Технические примечания на сертификате CAPF, со знаком CA для CUCM

Содержание

Введение

Этот документ описывает, как получить сертификат функции представительства сертифицирующей организации (CAPF), подписанный Центром сертификации (CA) для Cisco Unified Communications Manager (CUCM). Всегда существуют запросы подписаться, CAPF с внешним Этим документом CA. показывает, почему понять, как это работает , так же важно как процедура настройки.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Инфраструктура открытых ключей (PKI)
- Конфигурация безопасности CUCM

Используемые компоненты

Сведения в этом документе основываются на версии 8.6 Cisco Unified Communications Manager и выше.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в данном документе, были

запущены с конфигурацией по умолчанию. Если ваша сеть является оперативной, гарантируйте понимание потенциального воздействия любой команды.

Родственные продукты

Данный документ также может использоваться со следующими версиями программного и аппаратного обеспечения:

- CA. Microsoft Windows server 2008 года
- Cisco Jabber для Windows.

Общие сведения

Цель CA CAPF со знаком

Некоторые клиенты хотели бы выровняться с globle политикой сертификата с компанией, таким образом, существует потребность к со знаком CAPF с тем же CA как другие серверы.

Механизм для этого PKI

По умолчанию логически значимый сертификат (LSC) подписан CAPF, таким образом, CAPF является CA для телефонов в этом сценарии. Однако, когда вы пытаетесь подписать CAPF внешним CA, тогда CAPF в этом сценарии действия как подчиненный CA или промежуточный CA.

Различие между самоподписанным CAPF и подписанным CA CAPF: CAPF является узлом CA к LSC, когда выполнение самоподписало CAPF, CAPF зависимое (промежуточное звено) CA к LSC при выполнении подписанного CA CAPF.

Как CSR CAPF Отличается от других CSR?

Относительно к RFC5280, ключевое расширение использования определяет цель (например, шифровка, подпись, подписание сертификата) ключа, содержавшегося в сертификате. CAPF является прокси сертификата и CA и он может подписать сертификат к телефонам, но другой сертификат как CallManager, Tomcat, IPSec они действуют как лист (идентичность пользователя). При изучении CSR для них вы видите, что CSR CAPF имеет роль **Знака Сертификата**, но не другие.

CSR CAPF:

```
Attributes:
Requested Extensions:
    X509v3 Extended Key Usage:
        TLS Web Server Authentication, IPSec End System
    X509v3 Key Usage:
        Digital Signature, Certificate Sign
```

CSR Tomcat:

```
Attributes:
Requested Extensions:
    X509v3 Extended Key Usage:
```

```
            TLS Web Server Authentication, IPSec End System
        X509v3 Key Usage:
            Digital Signature, Certificate Sign
```

CSR CallManager:

```
    Attributes:
    Requested Extensions:
        X509v3 Extended Key Usage:
            TLS Web Server Authentication, IPSec End System
        X509v3 Key Usage:
            Digital Signature, Certificate Sign
```

CSR IPSec:

Атрибуты: запрошенные расширения: X509v3 расширенное ключевое использование: аутентификация Web-сервера TLS, аутентификация web - клиента TLS, конечная система IPSec использование ключа X509v3: цифровая подпись, ключевая шифровка, шифровка данных, согласование ключей

