CUCM Security By Default(CUCM 보안 기본) 및 ITL Operation(ITL 운영) 및 Troubleshooting(문제 해결) 이해

목차

소개

이 문서에서는 CUCM(Cisco Unified Communications Manager) 버전 8.0 이상의 SBD(Security By Default) 기능에 대해 설명합니다.

배경 정보

CUCM 버전 8.0 이상에서는 ITL(Identity Trust List) 파일과 TVS(Trust Verification Service)로 구성된 SBD 기능이 도입되었습니다.

이제 모든 CUCM 클러스터는 ITL 기반 보안을 자동으로 사용합니다. 관리자가 버전 8.0 CUCM 클러스터를 특정 변경 사항으로 변경하기 전에 반드시 숙지해야 하는 보안과 사용 편의성/관리 편의

성의 상충점이 있습니다.

이 문서는 공식 Security By Default 문서를 보완하는 역할을 하며, 관리자가 문제 해결 프로세스를 쉽게 수행할 수 있도록 운영 정보 및 문제 해결 팁을 제공합니다.

SBD의 핵심 개념인 비대칭 키 암호 Wikipedia 문서와 공용 키 인프라 Wikipedia 문서를 숙지하는 것이 좋습니다.

SBD 개요

이 섹션에서는 SBD가 제공하는 기능을 간략하게 살펴봅니다. 각 기능에 대한 전체 기술 세부 정보는 SBD Detail and Troubleshooting Information(SBD 세부 정보 및 문제 해결 정보) 섹션을 참조하십시오.

SBD는 지원되는 IP 전화에 대해 다음 세 가지 기능을 제공합니다.

- 서명 키를 사용하는 TFTP 다운로드 파일(컨피그레이션, 로캘, 벨소리 목록)의 기본 인증
- 서명 키를 사용하는 TFTP 컨피그레이션 파일의 선택적 암호화
- CUCM(TVS)의 원격 인증서 신뢰 저장소를 사용하는 전화에서 시작된 HTTPS 연결에 대한 인증서 확인

이 문서에서는 이러한 각 기능에 대한 개요를 제공합니다.

TFTP 다운로드 인증

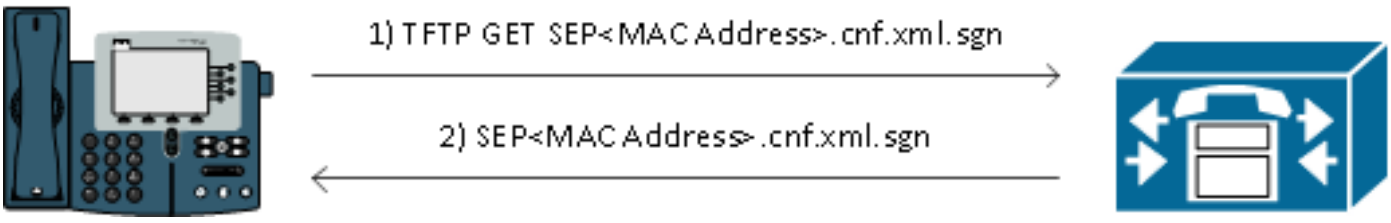
CTL(Certificate Trust List) 또는 ITL 파일이 있는 경우 IP Phone은 CUCM TFTP 서버에서 서명된 TFTP 컨피그레이션 파일을 요청합니다.

이 파일을 사용하면 전화기에서 컨피그레이션 파일이 신뢰할 수 있는 소스에서 왔는지를 확인할 수 있습니다. 전화기에 CTL/ITL 파일이 있는 경우, 컨피그레이션 파일은 신뢰할 수 있는 TFTP 서버에서 서명해야 합니다.

파일은 전송되는 동안 네트워크에 일반 텍스트이지만 특수 확인 서명이 함께 제공됩니다.

전화기에서 특수 서명이 있는 컨피그레이션 파일을 수신하기 위해 SEP<MAC Address>.cnf.xml.sgn을 요청합니다.

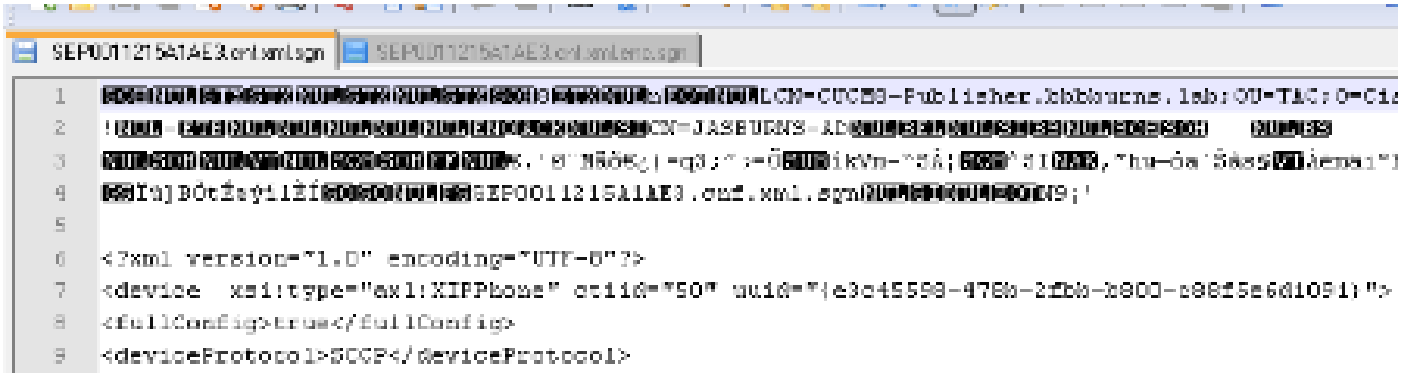
이 구성 파일은 OS(운영 체제) 관리 인증서 관리 페이지에서 CallManager.pem에 해당하는 TFTP 개인 키로 서명됩니다.



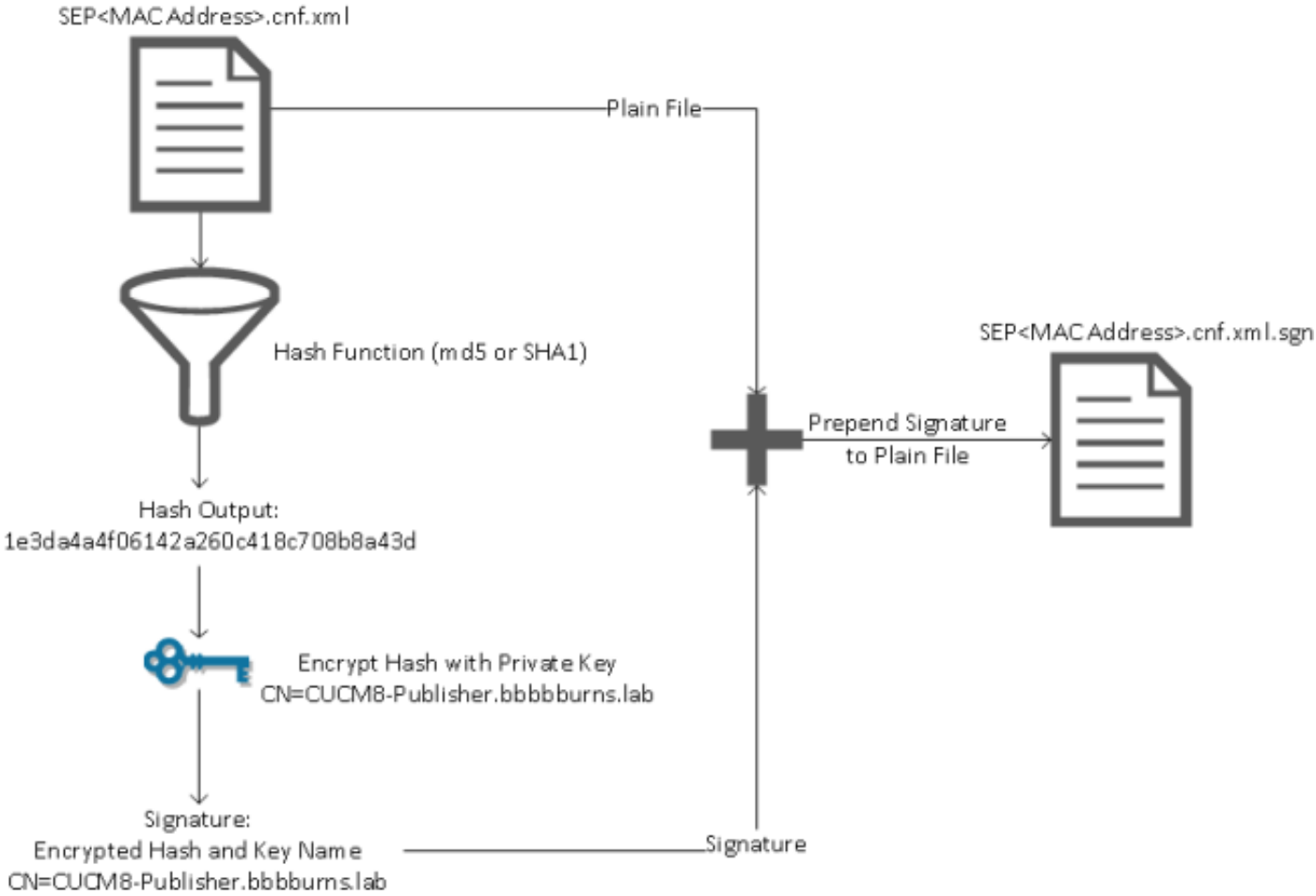
서명된 파일은 파일을 인증하기 위해 맨 위에 서명이 있지만, 그 외의 경우에는 일반 텍스트 XML로 되어 있습니다.

아래 그림에서는 컨피그레이션 파일의 서명자가 CN=CUCM8-Publisher.bbbburns.lab이며, 이는 CN=JASBURNS-AD에 의해 서명됩니다.

즉, 전화기에서 이 컨피그레이션 파일이 수락되기 전에 ITL 파일에 대해 CUCM8-Publisher.bbbburns.lab의 서명을 확인해야 합니다.



