CUCM のための CA によって署名する CAPF 証明書

目次

概要

この資料に Cisco Unified Communications Manager （CUCM）のための認証局（CA）によって署名するプロキシ 機能（CAPF）証明書を認証局（CA）得る方法を記述されています。 外部 CA の CAPF に署名する要求が常にあります。 この資料はなぜであるコンフィギュレーション手順重要どのようにはたらくか理解するために示したものです。

前提条件

要件

次の項目に関する知識が推奨されます。

- 公開キー インフラストラクチャ（PKI）
- CUCM セキュリティとコンフィギュレーション

使用するコンポーネント

この資料に記載されている情報は基づいた on Cisco Unified Communications Manager バージョン 8.6 および それ 以上です。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメン

トで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。

制限

別の CA は CSR に異なる必要条件があるかもしれません。 OpenSSL CA の別のバージョンが細目をしかし Microsoft Windows CA 作業をよく今のところ議論がこの記事で力バーされない、Cisco CAPF からの CSR と CSR 頼んでもらうというレポートがあります。

関連製品

このドキュメントは、次のバージョンのハードウェアとソフトウェアにも使用できます。

- Microsoft Windows サーバ 2008 CA。
- Cisco Jabber for Windows （異なる vervions は LSC を保存するフォルダの異なる名前があるかもしれません）。

背景説明

CA によって署名される CAPF の目的

何人かの顧客は会社によってが他のサーバとそうそこに必要性署名した同じ CA の CAPF にである globle 証明書 ポリシー whith と一直線に並ぶことを望みます。

この PKI のためのメカニズム

デフォルトで、ローカルで固有の証明書（LSC）は CAPF、従って CAPF によってですこのシナリオの電話のための CA 署名します。 ただし CAPF を外部 CA によって署名されて得ることを試みるときそしてこのシナリオの CAPF は下位 CA か中間 CA として機能します。

自己署名 CAPF と CA 署名付き CAPF の違いは次のとおりです: CAPF は LSC へ LSC へ CA 署名付き CAPF をするとき自己署名 CAPF をするとき、CAPF ルートCA です下位（中間） CA です。

どのように CAPF CSR 他の CSR と異なっていますか。

RFC5280 に見なして、キー使用状況拡張は証明書に含まれているキーの目的（例えば、暗号化、署名するシグニチャ、証明書）を定義します。 CAPF は証明書 プロキシであり、CA および電話にリーフ（ユーザ識別）として機能する IPSec 証明書 CallManager のような他の証明書に、Tomcat 署名、できますが。 それらのための CSR 調べるとき、CAPF CSR に CertificateSign **ロール**他がないことを見ることができます。

CAPF CSR:

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

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

Tomcat CSR:

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

CallManager CSR:

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

IPSec CSR:

属性: 要求された拡張機能: X509v3 拡張キー使用法: TLS Webサーバ認証、TLS Web クライエント認証、IPSec エンド システム X509v3 キー使用法: デジタル署名、キー暗号化、データ暗号化、キー協定

