Comprender la seguridad de CUCM de forma predeterminada y el funcionamiento y la resolución de problemas de ITL

Contenido

Introducción

Este documento describe la función Security By Default (SBD) de Cisco Unified Communications Manager (CUCM) Versiones 8.0 y posteriores.

Antecedentes

CUCM versión 8.0 y posterior presenta la función SBD, que consta de archivos de lista de confianza de identidad (ITL) y el servicio de verificación de confianza (TVS).

Cada clúster de CUCM utiliza ahora automáticamente la seguridad basada en ITL. Existe un equilibrio entre la seguridad y la facilidad de uso y administración que los administradores deben

tener en cuenta antes de realizar ciertos cambios en un clúster de CUCM versión 8.0.

Este documento sirve como complemento de los documentos oficiales de Security By Default, y proporciona información operativa y consejos de resolución de problemas para ayudar a los administradores y facilitar el proceso de resolución de problemas.

Es una buena idea familiarizarse con estos conceptos básicos de SBD: artículo de Wikipedia de criptografía de clave asimétrica y artículo de Wikipedia de infraestructura de clave pública.

Descripción general de SBD

Esta sección proporciona una descripción general rápida de lo que proporciona exactamente SBD. Para obtener información técnica completa de cada función, consulte la sección Información detallada y de resolución de problemas de SBD.

SBD proporciona estas tres funciones para los teléfonos IP compatibles:

- Autenticación predeterminada de los archivos descargados TFTP (configuración, configuración regional, lista de llamada) que utilizan una clave de firma
- Cifrado opcional de archivos de configuración TFTP que utilizan una clave de firma
- Verificación de certificados para conexiones HTTPS iniciadas por teléfono que utilizan un almacén de confianza de certificados remotos en CUCM (TVS)

Este documento proporciona una descripción general de cada una de estas funciones.

Autenticación de descarga TFTP

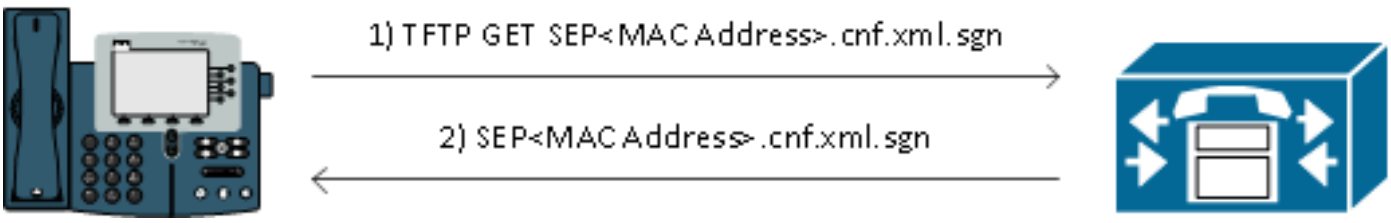
Cuando hay un archivo de lista de confianza de certificados (CTL) o ITL, el teléfono IP solicita un archivo de configuración TFTP firmado del servidor TFTP de CUCM.

Este archivo permite que el teléfono verifique que el archivo de configuración proviene de una fuente confiable. Con los archivos CTL/ITL presentes en los teléfonos, los archivos de configuración deben estar firmados por un servidor TFTP confiable.

El archivo es texto sin formato en la red mientras se transmite, pero viene con una firma de verificación especial.

El teléfono solicita SEP<Dirección MAC>.cnf.xml.sgn para recibir el archivo de configuración con la firma especial.

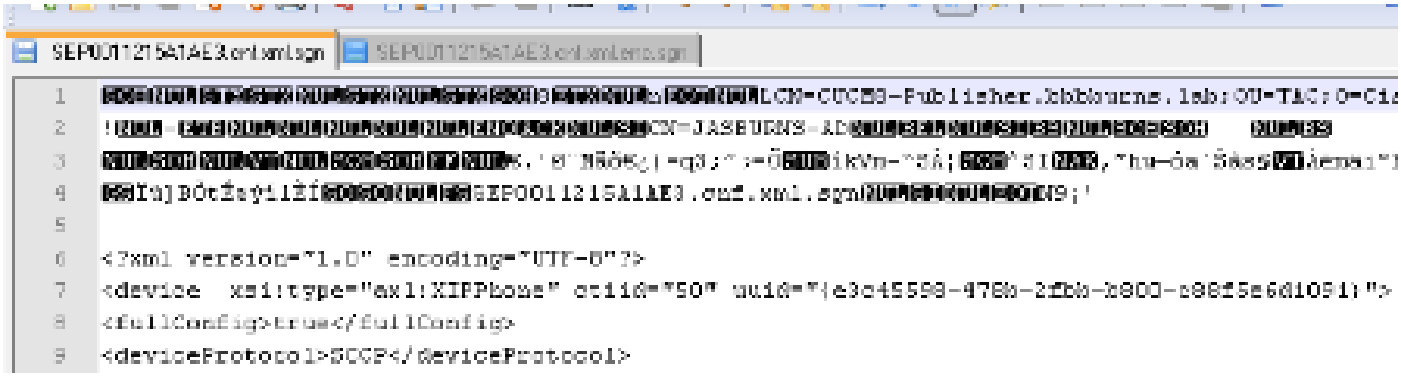
Este archivo de configuración está firmado por la clave privada TFTP que corresponde a CallManager.pem en la página Operating System (OS) Administration Certificate Management .



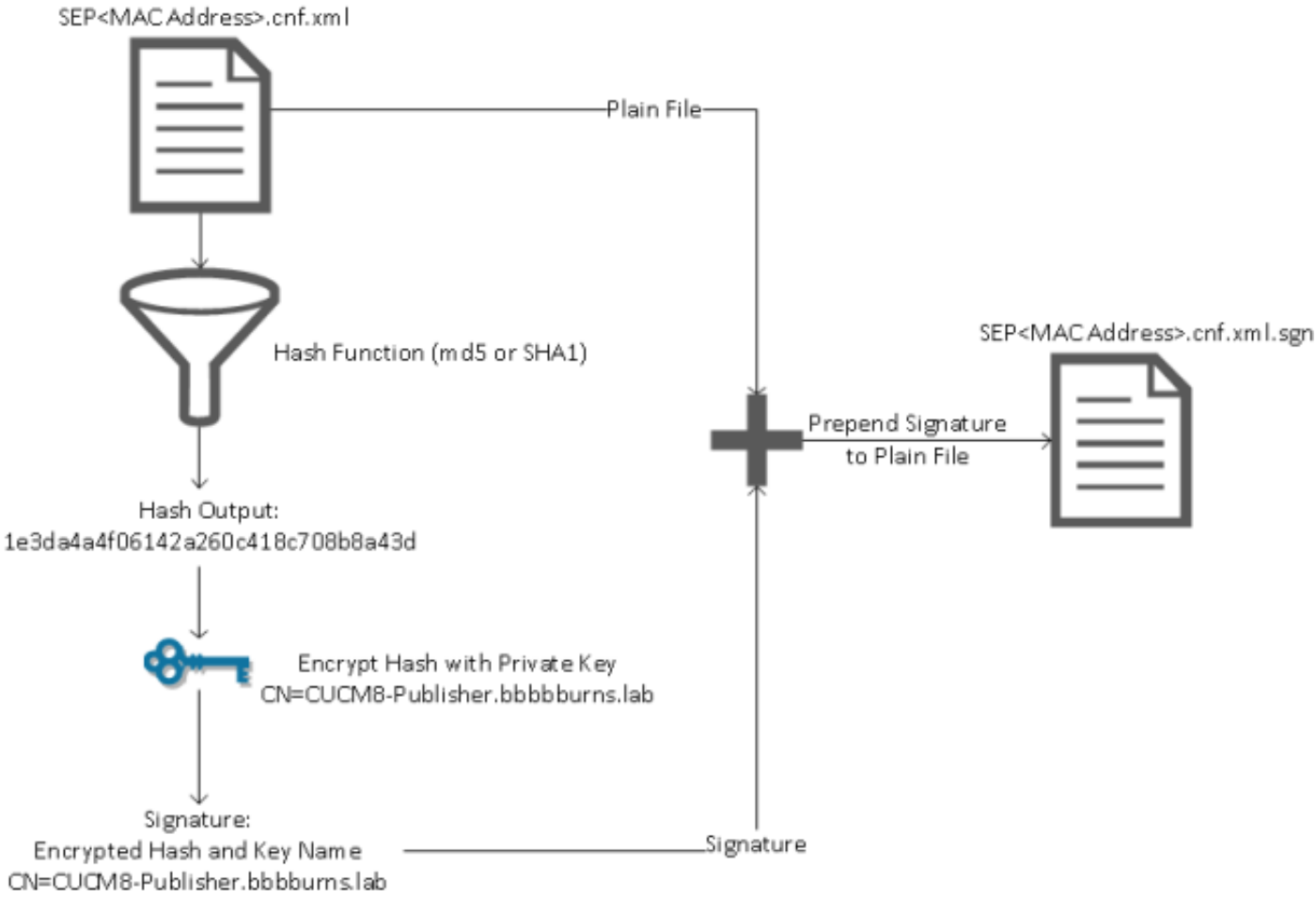
El archivo firmado tiene una firma en la parte superior para autenticar el archivo, pero por lo demás está en XML de texto sin formato.

La siguiente imagen muestra que el firmante del archivo de configuración es CN=CUCM8-Publisher.bbburns.lab, que a su vez está firmado por CN=JASBURNS-AD.

Esto significa que el teléfono necesita verificar la firma de CUCM8-Publisher.bbburns.lab con el archivo ITL antes de aceptar este archivo de configuración.



