Q.A para los CERTIFICADOS del TELÉFONO CUCM (LSC/MIC)

Contenido

Introducción

Este documentos abarca algunas de las preguntas y respuestas para los Certificados del teléfono del administrador de las Comunicaciones unificadas de Cisco (CUCM). Aquí está una vista rápida de los Certificados del teléfono.

Certificado instalado fabricante (MIC):

Mientras que el nombre indica, los teléfonos se instalan previamente con el MIC y esto no se

puede borrar/modificar por los administradores. El Certificate Authority (CA) certifica CAP-RTP-001, CAP-RTP-002, Cisco_Manufacturing_CA y Cisco que fabrica CA SHA2 se instala previamente en el CUCM para confiar en el MIC. El MIC no puede ser utilizado una vez que la validez se expira como el canto MIC CA esté con referencia a generado,

Localmente - certificado significativo (LSC):

El LSC posee la clave pública para el Cisco IP Phone, que es firmada por la clave privada de la función de proxy del Certificate Authority del administrador de las Comunicaciones unificadas de Cisco (CAPF). No está instalado en el teléfono por abandono. El administrador tiene control total sobre el LSC. El certificado de CA del CAPF se puede regenerar a su vez puede publicar el nuevo LSC a los teléfonos siempre que esté requerido.

¿Cuáles son las aplicaciones comunes para los Certificados del teléfono?

Aquí están algunas aplicaciones comunes para los Certificados del teléfono

Entre el CAPF y el teléfono para instalar/actualizando, borrando, o resolviendo problemas

El teléfono establece la conexión con instalar/actualización del CAPF, borrar, o resolver problemas el certificado en el teléfono. El teléfono Certficate es utilizado para establecer la conexión con el CAPF cuando modo de autenticación bajo conjunto de información de la función de proxy de las autoridades de certificación (CAPF) por al certificado existente (precedencia al LSC) o por el certificado existente (precedencia al MIC).

Por el certificado existente (precedencia al LSC): El teléfono utiliza el LSC para autenticar con el CAPF. Utilizará el MIC si el LSC no está instalado. La instalación falla con la razón “LSC inválido” si hay problemas con el certificado usado. El ejemplo, CA firmado para el LSC no está disponible en la confianza del CAPF. Ponga al día al modo de autenticación que usa el otro método del certificado o por la cadena nula para tales casos del error.

Por el certificado existente (precedencia al MIC): El teléfono utiliza el MIC para autenticar con el CAPF.

Entre el CallManager y el teléfono para la conexión de la Seguridad de la capa de Trasnsport (TLS)

El teléfono utiliza el LSC o el MIC para establecer la conexión TLS con el CallManager. El CallManager validará el Certficate presentado por el teléfono marcando la CallManager-confianza. El certificado respectivo del CAPF tiene que estar disponible en la CallManager-confianza para la fabricación CA LSC y de Cisco para el MIC.

Entre el teléfono y el servidor de autenticación para la autenticación del 802.1x

Los certs CAPF/Manufacturing CA están cargados a los servidores de autenticación como el Cisco Secure Access Control Server (ACS) o el Identity Services Engine (ISE). El servidor de

autenticación utiliza los Certificados cargados para autenticar el teléfono cuando él presente su certificado (LSC o MIC).

Para la autenticación basada certificado entre el teléfono y el dispositivo de seguridad adaptante de Cisco (ASA) para el VPN

Los certs CAPF/Manufacture CA están cargados en el ASA, cuando el teléfono actual LIC/MIC, ASA lo valida marcandolo confianza.

¿Cuando el LSC y el MIC están presentes, hay manera de seleccionar el LSC o el MIC explícitamente para las conexiones?

Ninguna opción a seleccionar si LSC o MIC para las conexiones. Si el LSC está instalado, el teléfono utiliza el LSC. El teléfono utiliza el MIC si el LSC no está instalado.