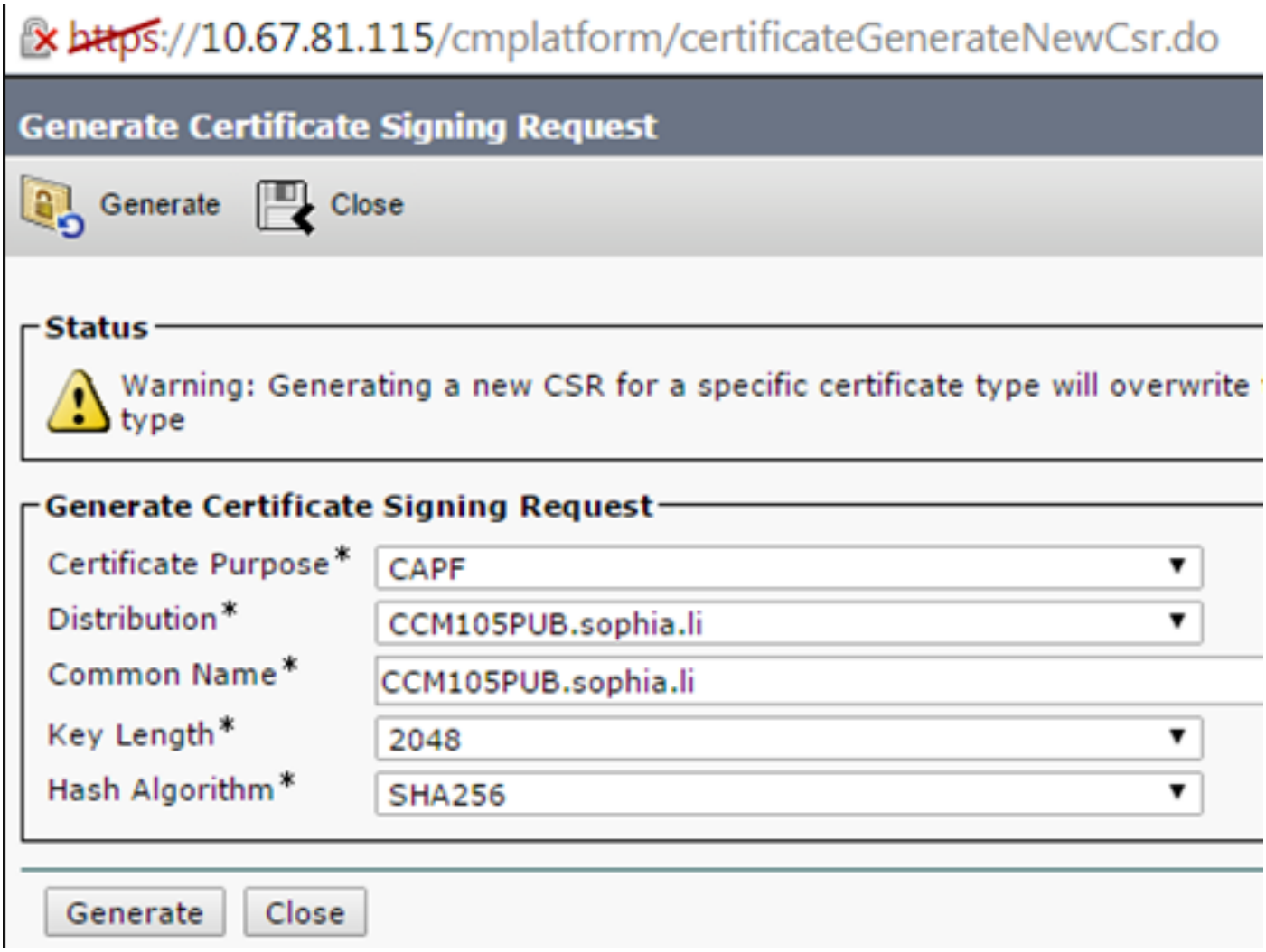
Настройка

Это - процедура для подписания CAPF с внешним CA.

Шаг 1. Сделайте свой кластер CUCM как кластер безопасности.

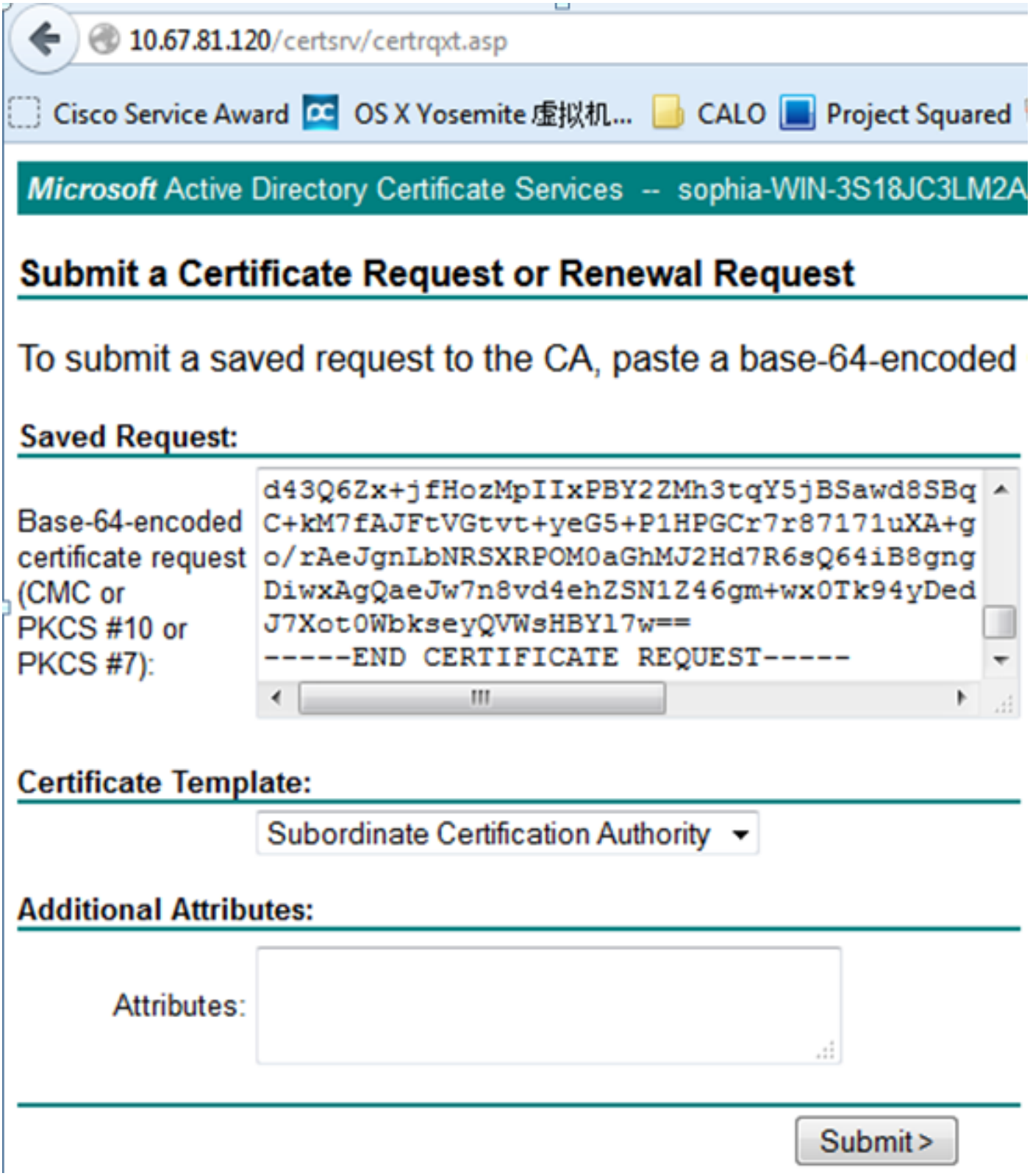
```
admin:utils ctl set-cluster mixed-mode
```

