоположение организации
состояние	состояние организации
страна	код страны не может быть изменен
alternatehostname	альтернативное имя хоста

Родственные продукты

Этот документ может также использоваться с этими версиями программного и аппаратного обеспечения:

- Cisco Unified Communications Manager (CUCM)
- Cisco унифицированный IM и присутствие
- Cisco унифицированный Unity Connection
- CUIS
- Cisco Meidasence
- Cisco Unified Contact Center Express (UCCX)

Проблема

В поддержке UC вы встречаетесь с большим количеством случаев, где подписанный сертификат CA не в состоянии быть загруженным на серверах UC. Вы не можете всегда определять то, что произошло во время создания подписанного сертификата, так как вы не человек, который использовал CSR для создания подписанного сертификата. В большинстве сценариев, оставляя новый сертификат занимает больше чем 24 часа. Серверы UC, такие как CUCM не имеют подробного журнала/трассировки для помощи в определении, почему загрузка сертификата отказывает, но они просто дают сообщение об ошибках. Эта статья предназначена для помощи в сужении проблемы, является ли это сервером UC или проблемой CA.

Общая практика для Сертификатов подписанный ЦС в CUCM

CUCM поддерживает интеграцию с независимым поставщиком CAs при помощи механизма CSR PKCS#10, который доступен в Менеджере сертификатов Операционной системы

Унифицированной связи Cisco GUI. Клиенты, которые в настоящее время используют независимого поставщика CAs, должны использовать механизм CSR для запуска сертификатов для Cisco CallManager, CAPF, IPSec и Tomcat.

Шаг 1. Измените Определение прежде, чем генерировать CSR

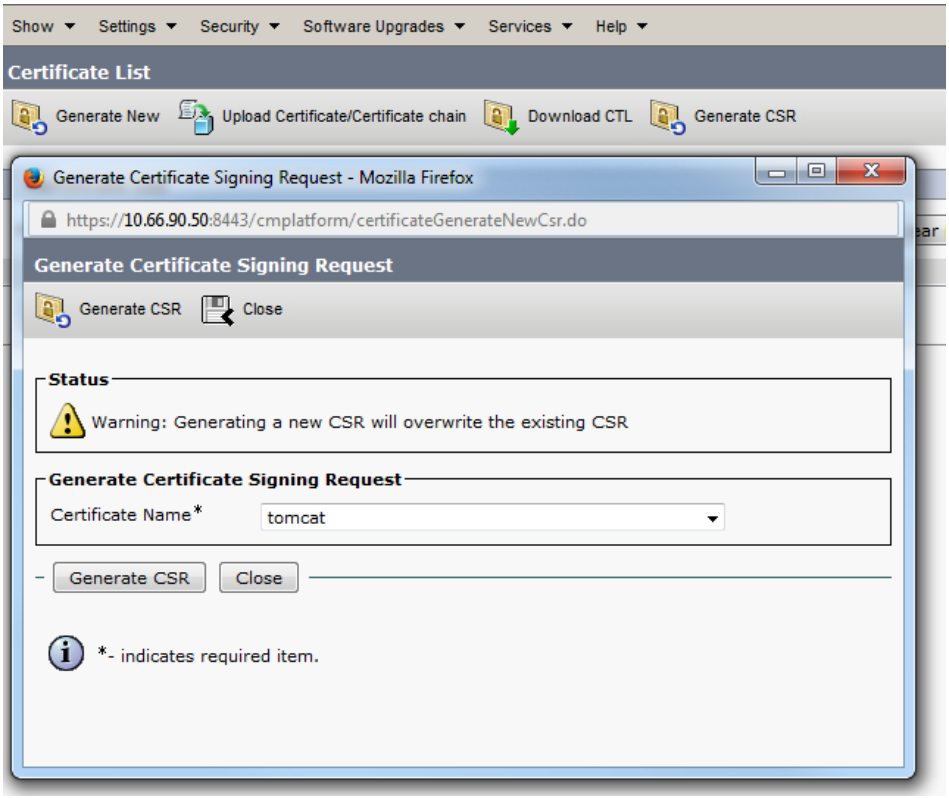
Идентичность сервера CUCM для генерации CSR может модифицироваться при помощи **веб-безопасности набора команд** как показано в этом образе.

```
admin:set web-security  ?
Syntax:
set web-security orgunit orgname locality state [country] [alternatehostname]
orgunit  mandatory   organizational unit
orgname  mandatory   organizational name
locality mandatory   location of organization
state    mandatory   state of organization
country  optional    country code can not be changed
alternatehostname  optional   alternate host name

admin:set web-security
```