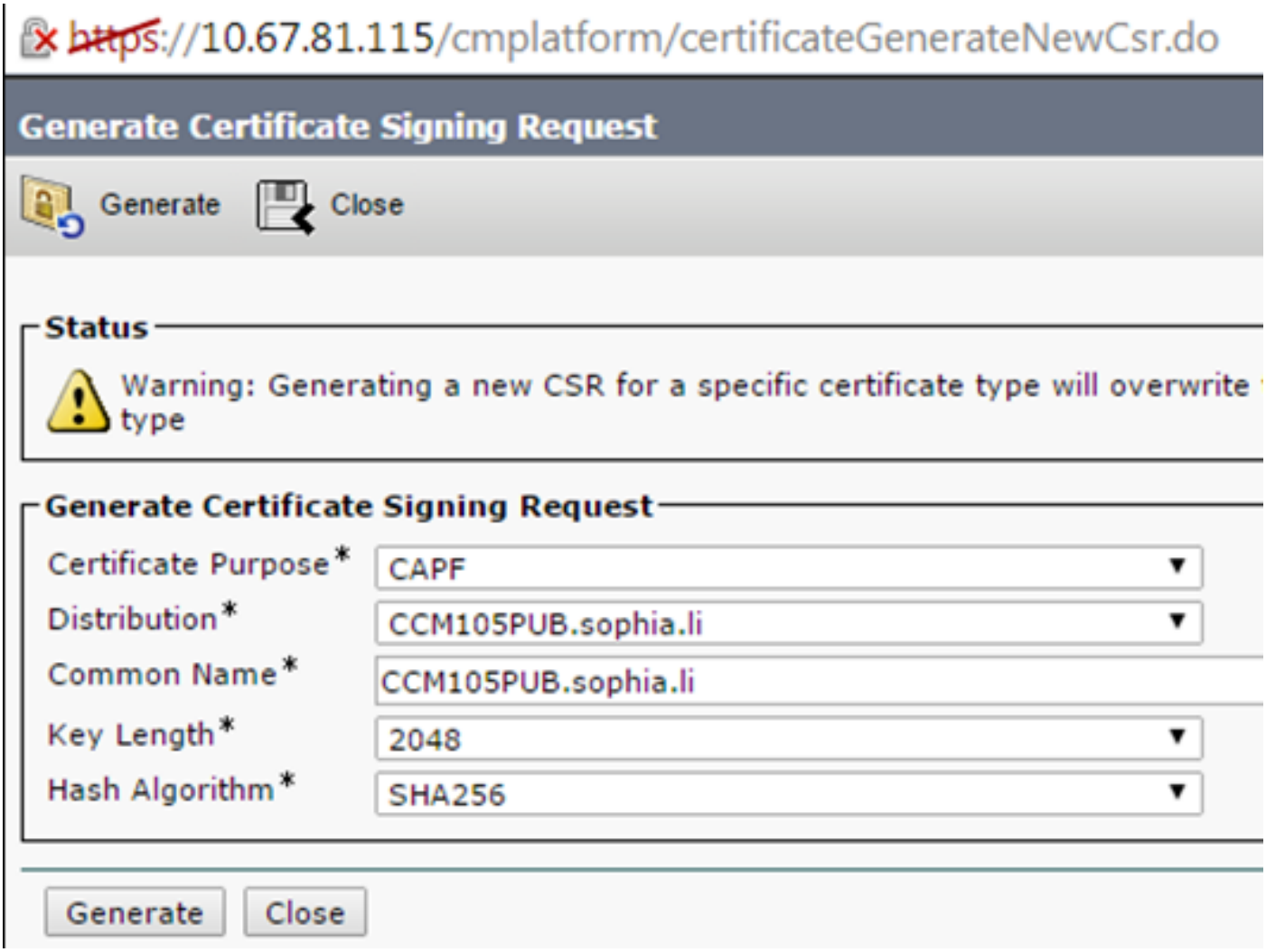
設定

1 シナリオは、外部ルートCA CAPF 証明書に署名するのに使用されていますここにあります: Jabber クライアントおよび IP 電話のための場合/メディアを暗号化しました。