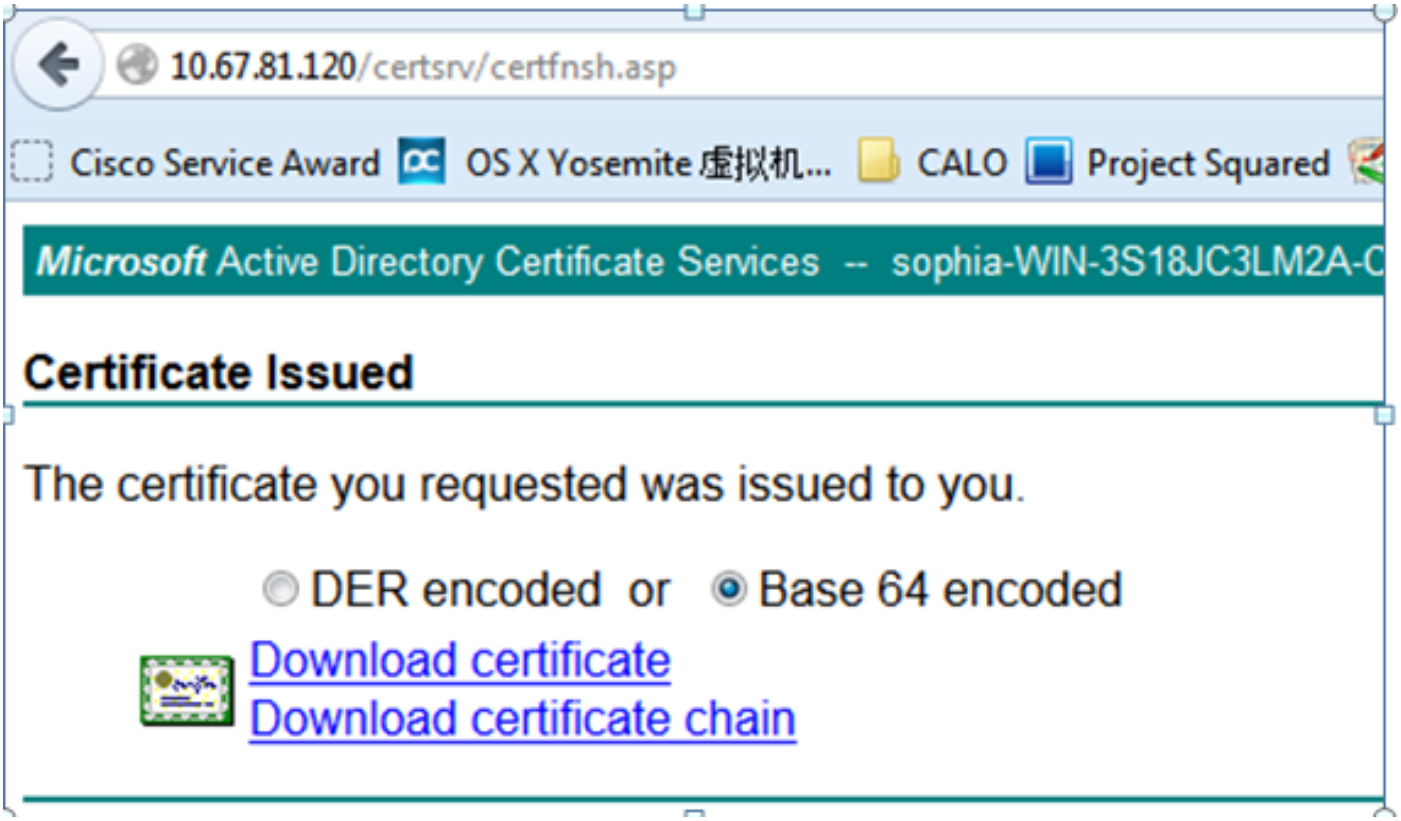
Шаг 2. Как показано в образе, генерируйте CSR CAPF.



