Segurança CUCM à revelia e operação e Troubleshooting ITL

Índice

Introdução

Este documento descreve a característica da Segurança à revelia (SBD) de versões 8.0 e mais recente do gerente das comunicações unificadas de Cisco (CUCM). Este documento serve como um suplemento aos documentos oficiais da Segurança à revelia, e fornece a informação operacional e os dicas de Troubleshooting para ajudar administradores e facilitar o processo de Troubleshooting.

Informações de Apoio

A versão 8.0 e mais recente CUCM introduz a característica SBD, que consiste nos arquivos da lista da confiança da identidade (ITL) e no serviço da verificação da confiança (TV). Cada

conjunto CUCM usa agora a Segurança ITL-baseada automaticamente. Há umas trocas entre a Segurança e a acessibilidade/facilidade da administração de que os administradores devem estar cientes antes que façam determinadas mudanças a um conjunto da versão 8.0 CUCM.

Éuma boa ideia tornar-se familiar com estes conceitos do núcleo do SBD: Artigo de Wikipedia do artigo e da infraestrutura de chave pública de Wikipedia da criptografia da chave assimétrica.

Vista geral SBD

Esta seção fornece uma visão rápida de exatamente o que o SBD fornece. Para detalhes técnico completos de cada função, veja o SBD seção detalhar e de informação de Troubleshooting.

O SBD fornece estas três funções para Telefones IP suportados:

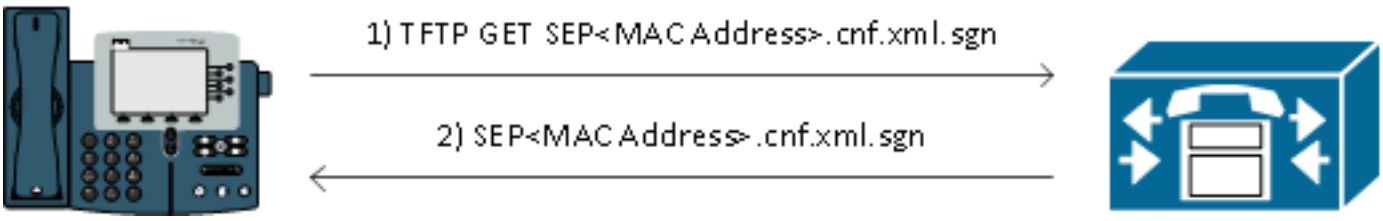
- Autenticação padrão de arquivos baixados TFTP (configuração, lugar, ringlist) esse uso uma chave de assinatura
- Criptografia opcional dos arquivos de configuração de TFTP que usam uma chave de assinatura
- Verificação de certificado para as conexões de HTTPS telefone-iniciadas que usam uma loja remota da confiança do certificado em CUCM (TV)

Este documento fornece uma vista geral de cada um destas funções.

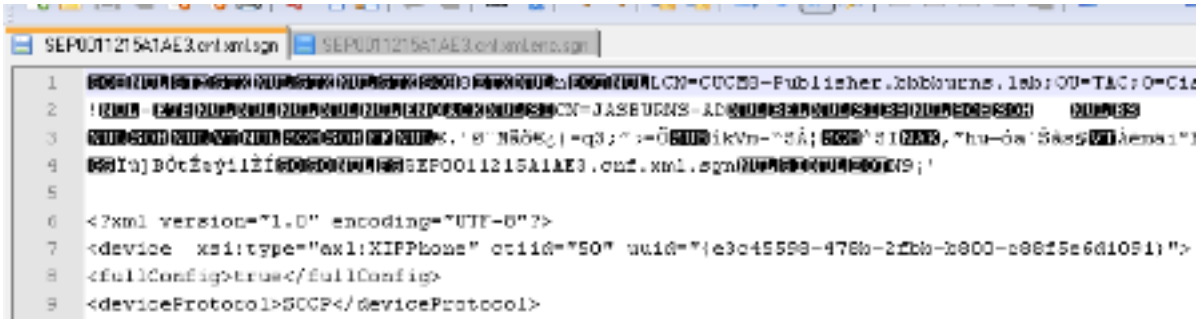
Autenticação da transferência TFTP

Quando um certificate trust list (CTL) ou o arquivo ITL estam presente, o telefone IP pede um arquivo de configuração de TFTP assinado do servidor TFTP CUCM. Este arquivo permite que o telefone verifique que o arquivo de configuração veio de um origem confiável. Com os arquivos CTL/ITL atuais em telefones, os arquivos de configuração devem ser assinados por um servidor TFTP confiado. O arquivo é texto simples na rede quando for transmitido, mas vem com uma assinatura especial da verificação.

