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

Contenu

Introduction

Ce document couvre certaines des questions et réponses pour des Certificats de téléphone de Cisco Unified Communications Manager (CUCM). Voici une vue rapide des Certificats de téléphone.

Certificat installé par fabricant (MIC) :

Pendant que le nom indique, des téléphones sont préinstallés avec la MIC et ceci ne peut pas être supprimé/modifié par les administrateurs. L'Autorité de certification (CA) délivre un certificat CAP-

RTP-001, CAP-RTP-002, Cisco_Manufacturing_CA et Cisco fabriquant CA SHA2 sont préinstallés dans le CUCM pour faire confiance à la MIC. La MIC ne peut pas être utilisée une fois que la validité est expirée comme pente MIC CA soit au sujet de généré,

Localement - certificat significatif (LSC) :

Le LSC possède la clé publique pour le téléphone IP de Cisco, qui est signée par la clé privée de la fonction de proxy d'autorité de certification de Cisco Unified Communications Manager (CAPF). Il n'est pas installé au téléphone par défaut. L'administrateur ont le plein contrôle au-dessus du LSC. Le certificat de CA CAPF peut être régénéré consécutivement peut fournir le nouveau LSC aux téléphones lorsque requis.

Quelles sont les utilisations communes pour des Certificats de téléphone ?

Voici quelques utilisations communes pour les Certificats de téléphone

Entre CAPF et téléphone pour installer/améliorant, supprimant, ou dépannant

Téléphonez établit la connexion avec installer CAPF pour/mise à jour, supprimer, ou dépanner le certificat au téléphone. Le téléphone Certficate est utilisé pour établir la connexion avec CAPF quand authentication mode sous le positionnement de l'information de la fonction de proxy d'autorité de certification (CAPF) à par le certificat existant (priorité au LSC) ou par le certificat existant (priorité à la MIC).

Par le certificat existant (priorité au LSC) : Le téléphone emploie le LSC pour authentifier avec CAPF. Il utilisera la MIC si le LSC n'est pas installé. L'installation échoue avec la raison « LSC non valide » s'il y a des questions avec le certificat utilisé. L'exemple, le CA signé pour le LSC n'est pas disponible dans la confiance CAPF. Mettez à jour l'authentication mode suivre l'autre méthode de certificat ou par la chaîne null pour de tels cas de panne.

Par le certificat existant (priorité à la MIC) : Le téléphone emploie la MIC pour authentifier avec CAPF.

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

Le téléphone emploie le LSC ou la MIC pour établir la connexion de TLS avec le CallManager. Le CallManager validera le Certficate présenté par le téléphone en vérifiant la CallManager-confiance. Le certificat respectif CAPF doit être disponible dans la CallManager-confiance pour le LSC et la fabrication Ca de Cisco pour la MIC.

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

Des CERT CAPF/Manufacturing CA sont téléchargés aux serveurs d'authentification comme le Cisco Secure Access Control Server (ACS) ou le Cisco Identity Services Engine (ISE). Le serveur d'authentification emploie les Certificats téléchargés pour authentifier le téléphone quand il présent son certificat (LSC ou MIC).

Pour le certificat basé authentification entre le téléphone et l'appliance de sécurité adaptable Cisco (ASA) pour le VPN

Des CERT CAPF/Manufacture CA sont téléchargés dans l'ASA, quand le téléphone LIC/MIC actuel, ASA la valide en la vérifiant confiance.

Quand le LSC et la MIC sont présents, y a-t-il une manière de sélectionner le LSC ou la MIC explicitement pour des connexions ?

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

Entrée de console quand le LSC n'est pas présent :

SECD : - PXY_NO_LSC : Aucun LSC pour [SCCP], n'essayera la MIC

Entrée de console quand le LSC est présent :

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

La sélection du LSC ou de la MIC est possible seulement entre CAPF et installer de téléphone/améliorant, supprimant, ou dépannant.