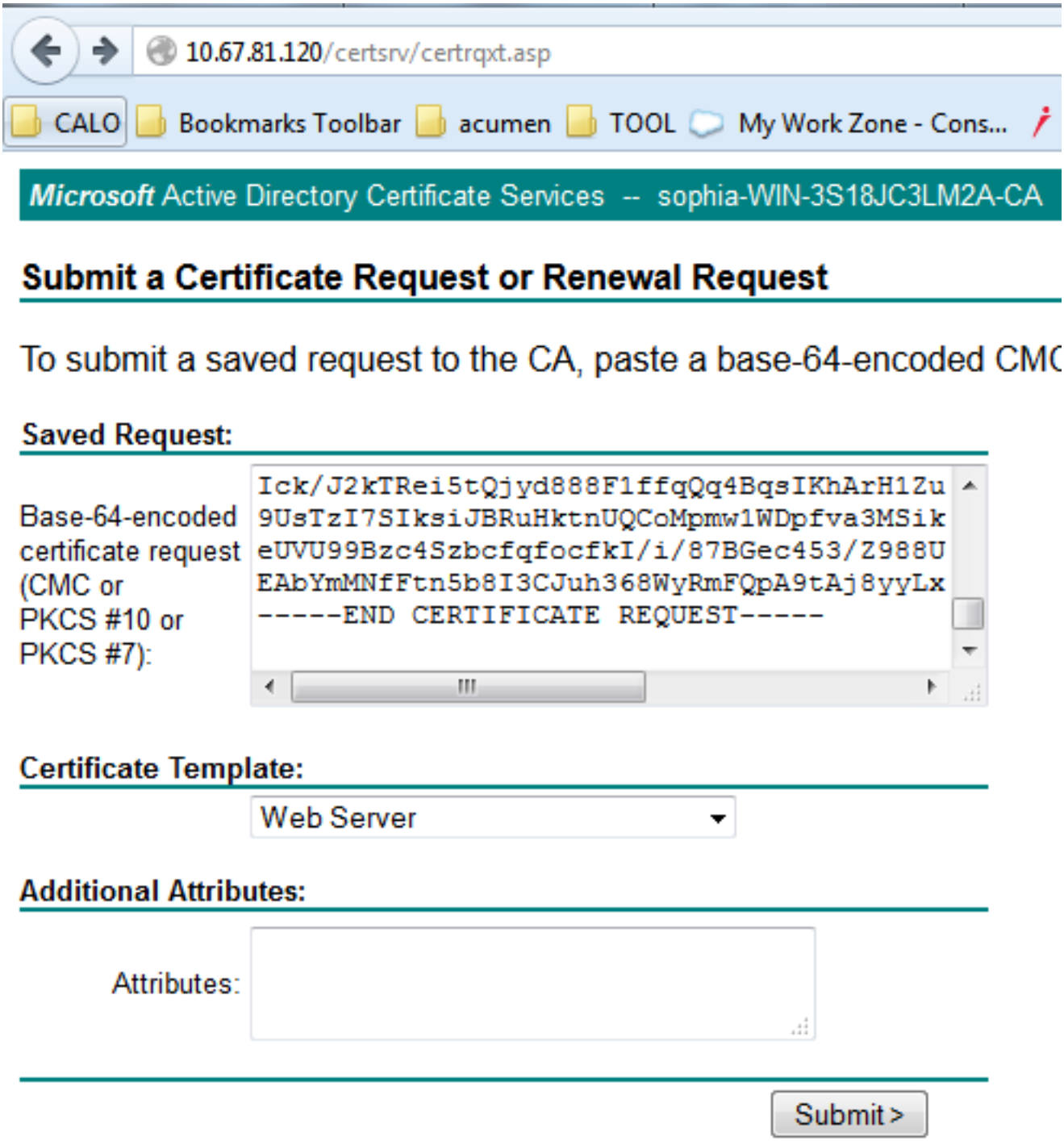
Если у вас есть пространство в вышеупомянутых полях, используйте?? достигнуть команды как:

```
admin:set web-security "Cisco Systems" "Cisco TAC" "St Leonard" NSW AU CUCM105.sophia.li

WARNING: Country code can not be changed.
Country code for existing web-security is : AU

WARNING: This operation creates self signed certificate for web access (tomcat) with the
r, certificates for other components (ipsec, callmanager, CAPF, etc.) still contain the o
erate these self-signed certificates to update them.

Regenerating web security certificates please wait ...

WARNING: This operation will overwrite any CA signed certificate previously imported for
Proceed with regeneration (yes|no)?
```