Шаг 3. Подписанный это с CA (использующий зависимый шаблон в Windows 2008 CA).

Примечание: Вы должны к пользовательскому шаблону **Центра сертификации Подчиненного** подписать этот сертификат.


10.67.81.120/certsrv/certrqxt.asp
Cisco Service Award
OS X Yosemite 虚拟机...
CALO
Project Squared
Microsoft Active Directory Certificate Services -- sophia-WIN-3S18JC3LM2A
Submit a Certificate Request or Renewal Request
To submit a saved request to the CA, paste a base-64-encoded
Saved Request:
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):
d43Q6Zx+jfHozMpIIxPBY2ZMh3tqY5jBSawd8SBq
C+kM7fAJFtVGtvt+yeG5+P1HPGCr7r87171uXA+g
o/rAeJgnLbNRSXRPOM0aGhMJ2Hd7R6sQ64iB8gng
DiwxAgQaeJw7n8vd4ehZSN1Z46gm+wx0Tk94yDed
J7Xot0WbkseyQVWsHBYl7w==
-----END CERTIFICATE REQUEST-----
Certificate Template:
Subordinate Certification Authority
Additional Attributes:
Attributes:
Submit >

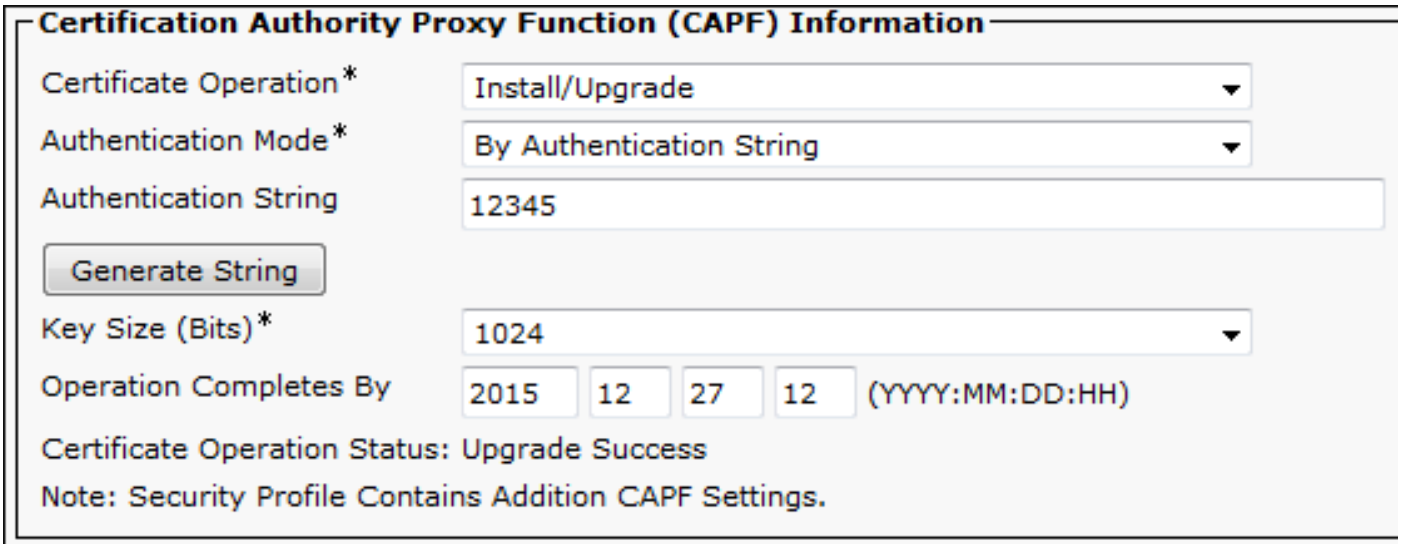


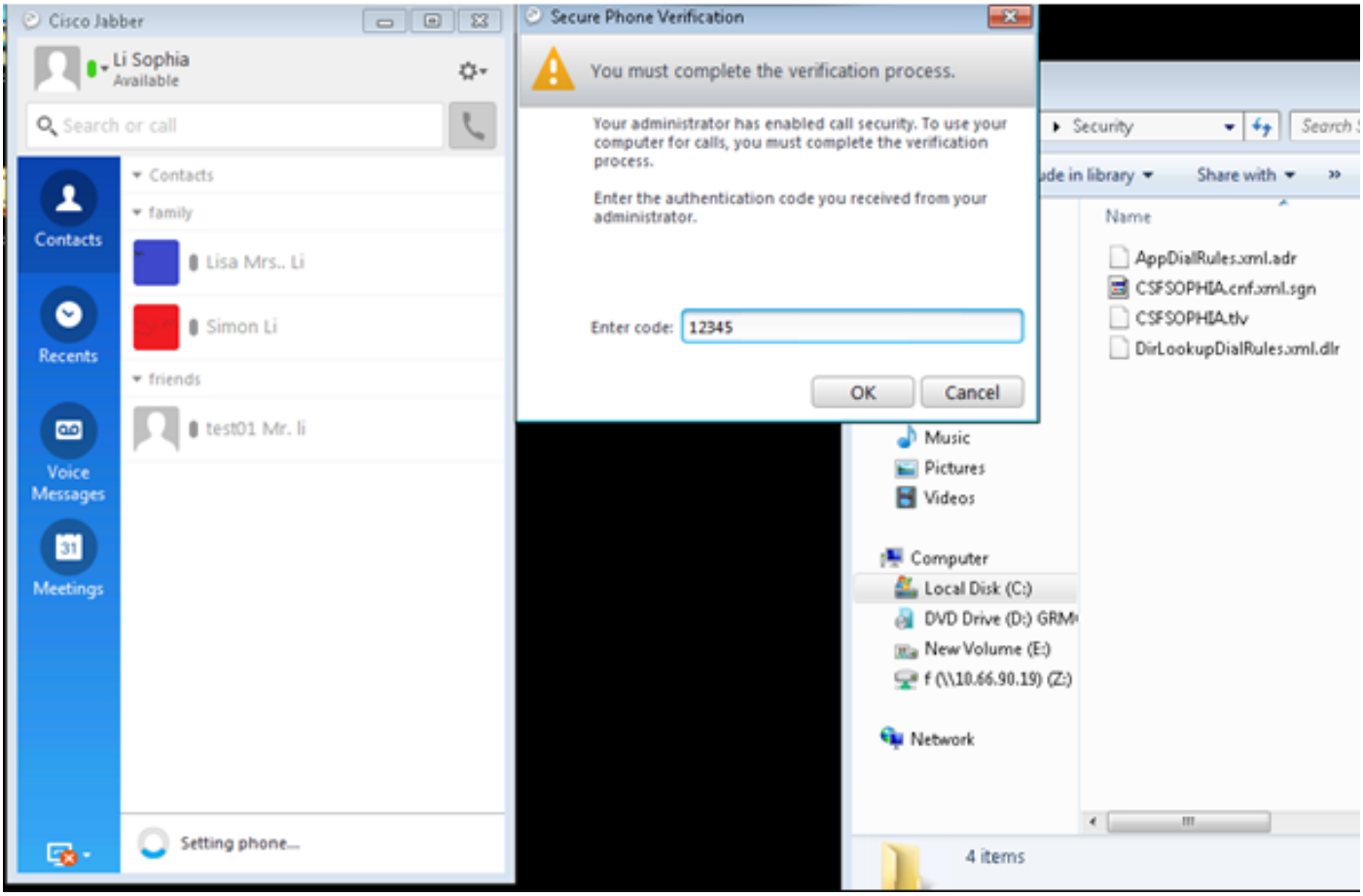
Шаг 4. . Загрузите узел CA, столь же трастовый CAPF и серверный сертификат как CAPF.

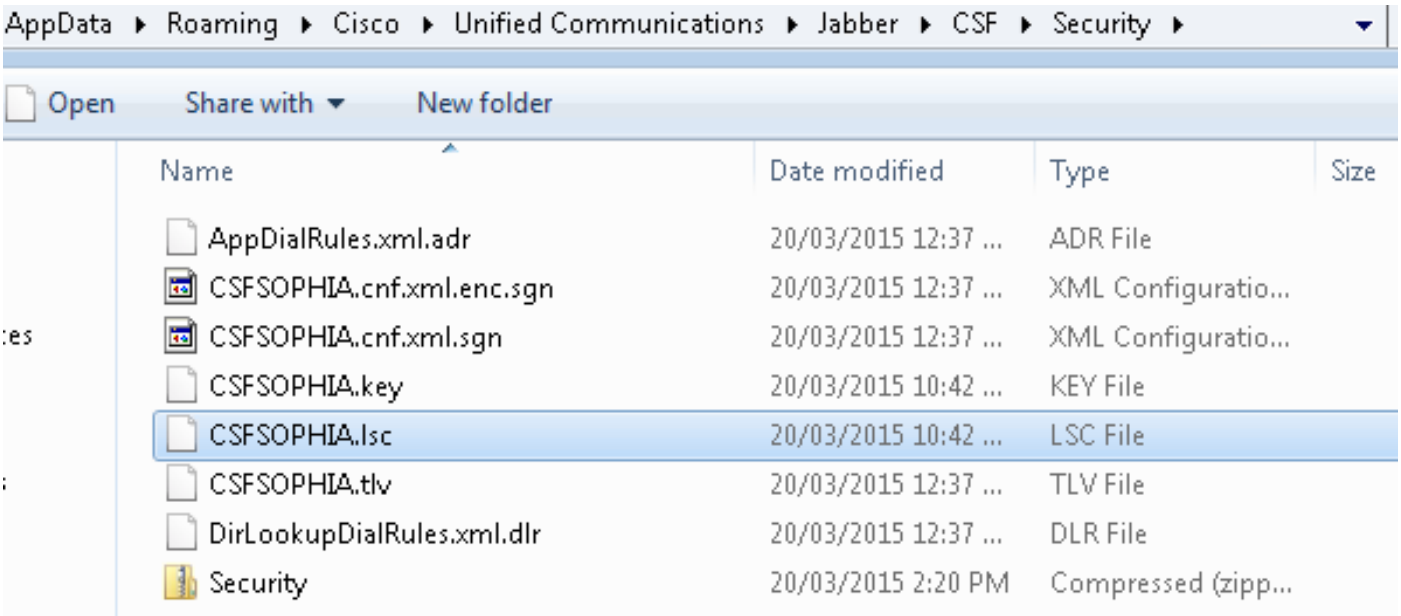
Шаг 5. . Перезапустите сервис CAPF.

