CUCM-Sicherheit standardmäßig und ITL-Betrieb und Fehlerbehebung

Inhalt

Einführung

In diesem Dokument wird die Funktion "Security By Default (SBD)" von Cisco Unified Communications Manager (CUCM) Version 8.0 und höher beschrieben. Dieses Dokument dient als Ergänzung zu den offiziellen Dokumenten "Security By Default" und enthält betriebliche Informationen und Tipps zur Fehlerbehebung, die Administratoren helfen und die Fehlerbehebung erleichtern.

Hintergrundinformationen

CUCM Version 8.0 und höher führt die SBD-Funktion ein, die aus ITL-Dateien (Identity Trust List) und dem Trust Verification Service (TVS) besteht. Jeder CUCM-Cluster verwendet jetzt

automatisch ITL-basierte Sicherheit. Es gibt einen Kompromiss zwischen Sicherheit und Benutzerfreundlichkeit/einfacher Administration, den Administratoren kennen müssen, bevor sie bestimmte Änderungen an einem CUCM-Cluster der Version 8.0 vornehmen.

Es empfiehlt sich, sich mit den folgenden Kernkonzepten vertraut zu machen: Wikipedia-Artikel und Wikipedia-Artikel über die asymmetrische Schlüsselkryptografie und die öffentliche Schlüsselinfrastruktur.

SBD - Überblick

Dieser Abschnitt bietet einen schnellen Überblick über die Funktionen von SBD. Ausführliche technische Details zu den einzelnen Funktionen finden Sie im Abschnitt SBD-Detailangaben und Informationen zur Fehlerbehebung.

Das SBD bietet die folgenden drei Funktionen für unterstützte IP-Telefone:

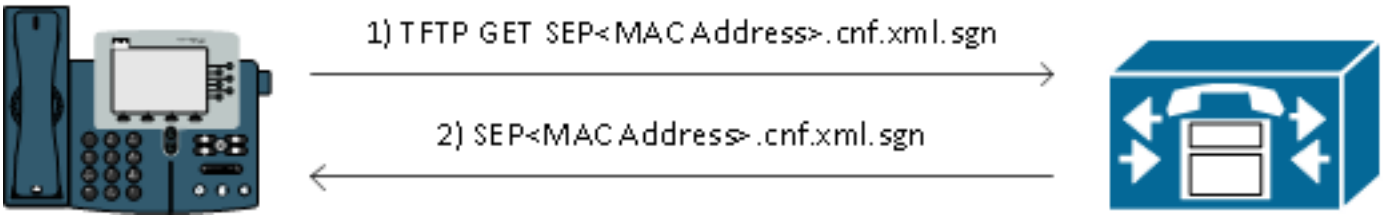
- Standardauthentifizierung von TFTP-heruntergeladenen Dateien (Konfiguration, Gebietsschema, Ringliste), die einen Signaturschlüssel verwenden
- Optionale Verschlüsselung von TFTP-Konfigurationsdateien mit einem Signaturschlüssel
- Zertifikatsüberprüfung für per Telefon initiierte HTTPS-Verbindungen, die einen Remote Certificate Trust Store auf dem CUCM (TVS) verwenden

Dieses Dokument bietet eine Übersicht über jede dieser Funktionen.

TFTP-Download-Authentifizierung

Wenn eine CTL- oder ITL-Datei (Certificate Trust List) vorhanden ist, fordert das IP-Telefon eine signierte TFTP-Konfigurationsdatei vom CUCM-TFTP-Server an. Mit dieser Datei kann das Telefon überprüfen, ob die Konfigurationsdatei von einer vertrauenswürdigen Quelle stammt. Wenn auf Telefonen CTL-/ITL-Dateien vorhanden sind, müssen Konfigurationsdateien von einem vertrauenswürdigen TFTP-Server signiert werden. Die Datei ist während der Übertragung im Netzwerk unverschlüsselter Text, wird jedoch mit einer speziellen Signatur zur Verifizierung ausgeliefert.

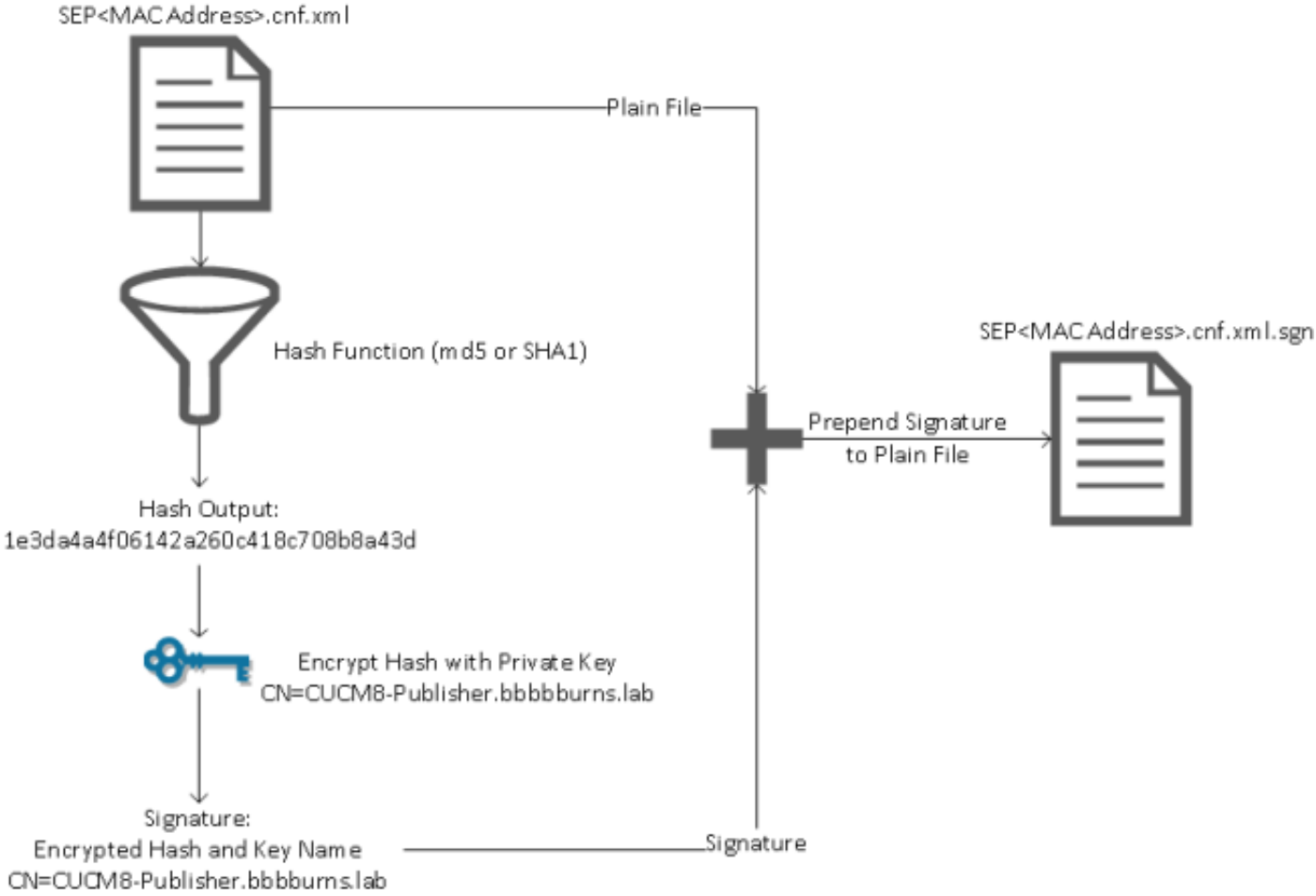
Das Telefon fordert **SEP*<MAC-Adresse>*.cnf.xml.sgn an**, um die Konfigurationsdatei mit der speziellen Signatur zu erhalten. Diese Konfigurationsdatei wird vom privaten TFTP-Schlüssel signiert, der auf der Seite für die Verwaltung des Verwaltungszertifikats des Betriebssystems (BS) CallManager.pem entspricht.



Die signierte Datei verfügt über eine Signatur am oberen Rand, um die Datei zu authentifizieren. Ansonsten ist sie im XML-Format mit einfachem Text enthalten. Das nachfolgende Bild zeigt, dass der Signator der Konfigurationsdatei **CN=CUCM8-Publisher.bbburns.lab** ist, das wiederum von **CN=JASBURNS-AD** signiert wird. Das bedeutet, dass das Telefon die Signatur von **CUCM8-Publisher.bbburns.lab** für die ITL-Datei überprüfen muss, bevor diese Konfigurationsdatei

