# Q.A voor CUCM-TELEFOONCERTIFICATEN (LSC/MIC)

## Inhoud



## Inleiding

Dit document behandelt een aantal vragen en antwoorden voor Cisco Unified Communications Manager (CUCM)-telefooncertificaten.  Hier volgt een snel overzicht van de telefooncertificaten.

Geïnstalleerd certificaat (MIC):

Zoals de naam aangeeft, worden de telefoons vooraf met de MIC geïnstalleerd en dit kan niet worden verwijderd / aangepast door de beheerders. De certificaten CAP-RTP-001, CAP-RTP-002, Cisco_Manufacturing_CA en Cisco Industrial CA SHA2 zijn vooraf in het CUCM geïnstalleerd om het MIC te vertrouwen. MIC kan niet worden gebruikt zodra de geldigheid is verlopen, aangezien

de MIC CA niet kan worden gegenereerd,

Lokaal belangrijk certificaat (LSC):

LSC heeft de openbare sleutel voor de Cisco IP-telefoon, die wordt ondertekend door de privé-sleutel van Cisco Unified Communications Manager Proxy-functie (CAPF). Het wordt standaard niet aan de telefoon geïnstalleerd. De beheerder heeft volledige controle over LSC. Het CAPF CA-certificaat kan op zijn beurt opnieuw worden gegenereerd kan nieuwe LSC aan de telefoons uitgeven wanneer nodig.

# Wat zijn de gemeenschappelijke toepassingen voor telefooncertificaten?

Hier zijn een aantal gebruikelijke toepassingen voor de telefooncertificaten

## Tussen CAPF en Phone voor installatie/upgrades, verwijderen of problemen oplossen

Telefonisch bevestigt de verbinding met CAPF om het certificaat van de Installatie te installeren/te verbeteren, te wissen of van de probleemoplossing op de Telefoon. Er wordt een telefooncertificaat gebruikt om de verbinding met CAPF tot stand te brengen wanneer de verificatiemodus onder CAPF-informatie (certificaatfunctie) wordt ingesteld bij bestaand certificaat (voorrang op LSC) of bij bestaand certificaat (voorrang op MIC).

Op bestaand certificaat (voorrang voor LSC):  De telefoon gebruikt LSC om voor authentiek te verklaren met CAPF. Deze toepassing maakt gebruik van MIC als LSC niet is geïnstalleerd. De installatie is mislukt met reden "ongeldig LSC" als er problemen zijn met het gebruikte certificaat. De ondertekende CA voor de LSC is bijvoorbeeld niet beschikbaar in het CAPF Trust. Update de authenticatiemodus met behulp van andere certificatiemethode of met een string die op dergelijke mislukkingen berust.

Op bestaand certificaat (voorrang voor MIC): De telefoon gebruikt MIC om voor authentiek te verklaren met CAPF.

## Tussen CallManager en IP-telefoon voor TLS-verbinding (Transport Layer Security)

De telefoon gebruikt LSC of MIC om TLS verbinding met CallManager te maken. CallManager zal het door de telefoon aangeboden certificaat valideren door het CallManager-vertrouwen te controleren. Het respectieve CAPF-certificaat moet beschikbaar zijn in CallManager-trust voor LSC en Cisco Fabriture CA's voor MIC.

## Tussen telefoon en verificatie-server voor 802.1x-verificatie

CAPF/Manufacturing CA-certs worden geüpload naar verificatie-servers zoals Cisco Secure Access Control Server (ACS) of Identity Services Engine (ISE). De verificatieserver gebruikt de geüploade certificaten om de telefoon te authenticeren wanneer het certificaat wordt overgelegd (LSC of MIC).

### Voor op certificaat gebaseerde verificatie tussen telefoon en Cisco adaptieve security applicatie (ASA) voor VPN

CAPF/Fabric CA certs worden geüpload in ASA, wanneer telefoon LIC/MIC aanbiedt, ASA geldig door het vertrouwen te controleren.

## Wanneer LSC en MIC aanwezig zijn, is er een manier om LSC of MIC expliciet te selecteren voor verbindingen?

Geen optie om te selecteren of LSC of MIC voor de verbindingen. Als LSC is geïnstalleerd, gebruikt de telefoon LSC. De telefoon gebruikt de MIC als LSC niet is geïnstalleerd.