Entrada de la consola cuando el LSC no está presente:

SECD: - PXY_NO_LSC: Ningún LSC para el [SCCP], intentará el MIC

Entrada de la consola cuando el LSC está presente:

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

La selección de LSC o de MIC es posible solamente entre el CAPF y instalar/actualizando del teléfono, borrando, o resolviendo problemas.

¿Cuál es la razón los teléfonos instalados LSC con el perfil asegurado no está consiguiendo registrada al moverse al nuevo cluster?

Esto puede suceder para los teléfonos ésos ya que tienen un LSC del VIEJO cluster. Cuando el MIC y el LSC están presentes, el LSC se utiliza para establecer la conexión TLS. TLS no puede ser establecido puesto que el nuevo CUCM no tiene CA para este LSC en su confianza del CallManager.

Demostraciones de los registros de la consola que el certificado se utiliza para establecer TLS. Debajo de las demostraciones de la entrada se utiliza el LSC.

3469 NO 00:01:31.935298 SECD: - PXY_CERT_CIPHER: [SCCP], [TLSv1], [LSC] CERT, cifra [AES256-SHA:AES128-SHA]

SSL3_Alert con “CA desconocido” para tales falló los casos en los registros de la consola:-

3486 ERR 00:01:31.938954 SECD: -STATE_SSL3_ALERT: [read] de la alerta SSL3: [fatal]: [CA desconocido

Una de las maneras de resolver este problema es, consigue el teléfono registrado usando el perfil seguro no- después borra el LSC existente. Instale el LSC del nuevo cluster después registre el

teléfono usando el perfil asegurado. Es también posible tener el teléfono con el perfil asegurado registrado usando el MIC sin instalar el LSC.

¿Se requiere para tener el LSC instalado para que los teléfonos lo consigan registrado usando el perfil asegurado autenticado o cifrado?

No. Si el LSC no está instalado, el teléfono utiliza el MIC para establecer la conexión TLS al CUCM.

4878 WRN 15:47:34.756063 SECD: - PXY_NO_LSC: Ningún LSC para el [SCCP], intentos MIC.

¿Es obligatorio que modo de la seguridad del dispositivo en el perfil de seguridad del dispositivo respectivo ser autenticado o instalar cifrado/actualización/cancelación un LSC?

No es obligatorio, él puede ser hecho usando el perfil NON-seguro de la norma predeterminada también donde en la seguridad del dispositivo está no seguro el modo.

¿Es obligatorio el cluster a estar en el modo mezclado para instalar el LSC en el teléfono?

No es obligatorio. El LSC instala/cancelación se puede hacer incluso cuando modo seguro del cluster en NON-seguro.

¿Cómo probar rápidamente si allí un problema con el LSC es utilizado por el teléfono?

Borre el LSC en uno del teléfono yendo a la página de administración del teléfono. Esto fuerza el teléfono para utilizar el MIC. Si entonces proceden todos muy bien con el MIC el troubleshooting con el LSC.

¿Cómo conseguir los Certificados del teléfono para resolver problemas?

Fije la operación del certificado para resolver problemas bajo el dispositivo/el teléfono. La salvaguardia del golpe entonces aplica los Config. Espere para ver el estado de la operación del certificado **para resolver problemas el éxito**. Recoja los registros de la **función de proxy del Certificate Authority de Cisco de la** herramienta del monitoreo en tiempo real (RTMT). Contiene los Certificados del teléfono.

¿Cómo verificar de las capturas de paquetes, si LSC o MIC del teléfono se utiliza para establecer la conexión TLS con el

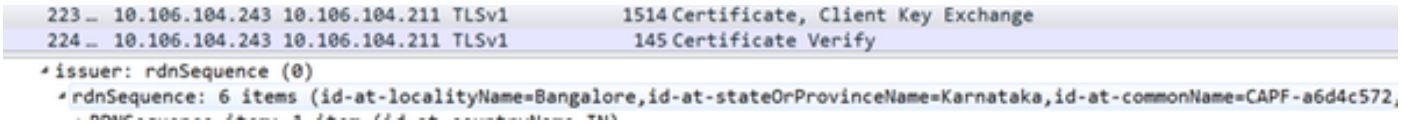
CallManager?