ステップ 1： セキュリティ クラスタとして CUCM クラスタを作って下さい。

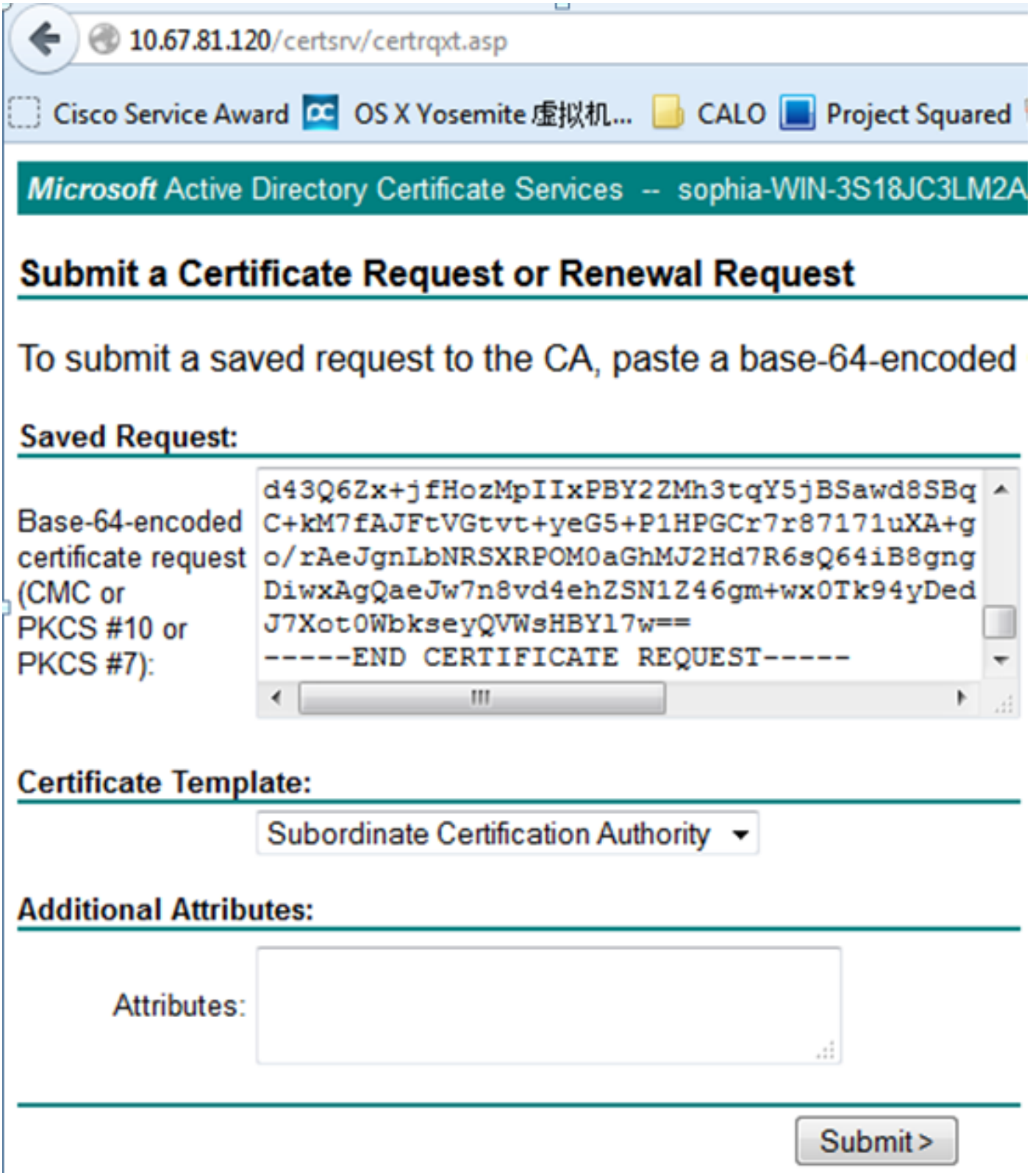
```
admin:utils ctl set-cluster mixed-mode
```