Шаг 6. Перезапустите CALLMANAGER/СЕРВИСЫ TFTP во всех примечаниях.

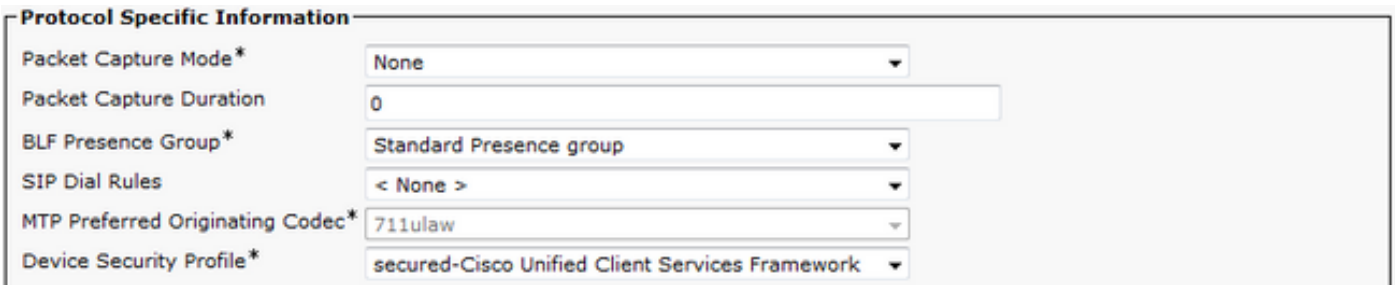
Шаг 7. Подписанный LSC программного телефона Jabber.