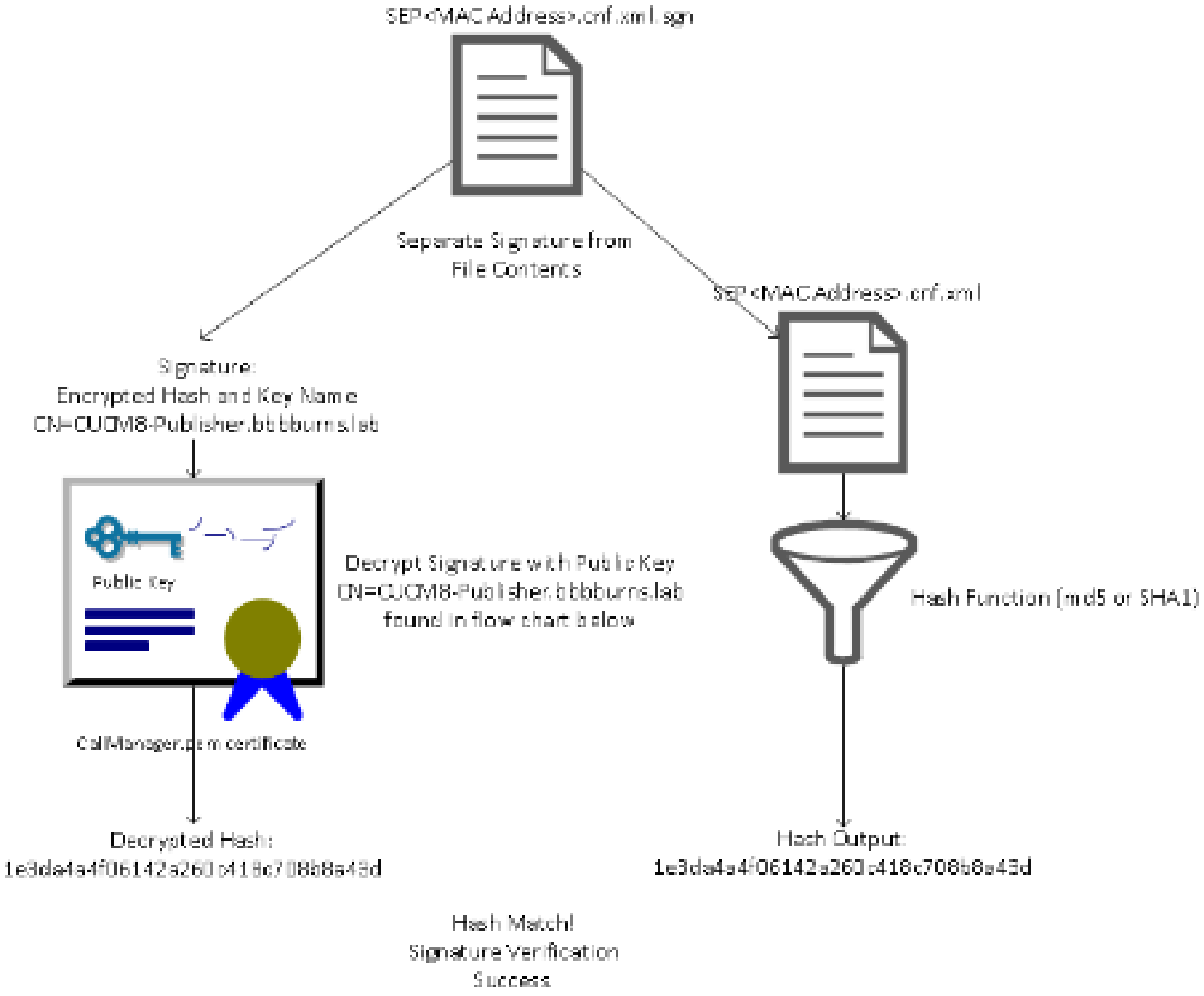
A continuación se muestra un diagrama que muestra cómo se utiliza la clave privada junto con una función hash de algoritmo de resumen de mensajes (MD)5 o algoritmo hash seguro (SHA)1 para crear el archivo firmado.



La verificación de la firma invierte este proceso mediante el uso de la clave pública que coincide

para descifrar el hash. Si los hashes coinciden, se muestra:

- Este archivo no se ha modificado en tránsito.
- Este archivo proviene de la parte que aparece en la firma, ya que cualquier elemento descifrado correctamente con la clave pública debe haberse cifrado con la clave privada.



Cifrado del archivo de configuración TFTP

Si el cifrado de configuración TFTP opcional está habilitado en el perfil de seguridad del teléfono asociado, el teléfono solicita un archivo de configuración cifrado.

Este archivo se firma con la clave privada TFTP y se cifra con una clave simétrica intercambiada entre el teléfono y CUCM (consulte la Guía de seguridad de Cisco Unified Communications Manager, versión 8.5(1) para obtener más información).

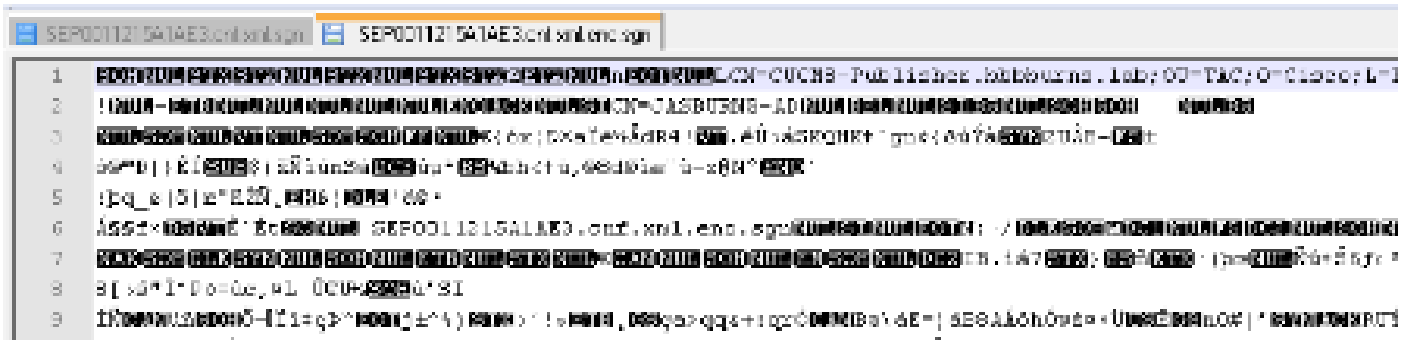
Su contenido no se puede leer con un sabueso de red a menos que el observador tenga las claves necesarias.

El teléfono solicita SEP<Dirección MAC>.cnf.xml.enc.sgn para obtener el archivo cifrado firmado.

El archivo de configuración cifrado también tiene la firma al principio, pero no hay datos de texto sin formato después, sólo datos cifrados (caracteres binarios confusos en este editor de texto).

La imagen muestra que el firmante es el mismo que en el ejemplo anterior, por lo que este firmante debe estar presente en el archivo ITL antes de que el teléfono acepte el archivo.

Además, las claves de descifrado deben ser correctas para que el teléfono pueda leer el contenido del archivo.



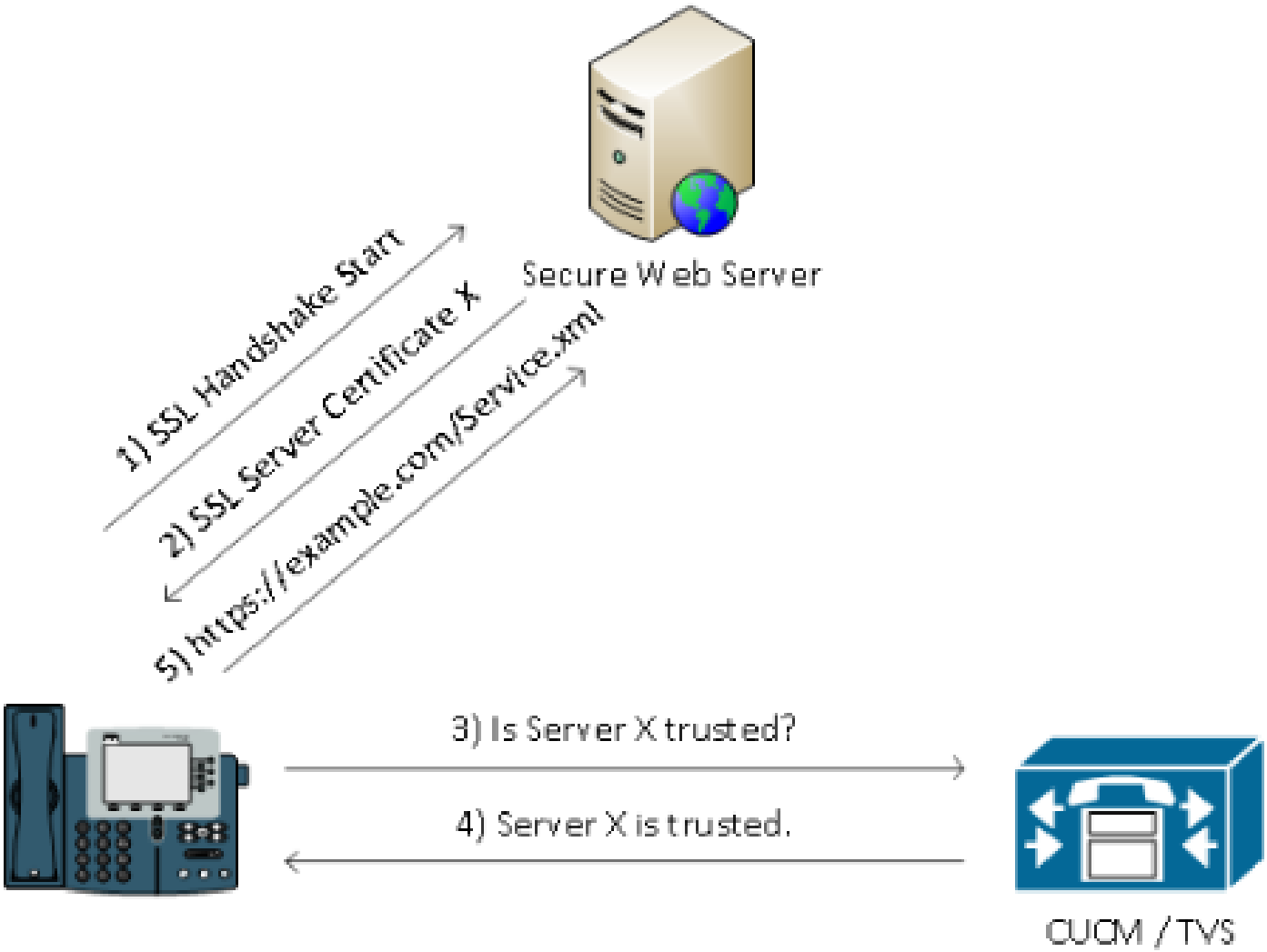
Servicio de verificación de confianza (verificación remota de certificados y firmas)

Los teléfonos IP contienen una cantidad de memoria limitada y también puede haber un gran número de teléfonos que administrar en una red.

CUCM actúa como un almacén de confianza remoto a través de TVS para que no sea necesario colocar un almacén de confianza de certificados completo en cada teléfono IP.

Cada vez que el teléfono no puede verificar una firma o certificado a través de los archivos CTL o ITL, solicita la verificación al servidor de TVS.

Este almacén de confianza central es más fácil de administrar que si el almacén de confianza estuviera presente en todos los teléfonos IP.



Información detallada y de resolución de problemas de SBD

En esta sección se detalla el proceso SBD.

Archivos y certificados de ITL presentes en CUCM

En primer lugar, hay varios archivos que deben estar presentes en el propio servidor de CUCM. La parte más importante es el certificado TFTP y la clave privada TFTP.