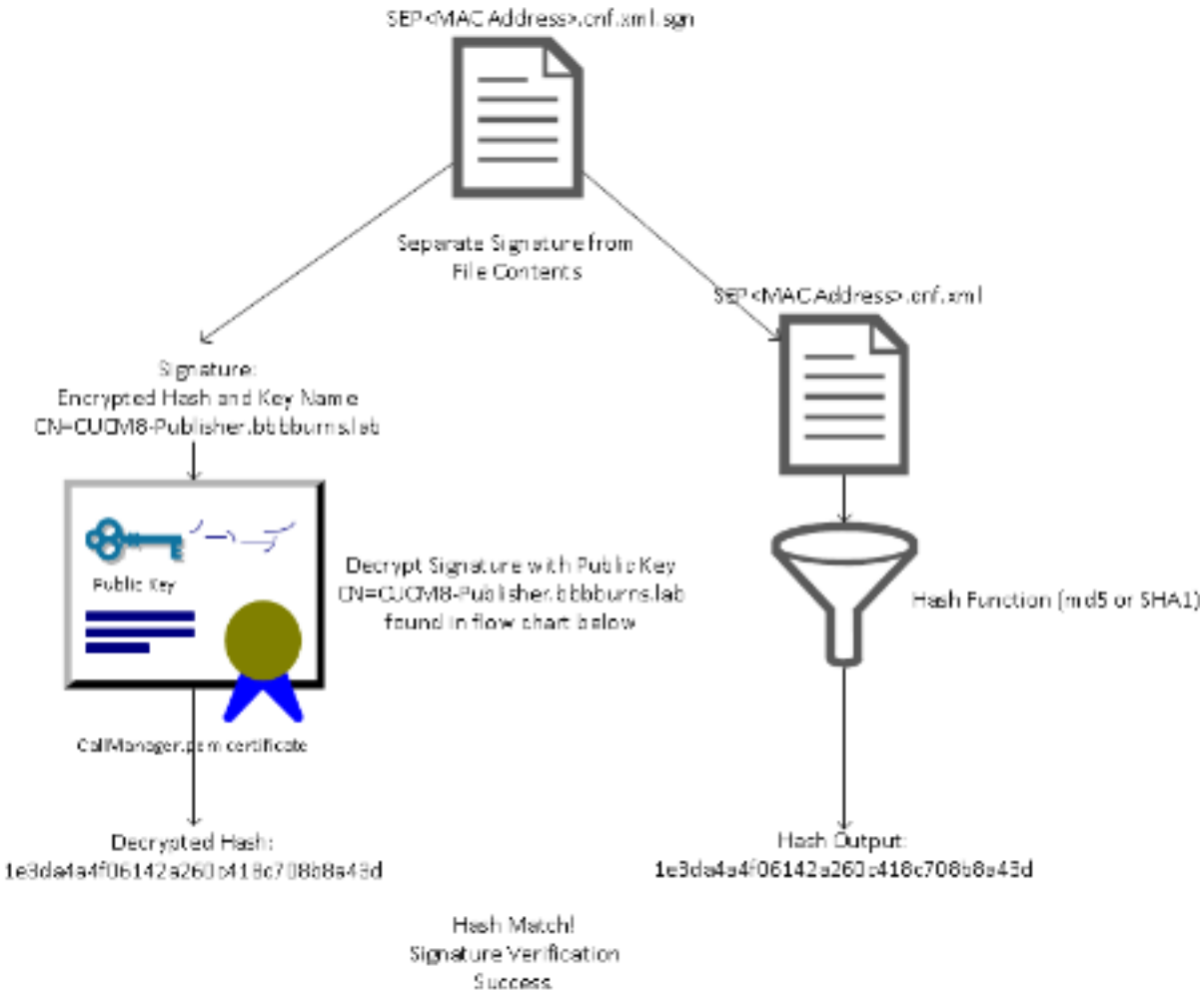
akzeptiert wird.

Das folgende Diagramm zeigt, wie der private Schlüssel zusammen mit einer Hash-Funktion Message Digest Algorithm (MD)5 oder Secure Hash Algorithm (SHA)1 verwendet wird, um die signierte Datei zu erstellen.



Bei der Signaturüberprüfung wird dieser Prozess mithilfe des öffentlichen Schlüssels umgekehrt, der zur Entschlüsselung des Hashs verwendet wird. Wenn die Hashes übereinstimmen, wird Folgendes angezeigt:

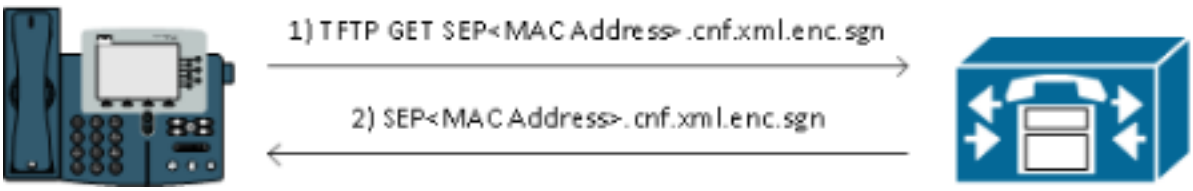
- Diese Datei wurde bei der Übertragung nicht geändert.
- Diese Datei stammt von der in der Signatur aufgeführten Partei, da alle erfolgreich mit dem öffentlichen Schlüssel entschlüsselten Dateien mit dem privaten Schlüssel verschlüsselt sein müssen.



Verschlüsselung der TFTP-Konfigurationsdatei

Wenn im verknüpften Telefonsicherheitsprofil die optionale TFTP-Konfigurationsverschlüsselung aktiviert ist, fordert das Telefon eine verschlüsselte Konfigurationsdatei an. Diese Datei wird mit dem privaten TFTP-Schlüssel signiert und mit einem symmetrischen Schlüssel verschlüsselt, der zwischen dem Telefon und dem CUCM ausgetauscht wird (vollständige Details finden Sie im Cisco Unified Communications Manager Security Guide, Release 8.5(1)), damit der Inhalt nicht mit einem Netzwerk-Sniffer gelesen werden kann, es sei denn, der Beobachter verfügt über die erforderlichen Schlüssel.

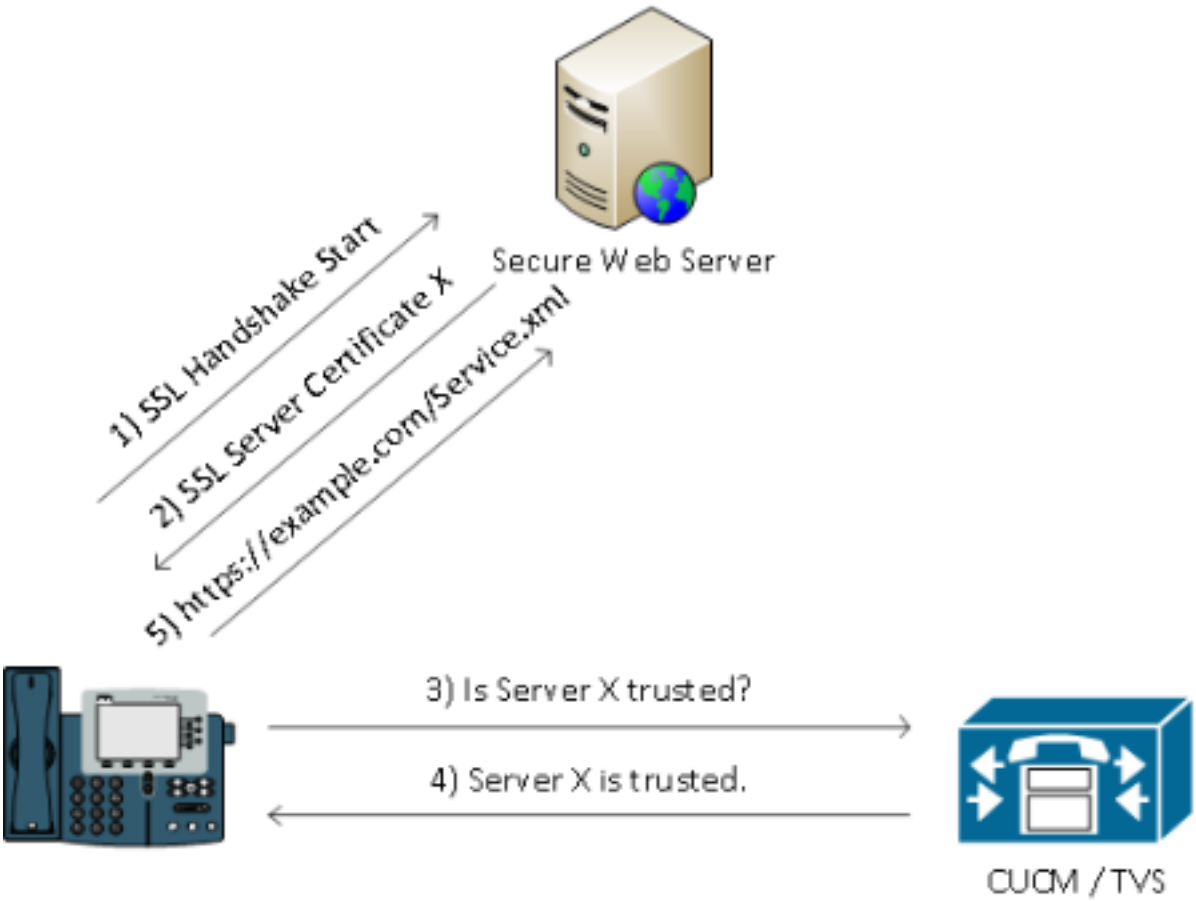
Das Telefon fordert **SEP*<MAC-Adresse>*.cnf.xml.enc.sgn an**, um die signierte verschlüsselte Datei abzurufen.



Die verschlüsselte Konfigurationsdatei hat auch die Signatur am Anfang, danach gibt es jedoch keine Klartextdaten, sondern nur verschlüsselte Daten (verschlüsselte Binärzeichen in diesem Texteditor). Das Bild zeigt, dass der Signierer mit dem im vorherigen Beispiel übereinstimmt. Daher muss dieser Signierer in der ITL-Datei vorhanden sein, bevor das Telefon die Datei akzeptiert. Außerdem müssen die Entschlüsselungsschlüssel korrekt sein, bevor das Telefon den Inhalt der Datei lesen kann.

Trust Verification Service (Fernüberprüfung von Zertifikaten und Signaturen)

IP-Telefone enthalten nur eine begrenzte Speicherkapazität, und in einem Netzwerk kann auch eine große Anzahl von Telefonen verwaltet werden. Der CUCM fungiert über den TVS als Remote-Vertrauensspeicher, sodass nicht auf jedem IP-Telefon ein vollständiger Zertifikats-Vertrauensspeicher platziert werden muss. Wenn das Telefon eine Signatur oder ein Zertifikat nicht über die CTL- oder ITL-Dateien verifizieren kann, fordert es den TVS-Server zur Überprüfung auf. Dieser zentrale Trust Store ist einfacher zu verwalten, als wenn der Trust Store auf allen IP-Telefonen vorhanden war.