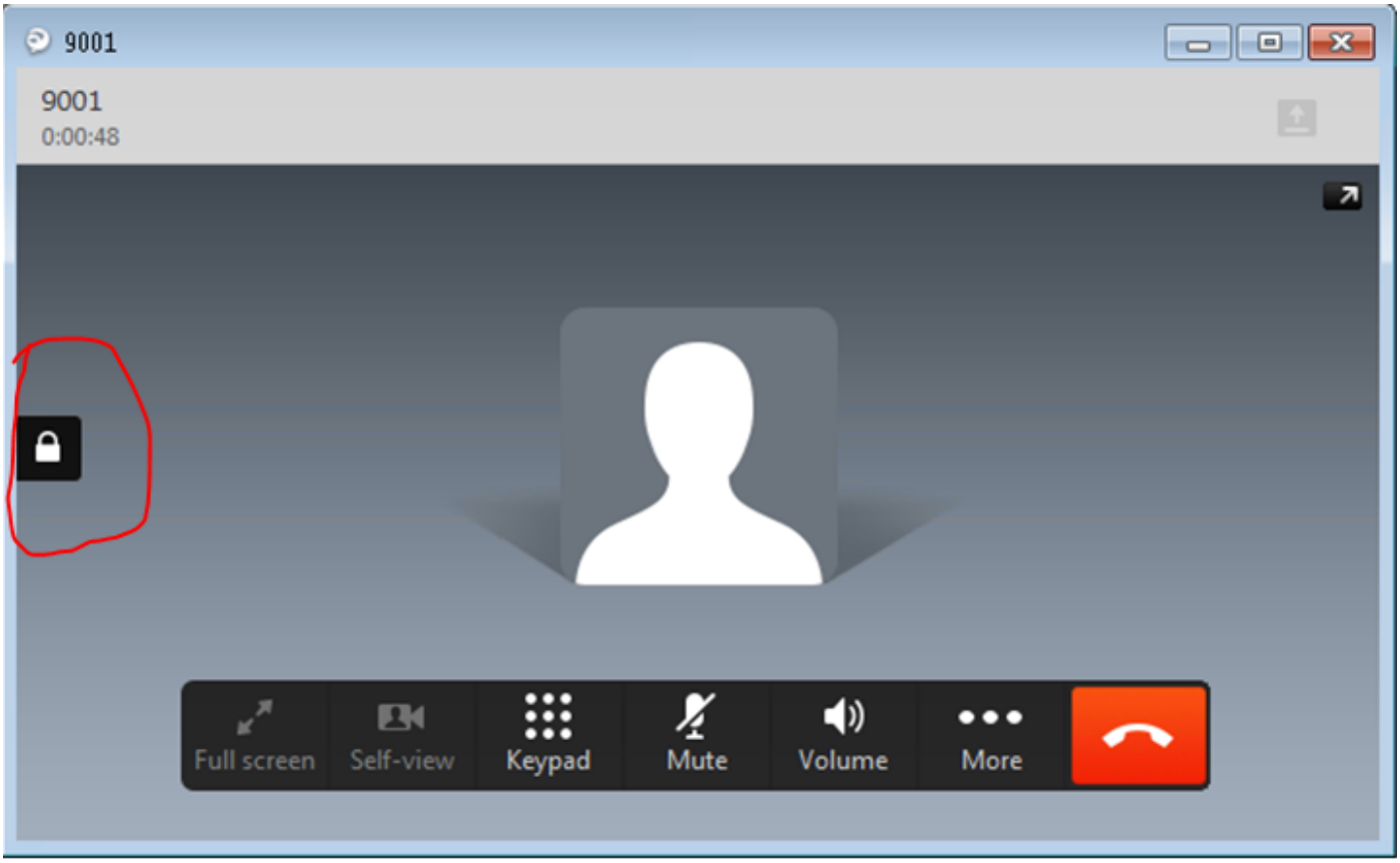




Шаг 8. Включите профиль безопасности для программного телефона Jabber.



Шаг 9. Теперь защищенный RTP происходит как:

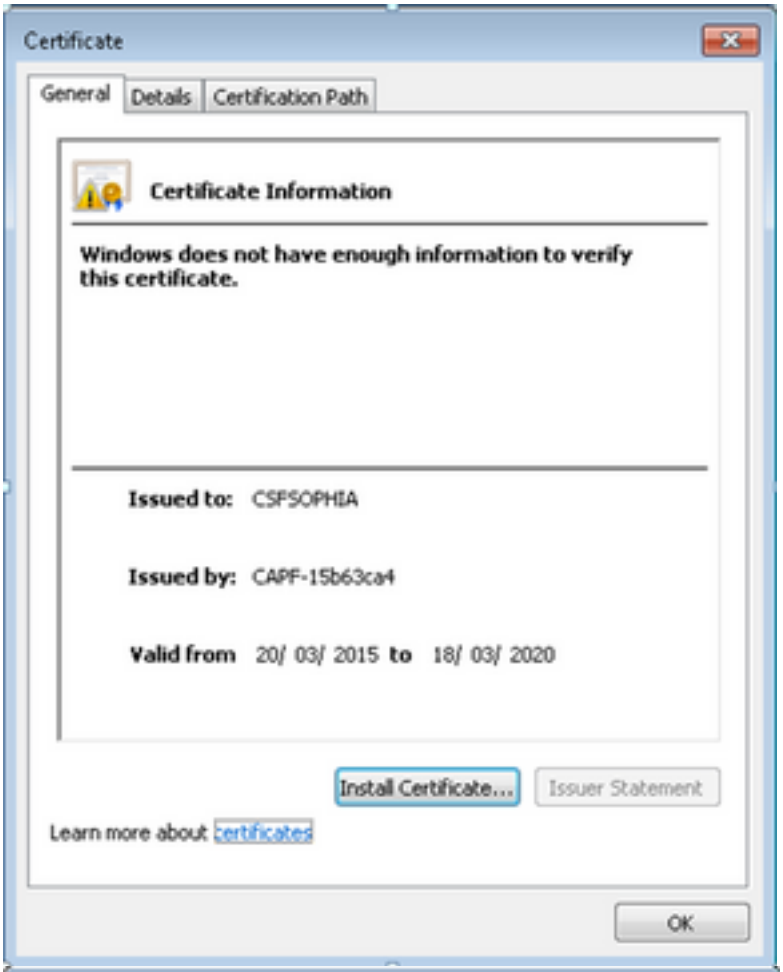


Проверка

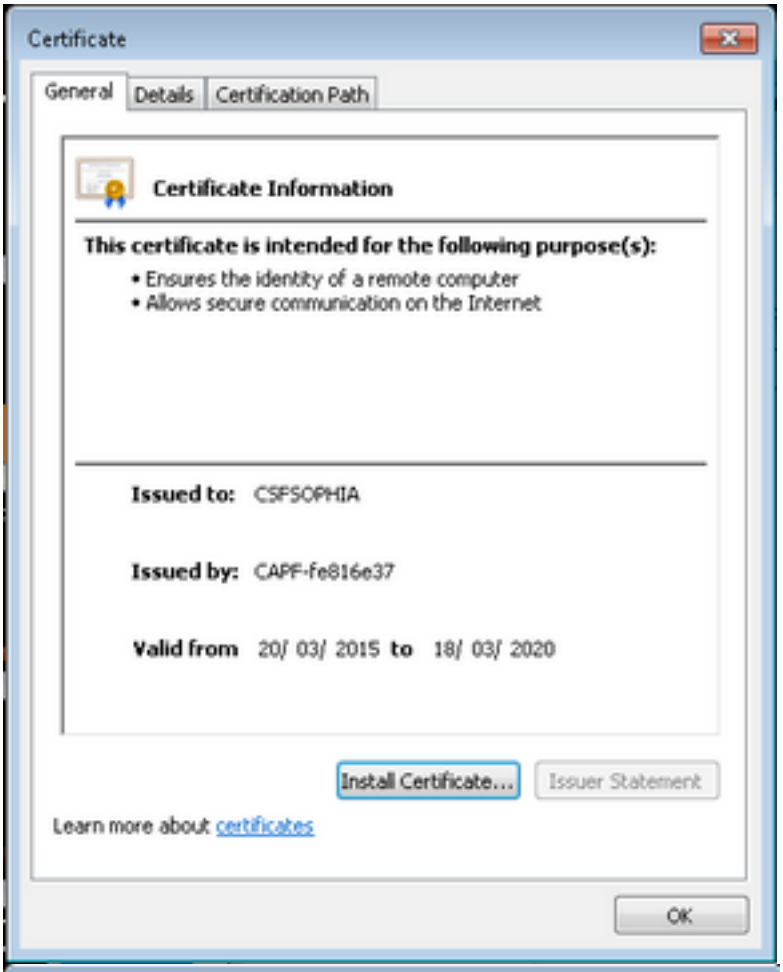
Сравните LSC когда самоподпаливший CAPF и подписанный CA CAPF:

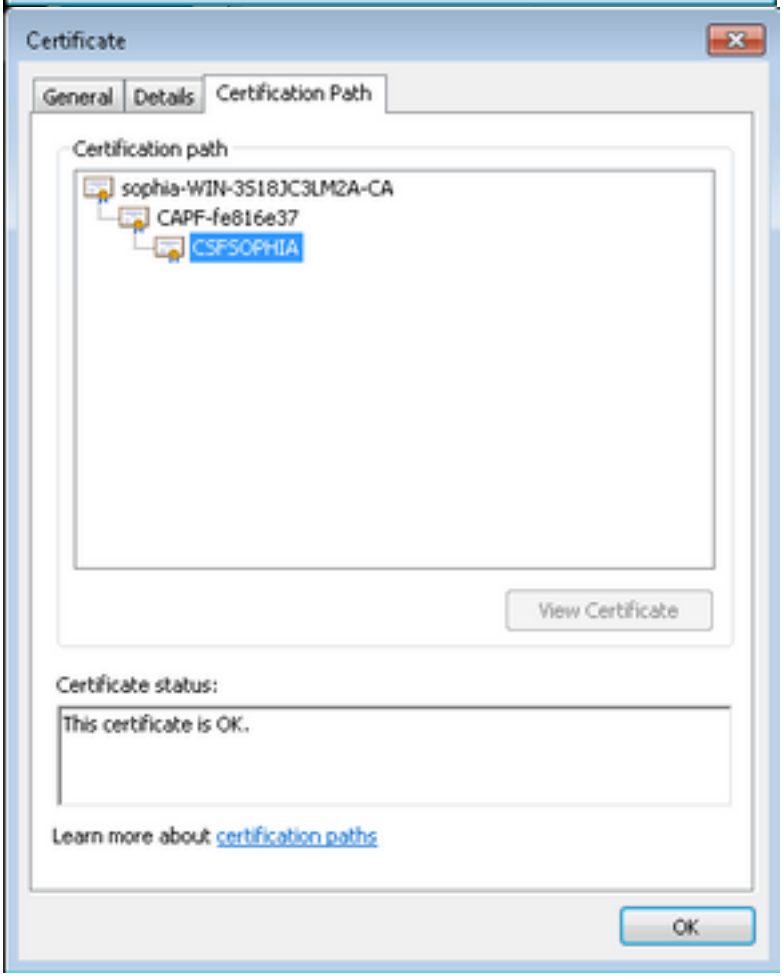
Как вы можете видеть от этих образов для LSC, с точки зрения LSC, CAPF является узлом CA при использовании самоподписанного CAPF, но CAPF зависимое (промежуточное звено) CA при использовании подписанного CA CAPF.

LSC, когда Самоподписанный CAPF



LSC, когда подписанный CA CAPF





Устранение неполадок

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

Дополнительные сведения

Известная неисправность: CA Сертификат CAPF со знаком, корневое свидетельство должно быть загружено как доверие CM: https://bst.cloudapps. cisco . com/bugsearch/bug/CSCut87382/? referring_site=bugquickviewredir