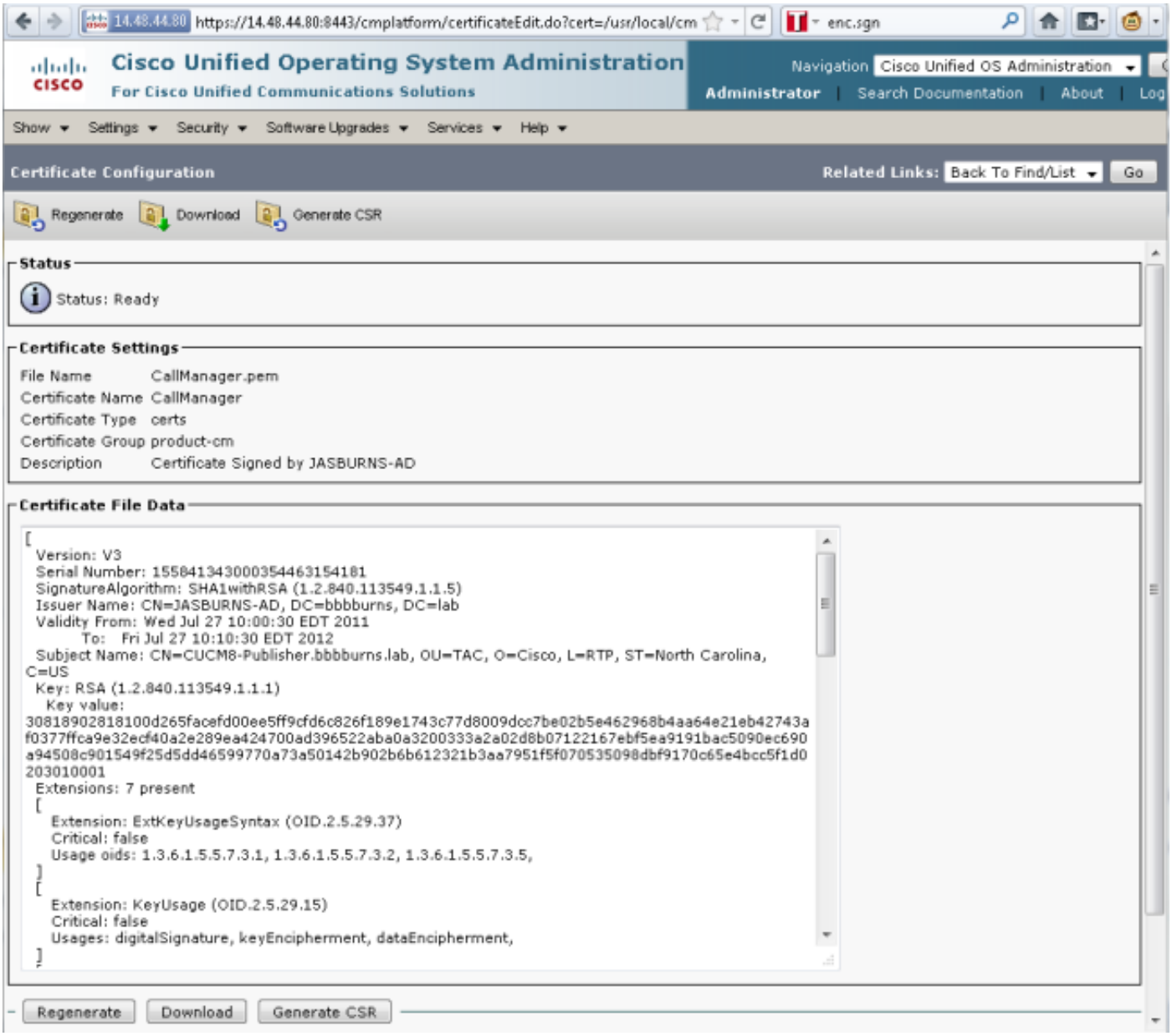
El certificado TFTP se encuentra en OS Administration > Security > Certificate Management > CallManager.pem.

El servidor de CUCM utiliza las claves privadas y públicas del certificado CallManager.pem para el servicio TFTP (así como para el servicio Cisco Call Manager (CCM)).

La imagen muestra que el certificado CallManager.pem se emite a CUCM8-publisher.bbburns.lab y está firmado por JASBURNS-AD. Todos los archivos de configuración TFTP están firmados por la clave privada que se muestra a continuación.

Todos los teléfonos pueden utilizar la clave pública TFTP en el certificado CallManager.pem para descifrar cualquier archivo cifrado con la clave privada TFTP, así como para verificar cualquier

archivo firmado con la clave privada TFTP.



Además de la clave privada del certificado CallManager.pem, el servidor de CUCM también almacena un archivo ITL que se presenta a los teléfonos.

El comando show itl muestra todo el contenido de este archivo ITL a través del acceso de Secure Shell (SSH) a la CLI del sistema operativo del servidor de CUCM.

En esta sección se desglosa el archivo ITL pieza por pieza, ya que contiene varios componentes importantes que utiliza el teléfono.

La primera parte es la información de la firma. Incluso el archivo ITL es un archivo firmado. Este resultado muestra que está firmado por la clave privada TFTP asociada con el certificado CallManager.pem anterior.

<#root>

```
admin:
```

show itl

```
Length of ITL file: 5438
The ITL File was last modified on Wed Jul 27 10:16:24 EDT 2011

        Parse ITL File
        ----------------

Version:        1.2
HeaderLength:   296 (BYTES)

BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
3       SIGNERID        2       110
4       SIGNERNAME      76      CN=CUCM8-Publisher.bbbburns.lab;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
5       SERIALNUMBER    10      21:00:2D:17:00:00:00:00:00:05
6       CANAME          15      CN=JASBURNS-AD
*Signature omitted for brevity*
```

Cada una de las secciones siguientes contiene su propósito dentro de un parámetro Function especial. La primera función es el token de seguridad del administrador del sistema. Ésta es la firma de la clave pública TFTP.

```
        ITL Record #:1
                  ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1972
2       DNSNAME         2
3       SUBJECTNAME     76      CN=CUCM8-Publisher.bbbburns.lab;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
4       FUNCTION        2       System Administrator Security Token
5       ISSUERNAME      15      CN=JASBURNS-AD
6       SERIALNUMBER    10      21:00:2D:17:00:00:00:00:00:05
7       PUBLICKEY       140
8       SIGNATURE       256
9       CERTIFICATE     1442    0E 1E 28 0E 5B 5D CC 7A 20 29 61 F5
                                8A DE 30 40 51 5B C4 89 (SHA1 Hash HEX)
This etoken was used to sign the ITL file.
```

La siguiente función es CCM+TFTP. Esta es nuevamente la clave pública TFTP que sirve para autenticar y descifrar los archivos de configuración TFTP descargados.

```
        ITL Record #:2
                  ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1972
2       DNSNAME         2
3       SUBJECTNAME     76      CN=CUCM8-Publisher.bbbburns.lab;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
```

```
4       FUNCTION        2       CCM+TFTP
5       ISSUERNAME      15      CN=JASBURNS-AD
6       SERIALNUMBER    10      21:00:2D:17:00:00:00:00:05
7       PUBLICKEY       140
8       SIGNATURE       256
9       CERTIFICATE     1442    0E 1E 28 0E 5B 5D CC 7A 20 29 61 F5
                                8A DE 30 40 51 5B C4 89 (SHA1 Hash HEX)
```

La siguiente función es TVS. Existe una entrada para la clave pública de cada servidor de TV al que se conecta el teléfono.

Esto permite al teléfono establecer una sesión de capa de conexión segura (SSL) en el servidor TVS.

```
        ITL Record #:3
                  ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       743
2       DNSNAME         2
3       SUBJECTNAME     76      CN=CUCM8-Publisher.bbbburns.lab;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
4       FUNCTION        2       TVS
5       ISSUERNAME      76      CN=CUCM8-Publisher.bbbburns.lab;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
6       SERIALNUMBER    8       2E:3E:1A:7B:DA:A6:4D:84
7       PUBLICKEY       270
8       SIGNATURE       256
11      CERTHASH        20      C7 E1 D9 7A CC B0 2B C2 A8 B2 90 FB
                                AA FE 66 5B EC 41 42 5D
12      HASH ALGORITHM  1       SHA-1
```

La última función incluida en el archivo del DIT es la función proxy de la autoridad certificadora (CAPF).

Este certificado permite a los teléfonos establecer una conexión segura con el servicio CAPF en el servidor de CUCM para que el teléfono pueda instalar o actualizar un certificado de importancia local (LSC).

```
        ITL Record #:4
                  ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       455
2       DNSNAME         2
3       SUBJECTNAME     61      CN=CAPF-9c4cba7d;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
4       FUNCTION        2       CAPF
5       ISSUERNAME      61      CN=CAPF-9c4cba7d;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
6       SERIALNUMBER    8       0A:DC:6E:77:42:91:4A:53
```

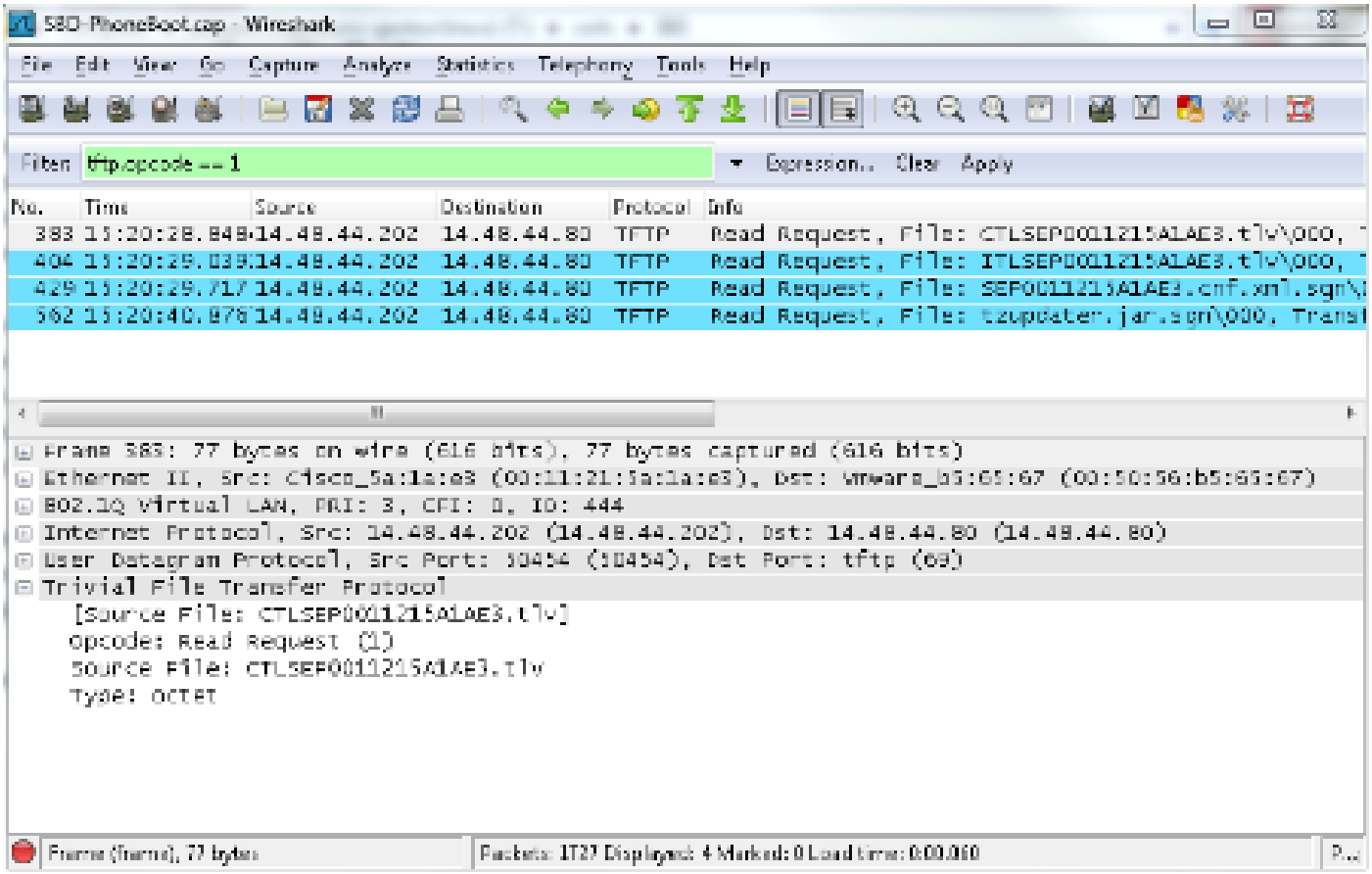
```
7       PUBLICKEY       140
8       SIGNATURE       128
11      CERTHASH        20      C7 3D EA 77 94 5E 06 14 D2 90 B1
                                A1 43 7B 69 84 1D 2D 85 2E
12      HASH ALGORITHM  1       SHA-1

The ITL file was verified successfully.
```

En la siguiente sección se explica exactamente qué ocurre cuando se inicia un teléfono.