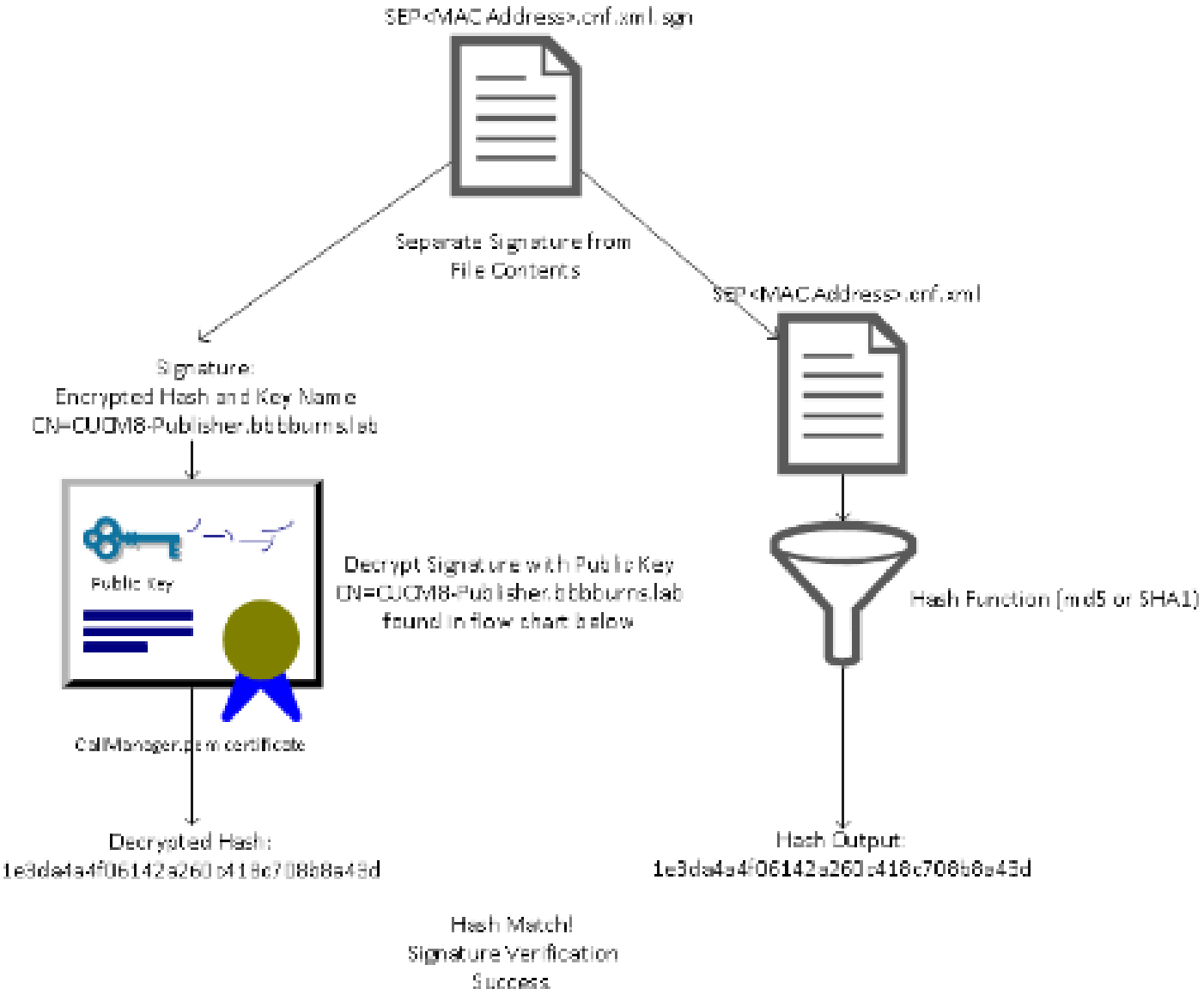
다음은 서명된 파일을 생성하기 위해 개인 키를 MD(Message Digest Algorithm) 5 또는 SHA(Secure Hash Algorithm) 1 해시 함수와 함께 사용하는 방법을 보여 주는 다이어그램입니다.



서명 확인은 해시를 해독하기 위해 일치하는 공개 키를 사용하여 이 프로세스를 되돌립니다. 해시가 일치하면 다음과 같이 표시됩니다.

- 이 파일은 전송 중에 수정되지 않았습니다.
- 이 파일은 서명에 나열된 파티에서 가져온 것입니다. 공개 키로 성공적으로 해독된 모든 파일

은 개인 키로 암호화되어 있어야 합니다.



TFTP 컨피그레이션 파일 암호화

연결된 Phone Security Profile(전화기 보안 프로파일)에서 선택적인 TFTP 컨피그레이션 암호화가 활성화된 경우 전화기는 암호화된 컨피그레이션 파일을 요청합니다.

이 파일은 TFTP 개인 키로 서명되고 전화기와 CUCM 간에 교환되는 대칭 키로 암호화됩니다(자세한 내용은 Cisco Unified Communications Manager 보안 가이드, 릴리스 8.5(1) 참조).

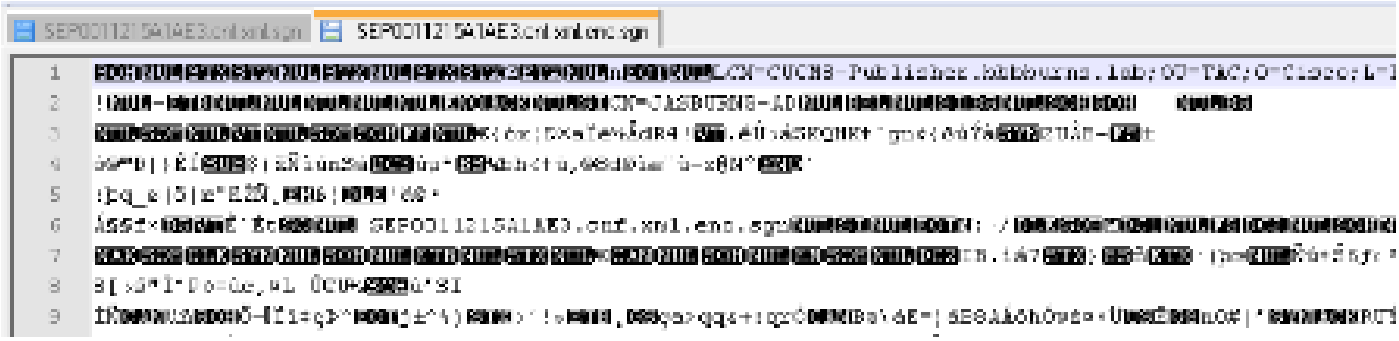
관찰자에게 필요한 키가 없으면 네트워크 스니퍼로 내용을 읽을 수 없습니다.

전화기에서 서명된 암호화 파일을 가져오기 위해 SEP<MAC Address>.cnf.xml.enc.sgn을 요청합니다.

암호화된 컨피그레이션 파일의 시작 부분에도 서명이 있지만 그 이후에는 일반 텍스트 데이터가 없고 암호화된 데이터(이 텍스트 편집기에서 왜곡된 이진 문자)만 있습니다.

이 그림에서는 서명자가 이전 예와 같으므로 전화기에서 파일을 승인하기 전에 이 서명자가 ITL 파일에 있어야 합니다.

또한 전화기에서 파일의 내용을 읽으려면 암호 해독 키가 정확해야 합니다.



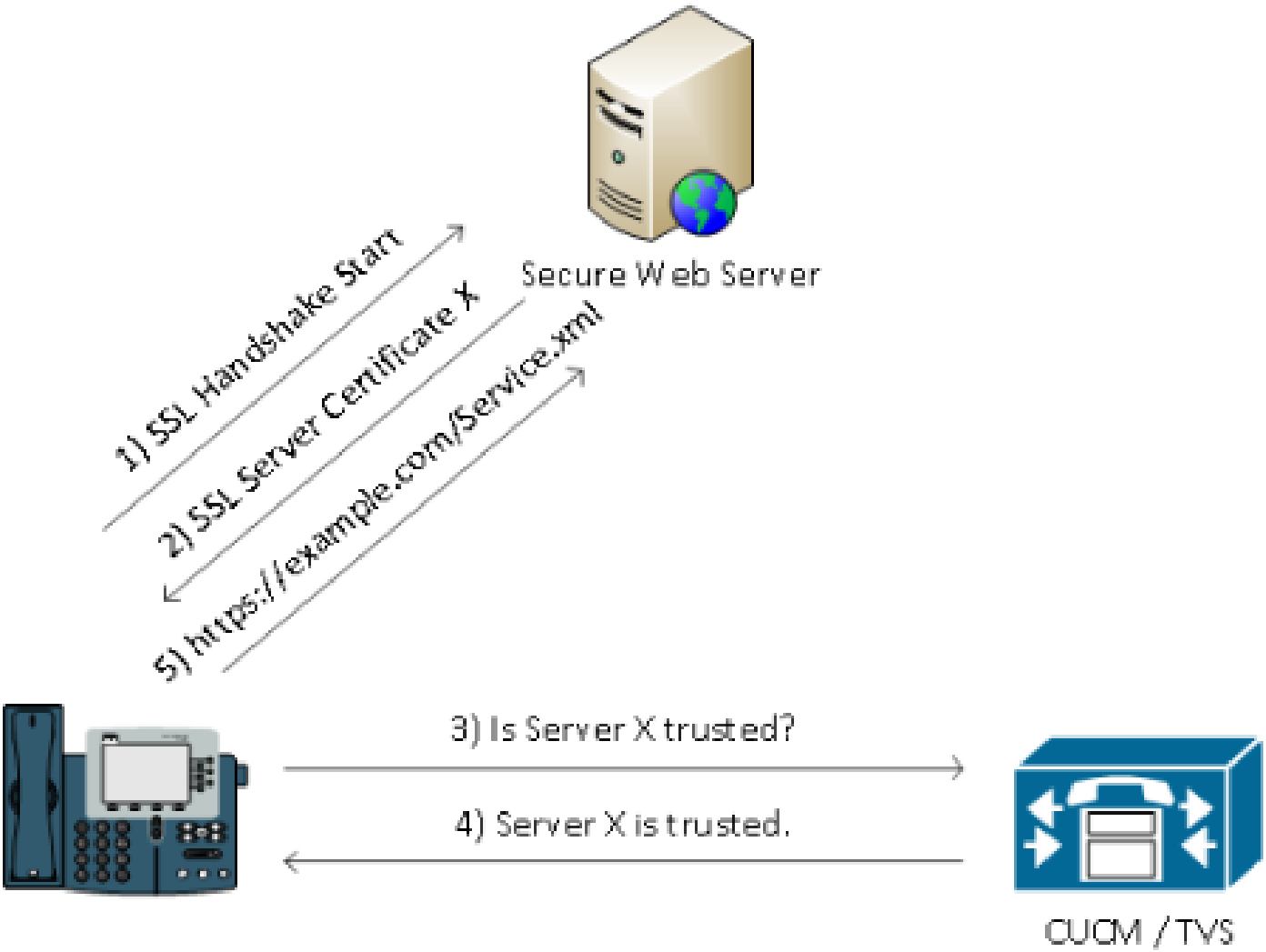
Trust Verification Service(원격 인증서 및 서명 확인)

IP 전화에는 제한된 양의 메모리가 포함되며, 네트워크에서 관리할 전화기의 수도 많습니다.