Queest-ce que la raison est-elle les téléphones installés par LSC avec le profil sécurisé ne sont pas obtenir enregistré en se déplaçant à la nouvelle batterie ?

Ceci peut se produire pour les téléphones ceux qui ont déjà un LSC de VIEILLE batterie. Quand la MIC et le LSC sont présents, le LSC est utilisé pour établir la connexion de TLS. Le TLS ne peut pas être établi puisque le nouveau CUCM n'a pas le CA pour ce LSC en sa confiance de CallManager.

Expositions de messages de console que le certificat est utilisé pour établir le TLS. Au-dessous des expositions d'entrée le LSC est utilisé.

3469 NON 00:01:31.935298 SECD : - PXY_CERT_CIPHER : [SCCP], [TLSv1], CERT [LSC], chiffrement [AES256-SHA:AES128-SHA]

SSL3_Alert avec « le CA inconnu » pour de tels cas défectueux dans la console se connecte : -

3486 ERRENT 00:01:31.938954 SECD : -STATE_SSL3_ALERT : Alerte SSL3 [lue] : [mortel] : [CA inconnu

Une des manières de résoudre ce problème est, obtient le téléphone enregistré utilisant non – le profil sécurisé puis suppriment le LSC existant. Installez le LSC de la nouvelle batterie puis enregistrez le téléphone utilisant le profil sécurisé. Il est également possible pour avoir le

téléphone avec le profil sécurisé enregistré utilisant la MIC sans installer le LSC.

Est-ce qu'on l'exige le pour avoir le LSC installé pour que les téléphones l'obtiennent-ils s'est enregistré utilisant authentifié ou Encrypted a-t-il sécurisé le profil ?

No. Si le LSC n'est pas installé, le téléphone emploie la MIC pour établir la connexion de TLS au CUCM.

4878 WRN 15:47:34.756063 SECD : - PXY_NO_LSC : Aucun LSC pour [SCCP], essais MIC.

Est-il obligatoire que mode de sécurité des périphériques dans le profil de sécurité des périphériques respectif d'être authentifié ou pour installer chiffré/mise à jour/effacement un LSC ?

Il n'est pas obligatoire, il peut être fait utilisant le profil Non-sécurisé de norme par défaut trop où dans la sécurité des périphériques le mode est non sécurisé.

Est-il obligatoire la batterie à être dans le mode mixte pour installer le LSC dans le téléphone ?

Ce n'est pas obligatoire. Le LSC installent/effacements peut être fait même lorsque security mode de batterie dans non-sécurisé.

Comment tester rapidement s'il y a une question avec le LSC utilisé par le téléphone ?

Supprimez le LSC dans un du téléphone en allant à la page d'admin de téléphone. Ceci force le téléphone pour utiliser la MIC. Si tout le bien avec la MIC se poursuivent alors le dépannage par le LSC.

Comment obtenir les Certificats de téléphone pour le dépannage ?

Placez l'exécution de certificat pour dépanner sous le périphérique/téléphone. La sauvegarde de hit appliquent alors le config. Attendez de voir l'état d'exécution de certificat **pour dépanner le succès**. Collectez les logs de **fonction de proxy d'autorité de certification de Cisco de l'**outil de suivi en temps réel (RTMT). Il contient les Certificats du téléphone.

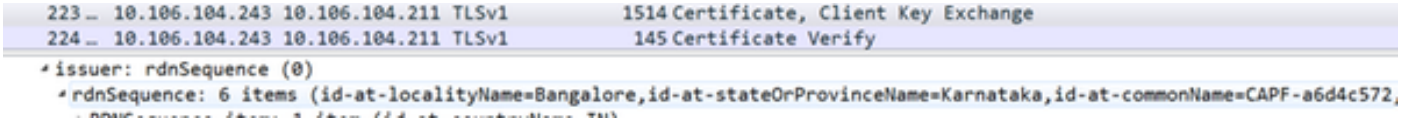
Comment vérifier des captures de paquet, si LSC ou MIC du téléphone est utilisé pour établir la connexion de TLS avec le CallManager ?