Descargas del teléfono ITL y archivo de configuración

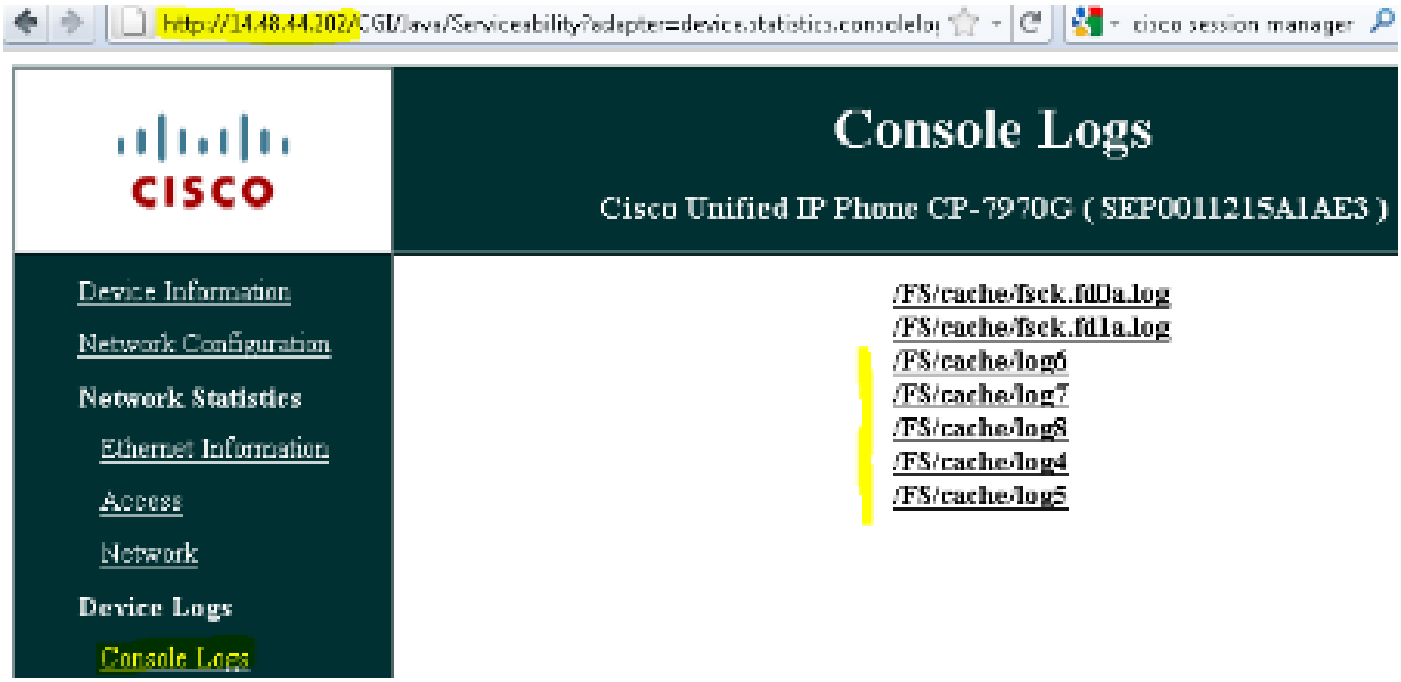
Una vez que el teléfono se inicia y obtiene una dirección IP, así como la dirección de un servidor TFTP, primero solicita los archivos CTL e ITL.

Esta captura de paquetes muestra una solicitud telefónica para el archivo ITL. Si filtra en tftp.opcode == 1, verá cada Solicitud de lectura TFTP del teléfono:



Dado que el teléfono recibió los archivos CTL e ITL del TFTP con éxito, el teléfono solicita un archivo de configuración firmado.

Los registros de la consola del teléfono que muestran este comportamiento están disponibles en la interfaz web del teléfono:



En primer lugar, el teléfono solicita un archivo CTL, que se ejecuta correctamente:

```
837: NOT 09:13:17.561856 SECD: tlRequestFile: Request CTLSEP0011215A1AE3.tlv
846: NOT 09:13:17.670439 TFTP: [27]:Requesting CTLSEP0011215A1AE3.tlv from
14 . 48 . 44 . 80
847: NOT 09:13:17.685264 TFTP: [27]:Finished --> rcvd 4762 bytes
```

A continuación, el teléfono también solicita un archivo ITL:

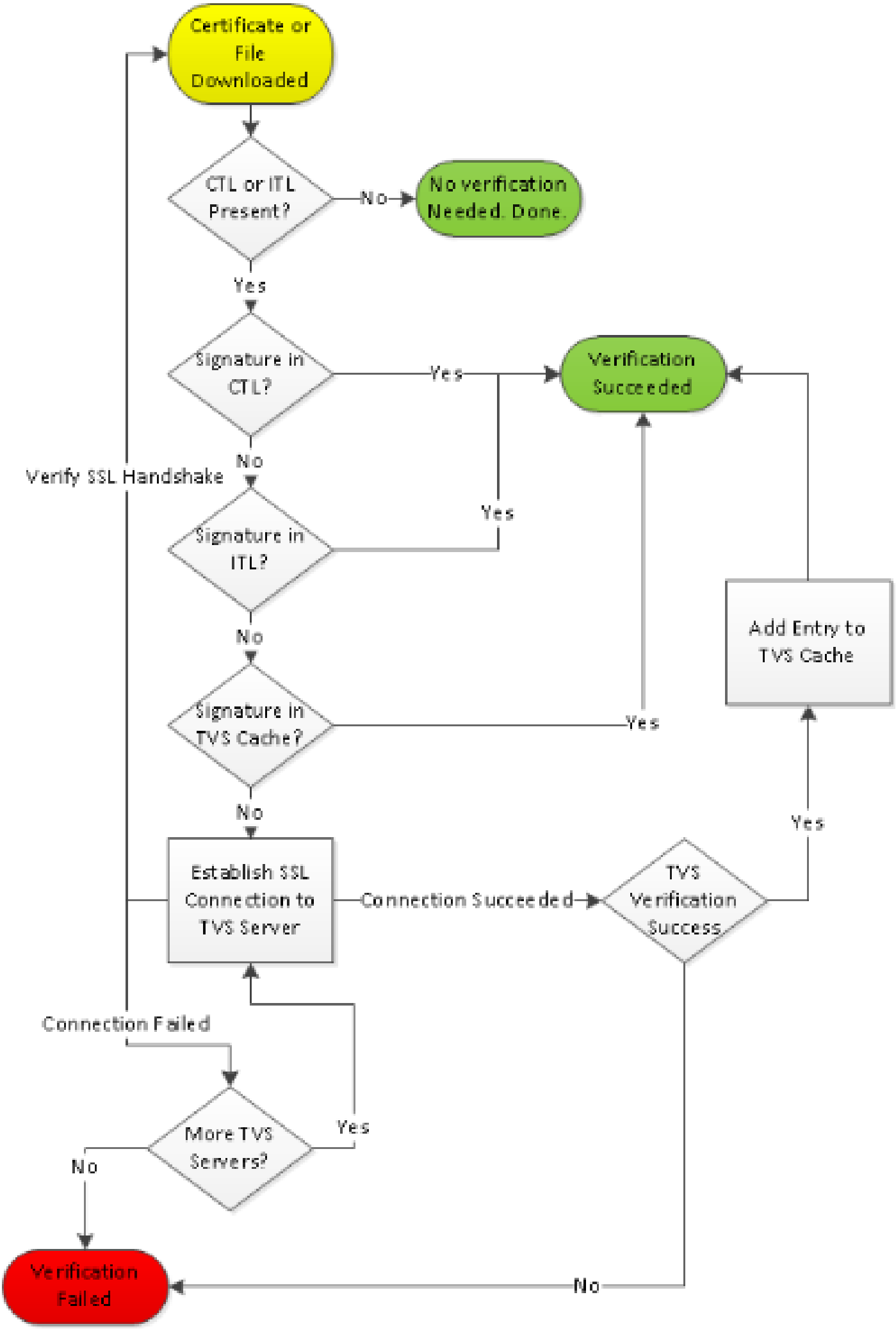
```
868: NOT 09:13:17.860613 TFTP: [28]:Requesting ITLSEP0011215A1AE3.tlv from
14 . 48 . 44 . 80
869: NOT 09:13:17.875059 TFTP: [28]:Finished --> rcvd 5438 bytes
```

El teléfono verifica el ITL y el archivo de configuración

Una vez descargado el archivo ITL, debe verificarse. Hay una serie de estados en los que puede encontrarse un teléfono en este momento, por lo que este documento los cubre todos.

- El teléfono no tiene ningún archivo CTL o ITL presente o ITL está vacío debido al parámetro Prepare Cluster for Rollback to Pre 8.0. en este estado, el teléfono confía ciegamente en el siguiente archivo CTL o ITL descargado y utiliza esta firma a partir de ahora.
- El teléfono ya tiene una CTL, pero no ITL. En este estado, el teléfono sólo confía en un ITL si puede ser verificado por la función CCM+TFTP en el archivo CTL.
- El teléfono ya tiene un archivo CTL y un archivo ITL. En este estado, el teléfono comprueba que los archivos descargados recientemente coinciden con la firma del servidor CTL, ITL o TVS.

Este es un diagrama de flujo que describe cómo verifica el teléfono los archivos firmados y los certificados HTTPS:



En este caso, el teléfono puede verificar la firma en los archivos ITL y CTL. El teléfono ya tiene un

```
File sign verify SUCCESS; header length <296>
```

Dado que el teléfono descargó los archivos CTL e ITL, desde este punto SOLO solicita archivos de configuración firmados.