Console-ingang wanneer LSC niet aanwezig is:

SECD: -PXY_NO_LSC: Er wordt geen LSC voor [SCCP] gebruikt om MIC te proberen

Console-ingang wanneer LSC aanwezig is:

SECD: -PXY_CERT_CIPHER: [SCCP], [TLSv1], cert [LSC]

Selecteren van LSC of MIC is alleen mogelijk tussen CAPF en Phone die wordt geïnstalleerd/bijgewerkt, verwijderd of probleemoplossing.

## Wat is de reden dat de LSC geïnstalleerde telefoons met beveiligd profiel niet geregistreerd worden wanneer ze naar een nieuw cluster gaan?

Dit kan gebeuren voor de telefoons die al een LSC van de OUDE Cluster hebben. Wanneer zowel MIC als LSC aanwezig zijn, wordt LSC gebruikt om de TLS-verbinding tot stand te brengen. TLS kan niet worden ingesteld omdat het nieuwe CUCM niet de CA voor deze LSC in zijn CallManager-trust heeft.

Logboeken van de console tonen welk certificaat wordt gebruikt om het TLS vast te stellen. Hieronder staat de LSC-code.

3469 NIET 00:01:31.935298 SECD: -PXY_CERT_CIPHER: [SCCP], [TLSv1], cert [LSC], algoritme [AES256-SHA:AES128-SHA]

SSL3_Alert met "onbekende CA" voor dergelijke mislukte gevallen in consols logs:-

3486 ERR 00:01:31.938954 SECD: -STATE_SSL3_ALERT: SSL3-waarschuwing [lees]:[fataal]:[onbekende CA]

Eén van de manieren om deze kwestie op te lossen is om de telefoon geregistreerd te krijgen met behulp van een niet-veilig profiel en de bestaande LSC te verwijderen. Installeer de LSC uit een nieuw cluster en registreer de telefoon met beveiligd profiel. Het is ook mogelijk om de telefoon met beveiligd profiel te hebben geregistreerd met MIC zonder de LSC te installeren.

## Is het vereist dat de LSC voor de telefoons geïnstalleerd is om deze te laten registreren met behulp van beveiligd of geversleuteld profiel?

Nee. Als LSC niet is geïnstalleerd, gebruikt de telefoon MIC om de TLS-verbinding met de CUCM in te stellen.

4878 WRN 15:47:34.756063 SECD: -PXY_NO_LSC: Geen LSC voor [SCCP] probeert MIC.

## Is het verplicht dat de Security Mode van het apparaat in het respectievelijke apparaat Security Profile wordt geauthenticeerd of versleuteld om een LSC te installeren/upgraden?

Het is niet verplicht, het kan worden gedaan met de standaard Niet-beveiligd profiel en ook waar dat niet veilig is in de Apparaatbeveiligingsmodus.

## Is het verplicht de Cluster in Gemengde Modus om de LSC in de Telefoon te installeren?

Het is niet verplicht. LSC installeren/verwijderen kan ook worden uitgevoerd als de beveiligingsmodus van het cluster niet veilig is.

## Hoe snel te testen als er een probleem is met de LSC die door de telefoon wordt gebruikt?

Verwijdert de LSC in een van de telefoons door naar de pagina Telefonisch beheer te gaan. Hiermee wordt de telefoon gedwongen om MIC te gebruiken. Als alle problemen met MIC opgelost zijn, gaat u naar de probleemoplossing met LSC.

## Hoe krijgt u de telefooncertificaten voor probleemoplossing?

Stel de certificaathandeling in op probleemoplossing onder het apparaat/de telefoon. Sla op en pas Config toe. Wacht tot de optie Handelscatus van het certificaat **is** ingesteld op **Probleemoplossing**. Verzamel **Cisco-functiekaarten** voor **proxy** van Real Time Monitoring Tool (RTMT). Het bevat de certificaten van de Telefoon.

## Hoe te verifiëren van pakketvastlegging, als LSC of MIC van de telefoon wordt gebruikt om de TLS verbinding met CallManager te vestigen?

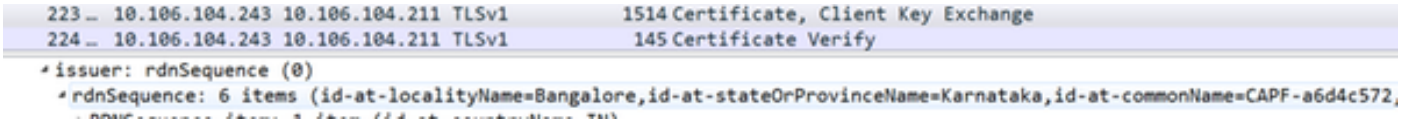
Verzamel de Packet Capture voor het opnieuw opstarten van de telefoon.