CUCM은 TVS를 통해 원격 신뢰 저장소 역할을 하므로 전체 인증서 신뢰 저장소를 각 IP 전화기에 둘 필요가 없습니다.

CTL 또는 ITL 파일을 통해 서명이나 인증서를 확인할 수 없는 경우 전화기는 TVS 서버에 확인을 요청합니다.

이 중앙 트러스트 저장소는 트러스트 저장소가 모든 IP 전화기에 있는 경우보다 관리하기 쉽습니다.



SBD 세부 정보 및 문제 해결 정보

이 섹션에서는 SBD 프로세스에 대해 자세히 설명합니다.

CUCM에 있는 ITL 파일 및 인증서

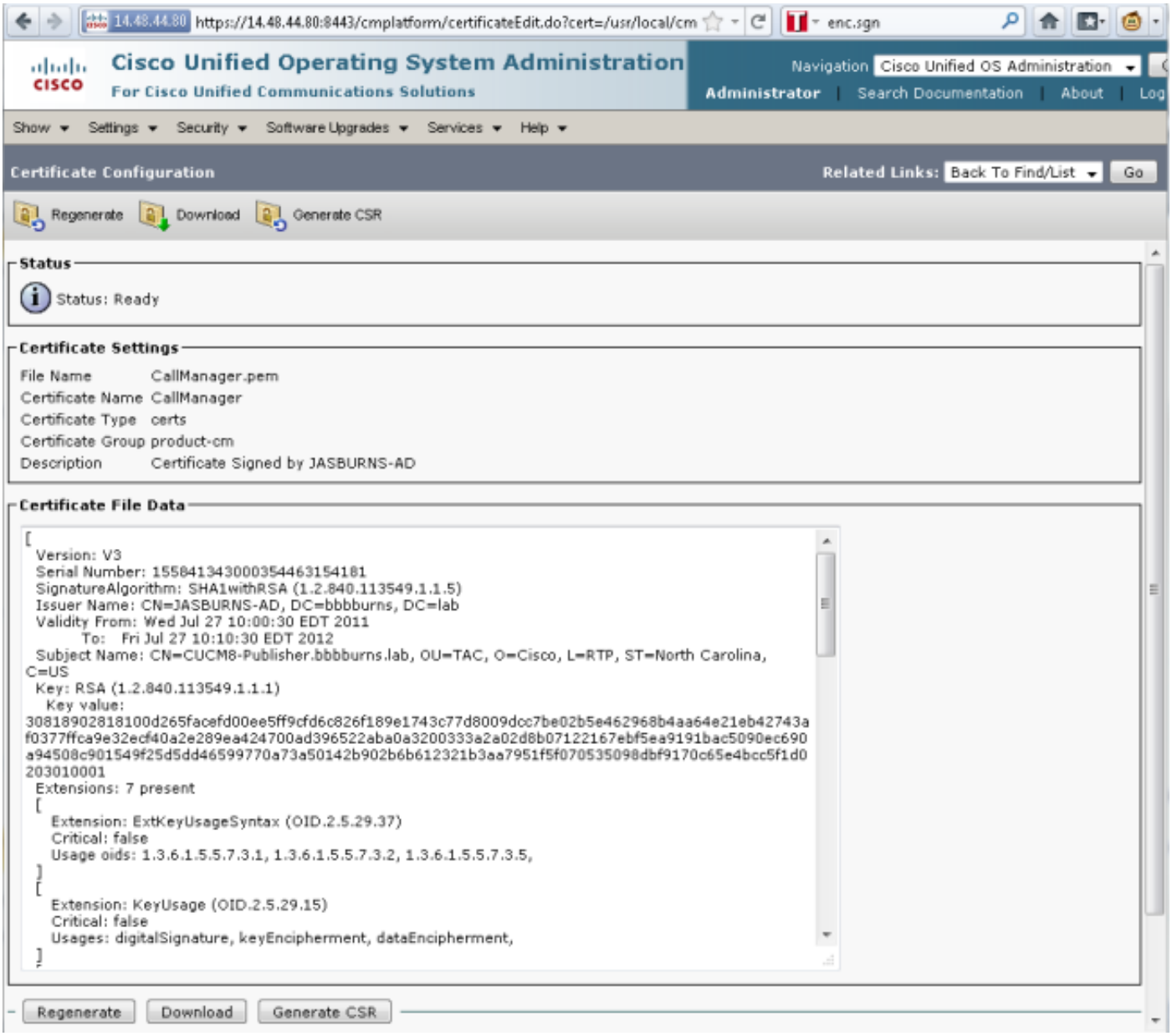
먼저, CUCM 서버 자체에 있어야 하는 많은 파일이 있습니다. 가장 중요한 부분은 TFTP 인증서와 TFTP 개인 키입니다.

TFTP 인증서는 OS Administration(OS 관리) > Security(보안) > Certificate Management(인증서 관리) > CallManager.pem 아래에 있습니다.

CUCM 서버는 TFTP 서비스(및 CCM(Cisco Call Manager) 서비스)를 위해 CallManager.pem 인증서 전용 및 공용 키를 사용합니다.

이 그림에서는 CallManager.pem 인증서가 CUCM8-publisher.bbbburns.lab에 발급되고 JASBURNS-AD에 의해 서명된 것을 보여줍니다. 모든 TFTP 컨피그레이션 파일은 아래의 개인 키로 서명됩니다.

모든 전화기는 CallManager.pem 인증서의 TFTP 공개 키를 사용하여 TFTP 개인 키로 암호화된 파일을 해독할 수 있으며 TFTP 개인 키로 서명된 파일을 확인할 수 있습니다.



CUCM 서버는 CallManager.pem 인증서 개인 키 외에도 전화기에 제공되는 ITL 파일을 저장합니다 .

show itl 명령은 CUCM 서버 OS CLI에 대한 SSH(Secure Shell) 액세스를 통해 이 ITL 파일의 전체 내용을 표시합니다.

전화기에서 사용하는 여러 가지 중요한 구성 요소가 있으므로 이 섹션에서는 ITL 파일을 하나씩 분류합니다.

첫 번째 부분은 서명 정보입니다. ITL 파일도 서명된 파일입니다. 이 출력은 이전 CallManager.pem 인증서와 연결된 TFTP 개인 키에 의해 서명되었음을 보여줍니다.

<#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*
```

다음 섹션에는 각각 특수 Function 매개 변수 내부에 해당 용도가 포함되어 있습니다. 첫 번째 기능은 시스템 관리자 보안 토큰입니다. TFTP 공개 키의 서명입니다.

```
        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.
```

다음 기능은 CCM+TFTP입니다. 이는 다운로드한 TFTP 컨피그레이션 파일을 인증하고 해독하는 역할을 하는 TFTP 공개 키이기도 합니다.

```
        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)
```

다음 기능은 TV입니다. 전화기가 연결되는 각 TVS 서버의 공개 키에 대한 항목이 있습니다.

이렇게 하면 전화기가 TVS 서버에 대한 SSL(Secure Sockets Layer) 세션을 설정할 수 있습니다.