Esto ilustra que la lógica del teléfono es determinar que el servidor TFTP es seguro, basado en la presencia de CTL e ITL, y luego pedir un archivo firmado:

```
917: NOT 09:13:18.433411 tftpClient: tftp request rcv'd from /usr/tmp/tftp,
srcFile = SEP0011215A1AE3.cnf.xml, dstFile = /usr/ram/SEP0011215A1AE3.cnf.xml
max size = 550001
918: NOT 09:13:18.457949 tftpClient: auth server - tftpList[0] = ::ffff:
14 . 48 . 44 . 80
919: NOT 09:13:18.458937 tftpClient: look up server - 0
920: NOT 09:13:18.462479 SECD: lookupCTL: TFTP SRVR secure
921: NOT 09:13:18.466658 tftpClient: secVal = 0x9 922: NOT 09:13:18.467762
tftpClient: ::ffff:14 . 48 . 44 . 80 is a secure server
923: NOT 09:13:18.468614 tftpClient: retval = SRVR_SECURE
924: NOT 09:13:18.469485 tftpClient: Secure file requested
925: NOT 09:13:18.471217 tftpClient: authenticated file approved - add .sgn
-- SEP0011215A1AE3.cnf.xml.sgn
926: NOT 09:13:18.540562 TFTP: [10]:Requesting SEP0011215A1AE3.cnf.xml.sgn
from 14 . 48 . 44 . 80 with size limit of 550001
927: NOT 09:13:18.559326 TFTP: [10]:Finished --> rcvd 7652 bytes
```

Una vez que se descarga el archivo de configuración firmado, el teléfono debe autenticarlo con la función para CCM+TFTP dentro del ITL:

```
937: NOT 09:13:18.656906 SECD: verifyFile: verify SUCCESS
</usr/ram/SEP0011215A1AE3.cnf.xml>
```

TVS de contactos del teléfono para certificado desconocido

El archivo ITL proporciona una función TVS que contiene el certificado del servicio TVS que se ejecuta en el puerto TCP 2445 del servidor CUCM.

TVS se ejecuta en todos los servidores donde el servicio CallManager está activado. El servicio TFTP de CUCM utiliza el grupo CallManager configurado para crear una lista de servidores TVS con los que el teléfono debe contactar en el archivo de configuración del teléfono.

Algunos laboratorios utilizan un único servidor CUCM. En un clúster de CUCM de varios nodos, puede haber hasta tres entradas de TV para un teléfono, una para cada CUCM del grupo CUCM del teléfono.

Este ejemplo muestra lo que sucede cuando se presiona el botón Directories en el teléfono IP. La

URL de Directorios está configurada para HTTPS, por lo que el teléfono se presenta con el certificado web Tomcat del servidor de Directorios.

Este certificado web de Tomcat (tomcat.pem en Administración del sistema operativo) no está cargado en el teléfono, por lo que el teléfono debe ponerse en contacto con TVS para autenticar el certificado.

Consulte el diagrama anterior de descripción general de la TV para obtener una descripción de la interacción. Esta es la perspectiva del registro de la consola telefónica:

En primer lugar, busque la dirección URL del directorio:

```
1184: NOT 15:20:55.219275 JVM: Startup Module Loader|cip.dir.TandunDirectories:
? - Directory url https://14 . 48 . 44 . 80:8443/ccmcip/xmldirectory.jsp
```

Se trata de una sesión HTTP segura SSL/Seguridad de la capa de transporte (TLS) que requiere verificación.

```
1205: NOT 15:20:59.404971 SECD: clpSetupSsl: Trying to connect to IPV4, IP:
14 . 48 . 44 . 80, Port : 8443
1206: NOT 15:20:59.406896 SECD: clpSetupSsl: TCP connect() waiting,
<14 . 48 . 44 . 80> c:8 s:9 port: 8443
1207: NOT 15:20:59.408136 SECD: clpSetupSsl: TCP connected,
<14 . 48 . 44 . 80> c:8 s:9
1208: NOT 15:20:59.409393 SECD: clpSetupSsl: start SSL/TLS handshake,
<14 . 48 . 44 . 80> c:8 s:9
1209: NOT 15:20:59.423386 SECD: srvr_cert_vfy: Server Certificate
Validation needs to be done
```

El teléfono primero verifica que el certificado presentado por el servidor SSL/TLS esté presente en la CTL. Luego el teléfono mira las funciones en el archivo ITL para ver si encuentra una coincidencia.

Este mensaje de error indica "el certificado HTTPS no está en CTL", lo que significa que "esa certificación no se puede encontrar en CTL o ITL".

```
1213: NOT 15:20:59.429176 SECD: findByCertAndRoleInTL: Searching TL from CTL file
1214: NOT 15:20:59.430315 SECD: findByCertAndRoleInTL: Searching TL from ITL file
1215: ERR 15:20:59.431314 SECD: EROR:https_cert_vfy: HTTPS cert not in CTL,
<14 . 48 . 44 . 80>
```

Después de comprobar el contenido directo del archivo CTL e ITL para el certificado, lo siguiente que comprueba el teléfono es la caché de TVS.

Esto se hace para reducir el tráfico de red si el teléfono ha solicitado recientemente al servidor TVS el mismo certificado.

Si el certificado HTTPS no se encuentra en la caché del teléfono, puede establecer una conexión TCP con el propio servidor de TVS.

```
1220: NOT 15:20:59.444517 SECD: processTvsClntReq: TVS Certificate
Authentication request
1221: NOT 15:20:59.445507 SECD: lookupAuthCertTvsCacheEntry: No matching
entry found at cache
1222: NOT 15:20:59.446518 SECD: processTvsClntReq: No server sock exists,
must be created
1223: NOT 15:20:59.451378 SECD: secReq_initClient: clnt sock fd 11 bound
to </tmp/secClnt_secd>
1224: NOT 15:20:59.457643 SECD: getTvsServerInfo: Phone in IPv4 only mode
1225: NOT 15:20:59.458706 SECD: getTvsServerInfo: Retreiving IPv4 address
1230: NOT 15:20:59.472628 SECD: connectToTvsServer: Successfully started
a TLS connection establishment to the TVS server: IP:14 . 48 . 44 . 80, port:2445
(default); Waiting for it to get connected.
```

Recuerde que la conexión a TVS es SSL/TLS (HTTP seguro o HTTPS), por lo que también es un certificado que debe autenticarse con la CTL en ITL.

Si todo va correctamente, el certificado del servidor de TVS se encuentra en la función TVS del archivo ITL. Consulte ITL Record #3 en el ejemplo anterior de archivo ITL.

```
1244: NOT 15:20:59.529938 SECD: srvr_cert_vfy: Server Certificate Validation
needs to be done
1245: NOT 15:20:59.533412 SECD: findByIssuerAndSerialAndRoleInTL:
Searching TL from CTL file
1246: NOT 15:20:59.534936 SECD: findByIssuerAndSerialAndRoleInTL:
Searching TL from ITL file
1247: NOT 15:20:59.537359 SECD: verifyCertWithHashFromTL: cert hash and
hash in TL MATCH
1248: NOT 15:20:59.538726 SECD: tvs_cert_vfy: TVS cert verified with hash
from TL, <14 . 48 . 44 . 80>
```

Éxito! El teléfono dispone ahora de una conexión segura al servidor de TVS. El siguiente paso es preguntar al servidor TVS "Hola, ¿confío en este certificado de servidor de Directorios?"

Este ejemplo muestra la respuesta a esa pregunta: una respuesta de 0 que significa éxito (sin error).

```
1264: NOT 15:20:59.789738 SECD: sendTvsClientReqToSrvr: Authenticate
Certificate : request sent to TVS server - waiting for response
1273: NOT 15:20:59.825648 SECD: processTvsSrvrResponse: Authentication Response
received, status : 0
```

Dado que hay una respuesta correcta de TVS, los resultados de ese certificado se guardan en la caché.

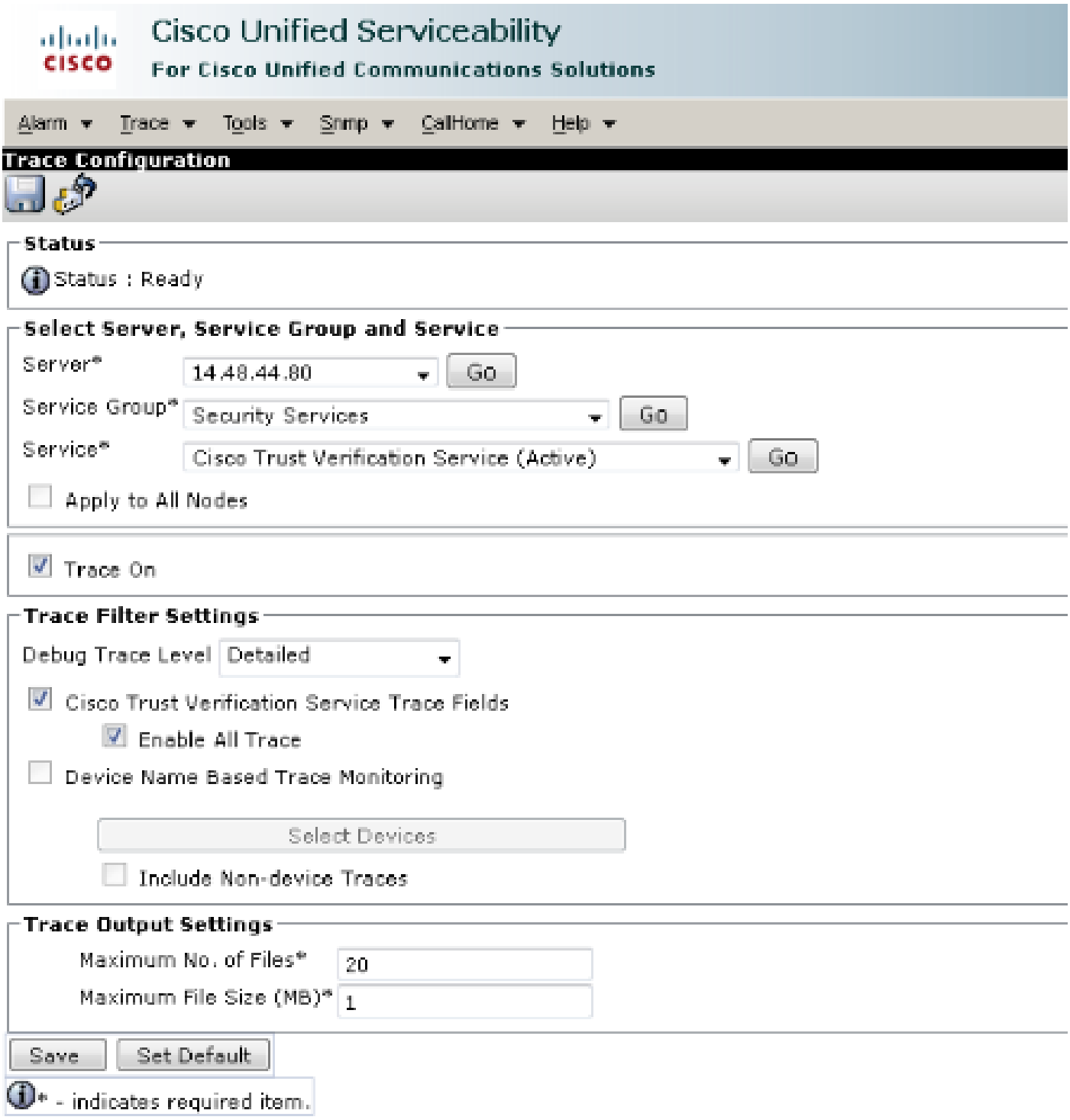
Esto significa que, si presiona el botón Directories nuevamente dentro de los próximos 86.400 segundos, no necesita comunicarse con el servidor TVS para verificar el certificado. Sólo tiene que acceder a la caché local.