Controleer het certificaatbericht, het bericht van de Clientuitwisseling. Controleer het certificaat dat

vanaf IP-telefoon wordt verzonden.

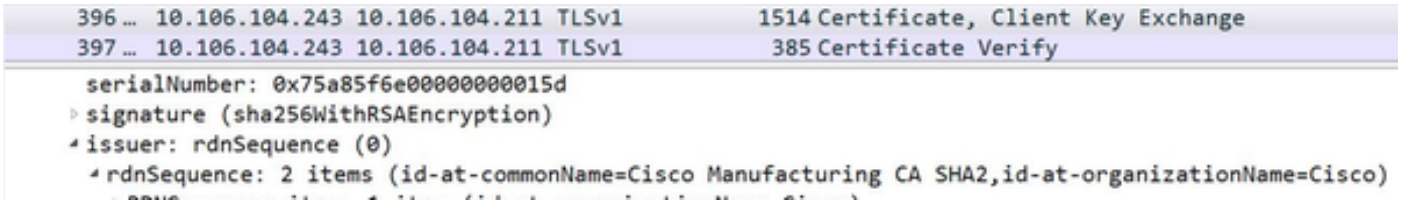
Voorbeeld LSC:

Voor het LSC wordt CAPF GN gezien in het uitgevende veld. De respectieve CAPF wortel moet in CallManager-vertrouwen aanwezig zijn.




Voorbeeld MIC:

Voor de MIC, Cisco Manufacturing CA in het uitgevende veld. Respectieve Root CA moet aanwezig zijn in CallManager-trust.




# Wat is het belang van de verificatiemodus onder informatie van de certificeringsinstantie Proxy (CAPF)? Is er betekenis voor de TLS-verbinding tussen CUCM en telefoon?

Het is niets anders dan een authenticatiemethode tussen Phone en CAPF voor het installeren/verbeteren/verwijderen en het oplossen van operaties. Het heeft geen betekenis voor TLS-verbinding tussen CUCM en telefoon.

# Wat zijn de basisoperaties van LSC voor de telefoons om na het CAPF certificaat opnieuw te genereren te overwegen?

In deze paragraaf wordt het nutteloze scenario behandeld waarbij geen offline CA wordt gebruikt voor de uitgifte van de LSC.

## TLS-verbinding met CallManager

Zorg ervoor dat u de nieuwe LSC per telefoon installeert voordat u het vorige CAPF-certificaat uit CallManager-trust verwijdert. Het verwijderen van het vorige CAPF-certificaat gevolgd door een herstart van de CallManager-service veroorzaakt de registratieproblemen met de telefoons die de LSC hebben afgegeven door dit CAPF-certificaat.

## LSC-bewerkingen met CAPF-vertrouwen

Zorg ervoor dat u de nieuwe LSC per telefoon installeert voordat u het vorige CAPF-certificaat uit CAPF-trust verwijdert. LSC-bewerkingen zoals installeren/verwijderen met behulp van verificatiemodus **door bestaand certificaat (voorrang op LSC)** mislukken met **Ongeldige LSC** voor telefoons die de LSC hebben afgegeven door dit CAPF-certificaat.

### Tussen telefoon en verificatie-server voor 802.1x-verificatie

Zorg ervoor dat het vorige CAPF-certificaat niet van de verificatieserver wordt verwijderd totdat het nieuwe CAPF-certificaat is geüpload en de telefoon de LSC krijgt die door nieuwe CAPF wordt verstrekt.

### Tussen ASA en IP

Zorg ervoor dat het vorige CAPF certificaat van ASA niet van ASA wordt gewist tot de telefoon het nieuwe LSC krijgt en het nieuwe CAPF CA certificaat aan ASA uploadt.

*Raadpleeg de* certificaatregeneratie voor de stappen die moeten worden gevolgd om het CAPF-certificaat te regenereren.

## Verwante informatie

- Cisco IP-telefooncertificaten en beveiligde communicatie
- IP-telefonie voor 802.1X ontwerpgids
- Cisco Unified Communications Manager-beveiligingsgids