SBD-Details und Informationen zur Fehlerbehebung

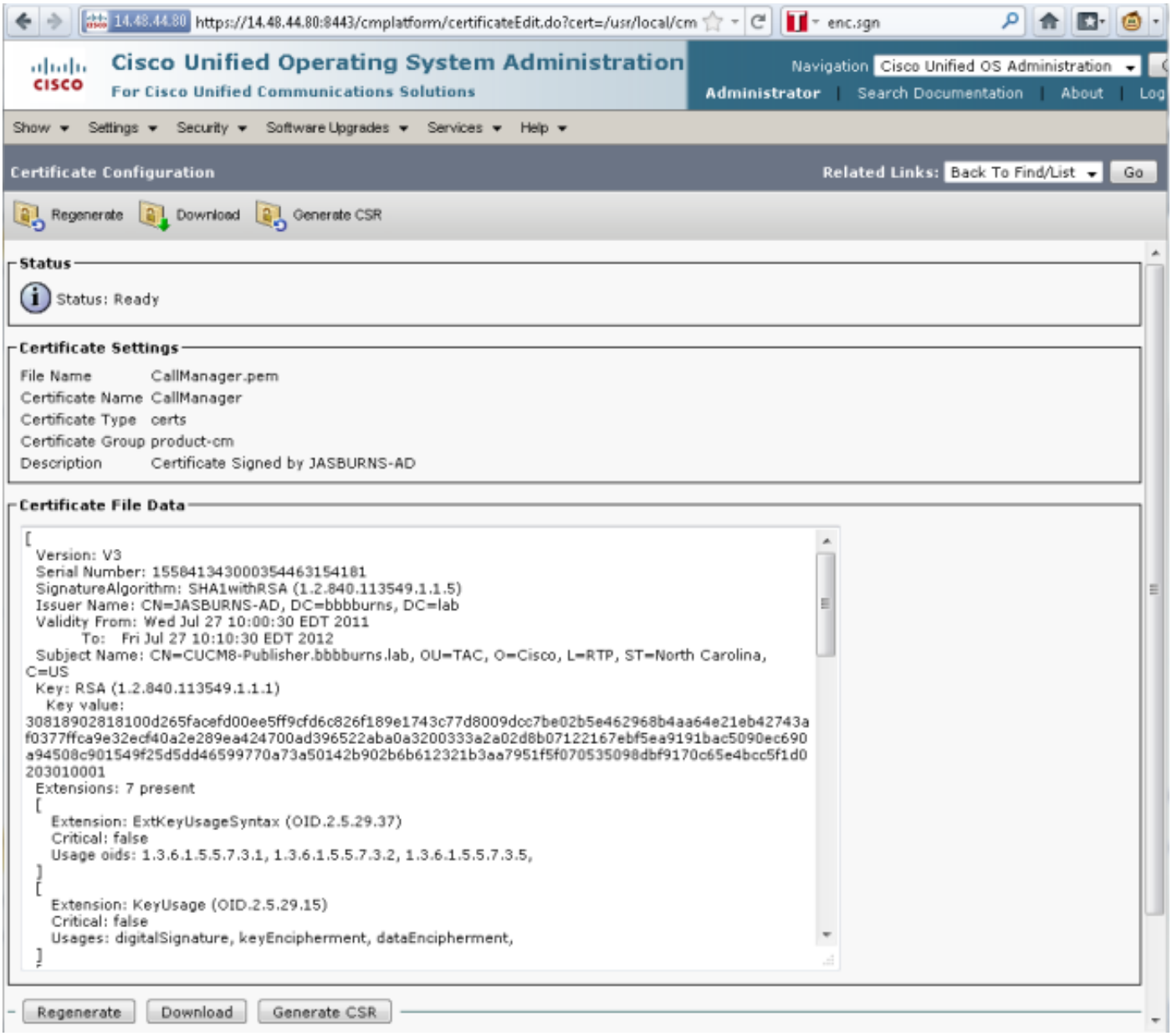
In diesem Abschnitt wird der SBD-Prozess beschrieben.

ITL-Dateien und Zertifikate auf CUCM vorhanden

Zunächst gibt es eine Reihe von Dateien, die auf dem CUCM-Server selbst vorhanden sein müssen. Das wichtigste Element ist das TFTP-Zertifikat und der private TFTP-Schlüssel. Das TFTP-Zertifikat befindet sich unter **OS Administration > Security > Certificate Management > CallManager.pem**.

Der CUCM-Server verwendet die privaten und öffentlichen Schlüssel des CallManager.pem-Zertifikats für den TFTP-Dienst (sowie für den Cisco Call Manager (CCM)-Dienst). Das Bild zeigt, dass das Zertifikat CallManager.pem an **CUCM8-publisher.bbburns.lab** ausgestellt und von **JASBURNS-AD** signiert wird. Alle TFTP-Konfigurationsdateien werden durch den privaten Schlüssel unten signiert.

Alle Telefone können den öffentlichen TFTP-Schlüssel im Zertifikat "CallManager.pem" verwenden, um alle mit dem privaten TFTP-Schlüssel verschlüsselten Dateien zu entschlüsseln und alle mit dem privaten TFTP-Schlüssel signierten Dateien zu überprüfen.



Neben dem privaten Schlüssel für das CallManager.pem-Zertifikat speichert der CUCM-Server auch eine ITL-Datei, die Telefonen angezeigt wird. Der Befehl **show itl** zeigt den vollständigen Inhalt dieser ITL-Datei über Secure Shell (SSH)-Zugriff auf die CUCM-Serverbetriebssystem-CLI.

In diesem Abschnitt wird die ITL-Datei Stück für Stück aufgeteilt, da sie eine Reihe wichtiger

Komponenten enthält, die das Telefon verwendet.

Der erste Teil sind die Signaturinformationen. Sogar die ITL-Datei ist eine signierte Datei. Diese Ausgabe zeigt, dass sie vom privaten TFTP-Schlüssel signiert wird, der dem vorherigen CallManager.pem-Zertifikat zugeordnet ist.

```
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*
```

Die nächsten Abschnitte enthalten jeweils ihren Zweck innerhalb eines speziellen **Function-**Parameters. Die erste Funktion ist das Sicherheitstoken für Systemadministratoren. Dies ist die Signatur des öffentlichen TFTP-Schlüssels.

```
        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.
```

Die nächste Funktion ist CCM+TFTP. Dies ist wiederum der öffentliche TFTP-Schlüssel, der zum Authentifizieren und Entschlüsseln der heruntergeladenen TFTP-Konfigurationsdateien dient.

```
        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:17:00:00:00:00:00:05
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)
```

Die nächste Funktion ist TVS. Es gibt einen Eintrag für den öffentlichen Schlüssel jedes TVS-Servers, mit dem das Telefon verbunden wird. Dadurch kann das Telefon eine SSL-Sitzung (Secure Sockets Layer) zum TVS-Server einrichten.

```
        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
```

Die letzte Funktion in der ITL-Datei ist die CAPF (Certificate Authority Proxy Function). Dieses Zertifikat ermöglicht es den Telefonen, eine sichere Verbindung zum CAPF-Dienst auf dem CUCM-Server herzustellen, sodass das Telefon ein LSC (Locally Significant Certificate) installieren oder aktualisieren kann. Dieser Prozess wird in einem anderen Dokument behandelt, das noch nicht veröffentlicht wird.

```
        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.
```

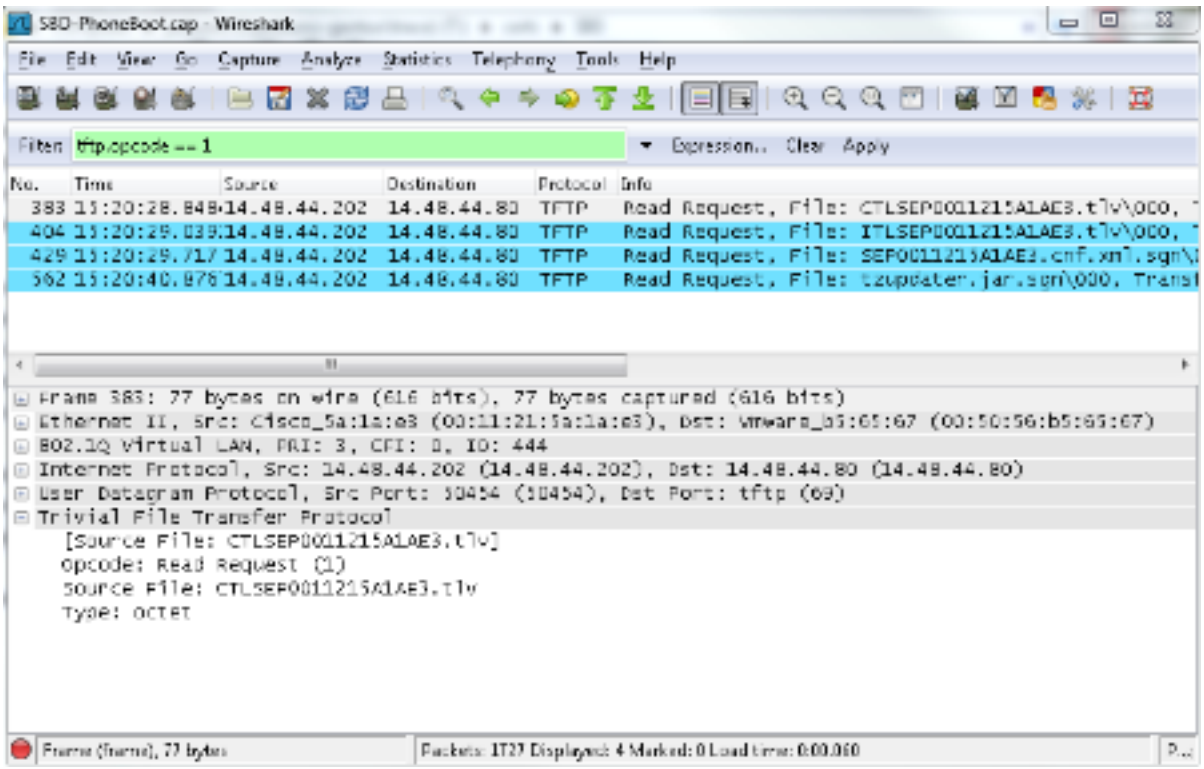
Im nächsten Abschnitt wird genau beschrieben, was beim Starten eines Telefons geschieht.