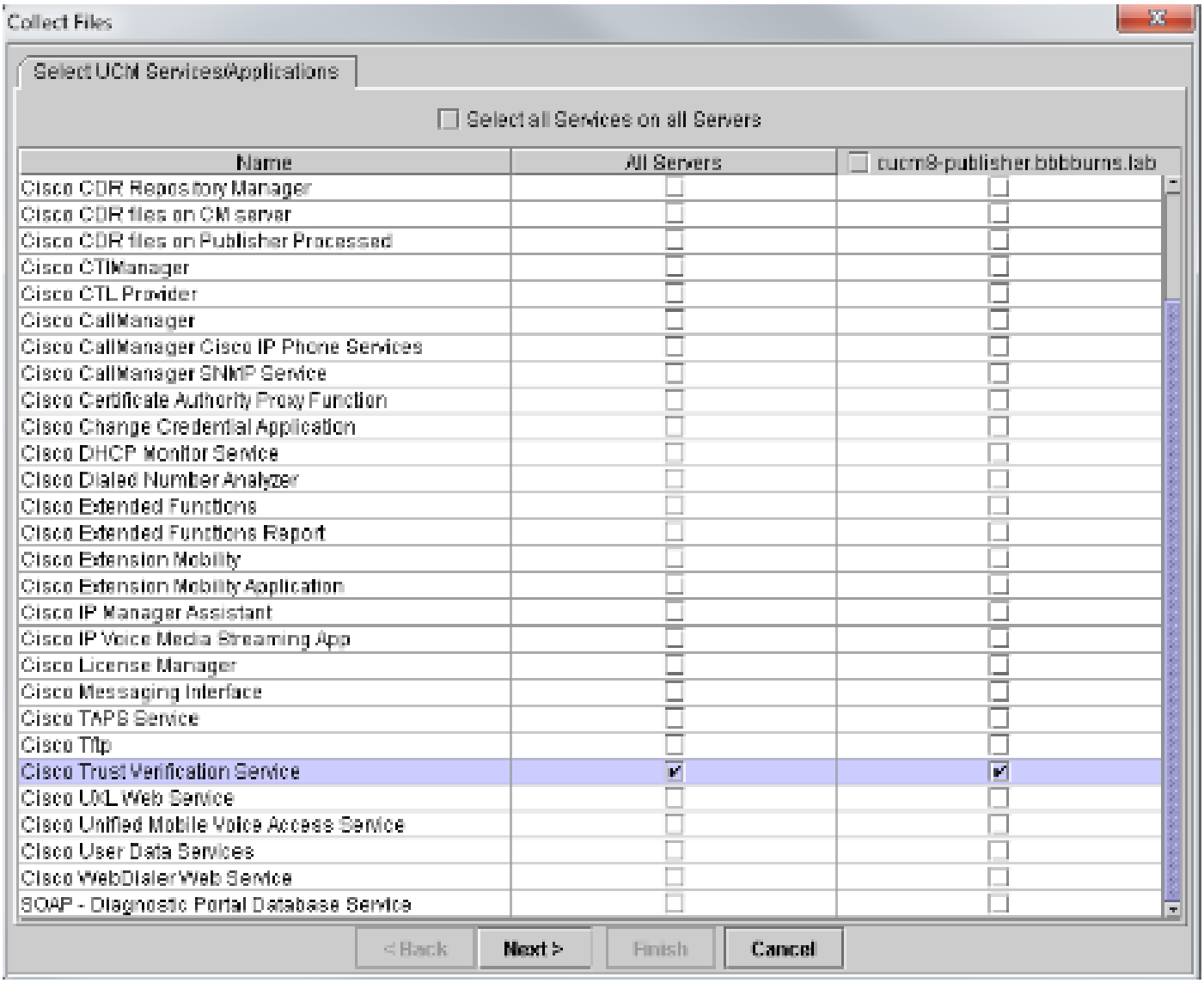
```
1279: NOT 15:20:59.837086 SECD: saveCertToTvsCache: Saving certificate
in TVS cache with default time-to-live value: 86400 seconds
1287: ERR 15:20:59.859993 SECD: Authenticated the HTTPS conn via TVS
```

Por último, compruebe que la conexión con el servidor Directories se ha realizado correctamente.

```
1302: ERR 15:21:01.959700 JVM: Startup Module Loader|cip.http.ae:?
- listener.httpSucceed:  https://14 . 48 . 44 . 80:8443/ccmcip/
xmldirectoryinput.jsp?name=SEP0011215A1AE3
```

Este es un ejemplo de lo que ocurre en el servidor de CUCM donde se ejecuta TVS. Puede recopilar registros de TVS con la herramienta Cisco Unified Real-Time Monitoring Tool (RTMT).


Cisco Unified Serviceability
For Cisco Unified Communications Solutions
Alarm
Trace
Tools
Snmp
CallHome
Help
Trace Configuration
Status
Status : Ready
Select Server, Service Group and Service
Server*
14.48.44.80
Go
Service Group*
Security Services
Go
Service*
Cisco Trust Verification Service (Active)
Go
Apply to All Nodes
Trace On
Trace Filter Settings
Debug Trace Level
Detailed
Cisco Trust Verification Service Trace Fields
Enable All Trace
Device Name Based Trace Monitoring
Select Devices
Include Non-device Traces
Trace Output Settings
Maximum No. of Files*
20
Maximum File Size (MB)*
1
Save
Set Default
* - indicates required item.



Los registros de TVS de CUCM muestran que el protocolo de enlace SSL con el teléfono, el teléfono pregunta a TVS acerca del certificado de Tomcat y, a continuación, TVS responde para indicar que el certificado coincide en el almacén de certificados de TVS.

```
15:21:01.954 |   debug 14 . 48 . 44 . 202: tvsSSLHandShake Session ciphers - AES256-SHA
15:21:01.954 |   debug TLS HS Done for ph_conn .
15:21:02.010 |   debug     MsgType               : TVS_MSG_CERT_VERIFICATION_REQ
15:21:02.011 |   debug tvsGetIssuerNameFromX509 - issuerName : CN=CUCM8-
Publisher.bbbburns.lab;OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US and Length: 75

15:21:02.011 |   debug CertificateDBCache::getCertificateInformation -
Certificate compare return =0
15:21:02.011 |   debug CertificateDBCache::getCertificateInformation -
Certificate found and equal
15:21:02.011 |   debug     MsgType               : TVS_MSG_CERT_VERIFICATION_RES
```

El almacén de certificados de TVS es una lista de todos los certificados contenidos en la página web Administración del SO > Administración de certificados.

Comprobar manualmente que el teléfono ITL coincide con el CUCM ITL

Una idea errónea común observada durante la resolución de problemas se refiere a la tendencia a eliminar el archivo ITL con la esperanza de que resuelva un problema de verificación de archivos.

A veces, es necesario eliminar el archivo ITL, pero el archivo ITL solo debe eliminarse cuando se cumplen TODAS estas condiciones.

- La firma del archivo ITL en el teléfono no coincide con la firma del archivo ITL en el servidor TFTP de CM.
- La firma TVS del archivo ITL no coincide con el certificado presentado por TVS.
- El teléfono muestra "Error de verificación" cuando intenta descargar el archivo ITL o los archivos de configuración.
- No existe una copia de seguridad de la clave privada TFTP anterior.

Así es como usted verifica las dos primeras condiciones.

En primer lugar, puede comparar la suma de comprobación del archivo ITL presente en CUCM con la suma de comprobación del archivo ITL del teléfono.

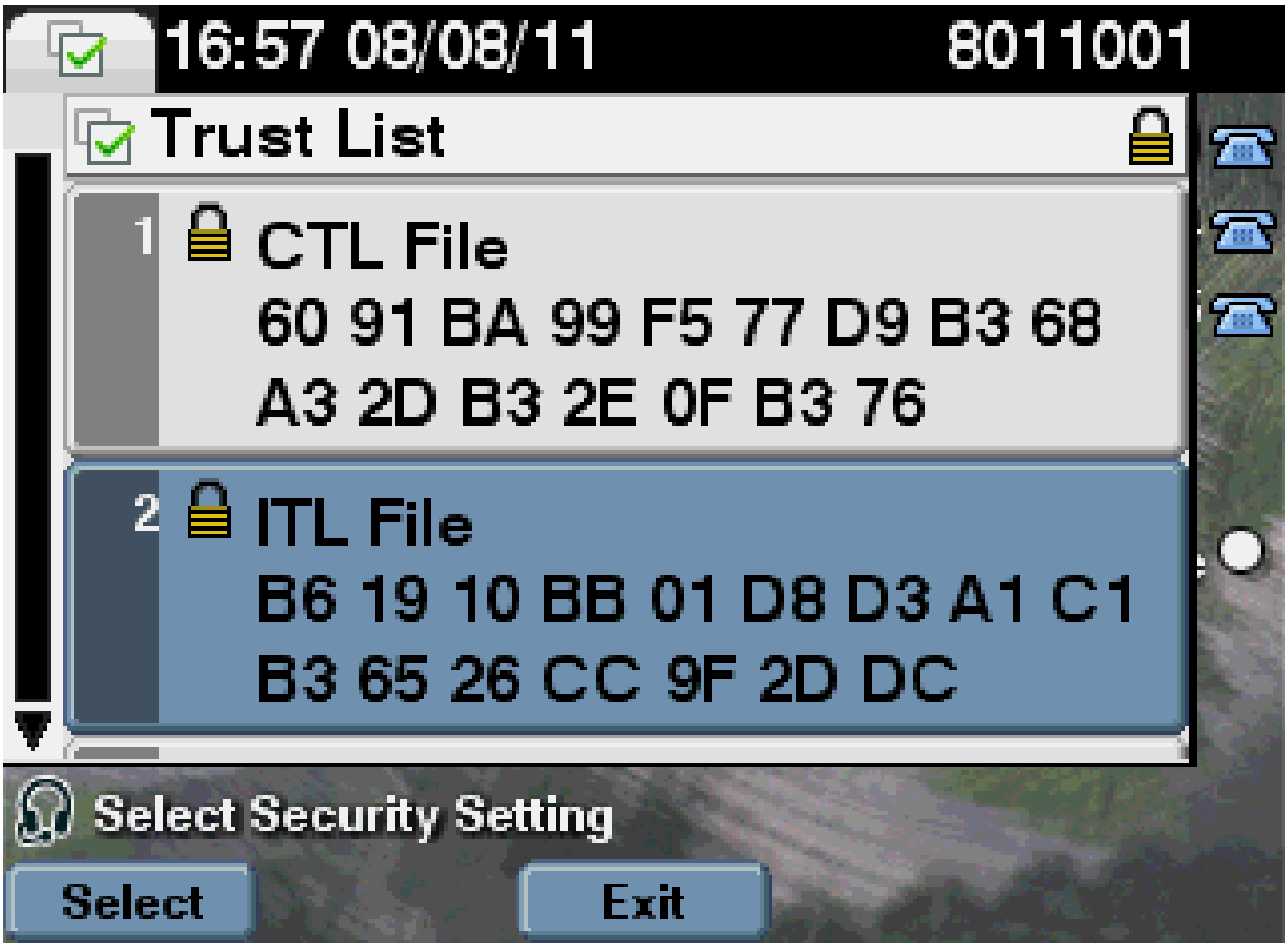
Actualmente no hay manera de ver la suma MD5 del archivo ITL en CUCM desde CUCM hasta que ejecute una versión con la corrección para este Id. de bug de Cisco CSCto60209.