```
        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
```

ITL 파일에 포함된 최종 기능은 CAPF(Certificate Authority Proxy Function)입니다.

이 인증서를 사용하면 전화기가 LSC(Locally Significant Certificate)를 설치하거나 업데이트할 수 있도록 CUCM 서버의 CAPF 서비스에 대한 보안 연결을 설정할 수 있습니다.

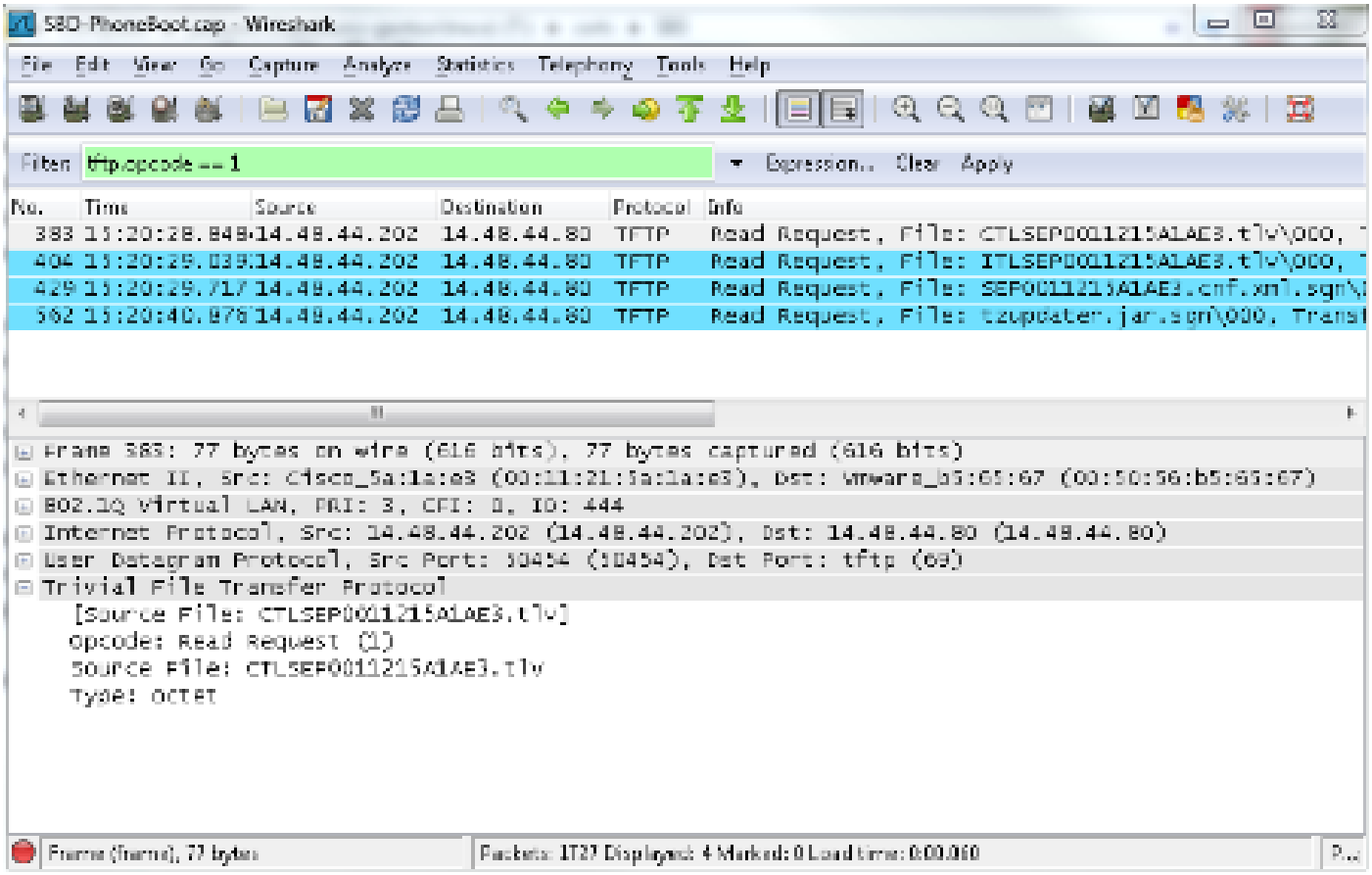
```
        ITL Record #:4
                  ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       455
2       DNSNAME         2
3       SUBJECTNAME     61      CN=CAPF-9c4cba7d;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
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.
```

다음 섹션에서는 전화기가 부팅될 때 정확히 어떤 일이 발생하는지 설명합니다.

전화기에서 ITL 및 컨피그레이션 파일 다운로드

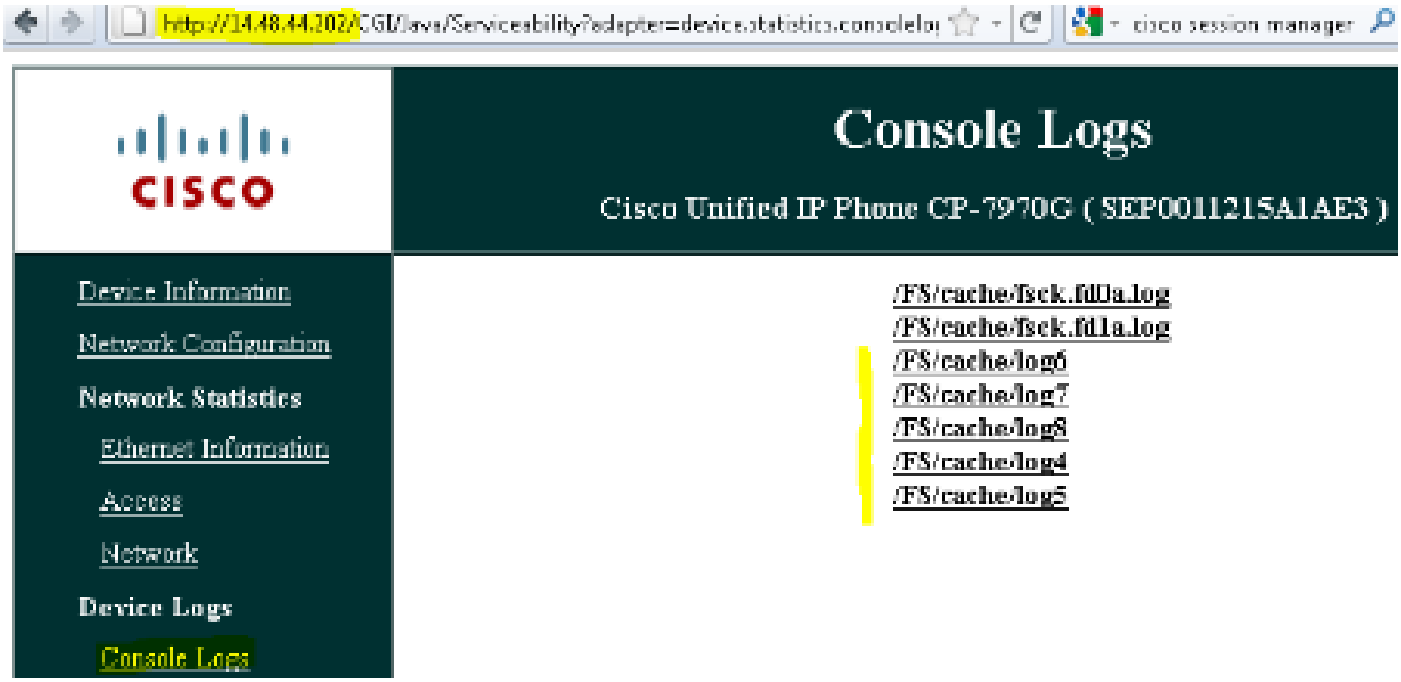
전화기가 부팅되고 TFTP 서버의 주소와 IP 주소를 얻은 후 먼저 CTL 및 ITL 파일을 요청합니다.

이 패킷 캡처는 ITL 파일에 대한 전화 요청을 표시합니다. tftp.opcode == 1에서 필터링하면 전화기에서 모든 TFTP 읽기 요청이 표시됩니다.



전화기가 TFTP에서 CTL 및 ITL 파일을 성공적으로 받았으므로 서명된 컨피그레이션 파일을 요청합니다.

이 동작을 보여주는 전화기 콘솔 로그는 전화기 웹 인터페이스에서 사용할 수 있습니다.



먼저 전화기에서 CTL 파일을 요청하면 다음 작업이 성공합니다.

```
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
```

다음으로 전화기에서 ITL 파일도 요청합니다.

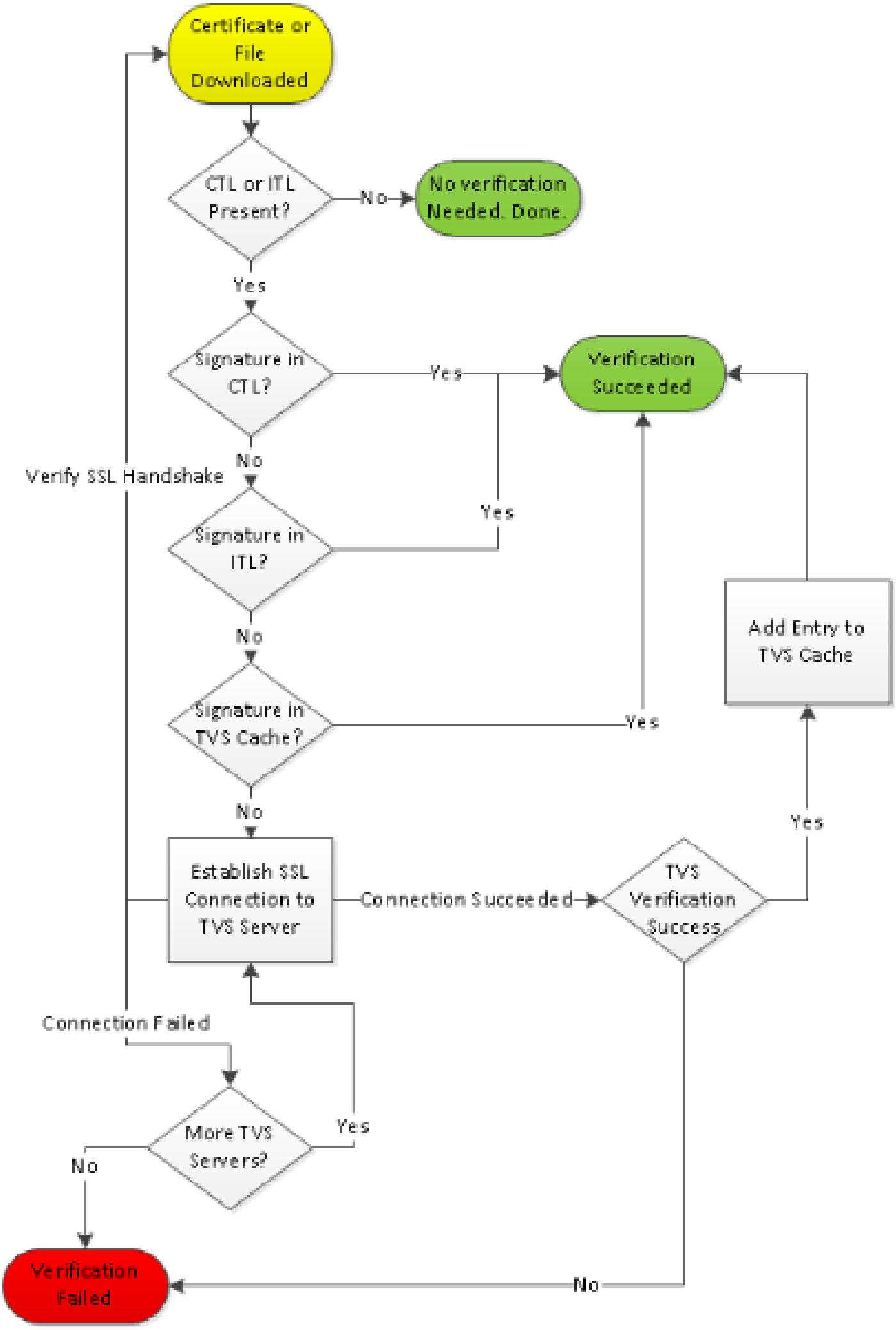
```
868: NOT 09:13:17.860613 TFTP: [28]:Requesting ITLSEP0011215A1AE3.tlv from
14 . 48 . 44 . 80
869: NOT 09:13:17.875059 TFTP: [28]:Finished --> rcvd 5438 bytes
```

전화기에서 ITL 및 컨피그레이션 파일 확인

ITL 파일을 다운로드한 후에는 확인해야 합니다. 이 시점에는 전화기가 있을 수 있다는 여러 가지 상태가 있으므로 이 문서에서는 전화기를 모두 다룹니다.

- 전화기에 CTL 또는 ITL 파일이 없거나 Prepare Cluster for Rollback to Pre 8.0 매개 변수 때문에 ITL이 비어 있습니다. 이 상태에서 전화기는 다운로드한 다음 CTL 또는 ITL 파일을 맹목적으로 신뢰하며 이 서명을 사용합니다.
- 전화기에 이미 CTL은 있지만 ITL은 없습니다. 이 상태에서 전화기는 CTL 파일의 CCM+TFTP 기능으로 확인할 수 있는 경우에만 ITL을 신뢰합니다.
- 전화기에 CTL 및 ITL 파일이 이미 있습니다. 이 상태에서 전화기는 최근에 다운로드한 파일이 CTL, ITL 또는 TVS 서버의 시그니처와 일치하는지 확인합니다.

전화기가 서명된 파일 및 HTTPS 인증서를 확인하는 방법을 설명하는 순서도는 다음과 같습니다.


Certificate or File Downloaded
CTL or ITL Present?
No
No verification Needed. Done.
Yes
Signature in CTL?
Yes
Verification Succeeded
No
Verify SSL Handshake
Yes
Signature in ITL?
No
Add Entry to TVS Cache
Signature in TVS Cache?
Yes
No
Yes
Establish SSL Connection to TVS Server
Connection Succeeded
TVS Verification Success
Connection Failed
More TVS Servers?
Yes
No
Verification Failed
No

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

전화기에서 CTL 및 ITL 파일을 다운로드했으므로 이 시점부터 서명된 컨피그레이션 파일만 요청합니다.

이는 CTL 및 ITL의 존재 여부에 따라 TFTP 서버가 안전한지 확인한 다음 서명된 파일을 요청하는 전화기 로직을 보여줍니다.