Recoja a las capturas de paquetes que cubren el reinicio del teléfono.

Marque el certificado, mensaje de intercambio de claves del cliente. Verifique el certificado enviado del teléfono del IP.

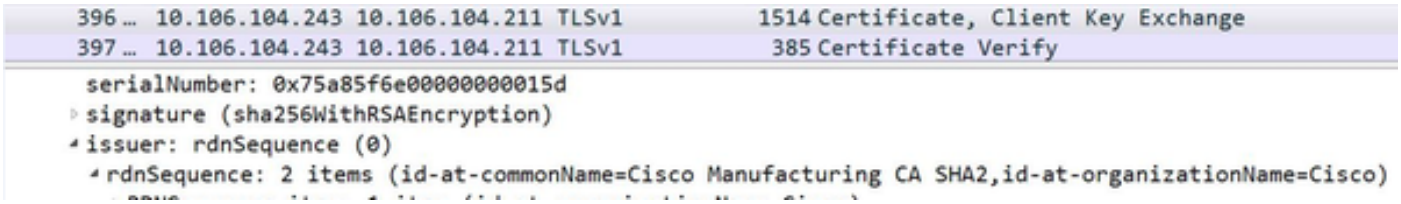
Ejemplo LSC:

Para el LSC, el CAPF CN se ve en el campo del emisor. La raíz respectiva del CAPF tiene que estar presente en la CallManager-confianza.



Ejemplo MIC:

Para el MIC, Cisco que fabrica CA en el campo del emisor. Respectivo raíz CA tiene que estar presente en la CallManager-confianza.



¿Cuál es la significación del modo de autenticación conforme a la información de la función de proxy de las autoridades de certificación (CAPF)? ¿Significación para la conexión TLS entre CUCM y el teléfono?

No es nada sino un método de autentificación entre el teléfono y el CAPF para instalar/el actualizar/borrando y resolviendo problemas las operaciones. No tiene ninguna significación para la conexión TLS entre CUCM y el teléfono.

¿Cuáles son las operaciones básicas LSC para que los teléfonos consideren después del certificado del CAPF regenerado?

Esta sección cubre el escenario ocioso donde no se utiliza ningún CA offline para publicar el LSC.

Conexión TLS con el CallManager

Asegure para instalar el nuevo LSC en el teléfono antes de borrar el certificado anterior del CAPF de la CallManager-confianza. Borrando el certificado anterior del CAPF seguido por un reinicio del servicio de CallManager cause los problemas del registro a los teléfonos que ésos tienen el LSC publicado por este certificado del CAPF.

Operaciones LSC con la CAPF-confianza

Asegure para instalar el nuevo LSC en el teléfono antes de borrar el certificado anterior del CAPF de la CAPF-confianza. Las operaciones LSC como instalan/cancelación usando el modo de autenticación **por el certificado existente (precedencia al LSC)** fallan con el error **LSC inválido** para los teléfonos que ésas tienen el LSC publicado por este certificado del CAPF.

Entre el teléfono y el servidor de autenticación para la autenticación del 802.1x

Asegure para no borrar el certificado anterior del CAPF del servidor de autenticación hasta que el nuevo certificado del CAPF cargado y el teléfono consiga el LSC publicado por el nuevo CAPF.

Entre el ASA y el teléfono

Asegure para no borrar el certificado anterior del CAPF del ASA hasta que el teléfono consiga el nuevo LSC y el nuevo certificado de CA cargado del CAPF al ASA.

Refiera a la regeneración del certificado para que los pasos sean seguidos para regenerar el certificado del CAPF.

Información relacionada

- Certificados y comunicaciones seguras del Cisco IP Phone
- Telefonía IP para la guía de diseño del 802.1x
- Guía de la Seguridad del administrador de las Comunicaciones unificadas de Cisco