Шаг 2. Генерируйте CSR.

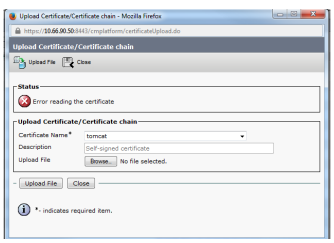


Шаг 3. Загрузите CSR и получите подписанный CA.



Шаг 4. Загрузите Сертификат подписанный ЦС к серверу.

Как только CSR генерируется, и сертификат подписан, если вы не в состоянии загружать его с сообщением об ошибках **Ошибка при чтении сертификат** (как показано в этом образе), тогда необходимо проверить, восстановлен ли CSR или является ли сам подписанный сертификат причиной проблемы.



Существует три способа проверить, восстановлен ли CSR, или сам подписанный сертификат является причиной проблемы.

Решение 1. Используйте Команду OpenSSL в root (или Linux)

1. Войдите к root и перейдите к папке.

```
[root@CCM105PUB keys]# pwd
/usr/local/platform/.security/tomcat/keys
[root@CCM105PUB keys]# ls -thl
total 28K
-rwxr-xr-x. 1 certbase ccmbase 1.7K Sep  1 23:22 tomcat_priv_csr.pem
-rwxr-xr-x. 1 certbase ccmbase 1.2K Sep  1 23:22 tomcat_priv_csr.der
-rwxr-xr-x. 1 certbase ccmbase 1.4K Sep  1 23:22 tomcat.csr
-rwxr-xr-x. 1 certbase ccmbase 1.2K Aug 13 16:11 tomcat_priv.der
-rwxr-xr-x. 1 certbase ccmbase 1.7K Aug 13 16:11 tomcat_priv.pem
-rwxr-xr-x. 1 certbase ccmbase   16 Apr 26 15:10 tomcat-trust.passphrase
-rwxr-xr-x. 1 certbase ccmbase   16 Apr 26 15:10 tomcat.passphrase
[root@CCM105PUB keys]#
```

2. Скопируйте подписанный сертификат к той же папке с помощью Безопасного FTP (SFTP). Если вы неспособны установить сервер SFTP, то загрузка его к папке TFTP также получает сертификат на CUCM.

```
[root@CCM105PUB keys]# sfpt cisco@10.66.90.19
bash: sfpt: command not found
[root@CCM105PUB keys]# sftp cisco@10.66.90.19
Connecting to 10.66.90.19...
Authenticated with partial success.
cisco@10.66.90.19's password:
Hello, I'm freeFTPd 1.0sftp> get tomcat.cer
Fetching /tomcat.cer to tomcat.cer
/tomcat.cer                                   100% 2140     2.1KB/s   00:00
sftp>
```