Telefon lädt ITL und Konfigurationsdatei herunter

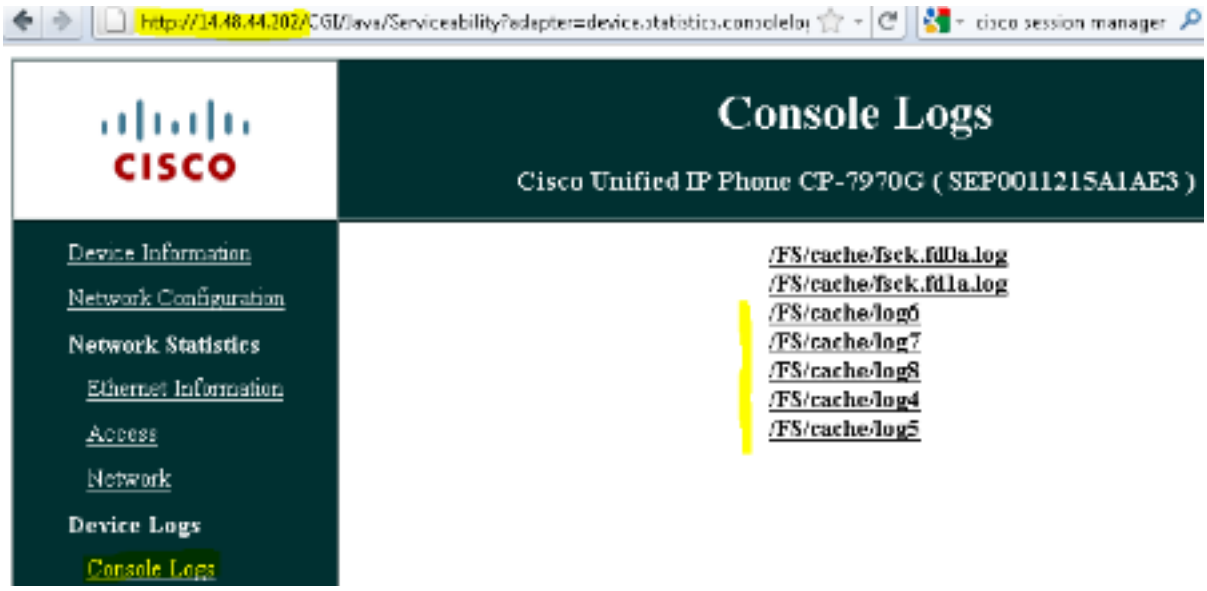
Nachdem das Telefon gestartet wurde und eine IP-Adresse sowie die Adresse eines TFTP-

Servers erhält, werden zuerst die CTL- und die ITL-Dateien angefordert.

Diese Paketerfassung zeigt eine Telefonanfrage für die ITL-Datei. Wenn Sie auf **tftp.opcode == 1** filtern, sehen Sie jede TFTP-Leseanforderung vom Telefon:



Da das Telefon CTL- und ITL-Dateien erfolgreich vom TFTP erhalten hat, fordert das Telefon eine signierte Konfigurationsdatei an. Die Telefonkonsolenprotokolle, die dieses Verhalten anzeigen, sind über die Webschnittstelle des Telefons verfügbar:



Zunächst fordert das Telefon eine CTL-Datei an, die erfolgreich ist:

```
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
```

Als Nächstes fordert das Telefon auch eine ITL-Datei an:

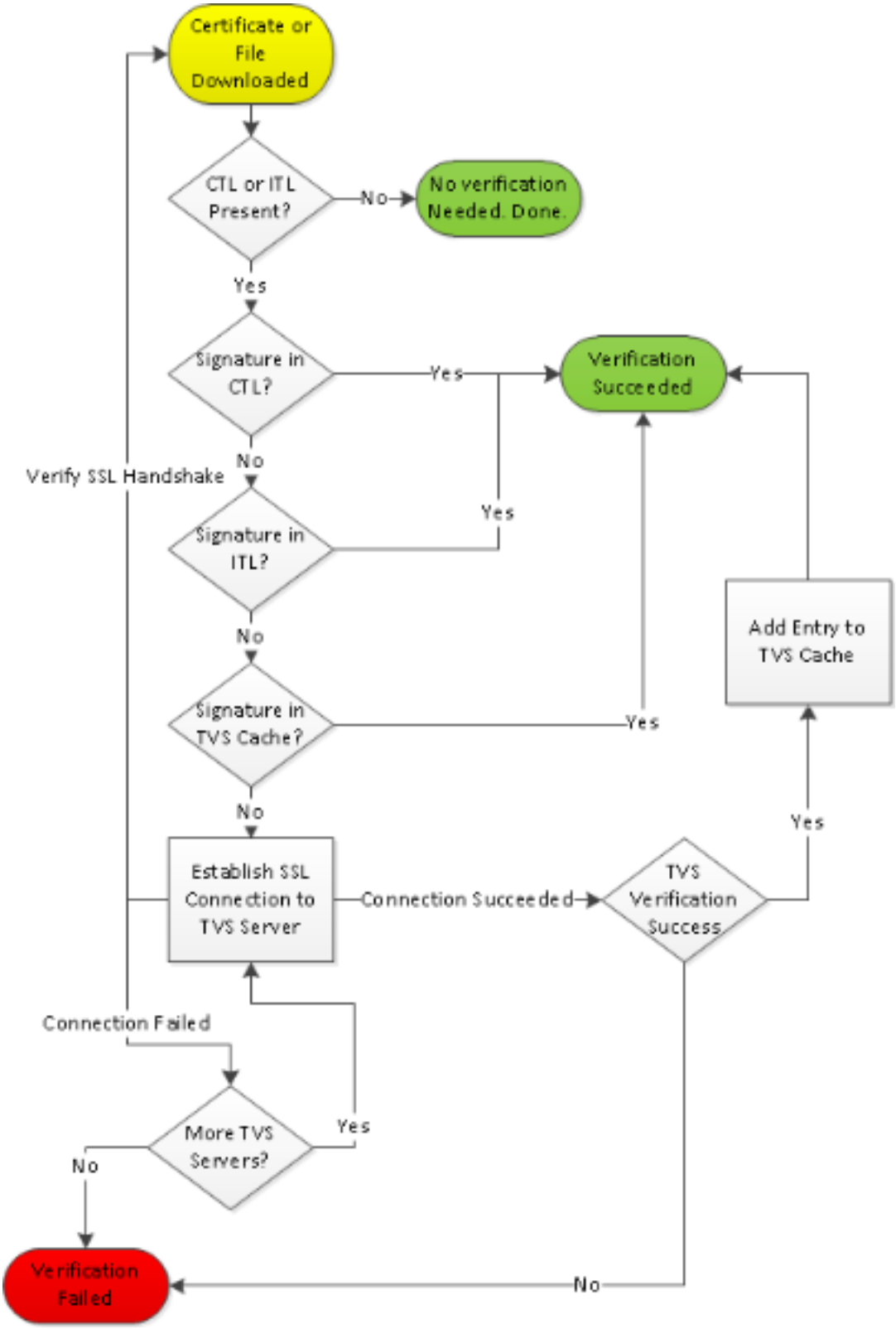
```
868: NOT 09:13:17.860613 TFTP: [28]:Requesting ITLSEP0011215A1AE3.tlv from
14.48.44.80
869: NOT 09:13:17.875059 TFTP: [28]:Finished --> rcvd 5438 bytes
```

Telefon prüft ITL und Konfigurationsdatei

Nachdem die ITL-Datei heruntergeladen wurde, muss sie verifiziert werden. Es gibt eine Reihe von Zuständen, in denen sich ein Telefon zu diesem Zeitpunkt befinden kann. Daher werden sie in diesem Dokument behandelt.

- Das Telefon verfügt über keine CTL- oder ITL-Datei, oder ITL ist leer, da der Parameter **Prepare Cluster for Rollback to Pre 8.0 (Cluster für die Vorbereitung für Rollback zu Pre 8.0)** vorhanden ist. In diesem Zustand vertraut das Telefon blind der nächsten heruntergeladenen CTL- oder ITL-Datei und verwendet diese Signatur.
- Das Telefon verfügt bereits über eine CTL, aber keine ITL. In diesem Zustand vertraut das Telefon einer ITL nur, wenn diese von der CCM+TFTP-Funktion in der CTL-Datei verifiziert werden kann.
- Das Telefon verfügt bereits über eine CTL- und eine ITL-Datei. In diesem Zustand prüft das Telefon, ob die kürzlich heruntergeladenen Dateien mit der Signatur im CTL-, ITL- oder TVS-Server übereinstimmen.

