Q.A pour CERTIFICATS DE TÉLÉPHONE CUCM (LSC/MIC)

Contenu

Introduction

Ce document couvre certaines des questions et réponses relatives aux certificats téléphoniques de Cisco Unified Communications Manager (CUCM). Voici une vue rapide des certificats téléphoniques.

Certificat installé du fabricant (MIC) :

Comme son nom l'indique, les téléphones sont préinstallés avec la carte MIC et cela ne peut pas être supprimé/modifié par les administrateurs. Les certificats d'autorité de certification CAP-RTP-001, CAP-RTP-002, Cisco_Manufacturing_CA et Cisco Manufacturing CA SHA2 sont préinstallés

dans CUCM pour faire confiance au MIC. La MIC ne peut pas être utilisée une fois la validité expirée car la CA MIC ne peut pas être générée à nouveau,

Certificat d'importance locale (LSC) :

Le LSC possède la clé publique du téléphone IP Cisco, qui est signée par la clé privée CAPF (Certificate Authority Proxy Function) de Cisco Unified Communications Manager. Il n'est pas installé sur le téléphone par défaut. L'administrateur a un contrôle total sur LSC. Le certificat CAPF CA peut être régénéré à son tour peut émettre un nouveau LSC sur les téléphones chaque fois que nécessaire.

Quelles sont les utilisations courantes des certificats téléphoniques ?

Voici quelques utilisations courantes des certificats téléphoniques

Entre CAPF et le téléphone pour l'installation/la mise à niveau, la suppression ou le dépannage

Le téléphone établit la connexion avec CAPF pour installer/mettre à niveau, supprimer ou dépanner le certificat sur le téléphone. Le certificat téléphonique est utilisé pour établir la connexion avec CAPF lorsque le mode d'authentification sous Informations CAPF (Certification Authority Proxy Function) définies sur Par certificat existant (Precedence to LSC) ou Par certificat existant (Precedence to MIC).

Par certificat existant (priorité à LSC) : le téléphone utilise LSC pour s'authentifier avec CAPF. Il utilisera MIC si LSC n'est pas installé. L'installation échoue avec la raison « LSC non valide » s'il y a des problèmes avec le certificat utilisé. Par exemple, l'autorité de certification signée pour le LSC n'est pas disponible dans l'approbation CAPF. Mettre à jour le mode d'authentification à l'aide d'une autre méthode de certificat ou d'une chaîne null pour de tels cas d'échec.

Par certificat existant (priorité à MIC) : Le téléphone utilise MIC pour s'authentifier avec CAPF.

Entre CallManager et le téléphone pour la connexion TLS (Transport Layer Security)

Le téléphone utilise LSC ou MIC pour établir une connexion TLS avec CallManager. CallManager validera le certificat présenté par le téléphone en vérifiant CallManager-trust. Le certificat CAPF respectif doit être disponible dans CallManager-trust pour LSC et les CA de fabrication Cisco pour MIC.

Entre le téléphone et le serveur d'authentification pour l'authentification 802.1x

Les certificats d'autorité de certification CAPF/Manufacturing sont téléchargés vers des serveurs d'authentification tels que Cisco Secure Access Control Server (ACS) ou Identity Services Engine (ISE). Le serveur d'authentification utilise les certificats téléchargés pour authentifier le téléphone lorsqu'il présente son certificat (LSC ou MIC).

Pour l'authentification basée sur un certificat entre le téléphone et Cisco Adaptive Security Appliance (ASA) pour VPN

Les certificats CAPF/Manufacture CA sont téléchargés dans ASA, lorsque le téléphone présente LIC/MIC, ASA le valide en vérifiant sa confiance.

Lorsque LSC et MIC sont présents, existe-t-il un moyen de sélectionner LSC ou MIC explicitement pour les connexions ?

Aucune option permettant de sélectionner LSC ou MIC pour les connexions. Si LSC est installé, le téléphone utilise LSC. Le téléphone utilise la carte MIC si LSC n'est pas installé.