Collectez les captures de paquet couvrant la reprise de téléphone.

Vérifiez le certificat, le message d'échange principal de client. Vérifiez le certificat envoyé du téléphone IP.

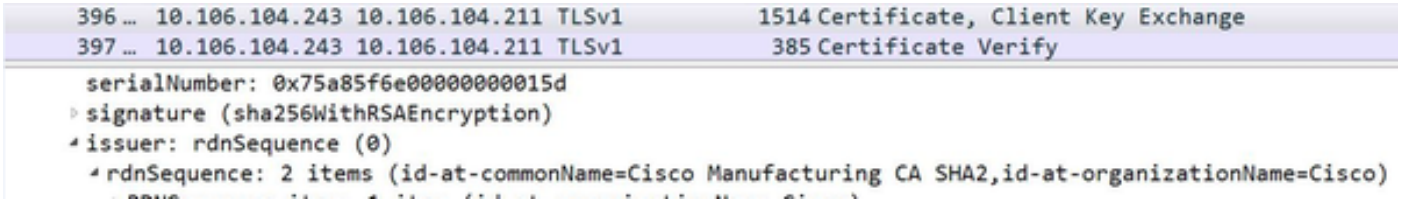
Exemple LSC :

Pour le LSC, la NC CAPF est vue dans le domaine d'émetteur. La racine respective CAPF doit être présente en CallManager-confiance.



Exemple MIC :

Pour la MIC, Cisco fabriquant le CA dans le domaine d'émetteur. La racine respective CA doit être présente en CallManager-confiance.



Quelle est l'importance de l'authentication mode sous les informations de la fonction de proxy d'autorité de certification (CAPF) ? Une importance pour la connexion de TLS entre CUCM et téléphone ?

Ce n'est rien mais une méthode d'authentification entre le téléphone et le CAPF pour installer/évolution/supprimant et dépannage des exécutions. Il n'a aucune importance pour la connexion de TLS entre CUCM et téléphone.

Quelles est-ce que sont les exécutions de base LSC pour que les téléphones considèrent après que le certificat CAPF l'ait régénéré ?

Cette section couvre le scénario de veille où aucun CA hors ligne n'est utilisé pour émettre le LSC.

Connexion de TLS avec le CallManager

Assurez pour installer le nouveau LSC au téléphone avant de supprimer le certificat précédent CAPF de la CallManager-confiance. En supprimant le certificat précédent CAPF suivi d'une reprise de CallManager entretenez la cause que l'enregistrement fournit aux téléphones ceux ont le LSC ont émis par ce certificat CAPF.

Exécutions LSC avec la CAPF-confiance

Assurez pour installer le nouveau LSC au téléphone avant de supprimer le certificat précédent CAPF de la CAPF-confiance. Les exécutions LSC comme installent/effacements utilisant l'authentication mode **par le certificat existant (priorité au LSC)** échoue avec l'erreur **LSC non valide** pour les téléphones que ceux ont le LSC émis par ce certificat CAPF.

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

Assurez pour ne pas supprimer le certificat précédent CAPF du serveur d'authentification jusqu'à ce que le nouveau certificat CAPF l'ait téléchargé et du téléphone obtient le LSC émis par nouveau CAPF.

Entre l'ASA et le téléphone

Assurez pour ne pas supprimer le certificat précédent CAPF de l'ASA jusqu'à ce que le téléphone obtienne le nouveau LSC et le nouveau certificat de CA téléchargé CAPF à l'ASA.

Référez-vous à la régénération de certificat pour que les étapes soient suivies pour régénérer le certificat CAPF.

Les informations relatives

- Certificats de téléphone IP de Cisco et communications protégées
- Téléphonie sur IP pour le guide de conception de 802.1X
- Guide de Sécurité de Cisco Unified Communications Manager