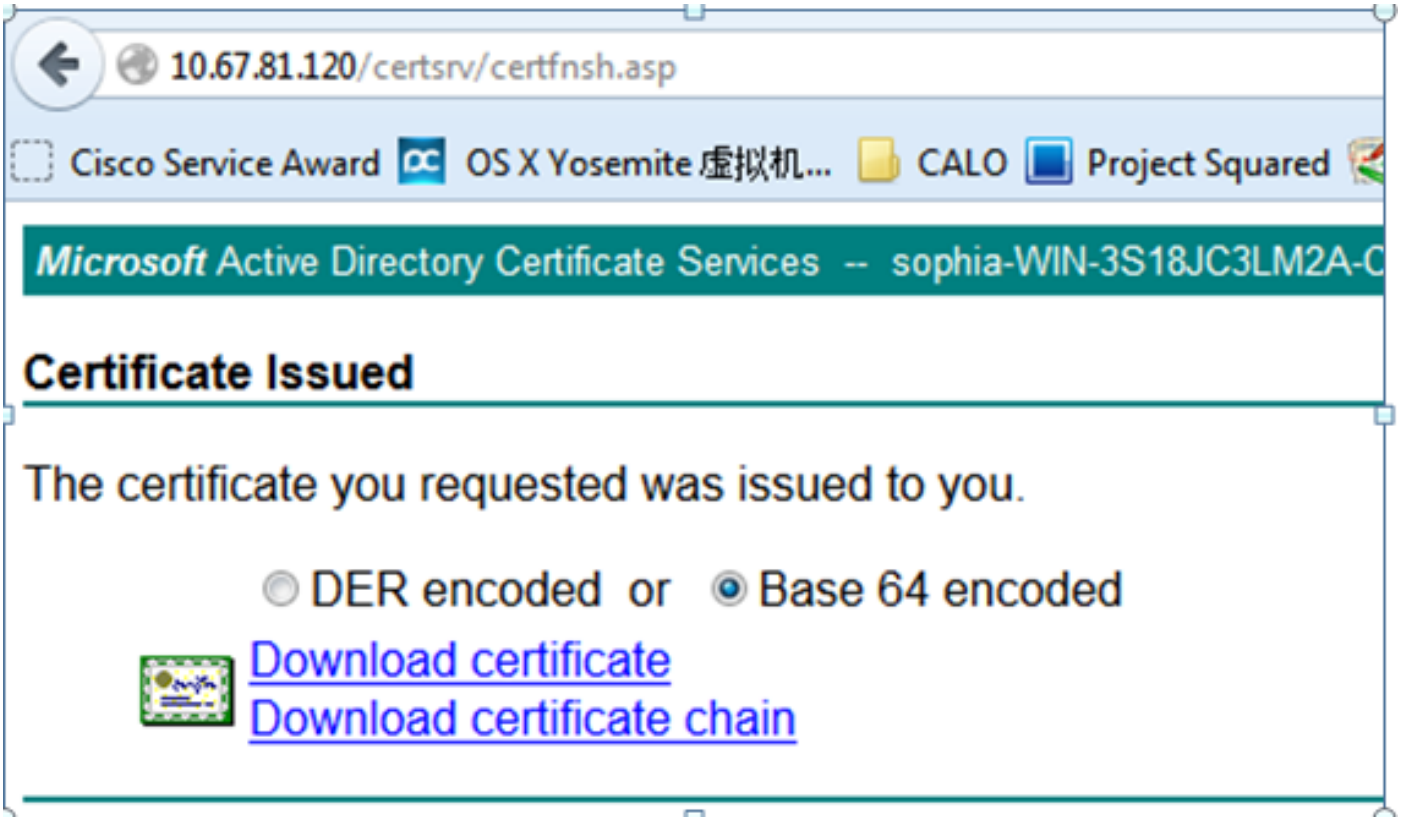
ステップ 2.イメージに示すように、CAPF CSR を生成して下さい。



ステップ 3. CA とこれに署名しました（Windows 2008 CA の従属テンプレートを使用して）。

注: ユーザ **下位認証局** テンプレートがこの証明書に署名することを必要とします。


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 >

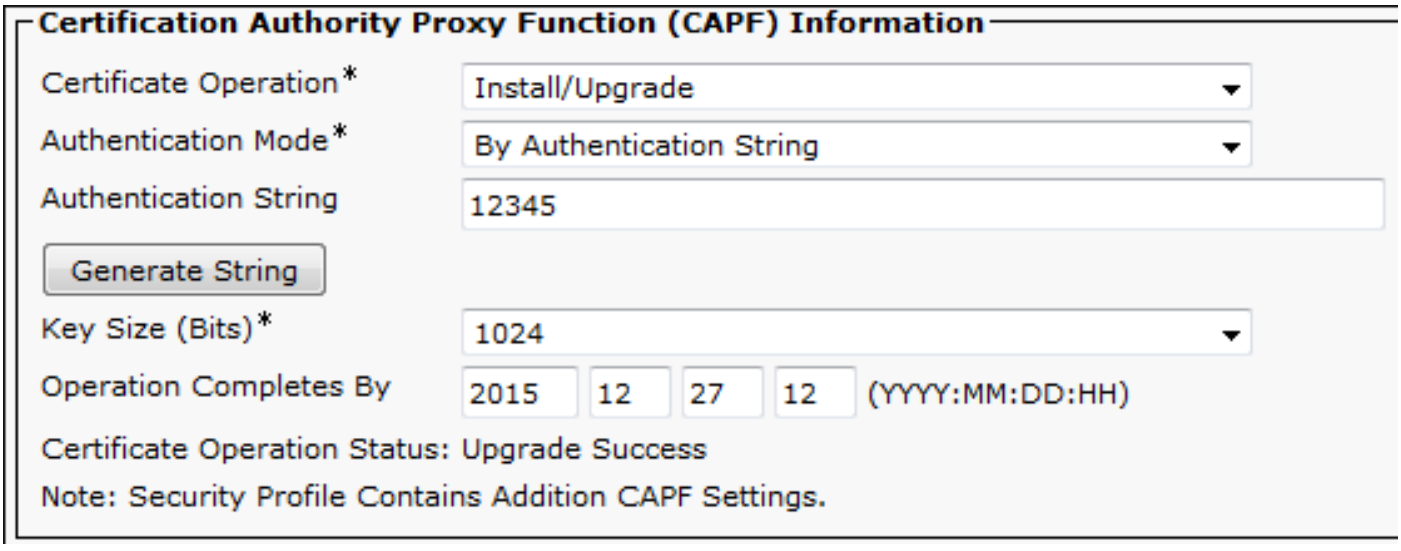


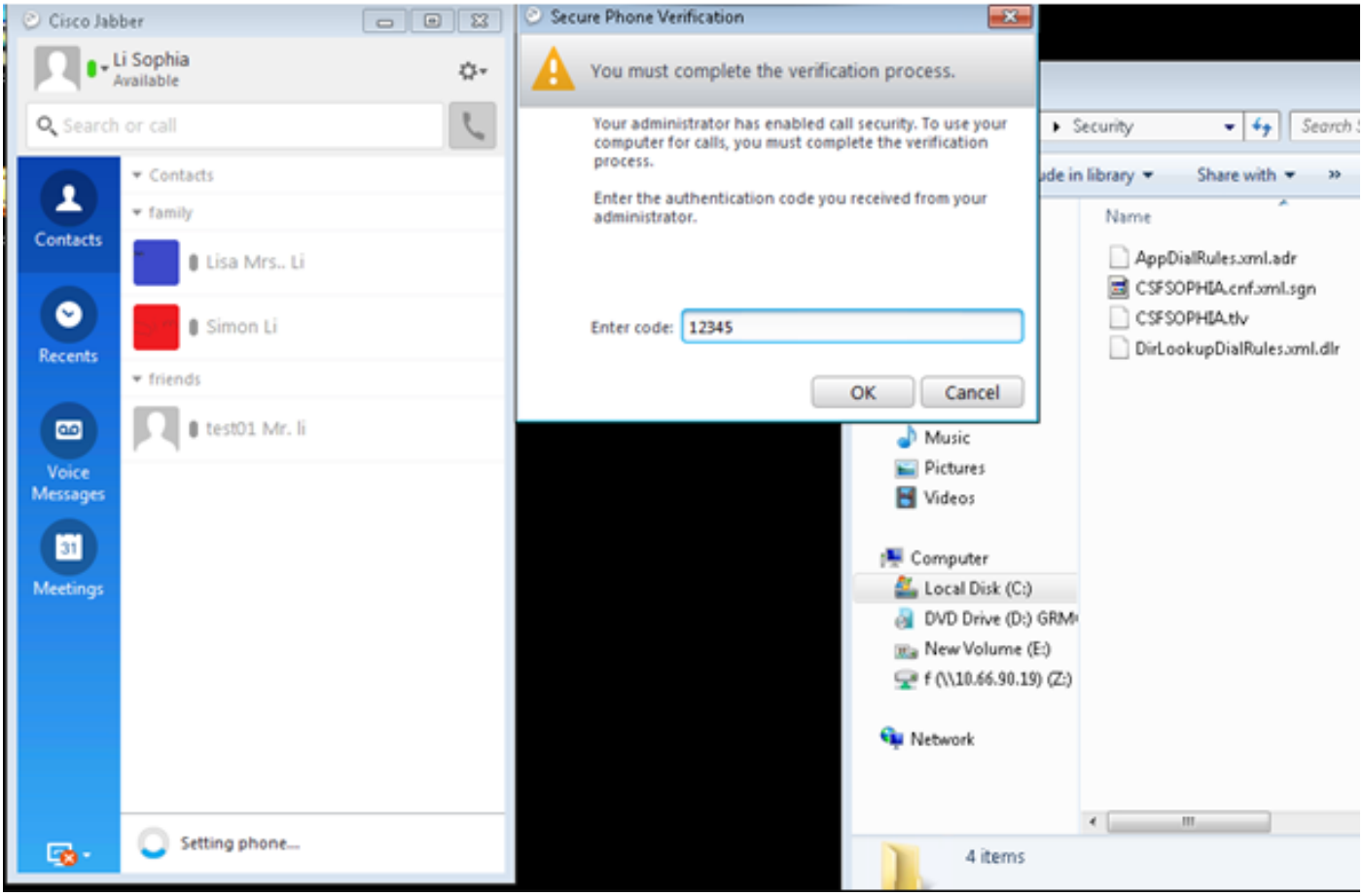
ステップ 4. CAPF 信頼としてルートCA および CAPF としてサーバ証明をアップ ロードして下さい。 このテストに関しては、CallManager 信頼が署名された LSC として Jabber と CallManagerサービス間の TLS 接続を持つために CallManagerサービスによって同様に信頼される必要があるようにまたこのルートCA をアップロードして下さい。 この技術情報の始めに述べられる、すべてのサーバのための CA を一直線に並べる必要があります従ってこの CA は場合/メディア暗号化のための CallManager に既にアップロードする必要があります。 IP 電話 802.1X の展開の screnario に関しては、ミックス モードとして CUCM を作るか、または CUCM サーバに CallManager 信頼として CAPF に署名する CA をアップロードする必要がありません。