Entrée de console lorsque LSC n'est pas présent :

SECD : -PXY_NO_LSC : Pas de LSC pour [SCCP], va essayer MIC

Entrée de console lorsque LSC est présent :

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

La sélection de LSC ou de MIC n'est possible qu'entre l'installation/mise à niveau, la suppression ou le dépannage du protocole CAPF et du téléphone.

Quelle est la raison pour laquelle les téléphones LSC installés avec un profil sécurisé ne sont pas enregistrés lors du passage à un nouveau cluster ?

Cela peut se produire pour les téléphones qui ont déjà un LSC de l'ancienne grappe. Lorsque MIC et LSC sont présents, LSC est utilisé pour établir la connexion TLS. TLS ne peut pas être établi car le nouveau CUCM n'a pas l'autorité de certification pour ce LSC dans sa confiance CallManager-trust.

Les journaux de console indiquent quel certificat est utilisé pour établir le TLS. L'entrée ci-dessous montre que LSC est utilisé.

3469 PAS 00:01:31.935298 DPE : -PXY_CERT_CIPHER : [SCCP], [TLSv1], cert [LSC], chiffrement [AES256-SHA:AES128-SHA]

SSL3_Alert avec “ ” d'autorité de certification inconnue pour de tels cas d'échec dans les journaux de console : -

3486 ERR 00:01:31.938954 SECD : -STATE_SSL3_ALERT : Alerte SSL3 [read] : [fatal] : [CA inconnue]

Une des façons de résoudre ce problème est d'enregistrer le téléphone à l'aide d'un profil non sécurisé, puis de supprimer le LSC existant. Installez le LSC à partir du nouveau cluster, puis enregistrez le téléphone à l'aide du profil sécurisé. Il est également possible d'enregistrer le téléphone avec profil sécurisé à l'aide de MIC sans installer le LSC.

Le LSC doit-il être installé pour que les téléphones puissent l'enregistrer à l'aide d'un profil sécurisé authentifié ou chiffré ?

Non. Si LSC n'est pas installé, le téléphone utilise MIC pour établir la connexion TLS au CUCM.

4878 WRN 15:47:34.756063 SECD : -PXY_NO_LSC : Pas de LSC pour [SCCP], essaie MIC.

Est-il obligatoire que le mode de sécurité du périphérique du profil de sécurité du périphérique respectif soit authentifié ou chiffré pour installer/mettre à niveau/supprimer un LSC ?

Il n'est pas obligatoire, il peut être fait en utilisant le profil non sécurisé standard par défaut, là aussi où en mode Sécurité du périphérique n'est pas sécurisé.

Le cluster doit-il être en mode mixte pour installer le LSC sur le téléphone ?

Ce n'est pas obligatoire. L'installation/suppression de LSC peut être effectuée même lorsque le mode de sécurité du cluster n'est pas sécurisé.

Comment tester rapidement en cas de problème avec le LSC utilisé par le téléphone ?

Supprimez le LSC dans l'un des téléphones en accédant à la page Phone Admin. Cela force le téléphone à utiliser MIC. Si tout va bien avec MIC, poursuivez le dépannage avec LSC.

Comment obtenir les certificats téléphoniques pour le dépannage ?

Définissez l'opération de certificat à dépanner sous le périphérique/téléphone. Appuyez sur Enregistrer, puis sur Appliquer la configuration. Attendez de voir l'état de l'opération de certificat pour **dépanner la réussite**. Collectez **les** journaux **des fonctions proxy de l'autorité de certification Cisco** à partir de l'outil de surveillance en temps réel (RTMT). Il contient les certificats du téléphone.

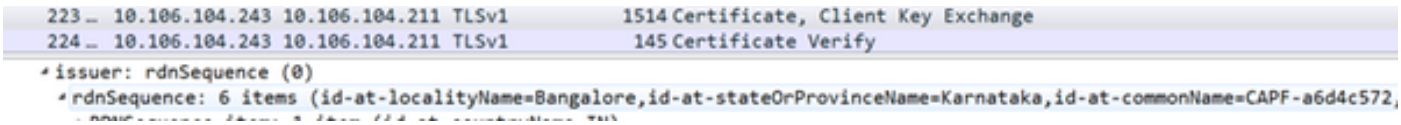
Comment vérifier à partir des captures de paquets, si LSC ou MIC du téléphone est utilisé pour établir la connexion TLS avec CallManager ?