Das folgende Flussdiagramm beschreibt, wie das Telefon signierte Dateien und HTTPS-Zertifikate überprüft:



In diesem Fall kann das Telefon die Signatur in den ITL- und CTL-Dateien überprüfen. Das Telefon verfügt bereits über eine CTL und eine ITL, sodass es einfach gegen sie abgeglichen und die richtige Signatur gefunden wurde.

```
877: NOT 09:13:17.925249 SECD: validate_file_envelope:
File sign verify SUCCESS; header length <296>
```

Da das Telefon die CTL- und ITL-Dateien heruntergeladen hat, fordert es NUR signierte Konfigurationsdateien an. Dies veranschaulicht, dass die Logik des Telefons darin besteht, zu bestimmen, ob der TFTP-Server sicher ist, basierend auf CTL und ITL, und anschließend eine signierte Datei anzufordern:

```
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
```

Nachdem die signierte Konfigurationsdatei heruntergeladen wurde, muss das Telefon sie mithilfe der Funktion für CCM+TFTP in der ITL authentifizieren:

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

Telefon kontaktiert TVS für unbekanntes Zertifikat

Die ITL-Datei stellt eine TVS-Funktion bereit, die das Zertifikat des TVS-Dienstes enthält, der auf dem TCP-Port 2445 des CUCM-Servers ausgeführt wird. Der TVS wird auf allen Servern ausgeführt, auf denen der CallManager-Dienst aktiviert ist. Der CUCM-TFTP-Dienst verwendet die konfigurierte CallManager-Gruppe, um eine Liste der TVS-Server zu erstellen, die das Telefon in der Konfigurationsdatei für das Telefon kontaktieren soll.

In einigen Übungen wird nur ein CUCM-Server verwendet. In einem Multi-Node-CUCM-Cluster können bis zu drei TVS-Einträge für ein Telefon vorhanden sein, einer für jeden CUCM in der CUCM-Gruppe des Telefons.

Dieses Beispiel zeigt, was passiert, wenn die Taste **Directories** (Verzeichnisse) auf dem IP-Telefon gedrückt wird. Die Directories-URL ist für HTTPS konfiguriert, sodass dem Telefon das Tomcat-Webzertifikat vom Directories-Server angezeigt wird. Dieses Tomcat Webzertifikat (tomcat.pem in der OS Administration) ist nicht im Telefon geladen, daher muss das Telefon sich an TVS wenden, um das Zertifikat zu authentifizieren.

Eine Beschreibung der Interaktion finden Sie im vorherigen TVS-Übersichtsdiagramm. Die Protokollperspektive der Telefonkonsole ist wie folgt:

Zuerst finden Sie die Verzeichnis-URL:

```
1184: NOT 15:20:55.219275 JVM: Startup Module Loader|cip.dir.TandunDirectories:
? - Directory url https://14.48.44.80:8443/ccmcip/xmldirectory.jsp
```

Dies ist eine sichere SSL/Transport Layer Security (TLS)-HTTP-Sitzung, die überprüft werden muss.

```
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
```

Das Telefon überprüft zunächst, ob das vom SSL/TLS-Server präsentierte Zertifikat im CTL vorhanden ist. Anschließend überprüft das Telefon die Funktionen in der ITL-Datei, um festzustellen, ob eine Übereinstimmung gefunden wurde. In dieser Fehlermeldung steht "HTTPS-Zertifikat nicht im CTL", d. h. "dass Zertifizierungen nicht im CTL oder ITL gefunden werden können".

```
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>
```

Nachdem der direkte Inhalt der CTL- und ITL-Datei auf das Zertifikat überprüft wurde, wird als Nächstes der TVS-Cache überprüft. Dies geschieht, um den Netzwerkverkehr zu reduzieren, wenn das Telefon kürzlich den TVS-Server um dasselbe Zertifikat gebeten hat. Wenn das HTTPS-Zertifikat nicht im Telefon-Cache gefunden wird, können Sie eine TCP-Verbindung zum TVS-Server selbst herstellen.

```
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.
```

Denken Sie daran, dass die Verbindung zum TVS selbst SSL/TLS (sicheres HTTP oder HTTPS) ist. Daher ist es auch ein Zertifikat, das gegen die CTL zu ITL authentifiziert werden muss. Wenn alles korrekt funktioniert, sollte das TVS-Server-Zertifikat in der TVS-Funktion der ITL-Datei gefunden werden. Siehe ITL-Eintrag Nr. 3 im vorherigen Beispiel der ITL-Datei.

```
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>
```

Erfolg! Das Telefon verfügt jetzt über eine sichere Verbindung zum TVS-Server. Der nächste Schritt besteht darin, den TVS-Server zu fragen: "Hallo, vertraue ich diesem Verzeichnis-Serverzertifikat?"

Dieses Beispiel zeigt die Antwort auf diese Frage - eine Antwort von 0, was Erfolg bedeutet (kein Fehler).

```
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
```

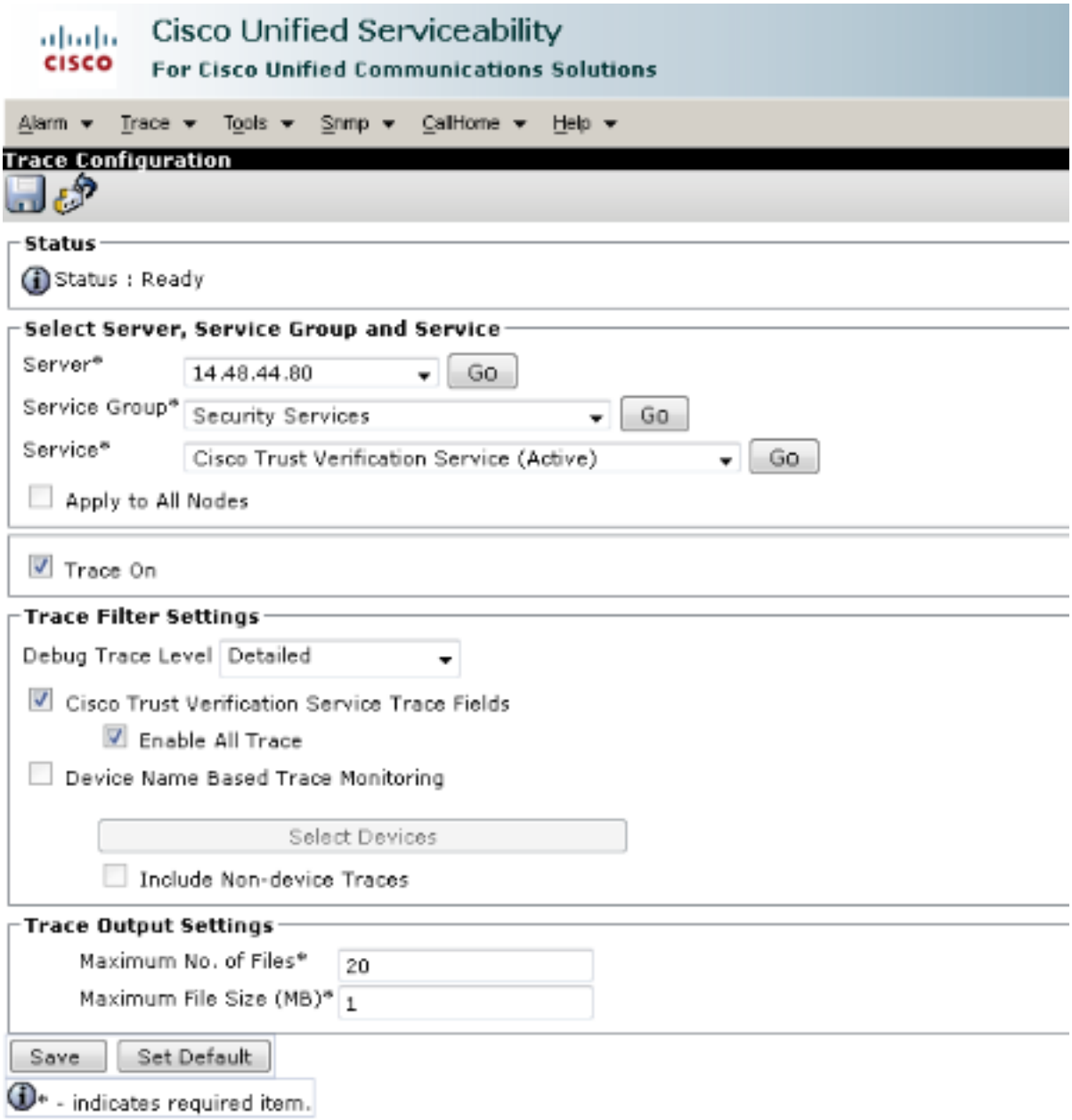
Da die TVS eine erfolgreiche Antwort gibt, werden die Ergebnisse für dieses Zertifikat im Cache gespeichert. Das bedeutet, dass Sie, wenn Sie innerhalb der nächsten 86.400 Sekunden die Schaltfläche **Verzeichnisse** erneut drücken, nicht den TVS-Server kontaktieren müssen, um das Zertifikat zu überprüfen. Sie können einfach auf den lokalen Cache zugreifen.

