Q.A für CUCM-TELEFONZERTIFIKATE (LSC/MIC)

Inhalt

Einführung

In diesem Dokument werden einige Fragen und Antworten zu den Cisco Unified Communications Manager (CUCM)-Telefonzertifikaten behandelt. Hier finden Sie eine kurze Übersicht über die Telefonzertifikate.

Vom Hersteller installiertes Zertifikat (MIC):

Wie der Name bereits andeutet, sind Telefone mit dem MIC vorinstalliert, und dieser Vorgang

kann von den Administratoren nicht gelöscht/geändert werden. Die Zertifikate CAP-RTP-001, CAP-RTP-002, Cisco_Manufacturing_CA und Cisco Manufacturing CA SHA2 sind im CUCM vorinstalliert, um das MIC zu vertrauen. MIC kann nicht verwendet werden, wenn die Gültigkeit abgelaufen ist, da die MIC CA nicht erneut generiert werden kann.

LSC (Locally Significant Certificate):

Das LSC verfügt über den öffentlichen Schlüssel für das Cisco IP-Telefon, der vom privaten Schlüssel der Cisco Unified Communications Manager Certificate Authority Proxy Function (CAPF) signiert wird. Standardmäßig ist es nicht auf dem Telefon installiert. Der Administrator hat die volle Kontrolle über LSC. Das CAPF CA-Zertifikat kann wiederum bei Bedarf neu generiert werden. Das Zertifikat kann den Telefonen dann bei Bedarf ein neues LSC ausstellen.

Was sind die häufigsten Verwendungszwecke für Telefonzertifikate?

Hier einige häufige Verwendungsmöglichkeiten für die Telefonzertifikate:

Zwischen CAPF und Telefon für Installation/Upgrade, Löschung oder Fehlerbehebung

Telefon stellt Verbindung mit CAPF her, um das Zertifikat für Installation/Upgrade, Löschen oder Fehlerbehebung auf dem Telefon zu installieren/zu löschen. Die Telefonbescheinigung dient zum Herstellen der Verbindung mit CAPF, wenn der Authentifizierungsmodus unter CAPF-Informationen (Certification Authority Proxy Function) auf By Existing Certificate (Precedence to LSC) oder By Existing Certificate (Precedence to MIC)festgelegt ist.

Durch bestehendes Zertifikat (Precedence to LSC): Telefon verwendet LSC für die Authentifizierung mit CAPF. Wenn LSC nicht installiert ist, wird MIC verwendet. Die Installation schlägt fehl, wenn Probleme mit dem verwendeten Zertifikat vorliegen. Beispielsweise ist die signierte CA für das LSC im CAPF Trust nicht verfügbar. Aktualisieren Sie den Authentifizierungsmodus mithilfe einer anderen Zertifikatmethode oder einer NULL-Zeichenfolge für solche Fehlerfälle.

Durch bestehendes Zertifikat (Rangfolge zum MIC): Telefon verwendet MIC zur Authentifizierung mit CAPF.

Zwischen CallManager und Phone for Transport Layer Security (TLS)-Verbindung

Das Telefon verwendet LSC oder MIC, um eine TLS-Verbindung mit CallManager herzustellen. CallManager überprüft CallManager-trust, um das vom Telefon bereitgestellte Zertifikat zu validieren. Das entsprechende CAPF-Zertifikat muss in CallManager-trust für LSC und Cisco Manufacture CAs für MIC verfügbar sein.

Zwischen Telefon und Authentifizierungsserver für 802.1x-Authentifizierung

CAPF/Manufacturing CA-Zertifikate werden auf Authentifizierungsserver wie Cisco Secure Access Control Server (ACS) oder Identity Services Engine (ISE) hochgeladen. Der

Authentifizierungsserver verwendet die hochgeladenen Zertifikate, um das Telefon zu authentifizieren, wenn es sein Zertifikat (LSC oder MIC) vorlegt.

Zur zertifikatsbasierten Authentifizierung zwischen Telefon und Cisco Adaptive Security Appliance (ASA) für VPN

CAPF/Manufacture CA-Zertifikate werden in ASA hochgeladen. Wenn das Telefon LIC/MIC vorlegt, validiert ASA diese Zertifikate, indem die Vertrauenswürdigkeit überprüft wird.

Wenn LSC und MIC vorhanden sind, gibt es eine Möglichkeit, LSC oder MIC explizit für Verbindungen auszuwählen?

Keine Option zur Auswahl von LSC oder MIC für die Verbindungen. Wenn LSC installiert ist, verwendet Telefon LSC. Das Telefon verwendet das MIC, wenn das LSC nicht installiert ist.