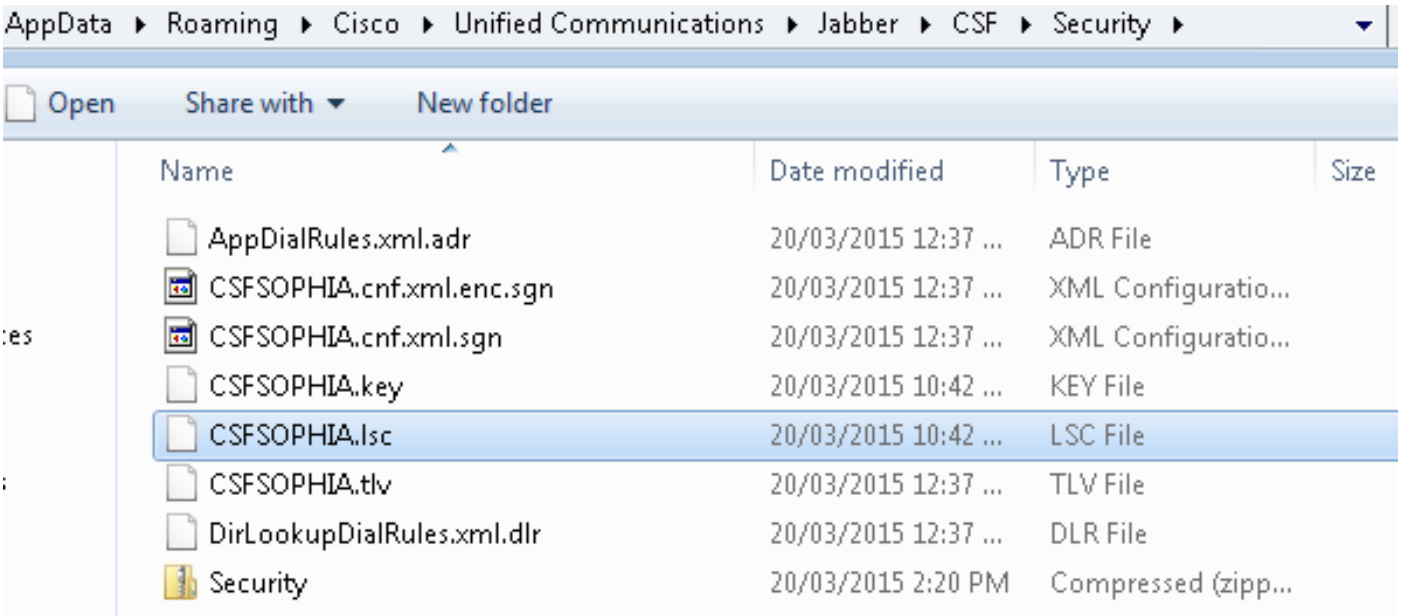
ステップ 5. CAPF サービスを再開して下さい。

ステップ 6.すべてのメモの CallManager/TFTP サービスを再開して下さい。

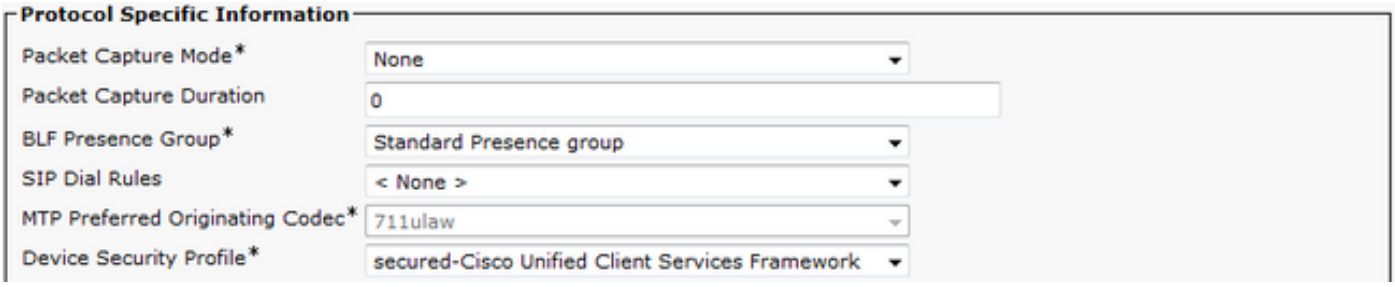