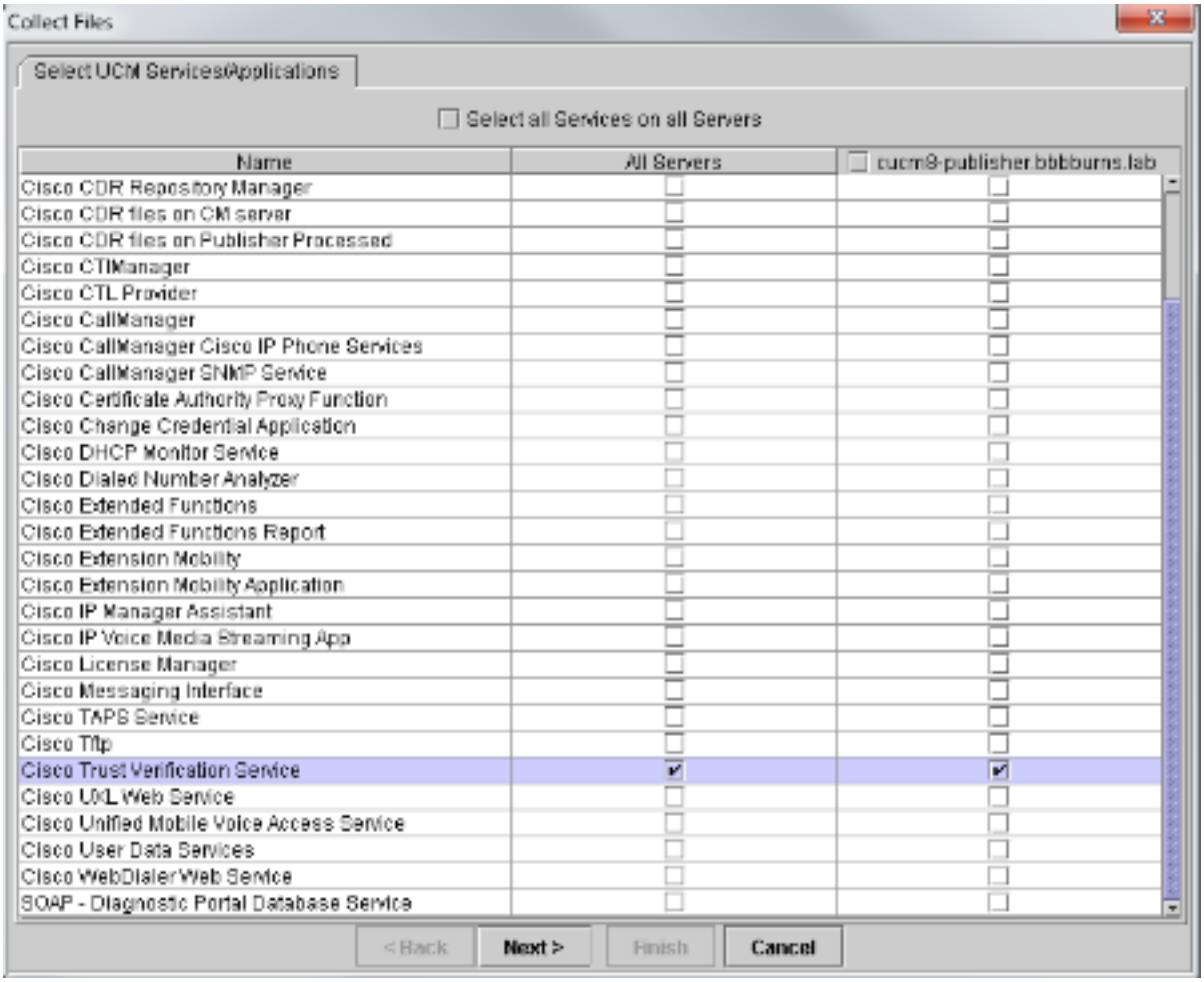
```
1279: NOT 15:20:59.837086 SECD: saveCertToTvsCache: Saving certificate
in TVS cache with default time-to-live value: 86400 seconds
1287: ERR 15:20:59.859993 SECD: Authenticated the HTTPS conn via TVS
```

Überprüfen Sie abschließend, ob die Verbindung zum Directories-Server erfolgreich war.

```
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
```

Hier ein Beispiel dafür, was auf dem CUCM-Server passiert, auf dem TVS ausgeführt wird. Sie können TVS-Protokolle mit dem Cisco Unified Real-Time Monitoring Tool (RTMT) sammeln.


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.



Die CUCM-TVS-Protokolle zeigen an, dass Sie SSL-Handshake mit dem Telefon, das Telefon fragt TVS über das Tomcat-Zertifikat, dann TVS antwortet, um anzugeben, dass das Zertifikat im TVS-Zertifikatsspeicher zugeordnet ist.

```
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
```

Der TVS-Zertifikatsspeicher ist eine Liste aller Zertifikate, die auf der Webseite **OS Administration > Certificate Management** enthalten sind.

Überprüfen Sie manuell, ob das Telefon-ITL mit dem CUCM ITL übereinstimmt.

Ein häufiges Missverständnis bei der Fehlerbehebung betrifft die Neigung zum Löschen der ITL-Datei, in der Hoffnung, dass dadurch ein Problem bei der Dateiverifizierung behoben wird. Manchmal ist das Löschen von ITL-Dateien erforderlich, aber es gibt möglicherweise eine bessere Möglichkeit.

Die ITL-Datei muss nur gelöscht werden, wenn ALL diese Bedingungen erfüllt sind.

- Die Signatur der ITL-Datei auf dem Telefon stimmt nicht mit der Signatur der ITL-Datei auf dem CM-TFTP-Server überein.
- Die TVS-Signatur in der ITL-Datei stimmt nicht mit dem TVS-Zertifikat überein.
- Das Telefon zeigt "Verification Failed" (Überprüfung fehlgeschlagen) an, wenn versucht wird, die ITL-Datei oder die Konfigurationsdateien herunterzuladen.
- Es ist keine Sicherung des alten privaten TFTP-Schlüssels vorhanden.

Hier sehen Sie, wie Sie die ersten beiden dieser Bedingungen überprüfen.

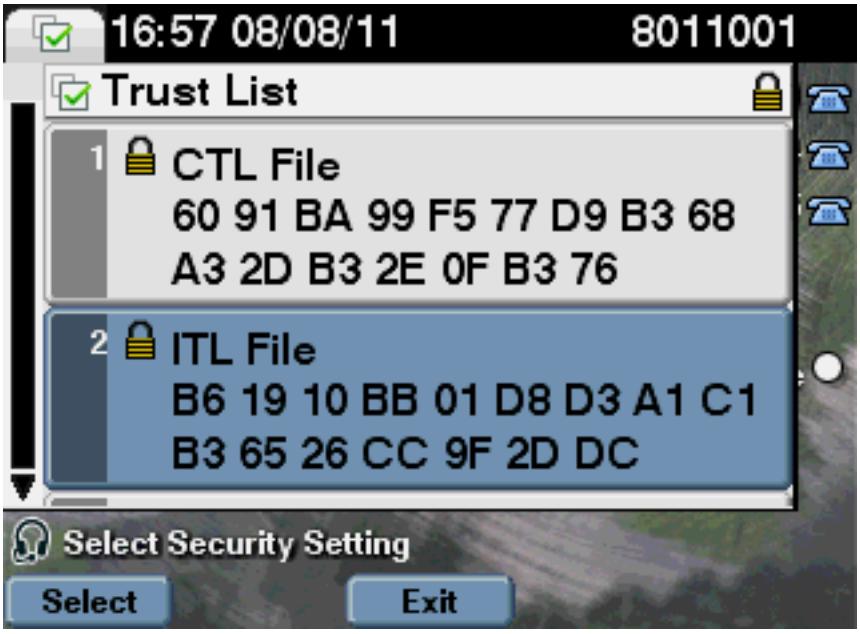
Zunächst können Sie die Prüfsumme der auf dem CUCM vorhandenen ITL-Datei mit der Prüfsumme der ITL-Datei des Telefons vergleichen. Es gibt derzeit keine Möglichkeit, die MD5sum-Datei der ITL-Datei auf dem CUCM selbst anzuzeigen, bevor Sie eine Version mit der Behebung für diese Cisco Bug-ID CSCto60209 ausführen.

Führen Sie diesen Vorgang in der Zwischenzeit mit Ihren bevorzugten GUI- oder CLI-Programmen aus:

```
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
```

Dies zeigt, dass die MD5-Summe der ITL-Datei in CUCM **b61910bb01d8d3a1c1b36526cc9f2ddc** ist.

Jetzt können Sie das Telefon selbst betrachten, um den Hash der dort geladenen ITL-Datei zu ermitteln: **Einstellungen > Sicherheitskonfiguration > Vertrauensliste**.

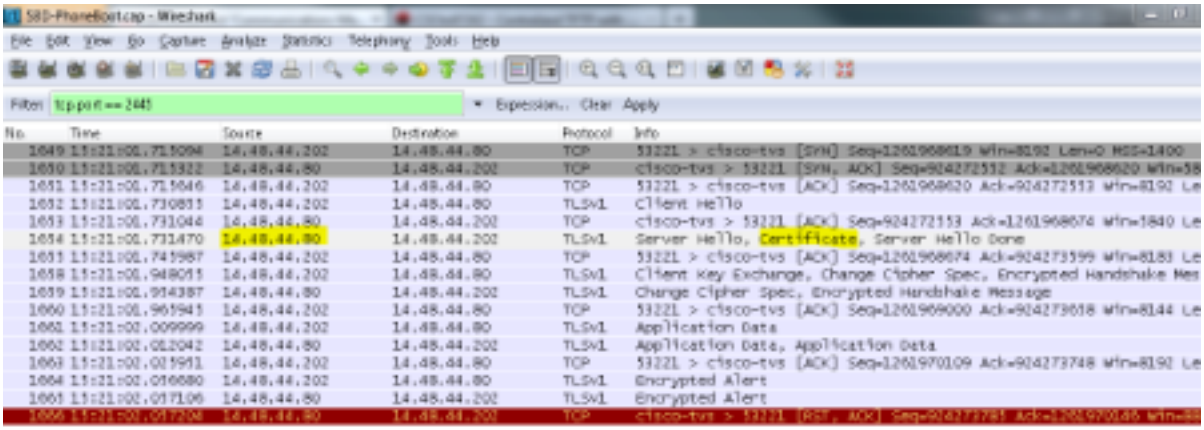


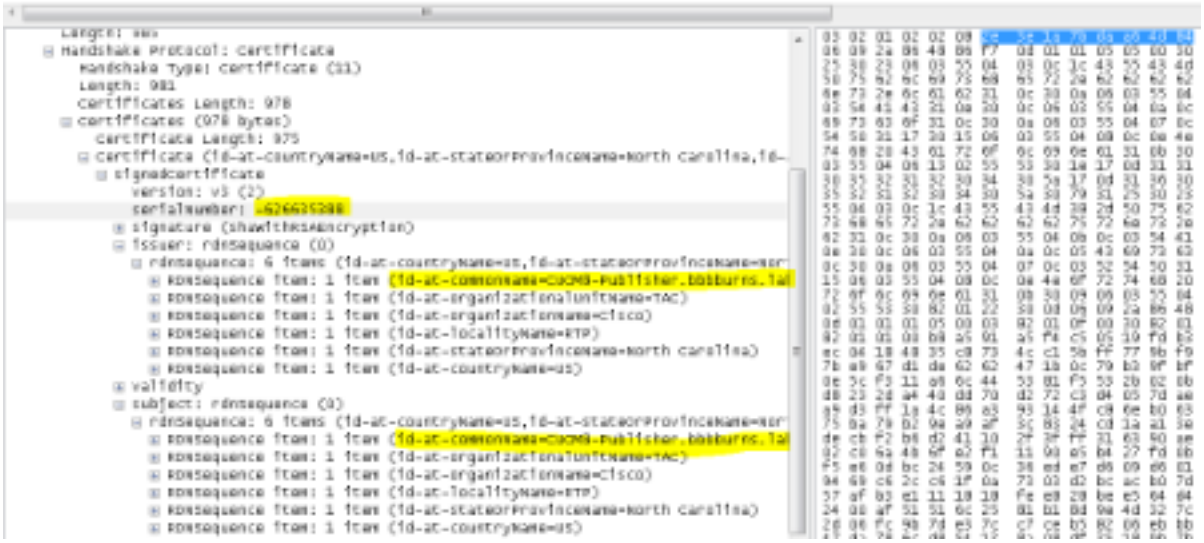
Dies zeigt, dass die MD5-Summen übereinstimmen. Dies bedeutet, dass die ITL-Datei auf dem Telefon mit der Datei auf dem CUCM übereinstimmt, sodass sie nicht gelöscht werden muss.