Konsoleneintrag, wenn kein LSC vorhanden ist:

ABSCHNITT: -PXY_NO_LSC: Kein LSC für [SCCP], versucht MIC

Konsoleneintrag bei LSC:

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

Die Auswahl von LSC oder MIC ist nur zwischen CAPF und Telefon mit Installation/Upgrade, Löschen oder Fehlerbehebung möglich.

Aus welchem Grund werden die bei LSC installierten Telefone mit gesichertem Profil beim Umstieg auf einen neuen Cluster nicht registriert?

Dies kann bei Telefonen passieren, die bereits über ein LSC aus dem älteren Cluster verfügen. Wenn sowohl MIC als auch LSC vorhanden sind, wird LSC zum Herstellen der TLS-Verbindung verwendet. TLS kann nicht eingerichtet werden, da der neue CUCM die CA für dieses LSC nicht in seiner CallManager-Vertrauenswürdigkeit hat.

Konsolenprotokolle zeigen, welches Zertifikat für die Einrichtung des TLS verwendet wird. Unten sehen Sie, dass LSC verwendet wird.

3469 NICHT 00:01:31.935298 ABSCHNITT: -PXY_CERT_CIPHER: [SCCP], [TLSv1], cert [LSC], cipher [AES256-SHA:AES128-SHA]

SSL3_Alert mit "unbekannter CA" für solche fehlgeschlagenen Fälle in Konsolenprotokollen:-

3486 ERR 00:01:31.938954 SECD: -STATE_SSL3_ALERT: SSL3-Warnung [read]:[fatal]:[unbekannte CA]

Eine Möglichkeit zur Lösung dieses Problems besteht darin, das Telefon mit einem nicht sicheren Profil zu registrieren und anschließend das vorhandene LSC zu löschen. Installieren Sie das LSC

aus einem neuen Cluster, und registrieren Sie das Telefon mithilfe des gesicherten Profils. Es ist auch möglich, das Telefon mit gesichertem Profil über MIC registrieren zu lassen, ohne das LSC zu installieren.

Muss das LSC für die Telefone installiert sein, damit es mit authentifiziertem oder verschlüsseltem sicherem Profil registriert werden kann?

Nein. Wenn LSC nicht installiert ist, verwendet Phone MIC, um die TLS-Verbindung zum CUCM herzustellen.

4878 WRN 15:47:34.756063 SECD: -PXY_NO_LSC: Kein LSC für [SCCP] versucht die MIC.

Muss der Gerätesicherheitsmodus im entsprechenden Gerätesicherheitsprofil authentifiziert oder verschlüsselt werden, um ein LSC zu installieren/zu aktualisieren/zu löschen?

Sie ist nicht obligatorisch, sondern kann auch mit dem Standard-Non-Secure-Profil durchgeführt werden, wenn der Gerätesicherheitsmodus nicht sicher ist.

Muss sich der Cluster im gemischten Modus befinden, um das LSC auf dem Telefon zu installieren?

Sie ist nicht obligatorisch. LSC-Installation/Löschen ist auch dann möglich, wenn der Cluster-Sicherheitsmodus nicht sicher ist.

Wie können Sie schnell testen, wenn ein Problem mit dem vom Telefon verwendeten LSC auftritt?

Löschen Sie das LSC in einem der Telefone, indem Sie zur Seite "Phone Admin" (Telefonadministrator) wechseln. Dadurch wird das Telefon gezwungen, MIC zu verwenden. Wenn alles in Ordnung mit MIC ist, fahren Sie mit der Fehlerbehebung mit LSC fort.

Wie erhalte ich die Telefonzertifikate zur Fehlerbehebung?

Stellen Sie die Zertifikatoperation auf Fehlerbehebung unter dem Gerät/Telefon ein. Drücken Sie Save (Speichern) und anschließend Apply Config (Konfiguration anwenden). Warten Sie, bis der Zertifikatsstatus für die **Fehlerbehebung angezeigt wird**. Sammeln Sie **Cisco Certificate Authority Proxy Function** Logs aus dem Real Time Monitoring Tool (RTMT). Sie enthält die Zertifikate des Telefons.

Wie kann anhand der Paketerfassung überprüft werden, ob LSC oder MIC des Telefons zum Herstellen der TLS-Verbindung mit

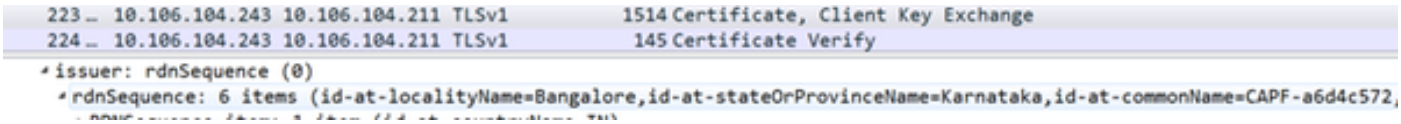
CallManager verwendet wird?