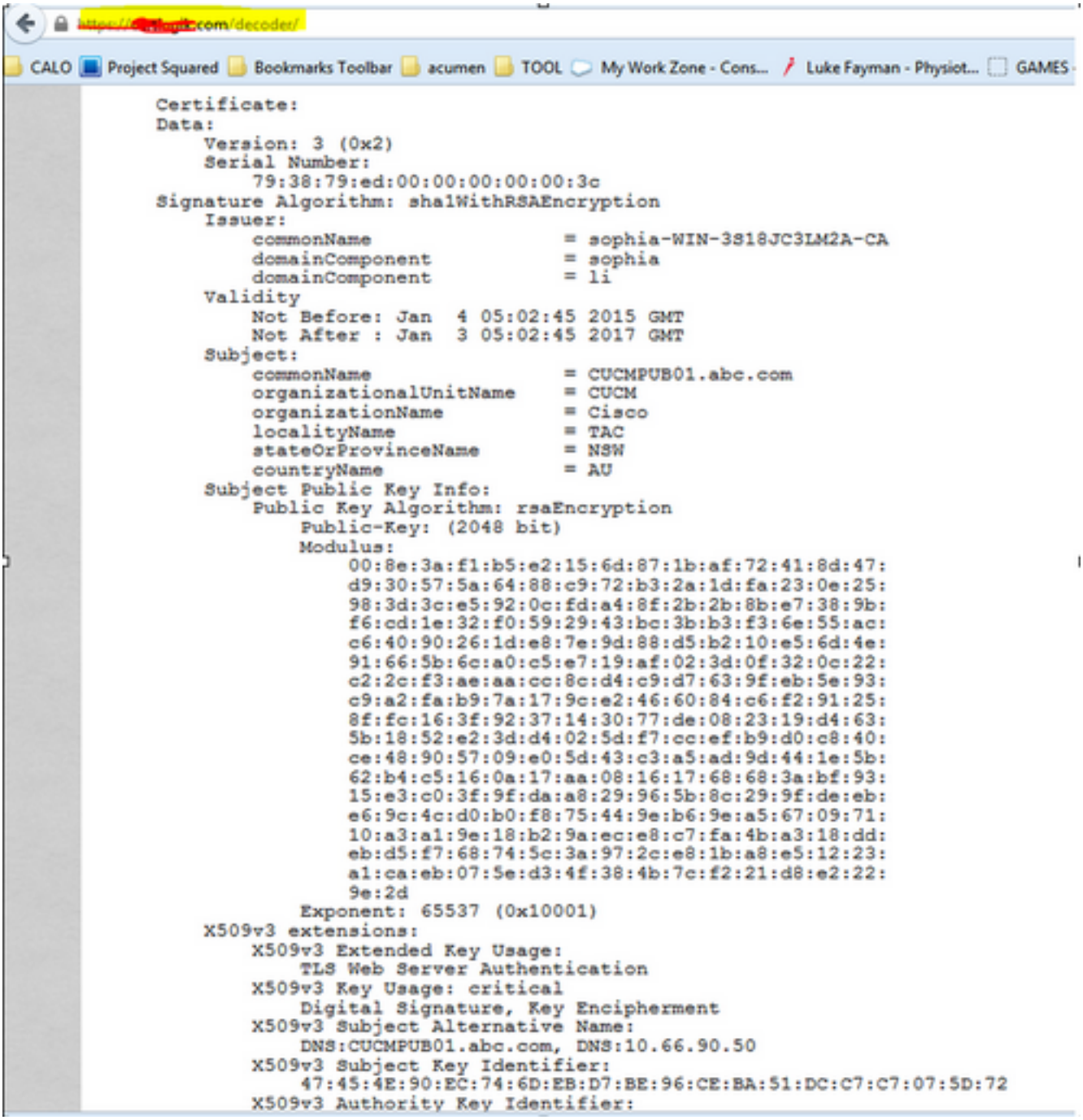
3. Проверьте MD5 для CSR и подписанного сертификата.

```
[root@CUCMPUB01 keys]# openssl req -noout -modulus -in tomcat.csr | openssl md5
cd78ed16b2abe2fa203e3f2e3499ee5c
[root@CUCMPUB01 keys]# openssl x509 -noout -modulus -in certnew.cer | openssl md5
cd78ed16b2abe2fa203e3f2e3499ee5c
[root@CUCMPUB01 keys]#
```

Решение 2. Используйте любой ключ сертификата SSL matcher из Интернета

Решение 3. Сравните Содержание от любого декодера CSR из Интернета

1. Скопируйте **Подробные сведения Сертификата** сеанса для каждого как показано в этом образе.



2. Сравните их в программном средстве, таком как Блокнот ++ со Сравнить плагином как показано в этом образе.