Wenn der TON übereinstimmt, müssen Sie mit dem nächsten Vorgang fortfahren. Bestimmen Sie, ob das TVS-Zertifikat in der ITL mit dem TVS-Zertifikat übereinstimmt. Diese Operation ist etwas stärker involviert.

Betrachten Sie zunächst die Paketerfassung des Telefons, das mit dem TVS-Server an TCP-Port 2445 verbunden ist.

Klicken Sie mit der rechten Maustaste auf ein beliebiges Paket in diesem Stream in Wireshark, klicken Sie auf **Decode As**, und wählen Sie **SSL**. Suchen Sie das Serverzertifikat, das wie folgt aussieht:





Sehen Sie sich das TVS-Zertifikat an, das in der vorherigen ITL-Datei enthalten ist. Sie sollten einen Eintrag mit der Seriennummer **2E3E1A7BDAA64D84** sehen.

```
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
```

Erfolg: Die **TVS.pem-Datei** in der ITL-Datei entspricht dem im Netzwerk angezeigten TVS-Zertifikat. Sie müssen die ITL nicht löschen, und TVS stellt das richtige Zertifikat bereit.

Wenn die Dateiauthentifizierung immer noch fehlschlägt, überprüfen Sie den Rest des vorherigen Flussdiagramms.

Einschränkungen und Interaktionen

Regenerieren von Zertifikaten/Neuerstellen eines Clusters/Ablauf von Zertifikaten

Das wichtigste Zertifikat ist jetzt das CallManager.pem-Zertifikat. Der private Schlüssel dieses Zertifikats wird zum Signieren aller TFTP-Konfigurationsdateien verwendet, die die ITL-Datei enthalten.

Wenn die Datei CallManager.pem neu generiert wird, wird ein neues CCM+TFTP-Zertifikat mit einem neuen privaten Schlüssel generiert. Außerdem wird die ITL-Datei jetzt mit diesem neuen CCM+TFTP-Schlüssel signiert.

Nachdem Sie CallManager.pem neu generiert und den TVS- und TFTP-Dienst neu gestartet haben, geschieht dies beim Starten eines Telefons.

1. Das Telefon versucht, die vom neuen CCM+TFTP signierte neue ITL-Datei vom TFTP-Server herunterzuladen. Das Telefon hat zu diesem Zeitpunkt nur die alte ITL-Datei, und die neuen Tasten befinden sich nicht in der ITL-Datei, die auf dem Telefon vorhanden ist.
2. Da das Telefon die neue CCM+TFTP-Signatur im alten ITL nicht finden konnte, versucht es, den TVS-Dienst zu kontaktieren.
   Hinweis: Dieser Teil ist äußerst wichtig. Das TVS-Zertifikat aus der alten ITL-Datei muss immer noch übereinstimmen. Wenn sowohl CallManager.pem als auch TVS.pem zur gleichen Zeit regeneriert werden, können die Telefone keine neuen Dateien herunterladen, ohne die ITL manuell vom Telefon zu löschen.
3. Wenn das Telefon das TVS kontaktiert, verfügt der CUCM-Server, der das TVS ausführt, über das neue CallManager.pem-Zertifikat im BS-Zertifikatsspeicher.
4. Der TVS-Server kehrt zum Erfolg zurück, und das Telefon lädt die neue ITL-Datei in den Speicher.
5. Das Telefon versucht nun, eine Konfigurationsdatei herunterzuladen, die vom neuen CallManager.pem-Schlüssel signiert wurde.
6. Nachdem die neue ITL geladen wurde, wird die neu signierte Konfigurationsdatei erfolgreich vom ITL im Speicher überprüft.

Wichtigste Punkte:

- Generieren Sie niemals gleichzeitig die Zertifikate CallManager.pem und TVS.pem neu.
- Wenn entweder TVS.pem oder CallManager.pem regeneriert wird, sollten TVS und TFTP neu gestartet und die Telefone zurückgesetzt werden, um die neuen ITL-Dateien abzurufen. Neuere Versionen von CUCM behandeln dieses Telefon automatisch zurück und warnen den Benutzer bei der Zertifikatwiederherstellung.
- Wenn mehr als ein TVS-Server vorhanden ist (mehr als ein Server in der CallManager-Gruppe), können die zusätzlichen Server das neue CallManager.pem-Zertifikat authentifizieren.

Verschieben von Telefonen zwischen Clustern

Wenn Sie Telefone von einem Cluster zu einem anderen mit vorhandenen ITLs verschieben, müssen der ITL und der private TFTP-Schlüssel berücksichtigt werden. Jede neue Konfigurationsdatei, die dem Telefon präsentiert wird, MUSS mit einer Signatur in CTL, ITL oder einer Signatur im aktuellen TVS-Dienst des Telefons übereinstimmen.

In diesem Dokument wird erläutert, wie Sie sicherstellen können, dass die ITL-Datei und die Konfigurationsdateien des neuen Clusters von der aktuellen ITL-Datei des Telefons vertrauenswürdig sind. https://supportforums.cisco.com/docs/DOC-15799.

Backup und Wiederherstellung

Das CallManager.pem-Zertifikat und der private Schlüssel werden über das Disaster Recovery System (DRS) gesichert. Wenn ein TFTP-Server neu erstellt wird, MUSS er aus dem Backup wiederhergestellt werden, damit der private Schlüssel wiederhergestellt werden kann. Ohne den privaten Schlüssel CallManager.pem auf dem Server vertrauen Telefone mit aktuellen ITLs, die den alten Schlüssel verwenden, signierten Konfigurationsdateien nicht.

Wenn ein Cluster neu erstellt und nicht aus dem Backup wiederhergestellt wird, entspricht dies genau dem Dokument "Verschieben von Telefonen zwischen Clustern". Dies liegt daran, dass ein Cluster mit einem neuen Schlüssel in Bezug auf die Telefone ein anderes Cluster ist.

Backup und Wiederherstellung sind mit einem schwerwiegenden Fehler verbunden. Wenn ein Cluster anfällig für die Cisco Bug-ID CSCtn50405 ist, enthalten die DRS-Sicherungen nicht das CallManager.pem-Zertifikat. Dadurch generiert jeder von dieser Sicherung wiederhergestellte Server beschädigte ITL-Dateien, bis eine neue CallManager.pem-Datei generiert wird. Wenn es keine anderen funktionierenden TFTP-Server gibt, die den Sicherungs- und Wiederherstellungsvorgang nicht durchlaufen haben, kann dies bedeuten, dass alle ITL-Dateien von den Telefonen gelöscht werden müssen.

Um zu überprüfen, ob Ihre CallManager.pem-Datei regeneriert werden muss, geben Sie den Befehl **show itl** gefolgt von:

```
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
```

In der ITL-Ausgabe sind folgende Schlüsselfehler zu suchen:

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

und

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

Die vorherige SQL-Abfrage (Structured Query Language) sucht nach Zertifikaten, die die Rolle "Authentifizierung und Autorisierung" haben. Das CallManager.pem-Zertifikat in der vorherigen Datenbankabfrage, das die Rolle Authentifizierung und Autorisierung besitzt, sollte auch auf der Webseite für das Zertifikatsmanagement der Betriebssystemverwaltung vorhanden sein. Wenn der vorherige Fehler auftritt, gibt es eine Diskrepanz zwischen den CallManager.pem-Zertifikaten

in der Abfrage und auf der Webseite des Betriebssystems.

Ändern von Hostnamen oder Domänennamen

Wenn Sie den Hostnamen oder den Domänennamen eines CUCM-Servers ändern, werden alle Zertifikate gleichzeitig auf diesem Server neu generiert. Im Abschnitt zur Zertifikatswiederherstellung wurde erklärt, dass die Regeneration von TVS.pem und CallManager.pem "schlecht" ist.

Es gibt einige Szenarien, in denen eine Änderung des Hostnamens fehlschlägt und einige, in denen sie problemlos funktioniert. In diesem Abschnitt werden alle Themen behandelt, und sie werden wieder mit dem verknüpft, was Sie in diesem Dokument bereits über TVS und ITL wissen.