Sammeln Sie die Paketerfassungen für den Telefonneustart.

Überprüfen Sie das Zertifikat, die Exchange-Nachricht des Client-Schlüssels. Überprüfen Sie das vom IP-Telefon gesendete Zertifikat.

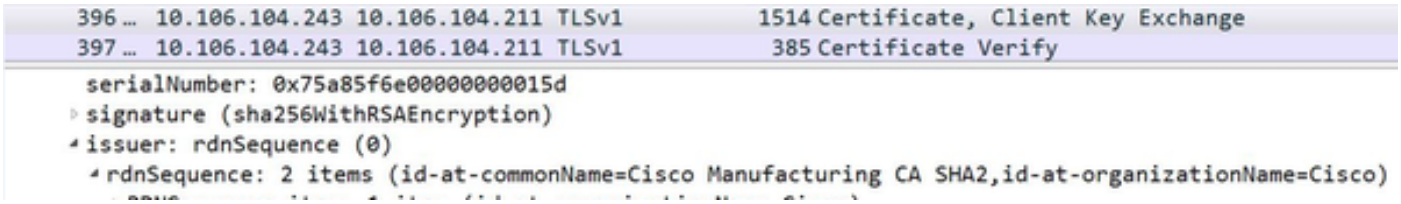
LSC-Beispiel:

Für das LSC ist die CAPF-CN im Feld "Emittenten" zu sehen. Der entsprechende CAPF-Root muss in CallManager-trust vorhanden sein.



Beispiel-MIC:

Für das MIC ist Cisco Manufacturing CA im Bereich Emittenten tätig. Die jeweilige Root-CA muss in CallManager-trust vorhanden sein.



Welche Bedeutung hat der Authentifizierungsmodus unter CAPF-Informationen (Certification Authority Proxy Function)? Welche Bedeutung hat die TLS-Verbindung zwischen CUCM und Telefon?

Dabei handelt es sich lediglich um eine Authentifizierungsmethode zwischen Telefon und CAPF für die Installation/Aktualisierung/Löschung und die Fehlerbehebung. Für die TLS-Verbindung zwischen CUCM und Telefon ist dies nicht von Bedeutung.

Welche grundlegenden LSC-Vorgänge müssen für die Telefone berücksichtigt werden, nachdem das CAPF-Zertifikat neu generiert wurde?

In diesem Abschnitt wird das Leerlaufszenario beschrieben, in dem keine Offline-CA zum Ausstellen des LSC verwendet wird.

TLS-Verbindung mit CallManager

Stellen Sie sicher, dass das neue LSC am Telefon installiert wird, bevor Sie das vorherige CAPF-Zertifikat von CallManager-trust löschen. Beim Löschen des vorherigen CAPF-Zertifikats gefolgt

von einem Neustart des CallManager-Dienstes treten die Registrierungsprobleme für die Telefone auf, für die das von diesem CAPF-Zertifikat ausgestellte LSC vorhanden ist.

LSC-Betrieb mit CAPF-Trust

Stellen Sie sicher, dass das neue LSC am Telefon installiert wird, bevor Sie das vorherige CAPF-Zertifikat von CAPF-trust löschen. LSC-Operationen wie das Installieren/Löschen im Authentifizierungsmodus **durch vorhandenes Zertifikat (Precedence to LSC)** schlagen fehl und **ungültiges LSC** für die Telefone, für die das LSC durch dieses CAPF-Zertifikat ausgestellt wurde, ist fehlerhaft.

Zwischen Telefon und Authentifizierungsserver für 802.1x-Authentifizierung

Stellen Sie sicher, dass das vorherige CAPF-Zertifikat vom Authentifizierungsserver nicht gelöscht wird, bis das neue CAPF-Zertifikat hochgeladen ist und Phone das vom neuen CAPF ausgestellte LSC abruft.

Zwischen ASA und Telefon

Stellen Sie sicher, dass das vorherige CAPF-Zertifikat von ASA nicht gelöscht wird, bis das Telefon das neue LSC erhält und das neue CAPF CA-Zertifikat in die ASA hochgeladen wird.

Unter Zertifikatregeneration finden Sie die Schritte zum Neugenerieren des CAPF-Zertifikats.

Weitere Informationen

- Zertifikate für Cisco IP-Telefone und sichere Kommunikation
- Designleitfaden für IP-Telefonie für 802.1X
- Cisco Unified Communications Manager-Sicherheitsleitfaden