Mientras tanto, ejecute esto con su GUI o programas CLI favoritos:

```
jasburns@jasburns-gentoo /data/trace/jasburns/certs/SBD $ tftp 14 . 48 . 44 . 80
tftp> get ITLSEP0011215A1AE3.tlv
Received 5438 bytes in 0.0 seconds
tftp> quit
jasburns@jasburns-gentoo /data/trace/jasburns/certs/SBD $ md5sum
ITLSEP0011215A1AE3.tlv
b61910bb01d8d3a1c1b36526cc9f2ddc  ITLSEP0011215A1AE3.tlv
```

Esto muestra que la suma MD5 del archivo ITL en CUCM es b61910bb01d8d3a1c1b36526cc9f2dc.

Ahora puede mirar el teléfono en sí para determinar el hash del archivo ITL cargado allí: Configuraciones > Configuración de Seguridad > Lista de Confianza.

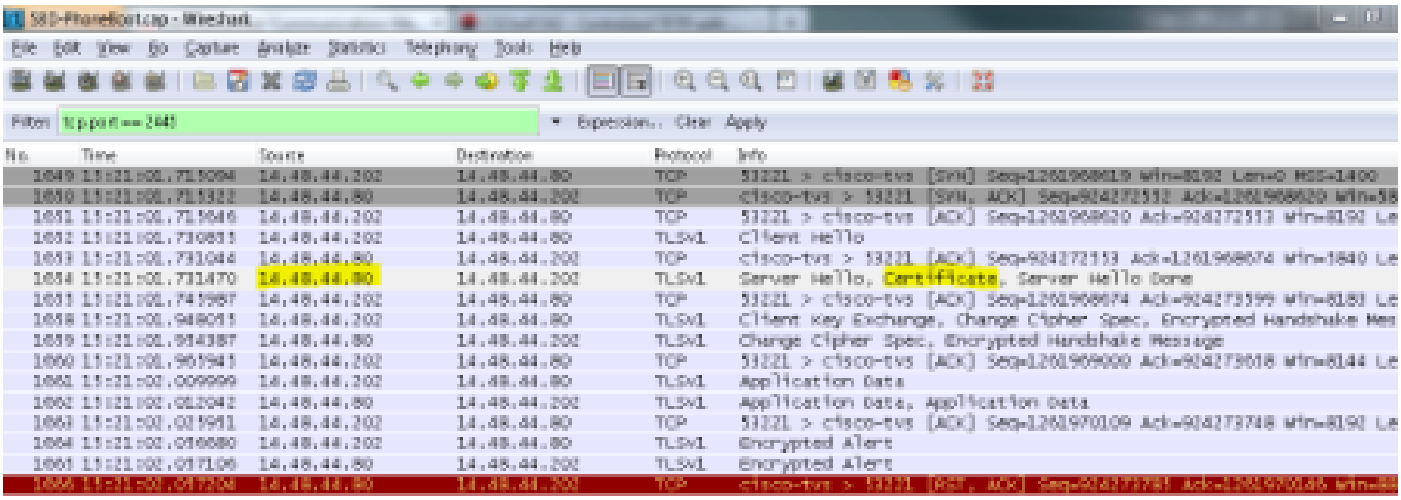


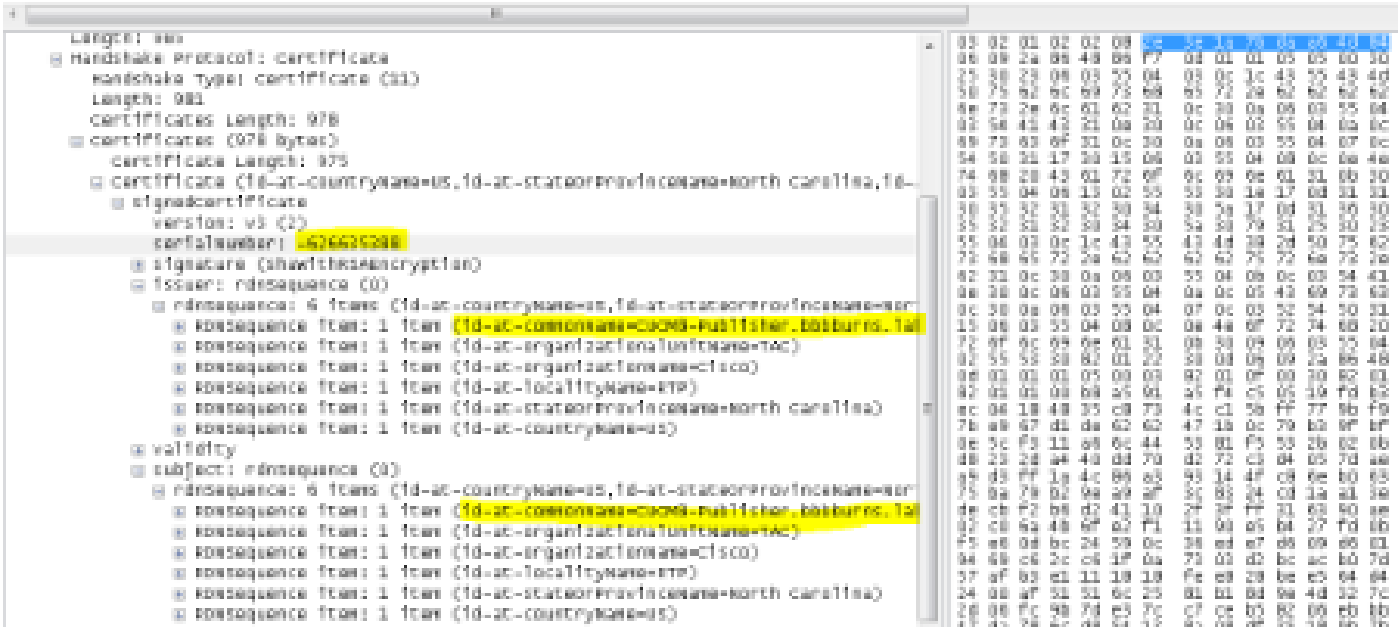
Esto muestra que las sumas MD5 coinciden. Esto significa que el archivo ITL del teléfono coincide con el archivo de CUCM, por lo que no es necesario eliminarlo.

Si SÍ coincide, debe pasar a la siguiente operación: determine si el certificado de TVS del DIT coincide o no con el certificado presentado por TVS. Esta operación está un poco más involucrada.

En primer lugar, observe la captura de paquetes del teléfono que se conecta al servidor TVS en el puerto TCP 2445.

Haga clic con el botón derecho del ratón en cualquier paquete de esta secuencia en Wireshark, haga clic en Decodificar como y seleccione SSL. Busque el certificado de servidor que tenga este aspecto:





Observe el certificado de TVS contenido en el archivo ITL anterior. A continuación, verá una entrada con el número de serie 2E3E1A7BDAA64D84.

<#root>

admin:

show itl

```
        ITL Record #:3
                    ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       743
2       DNSNAME         2
3       SUBJECTNAME     76      CN=CUCM8-Publisher.bbbburns.lab;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
4       FUNCTION        2       TVS
5       ISSUERNAME      76      CN=CUCM8-Publisher.bbbburns.lab;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
6       SERIALNUMBER    8       2E:3E:1A:7B:DA:A6:4D:84
```

Éxito, el archivo TVS.pem del archivo ITL coincide con el certificado TVS presentado en la red. No es necesario eliminar el DIT y TVS presenta el certificado correcto.

Si la autenticación de archivos sigue fallando, compruebe el resto del diagrama de flujo anterior.

Restricciones e interacciones

Regenere certificados/Reconstruya un clúster/Vencimiento de certificados

El certificado más importante es ahora el certificado CallManager.pem. Esta clave privada de certificado se utiliza para firmar todos los archivos de configuración TFTP, que incluye el archivo ITL.

Si se regenera el archivo CallManager.pem, se genera un nuevo certificado CCM+TFTP con una nueva clave privada. Además, el archivo ITL ahora está firmado por esta nueva clave CCM+TFTP.

Después de regenerar CallManager.pem y reiniciar el servicio TVS y TFTP, esto sucede cuando se inicia un teléfono.

1. El teléfono intenta descargar el nuevo archivo ITL firmado por el nuevo CCM+TFTP desde el servidor TFTP. En este momento, el teléfono solo tiene el archivo ITL antiguo y las nuevas claves no se encuentran en el archivo ITL presente en el teléfono.
2. Dado que el teléfono no pudo encontrar la nueva firma CCM+TFTP en el antiguo ITL, intenta ponerse en contacto con el servicio TVS.

   Nota: Esta parte es extremadamente importante. El certificado de TVS del archivo ITL antiguo debe seguir coincidiendo. Si CallManager.pem y TVS.pem se regeneran al mismo tiempo exacto, los teléfonos no pueden descargar ningún archivo nuevo sin eliminar el ITL del teléfono manualmente.

3. Cuando el teléfono entra en contacto con TVS, el servidor de CUCM que ejecuta TVS tiene el nuevo certificado CallManager.pem en el almacén de certificados del sistema operativo.
4. El servidor TVS devuelve el resultado correcto y el teléfono carga el nuevo archivo ITL en la memoria.
5. El teléfono ahora intenta descargar un archivo de configuración, que ha sido firmado por la nueva clave CallManager.pem.
6. Puesto que se ha cargado el nuevo DIT, el DIT en memoria verifica con éxito el archivo de configuración recién firmado.

Puntos clave:

- Nunca regenere los certificados CallManager.pem y TVS.pem al mismo tiempo.
- Si se regenera TVS.pem o CallManager.pem, se deben reiniciar TVS y TFTP y restablecer los teléfonos para obtener los nuevos archivos ITL.
- Las versiones más recientes de CUCM gestionan este restablecimiento del teléfono

automáticamente y avisan al usuario en el momento de la regeneración del certificado.
- Si existe más de un servidor TVS (más de un servidor en el grupo CallManager), los servidores adicionales pueden autenticar el nuevo certificado CallManager.pem.

Mover teléfonos entre clústeres

Cuando traslade teléfonos de un clúster a otro con los ITL instalados, se deben tener en cuenta los valores de ITL y la clave privada TFTP.

Cualquier nuevo archivo de configuración presentado al teléfono DEBE coincidir con una firma en CTL, ITL o una firma en el servicio TVS actual del teléfono.

