CUCM電話証明書(LSC/MIC)のQ.A

内容

概要

このドキュメントでは、Cisco Unified Communications Manager(CUCM)の電話証明書に関する質問と回答について説明します。 電話証明書の概要を次に示します。

製造元でインストールされる証明書(MIC):

名前が示すように、電話機にはMICがプリインストールされており、管理者はこれを削除または変更できません。認証局(CA)証明書CAP-RTP-001、CAP-RTP-002、Cisco_Manufacturing_CAおよびCisco Manufacturing CA SHA2は、MICを信頼するためにCUCMにプリインストールされます。MIC CAが期限切れになると、MICを生成されます

ローカルで有効な証明書(LSC):

LSCは、Cisco IP Phoneの公開キーを所有します。この公開キーは、Cisco Unified Communications Manager(CUCM)のCertificate Authority Proxy Function(CAPF)秘密キーによって

署名されます。デフォルトでは電話機にはインストールされません。管理者はLSCを完全に制御できます。CAPF CA証明書を再生成すると、必要に応じて電話機に新しいLSCを発行できます。

電話証明書の一般的な用途は何ですか。

電話証明書の一般的な用途を次に示します

CAPFと電話の間でのインストール/アップグレード、削除、またはトラブルシューティング

電話機は、CAPFとの接続を確立し、電話機の証明書をインストール、アップグレード、削除、またはトラブルシューティングします。Phone Certificateは、Certification Authority Proxy Function(CAPF)のAuthentication ModeがBy Existing Certificate(Precedence to LSC)またはBy Existing Certificate(Precedence to MIC)に設定されているときにCAPFとの接続を確立するために使用されます。

既存の証明書（LSCに優先）: 電話機はLSCを使用してCAPFで認証します。LSCがインストールされていない場合は、MICが使用されます。使用されている証明書に問題がある場合、インストールが失敗し、「invalid LSC」という理由が表示されます。たとえば、LSCの署名付きCAはCAPF信頼では使用できません。他の証明書方式を使用して認証モードを更新するか、そのような場合はnull文字列を使用します。

既存の証明書（MICに優先）:電話機はMICを使用してCAPFで認証します。

トランスポート層セキュリティ(TLS)接続のためのCallManagerと電話の間

電話機はLSCまたはMICを使用して、CallManagerとのTLS接続を確立します。CallManagerは、CallManager-trustをチェックして、電話機が提示した証明書を検証します。それぞれのCAPF証明書は、LSCのCallManager-trustおよびMICのCisco Manufacture CAで使用可能である必要があります。

802.1x認証用の電話機と認証サーバ間

CAPF/製造CA証明書は、Cisco Secure Access Control Server(ACS)やIdentity Services Engine(ISE)などの認証サーバにアップロードされます。 認証サーバは、証明書（LSCまたはMIC）を提示するときに、アップロードされた証明書を使用して電話機を認証します。

電話機とVPN用Cisco適応型セキュリティアプライアンス(ASA)間の証明書ベース認証

CAPF/Manufacture CA証明書がASAにアップロードされます。電話機にLIC/MICが存在する場合、ASAは信頼を確認して検証します。

LSCとMICが存在する場合、接続に対してLSCまたはMICを明示的に選択する方法はありますか。

接続にLSCまたはMICを選択するオプションはありません。LSCがインストールされている場合、電話機はLSCを使用します。LSCがインストールされていない場合、電話機はMICを使用します。

LSCがない場合のコンソールエントリ：

SECD:-PXY_NO_LSC:[SCCP]のLSCが存在しないため、MICが試行されます

LSCが存在する場合のコンソールエントリ：

SECD:-PXY_CERT_CIPHER:[SCCP]、[TLSv1]、証明書[LSC]

LSCまたはMICの選択は、CAPFと電話のインストール/アップグレード、削除、またはトラブルシューティングの間でのみ可能です。

新しいクラスタに移動するときに、LSCインストールされたプロファイルが保護された電話機が登録されない理由は何ですか。

これは、すでにOLD ClusterからLSCを持っている電話機で発生する可能性があります。MICとLSCの両方が存在する場合、LSCを使用してTLS接続が確立されます。新しいCUCMのCallManager-trustにこのLSCのCAがないため、TLSを確立できません。

コンソールログには、TLSの確立に使用される証明書が表示されます。次のエントリは、LSCが使用されていることを示しています。

3469 NOT 00:01:31.935298 SECD:-PXY_CERT_CIPHER:[SCCP]、[TLSv1]、証明書[LSC]、暗号[AES256-SHA:AES128-SHA]

コンソールログにこのような障害が発生した場合の「不明なCA」を含むSSL3_Alert :-

3486 ERR 00:01:31.938954 SECD:-STATE_SSL3_ALERT:SSL3アラート[read]:[fatal]:[unknown CA]

この問題を解決する方法の1つは、非セキュアプロファイルを使用して電話機を登録し、既存のLSCを削除することです。新しいクラスタからLSCをインストールし、セキュアなプロファイルを使用して電話機を登録します。LSCをインストールせずに、MICを使用してセキュアなプロファイルを持つ電話機を登録することもできます。