ステップ 7. Jabber softphone LSC に署名しました。



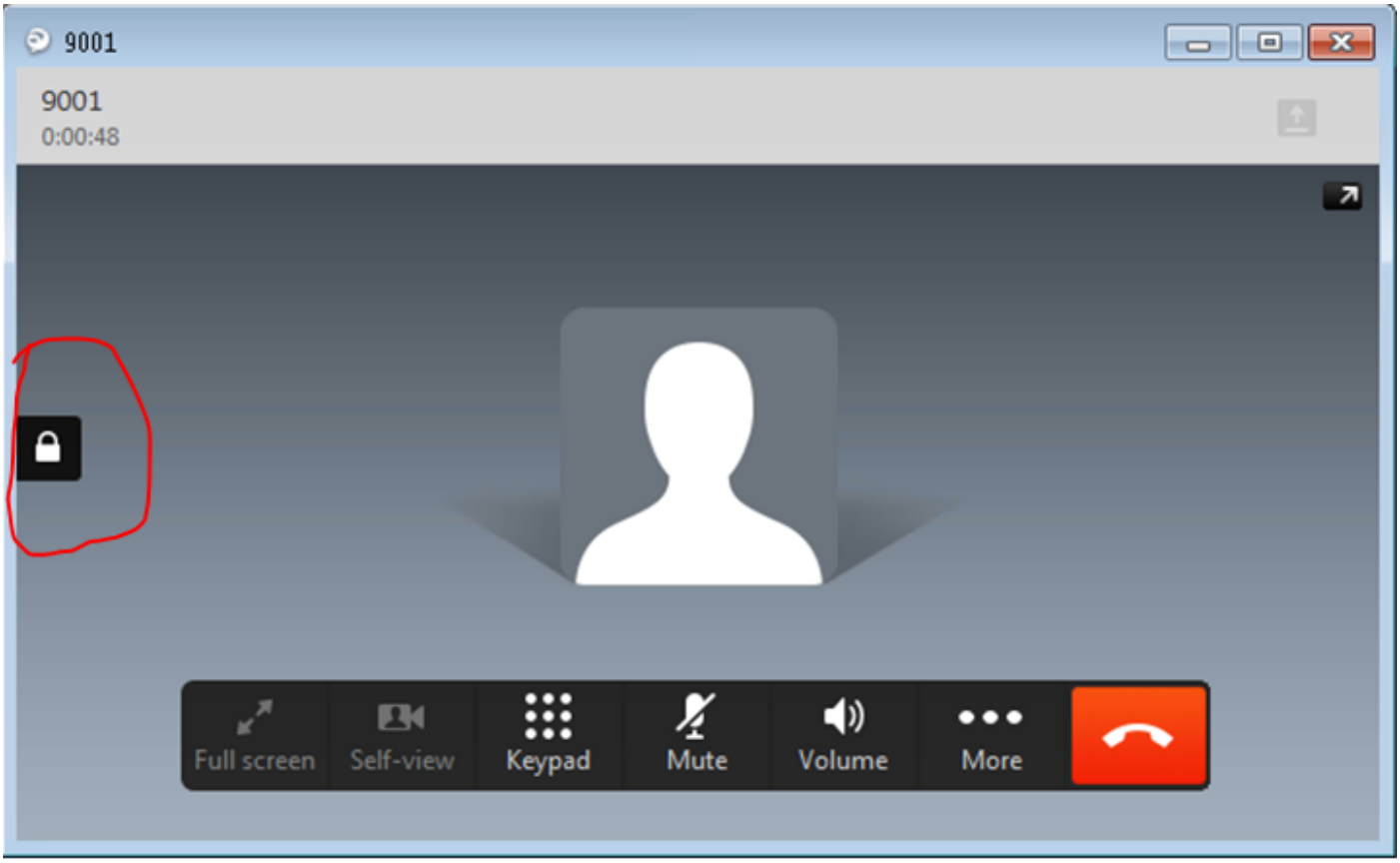




ステップ 8. Jabber softphone のためのセキュリティプロファイルを有効に して下さい。



ステップ 9： この場合保護された RTP はとして起こります:

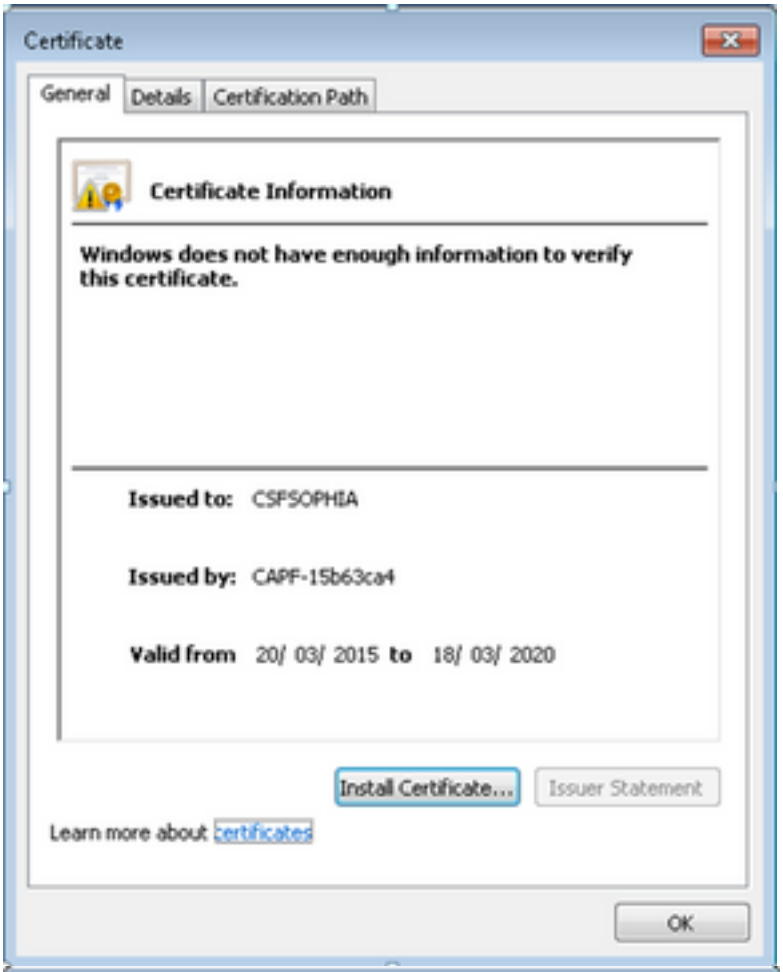


確認

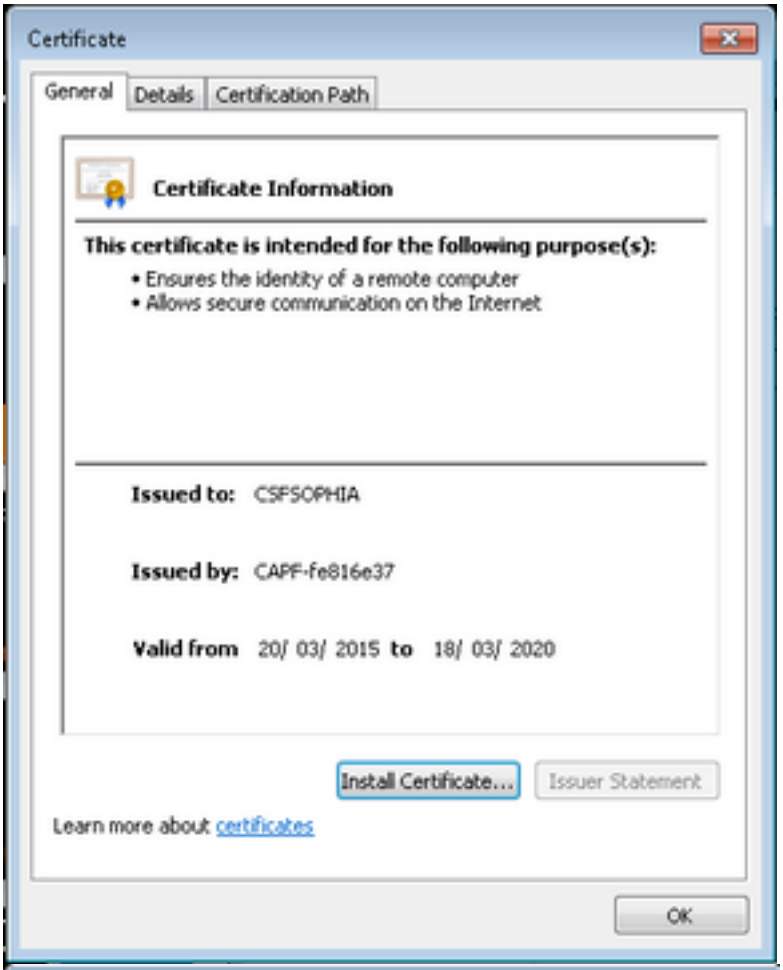
自己焼かれた CAPF および CA 署名付き CAPF 時 LSC を比較して下さい:

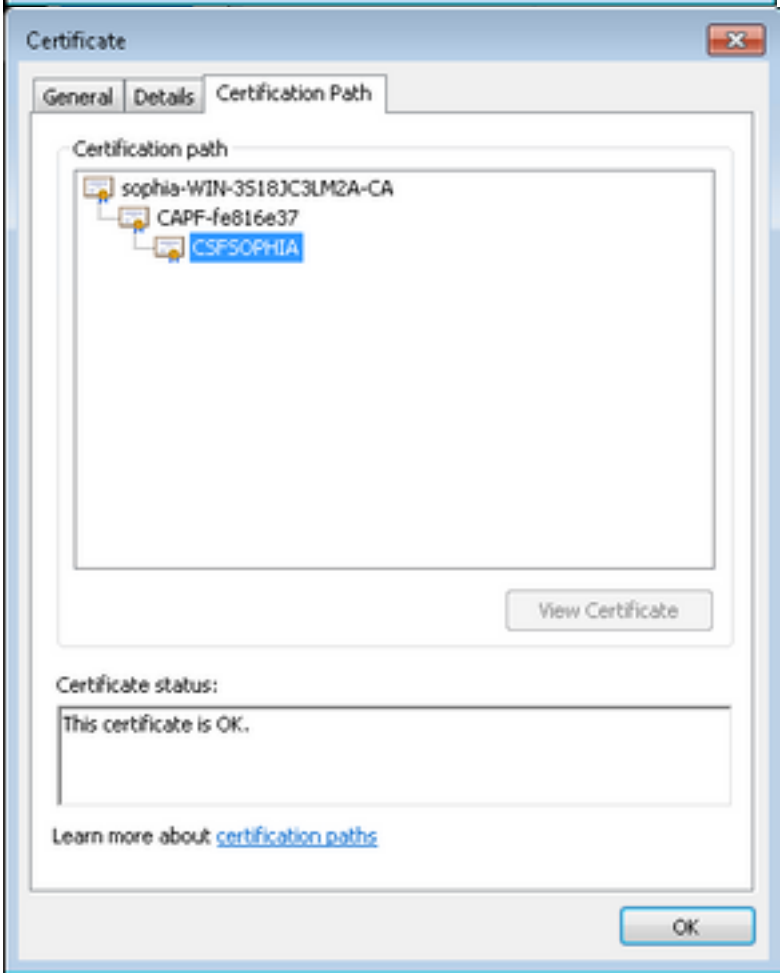
自己署名 CAPF CAPF を使用する場合の LSC についてはこれらのイメージから CAPF であるルートCA である下位（中間） CA CA 署名付き CAPF を使用しながら、LSC 観点からが、わかるように。

LSC 場合の自己署名 CAPF



LSC 場合の CA 署名付き CAPF





トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

既知問題: CA によって署名される CAPF 証明書は CM 信頼として、ルート CERT アップ ロードする必要があります:

https://bst.cloudapps.cisco.com/bugsearch/bug/CSCut87382/?referring_site=bugquickviewredir