Collectez les captures de paquets couvrant le redémarrage du téléphone.

Vérifiez le message d'échange de certificat et de clé client. Vérifiez le certificat envoyé à partir du téléphone IP.

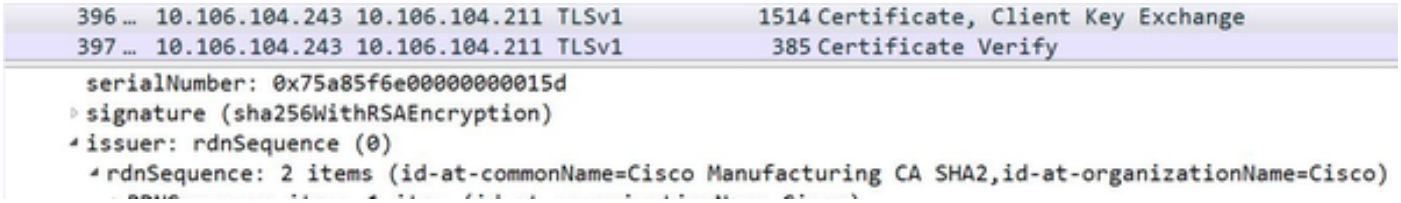
Exemple LSC :

Pour le LSC, le CN CAPF apparaît dans le champ émetteur. La racine CAPF correspondante doit être présente dans CallManager-trust.



Exemple de MIC :

Pour le MIC, CA de fabrication Cisco dans le champ émetteur. L'autorité de certification racine respective doit être présente dans CallManager-trust.



Quelle est la signification du mode d'authentification dans les informations CAPF (Certification Authority Proxy Function) ? Une signification pour la connexion TLS entre CUCM et Phone ?

Il ne s'agit que d'une méthode d'authentification entre Phone et CAPF pour l'installation/mise à niveau/suppression et le dépannage. Il n'a aucune signification pour la connexion TLS entre CUCM et Phone.

Quelles opérations LSC de base les téléphones doivent-ils prendre en compte après la régénération du certificat CAPF ?

Cette section couvre le scénario d'inactivité dans lequel aucune autorité de certification hors connexion n'est utilisée pour émettre le LSC.

Connexion TLS avec CallManager

Assurez-vous d'installer le nouveau LSC sur le téléphone avant de supprimer le précédent certificat CAPF de CallManager-trust. La suppression du précédent certificat CAPF suivi d'un redémarrage du service CallManager entraîne des problèmes d'enregistrement pour les téléphones dont le LSC est émis par ce certificat CAPF.

Opérations LSC avec CAPF-Trust

Assurez-vous d'installer le nouveau LSC sur le téléphone avant de supprimer le précédent certificat CAPF de CAPF-trust. Les opérations LSC telles que l'installation/la suppression en mode d'authentification **par certificat existant (priorité vers LSC)** échouent avec l'erreur **LSC non valide** pour les téléphones dont le LSC est émis par ce certificat CAPF.

Entre le téléphone et le serveur d'authentification pour l'authentification 802.1x

Veillez à ne pas supprimer le certificat CAPF précédent du serveur d'authentification tant que le nouveau certificat CAPF n'a pas été téléchargé et que Phone n'a pas reçu le LSC émis par le nouveau CAPF.

Entre ASA et téléphone

Veillez à ne pas supprimer le certificat CAPF précédent d'ASA tant que le téléphone n'a pas reçu le nouveau LSC et téléchargé le nouveau certificat CAPF CA vers ASA.

Reportez-vous à Régénération de certificat pour connaître les étapes à suivre pour régénérer le certificat CAPF.

Informations connexes

- Certificats de téléphone IP Cisco et communications sécurisées
- Guide de conception de la téléphonie IP pour 802.1X
- Guide de sécurité de Cisco Unified Communications Manager