LSCを電話機にインストールして、認証済みまたは暗号化済みのセキュアプロファイルを使用して登録する必要がありますか。

いいえ。LSCがインストールされていない場合、電話機はMICを使用してCUCMへのTLS接続を確立します。

4878 WRN 15:47:34.756063 SECD:-PXY_NO_LSC:[SCCP]のLSCがないため、MICが試行されます。

LSCをインストール/アップグレード/削除するには、各デバイスのセキュリティプロファイルのデバイスセキュリティモードを認

証または暗号化する必要がありますか。

これは必須ではありません。デバイスセキュリティモードが非セキュアであるデフォルト標準の非セキュアプロファイルを使用して実行できます。

電話機にLSCをインストールするには、クラスタを混合モードにする必要がありますか。

これは必須ではありません。LSCのインストール/削除は、クラスタセキュリティモードが非セキュアの場合でも実行できます。

電話機で使用されているLSCに問題がある場合の迅速なテスト方法

[Phone Admin]ページに移動して、いずれかの電話機のLSCを削除します。これにより、電話機はMICを使用するようになります。MICに問題がなければ、LSCのトラブルシューティングに進みます。

トラブルシューティング用の電話証明書の取得方法

[Device/Phone]で[Certificate Operation]を[Troubleshoot]に設定します。[Save]をクリックし、[Apply Config]をクリックします。 証明書の動作状態が表示されるまで待ってトラブルシューティングに成功します。Real Time Monitoring Tool(RTMT)からCisco Certificate Authority Proxy Function口グを収集します。 電話機からの証明書が含まれています。

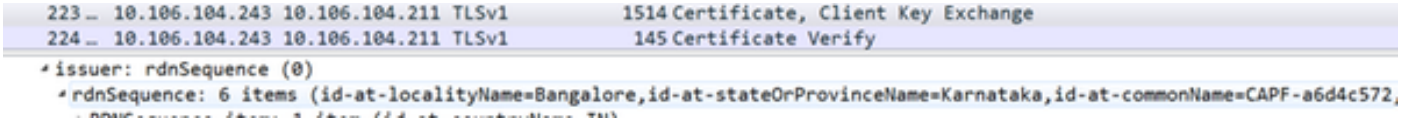
電話機のLSCまたはMICを使用してCallManagerとのTLS接続を確立する場合、パケットキャプチャから確認する方法を教えてください。

電話の再起動に関するパケットキャプチャを収集します。

[Certificate, Client key Exchange Message]を確認します。IP Phoneから送信された証明書を確認します。

LSCの例：

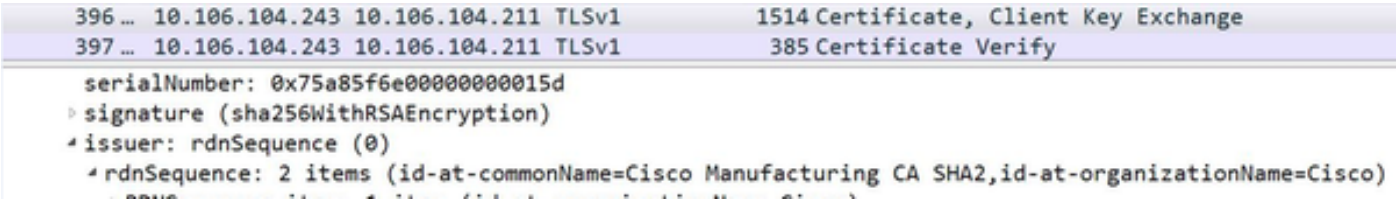
LSCの場合、CAPF CNはissuerフィールドに表示されます。それぞれのCAPFルートがCallManager-trustに存在する必要があります。



MICの例：

MICの場合は、[Issuer]フィールドにCisco Manufacturing CAと入力します。それぞれのルート

CAがCallManager-trustに存在する必要があります。



Certification Authority Proxy Function(CAPF)情報における認証モードの重要性は何ですか。CUCMと電話の間のTLS接続に何か意味がありますか。

これは、電話とCAPFの間の認証方式に過ぎず、インストール、アップグレード、削除、およびトラブルシューティング操作を行います。CUCMと電話の間のTLS接続には意味がありません。

CAPF証明書の再生後に電話機が考慮する基本的なLSC操作は何ですか。

このセクションでは、オフラインCAを使用してLSCを発行しないアイドルシナリオについて説明します。

CallManagerとのTLS接続

CallManager-trustから以前のCAPF証明書を削除する前に、必ず新しいLSCを電話機にインストールしてください。前のCAPF証明書を削除し、その後CallManagerサービスを再起動すると、このCAPF証明書によって発行されたLSCを持つ電話機に登録の問題が発生します。

CAPF-TrustによるLSCの動作

CAPF-trustから以前のCAPF証明書を削除する前に、必ず新しいLSCを電話機にインストールしてください。既存の証明書（LSCに優先）による認証モードを使用したインストール/削除などのLSC操作が失敗し、このCAPF証明書によって発行されたLSCを持つ電話機に対して無効なLSCが表示されます。

802.1x認証用の電話機と認証サーバ間

新しいCAPF証明書がアップロードされ、電話機が新しいCAPFによって発行されたLSCを取得するまで、前のCAPF証明書を認証サーバから削除しないでください。

ASAと電話間

電話機が新しいLSCを取得し、新しいCAPF CA証明書をASAにアップロードするまで、前のCAPF証明書をASAから削除しないでください。

*CAPF証明書を再生成する手順*については、「証明書の再生成」を参照してください。

関連情報

- Cisco IP Phone証明書とセキュアな通信
- 802.1X向けIPテレフォニー設計ガイド
- 『Cisco Unified Communications Manager Security Guide』