Este documento explica cómo asegurarse de que el archivo ITL actual del teléfono puede confiar en el nuevo archivo ITL del clúster y en los archivos de configuración. https://supportforums.cisco.com/docs/DOC-15799.

Backup Y Restauración

Se realiza una copia de seguridad del certificado y la clave privada de CallManager.pem a través del Sistema de recuperación ante desastres (DRS). Si se reconstruye un servidor TFTP, DEBE restaurarse desde la copia de seguridad para que se pueda restaurar la clave privada.

Sin la clave privada CallManager.pem en el servidor, los teléfonos con ITL actuales que utilizan la clave antigua no confían en los archivos de configuración firmados.

Si un clúster se reconstruye y no se restaura desde la copia de seguridad, es exactamente igual que el documento "Traslado de teléfonos entre clústeres". Esto se debe a que un clúster con una nueva clave es un clúster diferente en lo que respecta a los teléfonos.

Hay un defecto grave asociado con la copia de seguridad y la restauración. Si un clúster es susceptible al Id. de error de Cisco CSCtn50405, las copias de seguridad de DRS no contienen el certificado CallManager.pem.

Esto hace que cualquier servidor restaurado desde esta copia de seguridad genere archivos ITL dañados hasta que se genere un nuevo CallManager.pem.

Si no hay otros servidores TFTP funcionales que no hayan pasado por la operación de copia de seguridad y restauración, esto posiblemente significa que todos los archivos ITL deben eliminarse de los teléfonos.

Para verificar si su archivo CallManager.pem necesita ser regenerado, ingrese el comando show itl seguido de:

```
run sql select c.subjectname, c.serialnumber, c.ipv4address, t.name from
certificate as c, certificatetrustrolemap as r, typetrustrole as t where  c.pkid =
r.fkcertificate and t.enum = r.tktrustrole
```

En el resultado del DIT, los principales errores que hay que buscar son:

```
This etoken was not used to sign the ITL file.
```

y

```
Verification of the ITL file failed.
Error parsing the ITL file!!
```

La consulta SQL (Lenguaje de consulta estructurado) anterior busca los certificados que tienen una función de "Autenticación y autorización".

El certificado CallManager.pem de la consulta de base de datos anterior que tiene la función de Autenticación y Autorización también debe estar presente en la página web Administración de certificados del sistema operativo.

Si se encuentra el defecto anterior, hay una discordancia entre los certificados CallManager.pem en la consulta y en la página web del sistema operativo.

Cambiar nombres de host o nombres de dominio

Si cambia el nombre de host o el nombre de dominio de un servidor de CUCM, éste regenerará todos los certificados a la vez en ese servidor. La sección de regeneración de certificados explicó que la regeneración tanto de TVS.pem como de CallManager.pem es una "mala cosa".

Hay algunos escenarios donde un cambio de nombre de host falla, y algunos donde funciona sin problemas. Esta sección cubre todos ellos y los enlaza con lo que ya sabe sobre TVS e ITL de este documento.

Clúster de nodo único solo con ITL (tenga cuidado, se interrumpe sin preparación)

- Con un servidor Business Edition o una implementación sólo de editor, se vuelven a generar tanto CallManager.pem como TVS.pem al cambiar los nombres de host.
- Si el nombre de host se cambia en un clúster de nodo único sin utilizar primero el parámetro Rollback Enterprise que se trata aquí, los teléfonos no podrán verificar el nuevo archivo ITL o los archivos de configuración con su archivo ITL actual.
- Los teléfonos no se pueden conectar a TVS porque el certificado de TVS tampoco es de confianza.
- Los teléfonos muestran un error sobre "Fallo en la verificación de la lista de confianza", no surten efecto nuevos cambios de configuración y las URL de servicio seguro fallan.
- La única solución si la precaución del paso 2 no se toma primero es eliminar manualmente el DIT de cada teléfono.

Clúster de nodo único con CTL e ITL (se puede interrumpir temporalmente, pero se puede corregir fácilmente)

- Después de ejecutar el cambio de nombre de los servidores, vuelva a ejecutar el cliente CTL. Esto coloca el nuevo certificado CallManager.pem en el archivo CTL que descarga el teléfono.
- Se puede confiar en los nuevos archivos de configuración, que incluyen los nuevos archivos ITL, basándose en la función CCM+TFTP del archivo CTL.
- Esto funciona porque el archivo CTL actualizado es de confianza basado en una clave privada de eToken USB que permanece igual.

Clúster de varios nodos con solo ITL (esto suele funcionar, pero se puede interrumpir permanentemente si se realiza de forma precipitada)

- Dado que un clúster de varios nodos tiene varios servidores TVS, cualquier servidor individual puede tener sus certificados regenerados sin ningún problema. Cuando se presenta el teléfono con esta firma nueva y desconocida, se solicita a otro servidor de TVS que compruebe el nuevo certificado de servidor.
- Hay dos problemas principales que pueden hacer que esto falle:
    - Si se cambia el nombre de todos los servidores y se reinician al mismo tiempo, ninguno de los servidores TVS es accesible con certificados conocidos cuando los servidores y teléfonos vuelvan a estar activos.
    - Si un teléfono tiene un solo servidor en el grupo CallManager, los servidores TVS adicionales no hacen ninguna diferencia. Consulte el escenario "Single Node Cluster" para resolver esto o agregue otro servidor al CallManager Group del teléfono.

Clúster de varios nodos con CTL e ITL (esto no se puede interrumpir permanentemente)

- Después de ejecutar los cambios de nombre, el servicio TVS autentica los nuevos certificados.
- Incluso si todos los servidores TVS no están disponibles por alguna razón, el cliente CTL se puede seguir utilizando para actualizar los teléfonos con los nuevos certificados CallManager.pem CCM+TFTP.

TFTP centralizado

Cuando se inicia un teléfono con un ITL, solicita estos archivos: CTLSEP<Dirección MAC>.tlv, ITLSEP<Dirección MAC>.tlv y SEP<Dirección MAC>.cnf.xml.sgn.

Si el teléfono no puede encontrar estos archivos, solicita los archivos ITLFile.tlv y CTLFile.tlv, que un servidor TFTP centralizado proporciona a cualquier teléfono que lo solicite.

Con el TFTP centralizado, hay un solo clúster TFTP que apunta a varios otros subclústeres.

A menudo, esto se hace porque los teléfonos en varios clústeres de CUCM comparten el mismo ámbito DHCP y, por lo tanto, deben tener el mismo servidor TFTP de la opción DHCP 150.

Todos los teléfonos IP apuntan al clúster TFTP central, incluso si se registran en otros clústeres.

Este servidor TFTP central consulta a los servidores TFTP remotos cada vez que recibe una solicitud de un archivo que no puede encontrar.

Debido a esta operación, el TFTP centralizado sólo funciona en un entorno homogéneo de ITL.

Todos los servidores deben ejecutar CUCM versión 8.x o posterior, o bien todos los servidores deben ejecutar versiones anteriores a la versión 8.x.

Si se presenta un archivo ITLFile.tlv desde el servidor TFTP centralizado, los teléfonos no confían en ningún archivo del servidor TFTP remoto porque las firmas no coinciden.

Esto sucede en una mezcla heterogénea. En una mezcla homogénea, el teléfono solicita ITLSEP<MAC>.tlv, que se extrae del clúster remoto correcto.

En un entorno heterogéneo con una mezcla de clústeres anteriores a la versión 8.x y a la versión 8.x, se debe habilitar "Prepare Cluster for Rollback to Pre 8.0" en el clúster de la versión 8.x, tal como se describe en Id. de error de Cisco CSCto87262 .

Configure los "Parámetros de URL de teléfono seguro" con HTTP en lugar de HTTPS. De este modo se desactivan las funciones del DIT en el teléfono.

Preguntas Frecuentes

¿Puedo desactivar SBD?

Solo puede desactivar SBD si SBD e ITL funcionan actualmente.

SBD se puede deshabilitar temporalmente en teléfonos con el parámetro empresarial "Prepare Cluster for Rollback to pre 8.0" y configurando los "Parámetros de URL de teléfono seguro" con HTTP en lugar de HTTPS.

Cuando se establece el parámetro Rollback, se crea un archivo ITL firmado con entradas de función en blanco.

El archivo ITL "vacío" aún está firmado, por lo que el clúster debe estar en un estado de seguridad completamente funcional para poder habilitar este parámetro.

Una vez habilitado este parámetro y descargado y verificado el nuevo archivo ITL con entradas en blanco, los teléfonos aceptan cualquier archivo de configuración, sin importar quién lo haya firmado.

No se recomienda dejar el clúster en este estado, ya que ninguna de las tres funciones mencionadas anteriormente (archivos de configuración autenticados, archivos de configuración cifrados y URL HTTPS) está disponible.

¿Puedo eliminar fácilmente el archivo ITL de todos los teléfonos una vez que se ha perdido CallManager.pem?

Actualmente no existe ningún método para eliminar todos los DIT de un teléfono proporcionado por Cisco de forma remota. Es por ello que los procedimientos e interacciones descritos en este documento son tan importantes de tener en cuenta.

Actualmente hay una mejora sin resolver del Id. de bug Cisco CSCto47052 que solicita esta funcionalidad, pero aún no se ha implementado.

Mientras tanto, se ha agregado una nueva función a través del ID de bug de Cisco CSCts01319 que posiblemente permite que el Cisco Technical Assistance Center (TAC) vuelva al ITL anteriormente confiable si aún está disponible en el servidor.

Esto sólo funciona en determinados casos en los que el clúster se encuentra en una versión con este defecto y en los que el DIT anterior existe en una copia de seguridad almacenada en una ubicación especial del servidor.

Vea el defecto para ver si su versión tiene la corrección. Póngase en contacto con el TAC de Cisco para realizar el procedimiento de recuperación potencial que se explica en el defecto.

Si el procedimiento anterior no está disponible, los botones del teléfono deben pulsarse manualmente en el teléfono para eliminar el archivo ITL. Este es el equilibrio entre seguridad y facilidad de administración. Para que el archivo ITL sea realmente seguro, no debe ser removido fácilmente de forma remota.

Incluso con pulsaciones de botones con scripts y objetos XML de protocolo simple de acceso a objetos (SOAP), el ITL no se puede eliminar de forma remota.

Esto se debe a que, en este momento, el acceso TVS (y, por lo tanto, el acceso URL de autenticación segura para validar los objetos de pulsación de botones XML de SOAP entrantes) no funciona.

Si la URL de autenticación no está configurada como segura, es posible escribir un script en las pulsaciones de teclas para eliminar un ITL, pero este script no está disponible en Cisco.

Otros métodos para realizar scripts de pulsaciones de teclas remotas sin utilizar la URL de autenticación están posiblemente disponibles de un tercero, pero Cisco no proporciona estas aplicaciones.

El método más utilizado para eliminar el DIT es la difusión por correo electrónico a todos los usuarios del teléfono, en la que se les indica la secuencia de teclas.

Si el acceso a los parámetros está establecido en Restricted o Disabled, el teléfono debe restablecerse de fábrica, ya que los usuarios no tienen acceso al menú Settings del teléfono.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).