Single-Node-Cluster nur mit ITL (Vorsicht verwenden, dies bricht ohne Vorbereitung ab)

- Bei einer Bereitstellung auf einem Server der Business Edition oder einer Bereitstellung, die ausschließlich auf Publisher beschränkt ist, werden sowohl CallManager.pem als auch TVS.pem bei der Änderung von Hostnamen neu generiert.
- Wenn der Hostname in einem einzelnen Knoten-Cluster geändert wird, ohne zuerst den hier behandelten Rollback Enterprise-Parameter zu verwenden, können die Telefone die neue ITL-Datei oder die neuen Konfigurationsdateien nicht mit der aktuellen ITL-Datei abgleichen. Darüber hinaus können sie keine Verbindung zum TVS herstellen, da das TVS-Zertifikat ebenfalls nicht mehr vertrauenswürdig ist.
- Die Telefone zeigen den Fehler "Überprüfung der Vertrauenslisten fehlgeschlagen" an, es treten keine neuen Konfigurationsänderungen auf, und die sicheren Service-URLs schlagen fehl.
- Wenn die Vorsichtsmaßnahme in Schritt 2 nicht zuerst getroffen wird, ist es die einzige Lösung, die ITL von jedem Telefon manuell zu löschen.

Single-Node-Cluster mit CTL und ITL (dies kann vorübergehend unterbrochen, aber leicht repariert werden)

- Führen Sie nach dem Umbenennen der Server den CTL-Client erneut aus. Dadurch wird das neue CallManager.pem-Zertifikat in die CTL-Datei eingefügt, die vom Telefon heruntergeladen wird.
- Neue Konfigurationsdateien, einschließlich der neuen ITL-Dateien, können anhand der CCM+TFTP-Funktion in der CTL-Datei als vertrauenswürdig eingestuft werden.
- Dies funktioniert, weil die aktualisierte CTL-Datei auf der Grundlage eines privaten USB-eToken-Schlüssels vertrauenswürdig ist, der identisch ist.

Multi-Node-Cluster nur mit ITL (dies funktioniert in der Regel, kann aber dauerhaft unterbrochen werden, wenn es hastig geschieht)

- Da ein Multi-Node-Cluster über mehrere TVS-Server verfügt, können die Zertifikate jedes einzelnen Servers problemlos regeneriert werden. Wenn dem Telefon diese neue, unbekannte Signatur angezeigt wird, fordert es einen anderen TVS-Server auf, das neue Serverzertifikat zu überprüfen.
- Es gibt zwei Hauptprobleme, die zu einem Ausfall führen können:
  Wenn alle Server gleichzeitig umbenannt und neu gestartet werden, ist bei der Wiederherstellung der Server und Telefone kein TVS-Server mit bekannten Zertifikaten

erreichbar.Wenn ein Telefon nur einen Server in der CallManager-Gruppe hat, machen die zusätzlichen TVS-Server keinen Unterschied. Um dies zu beheben, sehen Sie sich das Szenario "Single Node Cluster" an, oder fügen Sie der CallManager-Gruppe des Telefons einen weiteren Server hinzu.

Multi-Node-Cluster mit CTL und ITL (dies kann nicht dauerhaft unterbrochen werden)

- Nachdem Sie die Umbenennungen durchlaufen haben, authentifiziert der TVS-Dienst die neuen Zertifikate.
- Auch wenn alle TVS-Server aus irgendeinem Grund nicht verfügbar sind, kann der CTL-Client weiterhin verwendet werden, um die Telefone mit den neuen CallManager.pem CCM+TFTP-Zertifikaten zu aktualisieren.

Zentrales TFTP

Wenn ein Telefon mit ITL bootet, werden folgende Dateien angefordert: **CTLSEP*<MAC-Adresse>*.tlv**, **ITLSEP*<MAC-Adresse>*.tlv** und **SEP*<MAC-Adresse>.cnf.xml.sgn.***

Wenn das Telefon diese Dateien nicht finden kann, fordert es **ITLFile.tlv** und **CTLFile.tlv an**, die ein zentralisierter TFTP-Server für jedes Telefon bereitstellt, das sie anfordert.

Bei zentralisiertem TFTP gibt es ein einzelnes TFTP-Cluster, das auf eine Reihe anderer untergeordneter Cluster zeigt. Häufig ist dies der Fall, weil Telefone in mehreren CUCM-Clustern denselben DHCP-Bereich verwenden und daher denselben DHCP-Option 150 TFTP-Server verwenden müssen. Alle IP-Telefone verweisen auf den zentralen TFTP-Cluster, selbst wenn sie sich bei anderen Clustern registrieren. Dieser zentrale TFTP-Server fragt die Remote-TFTP-Server ab, wenn er eine Anfrage für eine Datei empfängt, die er nicht finden kann.

Dadurch funktioniert das zentralisierte TFTP nur in einer homogenen ITL-Umgebung. Auf allen Servern muss CUCM Version 8.x oder höher ausgeführt werden, oder alle Server müssen Versionen vor Version 8.x ausführen.

Wenn vom zentralen TFTP-Server eine ITLFile.tlv-Datei angezeigt wird, vertrauen die Telefone keine Dateien vom Remote-TFTP-Server, da die Signaturen nicht übereinstimmen. Dies geschieht in einer heterogenen Mischung. In einer homogenen Mischung fordert das Telefon **ITLSEP*<MAC>*.tlv an**, das aus dem korrekten Remote-Cluster gezogen wird.

In einer heterogenen Umgebung mit einer Mischung aus Pre-Version 8.x- und Version 8.x-Clustern muss "Prepare Cluster for Rollback to Pre 8.0" im Cluster Version 8.x aktiviert werden, wie unter Cisco Bug ID CSCto87262 und den "Secured Phone URL Parameters" beschrieben, die mit HTTP anstelle von HTTPS konfiguriert sind. Dadurch werden die ITL-Funktionen des Telefons praktisch deaktiviert.

Häufig gestellte Fragen

Kann ich die SBD ausschalten?

Sie können SBD nur deaktivieren, wenn SBD und ITL derzeit arbeiten.

Die SBD kann auf Telefonen mit dem Prepare Cluster for Rollback to pre 8.0" Enterprise Parameter vorübergehend deaktiviert werden und indem die "Secured Phone URL Parameters" (Sicherere Telefon-URL-Parameter) mit HTTP anstelle von HTTPS konfiguriert werden. Wenn Sie den Rollback-Parameter festlegen, wird eine signierte ITL-Datei mit leeren Funktionseinträgen erstellt. Die "leere" ITL-Datei ist noch signiert, daher muss sich der Cluster in einem voll funktionsfähigen Sicherheitszustand befinden, bevor dieser Parameter aktiviert werden kann.

Nachdem dieser Parameter aktiviert und die neue ITL-Datei mit leeren Einträgen heruntergeladen und verifiziert wurde, akzeptieren die Telefone jede Konfigurationsdatei, unabhängig davon, wer sie unterzeichnet hat.

Es wird nicht empfohlen, den Cluster in diesem Zustand zu belassen, da keine der drei zuvor erwähnten Funktionen (authentifizierte Konfigurationsdateien, verschlüsselte Konfigurationsdateien und HTTPS-URLs) verfügbar ist.

Kann ich die ITL-Datei problemlos von allen Telefonen löschen, wenn CallManager.pem verloren geht?

Es gibt derzeit keine Möglichkeit, alle ITLs von einem von Cisco remote bereitgestellten Telefon zu löschen. Deshalb sind die in diesem Dokument beschriebenen Verfahren und Wechselwirkungen so wichtig zu berücksichtigen.

Derzeit gibt es eine noch nicht aufgelöste Erweiterung der Cisco Bug-ID CSCto47052, die diese Funktionalität anfordert, aber noch nicht implementiert wurde.

In der Zwischenzeit wurde über Cisco Bug ID CSCts01319 eine neue Funktion hinzugefügt, die es dem Cisco Technical Assistance Center (TAC) ermöglichen könnte, auf die zuvor vertrauenswürdige ITL zurückzukehren, wenn diese noch auf dem Server verfügbar ist. Dies funktioniert nur in bestimmten Fällen, in denen sich der Cluster auf einer Version befindet, die diesen Fehler beheben kann, und in denen die vorherige ITL in einer Sicherung existiert, die an einem bestimmten Speicherort auf dem Server gespeichert ist. Sehen Sie sich den Fehler an, um zu sehen, ob Ihre Version die Behebung aufweist. Wenden Sie sich an das Cisco TAC, um das im Fehler beschriebene potenzielle Wiederherstellungsverfahren zu durchlaufen.

Wenn die vorherige Prozedur nicht verfügbar ist, müssen die Telefontasten manuell auf dem Telefon gedrückt werden, um die ITL-Datei zu löschen. Dies ist der Kompromiss zwischen Sicherheit und einfacher Administration. Damit die ITL-Datei wirklich sicher ist, darf sie nicht einfach per Fernzugriff entfernt werden.

Selbst bei Skripttastenbetätigungen mit SOAP-XML-Objekten (Simple Object Access Protocol) kann die ITL nicht remote entfernt werden. Der Grund hierfür ist, dass der TVS-Zugriff (und damit der URL-Zugriff für die sichere Authentifizierung zur Validierung eingehender Druckobjekte der SOAP-XML-Schaltfläche) an diesem Punkt nicht funktioniert. Wenn die Authentifizierungs-URL nicht als sicher konfiguriert ist, kann es möglich sein, die Tasteneingaben zu schreiben, um eine ITL zu löschen. Dieses Skript ist jedoch nicht bei Cisco verfügbar.

Andere Methoden zur Skripterstellung für Tasteneingaben an Remote-Standorten ohne Verwendung der Authentifizierungs-URL sind möglicherweise von einem Drittanbieter verfügbar, werden jedoch von Cisco nicht bereitgestellt.

Die am häufigsten verwendete Methode zum Löschen der ITL ist eine E-Mail-Übertragung an alle

Telefonbenutzer, die sie über die Tastenfolge informieren. Wenn der Zugriff auf die Einstellungen auf **Eingeschränkt** oder **Deaktiviert** eingestellt ist, muss das Telefon auf die Werkseinstellungen zurückgesetzt werden, da die Benutzer nicht auf das Menü Einstellungen des Telefons zugreifen können.