```
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
```

서명된 컨피그레이션 파일이 다운로드되면 전화기는 ITL 내부의 CCM+TFTP용 기능에 대해 이를 인증해야 합니다.

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

알 수 없는 인증서에 대해 TVS에 전화 연결

ITL 파일은 CUCM 서버 TCP 포트 2445에서 실행되는 TVS 서비스의 인증서를 포함하는 TVS 기능을 제공합니다.

TVS는 CallManager 서비스가 활성화된 모든 서버에서 실행됩니다. CUCM TFTP 서비스는 전화기가 전화기 컨피그레이션 파일에 접속해야 하는 TVS 서버 목록을 작성하기 위해 구성된 CallManager 그룹을 사용합니다.

일부 랩에서는 단일 CUCM 서버만 사용합니다. 다중 노드 CUCM 클러스터에서는 전화기에 대해 최대 3개의 TVS 항목이 있을 수 있습니다. 이는 전화기의 CUCM 그룹에 있는 각 CUCM에 하나씩 해당합니다.

이 예에서는 IP 전화의 디렉터리 단추를 누르면 어떻게 되는지 보여줍니다. 디렉터리 URL은

HTTPS용으로 구성되어 있으므로 전화기는 디렉터리 서버의 Tomcat 웹 인증서와 함께 제공됩니다
.

이 Tomcat 웹 인증서(OS 관리의 tomcat.pem)는 전화기에 로드되지 않으므로 전화기가 인증서를 인증하려면 TVS에 문의해야 합니다.

상호 작용에 대한 설명은 이전 TVS 개요 다이어그램을 참조하십시오. 다음은 폰 콘솔 로그 관점입니다.

먼저 디렉터리 URL을 찾습니다.

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

이는 확인이 필요한 SSL/TLS(Transport Layer Security) 보안 HTTP 세션입니다.

```
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
```

전화기는 먼저 SSL/TLS 서버에서 제공하는 인증서가 CTL에 있는지 확인합니다. 그러면 전화기에서 ITL 파일의 Functions(함수)를 확인하여 일치하는 항목을 찾을 수 있는지 확인합니다.

이 오류 메시지에는 "HTTPS cert not in CTL"이라고 표시되어 있습니다. 즉 "CTL 또는 ITL에서 인증을 찾을 수 없습니다."라는 의미입니다.

```
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>
```

CTL 및 ITL 파일의 직접 내용이 인증서에 대해 검사되고 나면 전화기에서 다음으로 확인하는 것은 TVS 캐시입니다.

이 작업은 전화기가 최근에 TVS 서버에 동일한 인증서를 요청한 경우 네트워크 트래픽을 줄이기 위해 수행됩니다.

HTTPS 인증서가 폰 캐시에 없는 경우 TVS 서버 자체에 TCP 연결을 설정할 수 있습니다.

```
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.
```

TVS에 대한 연결 자체가 SSL/TLS(secure HTTP 또는 HTTPS)이므로 CTL to ITL에 대해 인증해야 하는 인증서이기도 합니다.

모든 것이 제대로 된다면 TVS 서버 인증서는 ITL 파일의 TVS 기능에서 찾을 수 있다. 이전 예제 ITL 파일#3 ITL 레코드 레코드를 참조하십시오.

```
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>
```

성공! 이제 전화기가 TVS 서버에 안전하게 연결됩니다. 다음 단계는 TVS 서버에 "안녕하세요, 이 디렉터리 서버 인증서를 신뢰합니까?"를 묻는 것입니다.

이 예에서는 해당 질문에 대한 대답을 보여 줍니다. 즉, 0으로 응답하면 성공(오류 없음)을 의미합니다.

```
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
```

TVS에서 성공적으로 응답했으므로 해당 인증서의 결과가 캐시에 저장됩니다.

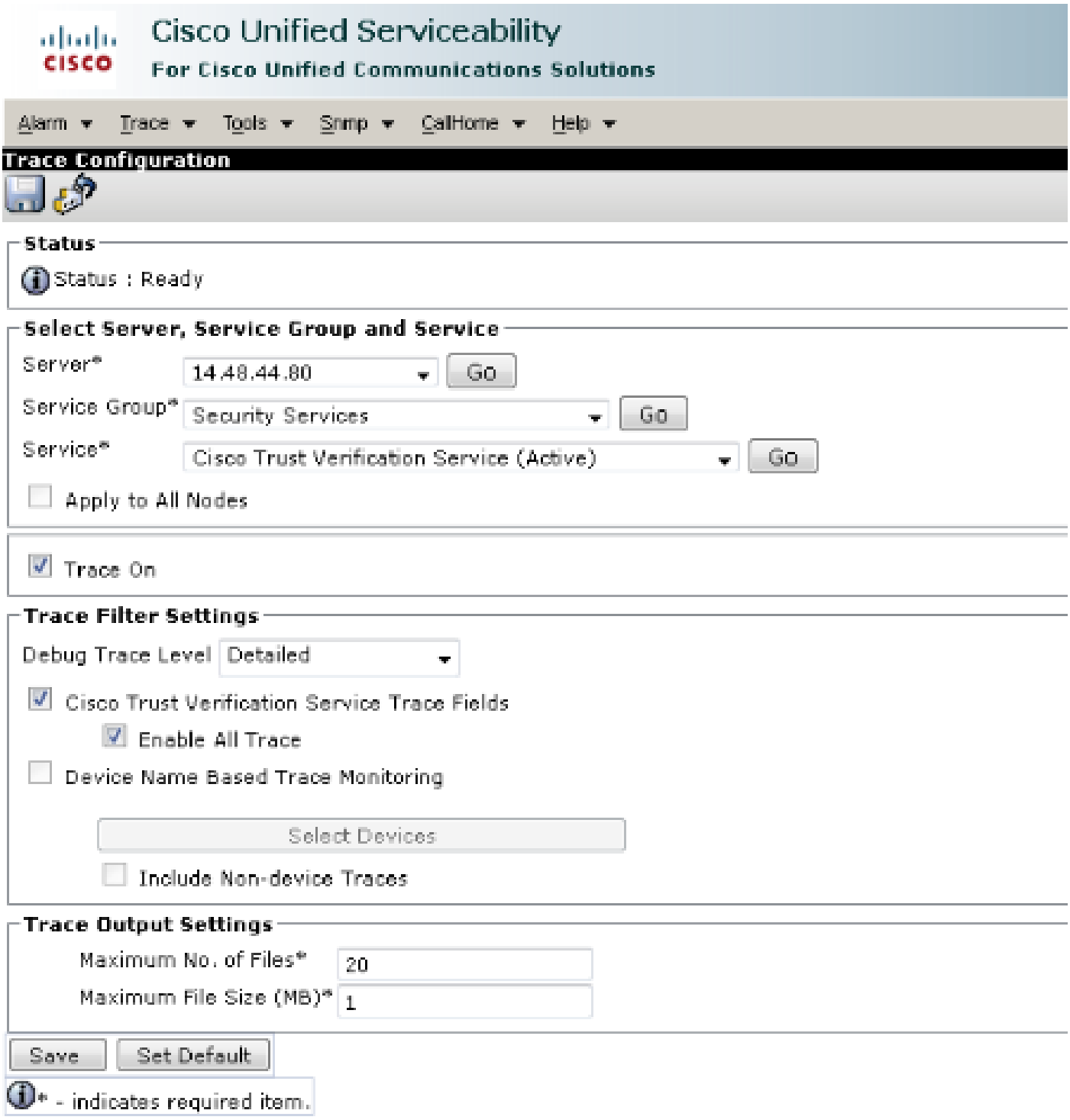
즉, 다음 86,400초 내에 Directories(디렉토리) 버튼을 다시 누르면 인증서를 확인하기 위해 TVS 서버에 연결할 필요가 없습니다. 로컬 캐시에 액세스하기만 하면 됩니다.

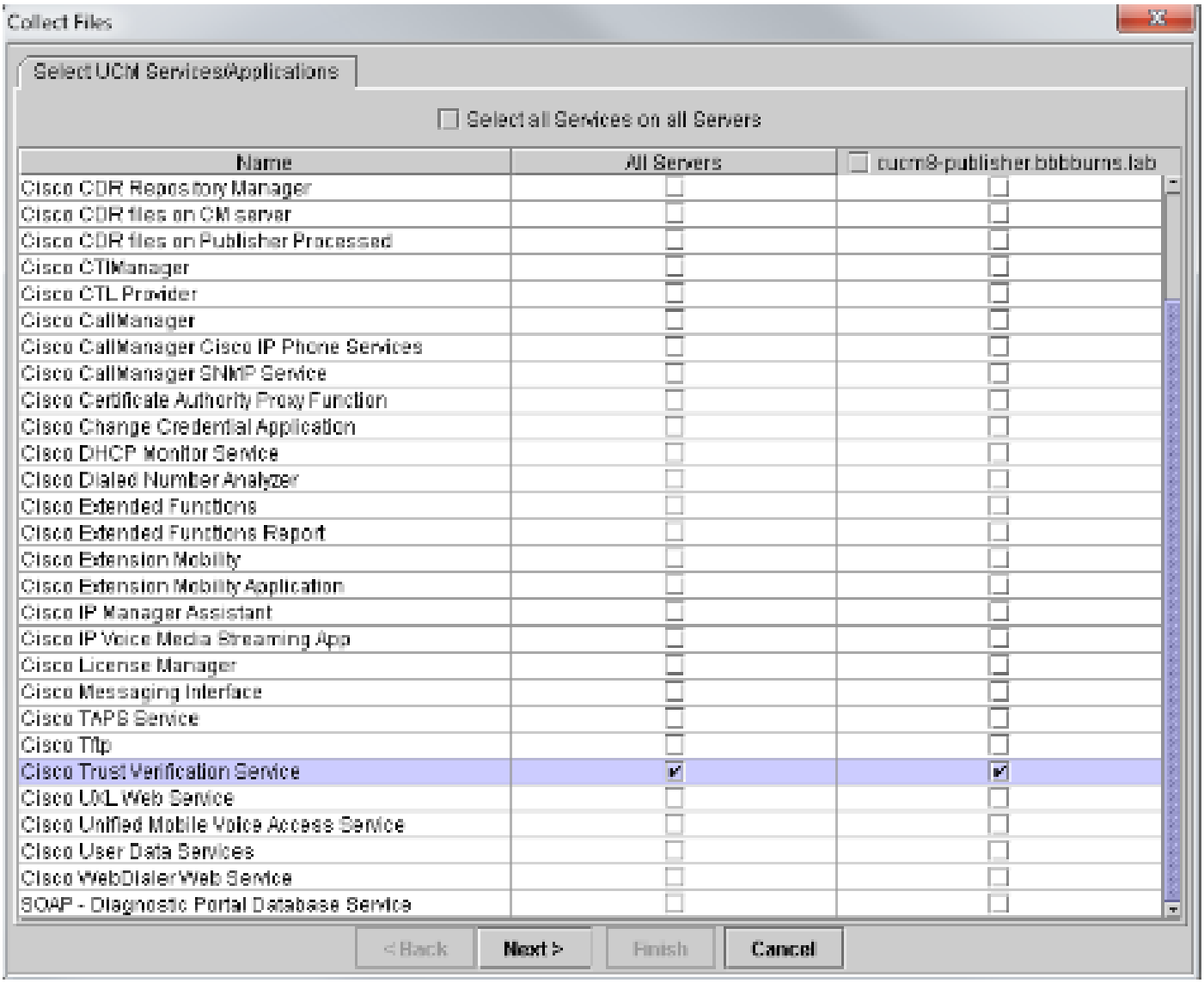
```
1279: NOT 15:20:59.837086 SECD: saveCertToTvsCache: Saving certificate
in TVS cache with default time-to-live value: 86400 seconds
1287: ERR 15:20:59.859993 SECD: Authenticated the HTTPS conn via TVS
```

마지막으로 디렉터리 서버에 연결되었는지 확인합니다.

```
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
```

다음은 TVS가 실행되는 CUCM 서버에서 발생하는 일의 예입니다. Cisco Unified RTMT(Real-Time Monitoring Tool)를 사용하여 TVS 로그를 수집할 수 있습니다.


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.



CUCM TVS 로그는 전화기와 SSL 핸드셰이크를 수행하고 전화기가 TVS에 Tomcat 인증서에 대해 질문한 다음 TVS가 응답하여 인증서가 TVS 인증서 저장소에 일치함을 나타냅니다.

```
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
```

TVS 인증서 저장소는 OS Administration(OS 관리) > Certificate Management(인증서 관리) 웹 페이지에 포함된 모든 인증서 목록입니다.

전화기 ITL이 CUCM ITL과 일치하는지 수동으로 확인

트러블슈팅 중에 발견되는 한 가지 일반적인 오해는 ITL 파일이 파일 확인 문제를 해결하기를 바라는 ITL 파일 삭제 경향과 관련이 있습니다.

ITL 파일을 삭제해야 하는 경우도 있지만, 이러한 모든 조건이 충족되는 경우에만 ITL 파일을 삭제해야 합니다.

- 전화기에 있는 ITL 파일의 서명이 CM TFTP 서버에 있는 ITL 파일의 서명과 일치하지 않습니다.
- ITL 파일의 TVS 서명이 TVS에서 제공한 인증서와 일치하지 않습니다.
- 전화기에서 ITL 파일 또는 컨피그레이션 파일을 다운로드하려고 할 때 "Verification Failed(확인 실패)"가 표시됩니다.
- 이전 TFTP 개인 키의 백업이 없습니다.

이 조건 중 처음 두 가지를 확인하는 방법은 다음과 같습니다.

먼저 CUCM에 있는 ITL 파일의 체크섬을 전화기의 체크섬 ITL 파일과 비교할 수 있습니다.

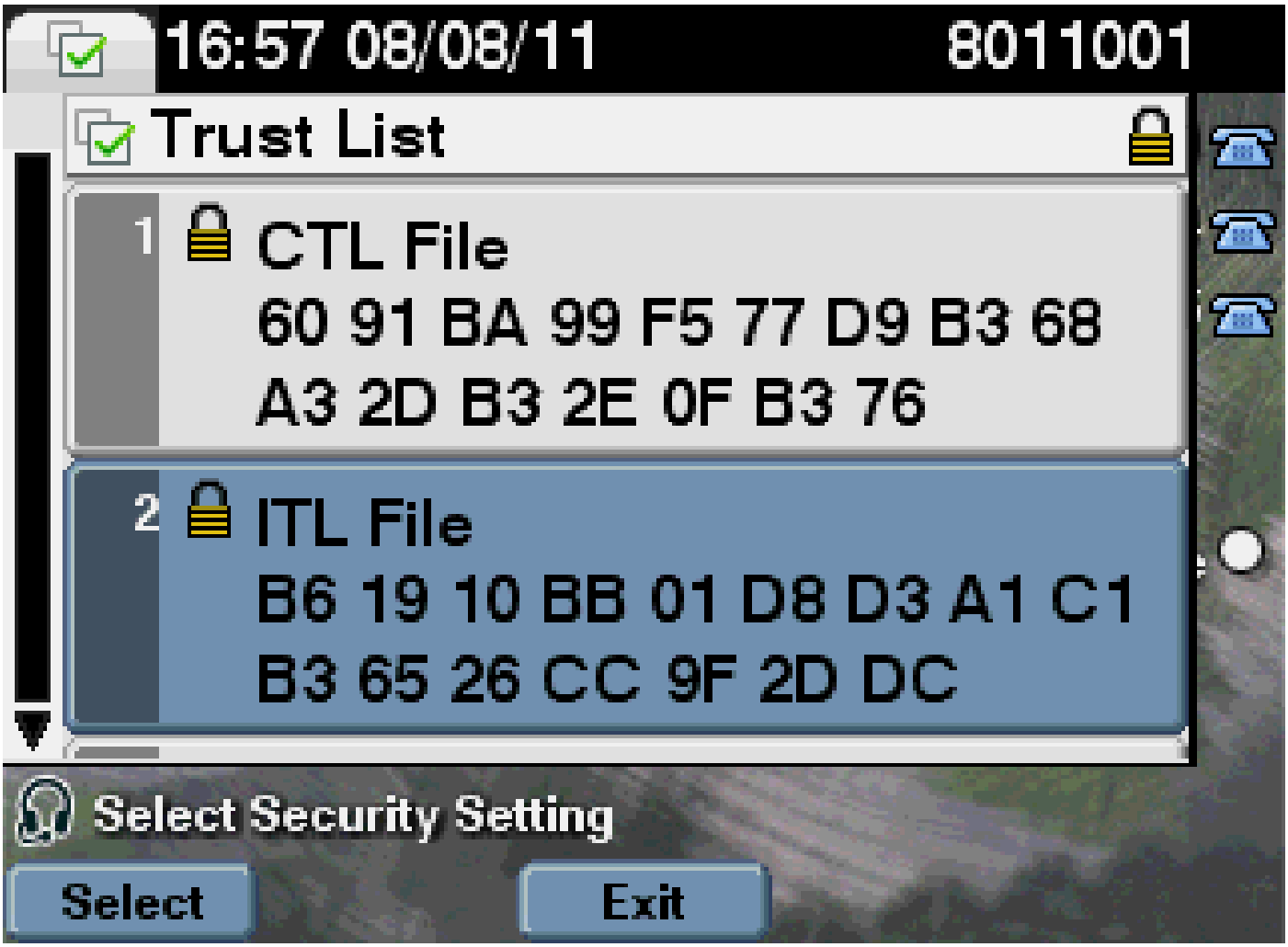
이 Cisco 버그 ID CSCto60209에 대한 수정 버전을 실행할 때까지 현재 CUCM에서 CUCM의 ITL 파일의 MD5sum을 확인할 수 있는 방법은 없습니다.

그 동안 자주 사용하는 GUI 또는 CLI 프로그램을 사용하여 다음을 실행합니다.

```
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
```

이는 CUCM에 있는 ITL 파일의 MD5sum이 b61910bb01d8d3a1c1b36526cc9f2ddc임을 보여줍니다.

이제 전화기 자체를 보고 로드된 ITL 파일의 해시를 확인할 수 있습니다. Settings(설정) > Security Configuration(보안 컨피그레이션) > Trust List(신뢰 목록).

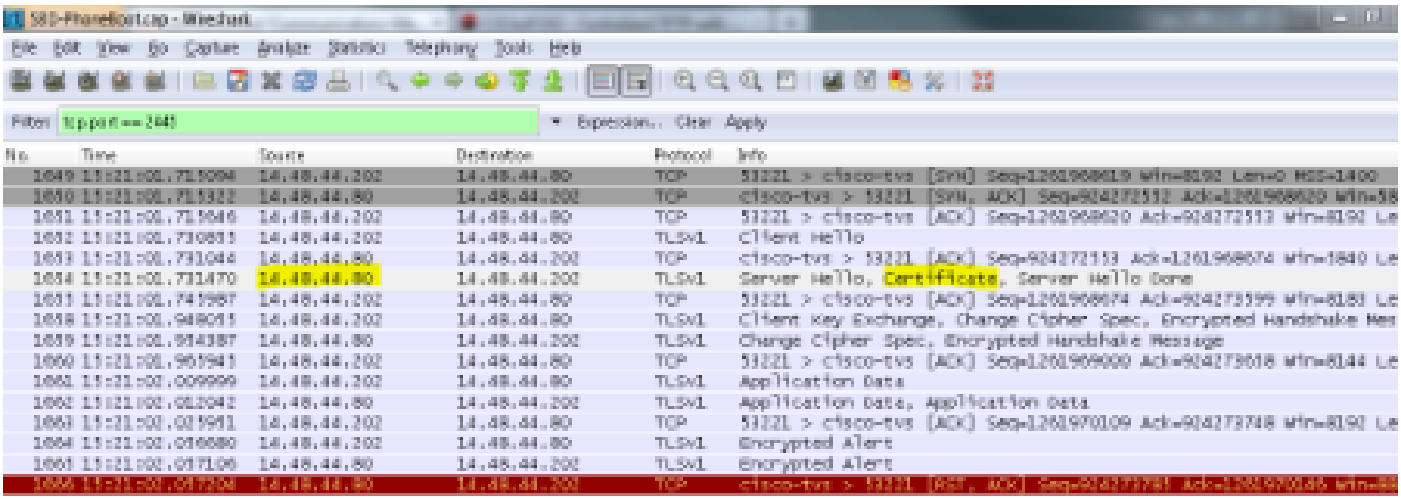


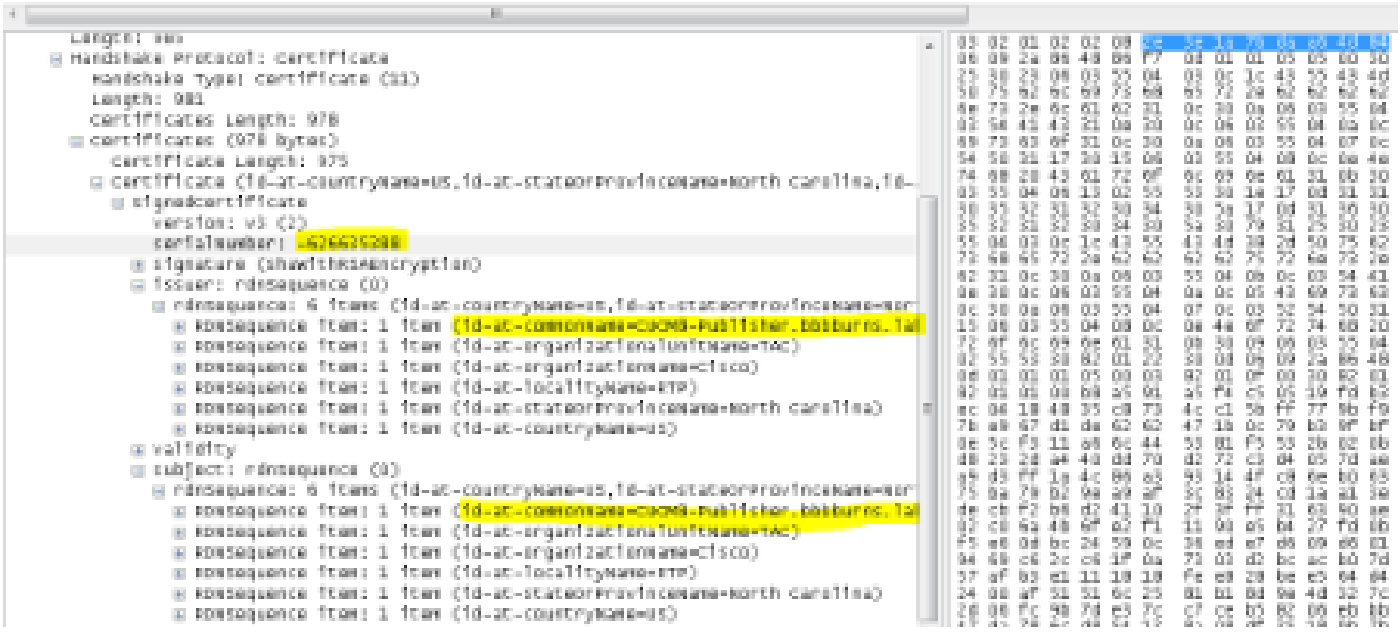
MD5sum이 일치함을 보여 줍니다. 즉, 전화기의 ITL 파일이 CUCM의 파일과 일치하므로 삭제할 필요가 없습니다.

일치하는 경우 다음 작업으로 이동해야 합니다. ITL의 TVS 인증서가 TVS에서 제공한 인증서와 일치하는지 여부를 결정합니다. 이 작업은 좀 더 관여되어 있습니다.

먼저 TCP 포트 2445의 TVS 서버에 연결되는 전화기의 패킷 캡처를 살펴봅니다.

Wireshark에서 이 스트림의 패킷을 마우스 오른쪽 버튼으로 클릭하고 Decode As(다른 이름으로 디코딩)를 클릭한 다음 SSL을 선택합니다. 다음과 같은 서버 인증서를 찾습니다.





이전 ITL 파일에 포함된 TVS 인증서를 확인합니다. 그런 다음 일련 번호가 2E3E1A7BDAA64D84인 항목이 표시됩니다.

<#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
```

성공, ITL 파일의 TVS.pem이 네트워크에 표시된 TVS 인증서와 일치합니다. ITL은 삭제할 필요가 없으며 TVS는 올바른 인증서를 제공합니다.

파일 인증이 계속 실패할 경우 이전 순서도의 나머지 부분을 선택합니다.

제한 사항 및 상호 작용

인증서 재생성/클러스터 재구축/인증서 만료

가장 중요한 인증서는 이제 CallManager.pem 인증서입니다. 이 인증서 개인 키는 ITL 파일을 포함하는 모든 TFTP 컨피그레이션 파일에 서명하는 데 사용됩니다.

CallManager.pem 파일이 다시 생성되면 새 개인 키로 새 CCM+TFTP 인증서가 생성됩니다. 또한 ITL 파일은 이제 이 새로운 CCM+TFTP 키로 서명됩니다.

CallManager.pem을 다시 생성하고 TVS 및 TFTP 서비스를 다시 시작한 후 전화기가 부팅될 때 이러한 현상이 발생합니다.

1. 전화기는 TFTP 서버에서 새 CCM+TFTP가 서명한 새 ITL 파일을 다운로드하려고 시도합니다. 현재 전화기에는 이전 ITL 파일만 있으며 새 키는 전화기에 있는 ITL 파일에 없습니다.
2. 이전 ITL에서 새 CCM+TFTP 서명을 찾을 수 없으므로 전화기는 TVS 서비스에 연결을 시도합니다.

   참고: 이 부분은 매우 중요합니다. 이전 ITL 파일의 TVS 인증서가 여전히 일치해야 합니다. CallManager.pem과 TVS.pem이 동시에 재생성되는 경우 전화기에서 ITL을 수동으로 삭제하지 않으면 새 파일을 다운로드할 수 없습니다.

3. 전화기가 TVS에 연결되면 TVS를 실행하는 CUCM 서버에 OS 인증서 저장소에 새 CallManager.pem 인증서가 있습니다.
4. TVS 서버는 성공을 반환하고 전화기는 새 ITL 파일을 메모리에 로드합니다.
5. 이제 전화기에서 새 CallManager.pem 키로 서명된 컨피그레이션 파일의 다운로드를 시도합니다.
6. 새 ITL이 로드되었으므로 새로 서명된 컨피그레이션 파일은 메모리의 ITL에서 성공적으로 검증됩니다.

요점:

- CallManager.pem 및 TVS.pem 인증서를 동시에 다시 생성하지 마십시오.
- TVS.pem 또는 CallManager.pem이 다시 생성되는 경우 새 ITL 파일을 가져오려면 TVS 및 TFTP를 다시 시작하고 전화기를 재설정해야 합니다.
- 최신 버전의 CUCM은 이 전화기를 자동으로 재설정하고 인증서 재생성 시 사용자에게 경고합니다.
- 둘 이상의 TVS 서버가 있는 경우(CallManager 그룹에 둘 이상의 서버가 있는 경우) 추가 서버는 새 CallManager.pem 인증서를 인증할 수 있습니다.

클러스터 간에 전화 이동

ITL이 있는 한 클러스터에서 다른 클러스터로 전화기를 이동할 때는 ITL 및 TFTP 개인 키를 고려해야 합니다.

전화기에 제공되는 새 구성 파일은 CTL, ITL의 시그니처 또는 현재 TVS 서비스의 시그니처와 일치해야 합니다.

이 문서에서는 전화기의 현재 ITL 파일에서 새 클러스터 ITL 파일 및 구성 파일을 신뢰할 수 있는지 확인하는 방법에 대해 설명합니다. https://supportforums.cisco.com/docs/DOC-15799.

백업 및 복원

CallManager.pem 인증서 및 개인 키는 DRS(Disaster Recovery System)를 통해 백업됩니다. TFTP 서버를 재구축하는 경우 개인 키를 복원할 수 있도록 백업에서 복원해야 합니다.

서버에 CallManager.pem 개인 키가 없으면 이전 키를 사용하는 현재 ITL이 있는 전화기는 서명된 컨피그레이션 파일을 신뢰하지 않습니다.

클러스터가 재구축되고 백업에서 복원되지 않는 경우 "클러스터 간 전화기 이동" 문서와 동일합니다. 새 키를 가진 클러스터는 전화기에 관한 한 다른 클러스터이기 때문입니다.

백업 및 복원과 관련된 한 가지 심각한 결함이 있습니다. 클러스터가 Cisco 버그 ID CSCtn50405에 영향을 받기 쉬운 경우, DRS 백업에는 CallManager.pem 인증서가 포함되지 않습니다.

이렇게 하면 새 CallManager.pem이 생성될 때까지 이 백업에서 복원된 모든 서버에서 손상된 ITL 파일이 생성됩니다.

백업 및 복원 작업을 거치지 않은 다른 기능적 TFTP 서버가 없는 경우, 이는 전화기에서 모든 ITL 파일을 삭제해야 함을 의미할 수 있습니다.

CallManager.pem 파일을 다시 생성해야 하는지 확인하려면 show itl 명령 다음에 다음을 입력합니다.

```
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
```

ITL 출력에서 검색할 주요 오류는 다음과 같습니다.

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

및

```
Verification of the ITL file failed.
```

```
Error parsing the ITL file!!
```

이전 SQL(Structured Query Language) 쿼리는 "인증 및 권한 부여" 역할을 가진 인증서를 검색합니다.

인증 및 권한 부여 역할이 있는 이전 데이터베이스 쿼리의 CallManager.pem 인증서도 OS 관리 인증서 관리 웹 페이지에 있어야 합니다.

이전 결함이 발생하면 쿼리와 OS 웹 페이지의 CallManager.pem 인증서가 일치하지 않습니다.

호스트 이름 또는 도메인 이름 변경

CUCM 서버의 호스트 이름 또는 도메인 이름을 변경하면 해당 서버에서 모든 인증서가 한 번에 재생성됩니다. 인증서 재생성 부분에서는 TVS.pem과 CallManager.pem을 모두 재생성하는 것이 '나쁜 일'이라고 설명했다.

호스트 이름 변경이 실패하는 경우와 문제 없이 작동하는 경우가 있습니다. 이 섹션에서는 이러한 모든 내용을 다루고 이 문서에서 TV 및 ITL에 대해 이미 알고 있는 내용으로 다시 연결합니다.

ITL만 있는 단일 노드 클러스터(주의, 준비 없이 중단됨)

- Business Edition 서버 또는 게시자 전용 배포에서는 호스트 이름을 변경할 때 CallManager.pem과 TVS.pem이 동시에 다시 생성됩니다.
- 여기서 다루는 Rollback Enterprise 매개 변수를 먼저 사용하지 않고 단일 노드 클러스터에서 호스트 이름을 변경하면 전화기는 현재 ITL 파일에 대해 새 ITL 파일 또는 컨피그레이션 파일을 확인할 수 없습니다.
- TVS 인증서도 더 이상 신뢰할 수 없으므로 전화기에서 TVS에 연결할 수 없습니다.
- 전화기에 "Trust List Verification Failed(신뢰 목록 확인 실패)"에 대한 오류가 표시되고, 새 컨피그레이션 변경 사항이 적용되지 않으며, 보안 서비스 URL이 실패합니다.
- 2단계의 예방 조치가 처음이 아닌 경우 유일한 해결 방법은 모든 전화기에서 ITL을 수동으로 삭제하는 것입니다.

CTL 및 ITL이 모두 포함된 단일 노드 클러스터(일시적으로 중단될 수 있지만 쉽게 수정할 수 있음)

- 서버 이름 바꾸기를 실행한 후 CTL 클라이언트를 다시 실행합니다. 이렇게 하면 전화기가 다운로드하는 CTL 파일에 새 CallManager.pem 인증서가 배치됩니다.
- 새 ITL 파일을 포함하는 새 컨피그레이션 파일은 CTL 파일의 CCM+TFTP 기능을 기반으로 신뢰할 수 있습니다.
- 이는 업데이트된 CTL 파일이 동일하게 유지되는 USB eToken 개인 키를 기반으로 하여 신뢰되기 때문입니다.

ITL만 있는 다중 노드 클러스터(일반적으로 작동하지만 서둘러 수행하면 영구적으로 손상될 수 있음)

- 다중 노드 클러스터에는 여러 TVS 서버가 있으므로 모든 단일 서버에서 인증서를 문제 없이 재생성할 수 있습니다. 전화기에 이 새롭고 생소한 서명이 표시되면 TVS 서버 중 다른 서버에 새 서버 인증서를 검증하도록 요청합니다.

- 이 작업을 실패할 수 있는 두 가지 주요 문제는 다음과 같습니다.
  - 모든 서버의 이름을 바꾸고 동시에 리부팅하는 경우 서버와 전화가 다시 시작될 때 알려진 인증서를 사용하여 연결할 수 있는 TVS 서버가 없습니다.
  - CallManager 그룹에 서버가 하나뿐인 전화기의 경우 추가 TVS 서버는 다를 바 없습니다. 이 문제를 해결하려면 "단일 노드 클러스터" 시나리오를 참조하거나 phone CallManager 그룹에 다른 서버를 추가하십시오.

CTL과 ITL이 모두 포함된 다중 노드 클러스터(영구적으로 손상될 수 없음)

- 이름 바꾸기를 실행하면 TVS 서비스가 새 인증서를 인증합니다.
- 어떤 이유로든 모든 TVS 서버를 사용할 수 없는 경우에도 CTL 클라이언트를 사용하여 전화기를 새 CallManager.pem CCM+TFTP 인증서로 업데이트할 수 있습니다.

중앙 집중식 TFTP

ITL이 있는 전화기가 부팅될 때 CTLSEP<MAC Address>.tlv, ITLSEP<MAC Address>.tlv 및 SEP<MAC Address>.cnf.xml.sgn 파일을 요청합니다.

전화기에서 이러한 파일을 찾을 수 없는 경우 ITLFile.tlv와 CTLFile.tlv를 요청하며, 중앙 집중식 TFTP 서버가 이를 요청하는 전화기에 제공합니다.

중앙 집중식 TFTP에서는 여러 개의 다른 하위 클러스터를 가리키는 단일 TFTP 클러스터가 있습니다.

이 작업은 여러 CUCM 클러스터의 전화기가 동일한 DHCP 범위를 공유하므로 DHCP Option 150 TFTP 서버가 동일해야 하기 때문에 수행하는 경우가 많습니다.

모든 IP 전화는 다른 클러스터에 등록하더라도 중앙 TFTP 클러스터를 가리킵니다. 이 중앙 TFTP 서버는 찾을 수 없는 파일에 대한 요청을 받을 때마다 원격 TFTP 서버를 쿼리합니다.

이 작업 때문에 중앙 집중식 TFTP는 ITL 동종 환경에서만 작동합니다.

모든 서버는 CUCM 버전 8.x 이상을 실행해야 합니다. 또는 모든 서버는 버전 8.x 이전 버전을 실행해야 합니다.

ITLFile.tlv가 중앙 집중식 TFTP 서버에서 제공되는 경우 서명이 일치하지 않기 때문에 전화기가 원격 TFTP 서버의 파일을 신뢰하지 않습니다.

이것은 이질적인 혼합에서 발생합니다. 동질적인 혼합에서 전화기는 올바른 원격 클러스터에서 ITLSEP<MAC>.tlv를 요청합니다.

Pre-Version 8.x 클러스터와 Version 8.x 클러스터가 혼합된 이기종 환경에서는 Cisco 버그 ID CSCto87262에 설명된 대로 Version 8.x 클러스터에서 "Prepare Cluster for Rollback to Pre 8.0"을 활성화해야 합니다.

HTTPS 대신 HTTP를 사용하여 "보안 전화 URL 매개변수"를 구성합니다. 이렇게 하면 전화기의 ITL 기능이 효과적으로 비활성화됩니다.

자주 묻는 질문(FAQ)

SBD를 끌 수 있습니까?

SBD와 ITL이 현재 작동하는 경우에만 SBD를 끌 수 있습니다.

SBD는 Prepare Cluster for Rollback to pre 8.0" Enterprise Parameter를 사용하고 HTTPS 대신 HTTP를 사용하여 "Secured Phone URL Parameters"를 구성하여 전화기에서 일시적으로 비활성화할 수 있습니다.

Rollback 매개변수를 설정하면 빈 함수 항목이 있는 서명된 ITL 파일이 생성됩니다.

"비어 있는" ITL 파일은 여전히 서명되어 있으므로 이 매개변수를 활성화하려면 클러스터가 완전한 보안 상태에 있어야 합니다.

이 매개변수가 활성화되고 항목이 비어 있는 새 ITL 파일이 다운로드되고 확인되면 전화기에서 서명된 사용자에 관계없이 모든 컨피그레이션 파일을 수락합니다.

이전에 언급한 세 가지 기능(인증된 구성 파일, 암호화된 구성 파일 및 HTTPS URL) 중 사용할 수 있는 기능이 없기 때문에 클러스터를 이 상태로 두는 것이 좋습니다.

CallManager.pem이 손실된 후 모든 전화기에서 ITL 파일을 쉽게 삭제할 수 있습니까?

현재 Cisco에서 원격으로 제공하는 전화기에서 모든 ITL을 삭제할 수 있는 방법은 없습니다. 그렇기 때문에 이 문서에 설명된 절차와 상호 작용이 매우 중요합니다.

현재 이 기능을 요청하는 Cisco 버그 ID CSCto47052에 대한 해결되지 않은 개선 사항이 있지만 아직 구현되지 않았습니다.

이 기간 동안 Cisco 버그 ID CSCts01319를 통해 새로운 기능이 추가되었으며, 이 기능을 통해 Cisco TAC(Technical Assistance Center)에서 이전에 신뢰했던 ITL을 서버에서 계속 사용할 수 있는 경우 되돌릴 수 있습니다.

이 문제는 클러스터가 이 결함 해결 기능이 있는 버전에 있고 이전 ITL이 서버의 특정 위치에 저장된 백업에 있는 특정 경우에만 작동합니다.

결함을 확인하여 버전에 수정 사항이 있는지 확인합니다. Cisco TAC에 문의하여 결함에 설명된 잠재적 복구 절차를 진행하십시오.

이전 절차를 사용할 수 없는 경우 ITL 파일을 삭제하려면 전화기에서 전화기 버튼을 수동으로 눌러야 합니다. 이것이 보안과 관리의 용이성 사이에서 이루어지는 절충안이다. ITL 파일이 안전하게 보호되려면 원격으로 쉽게 제거할 수 없습니다.

SOAP(Simple Object Access Protocol) XML 객체를 사용하여 스크립팅된 단추를 눌러도 ITL을 원격으로 제거할 수 없습니다.

이 시점에서는 TVS 액세스(및 이에 따라 수신 SOAP XML 버튼 푸시 개체를 검증하는 보안 인증

URL 액세스)가 작동하지 않기 때문입니다.

인증 URL이 보안으로 구성되지 않은 경우 ITL을 삭제하기 위해 키를 누르는 스크립트를 작성할 수 있지만 Cisco에서는 이 스크립트를 사용할 수 없습니다.

인증 URL을 사용하지 않고 원격 키 누름 스크립트를 작성하기 위한 다른 방법은 서드파티에서 사용할 수 있지만 이러한 애플리케이션은 Cisco에서 제공하지 않습니다.

ITL을 삭제하기 위해 가장 자주 사용되는 방법은 모든 전화 사용자에게 키 시퀀스를 지시하는 이메일 브로드캐스트입니다.

설정 액세스가 Restricted 또는 Disabled로 설정된 경우 사용자가 전화기의 Settings 메뉴에 액세스할 수 없으므로 전화기를 초기 설정으로 재설정해야 합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.