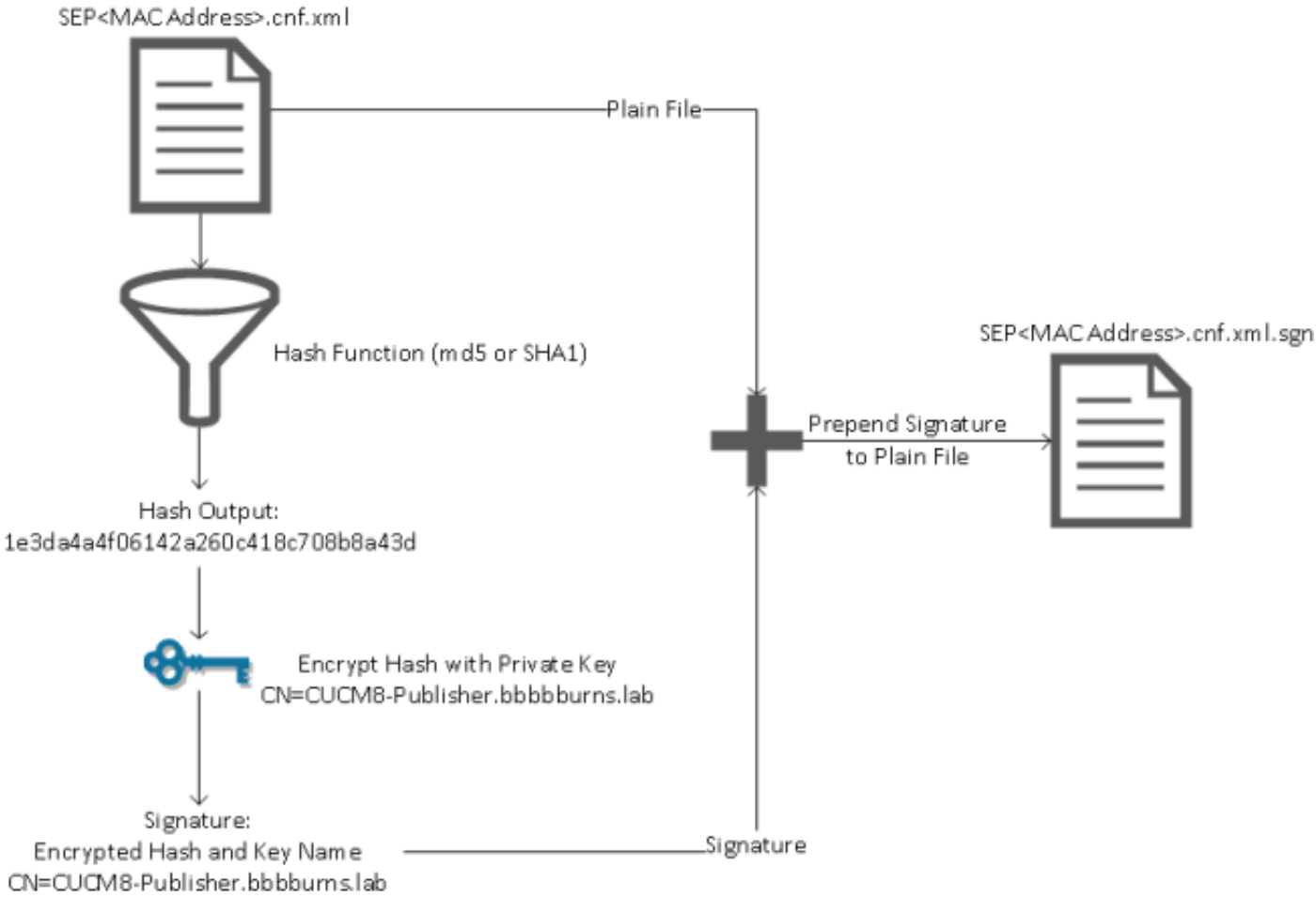
O telefone pede **SEP *< MAC address >.cnf.xml.sgn* a fim** receber o arquivo de configuração com a assinatura especial. Este arquivo de configuração é assinado pela chave privada TFTP que corresponde a CallManager.pem na página do gerenciamento certificado da administração do operating system (OS).



O arquivo assinado tem uma assinatura no superior a fim autenticar o arquivo, mas está de outra maneira no texto simples XML. A imagem abaixo mostra que o signatário do arquivo de configuração é **CN=CUCM8-Publisher.bbbburns.lab** qual por sua vez é assinado por **CN=JASBURNS-AD**. Isto significa que o telefone precisa de verificar a assinatura de **CUCM8-Publisher.bbbburns.lab** contra o arquivo ITL antes que este arquivo de configuração esteja aceitado.

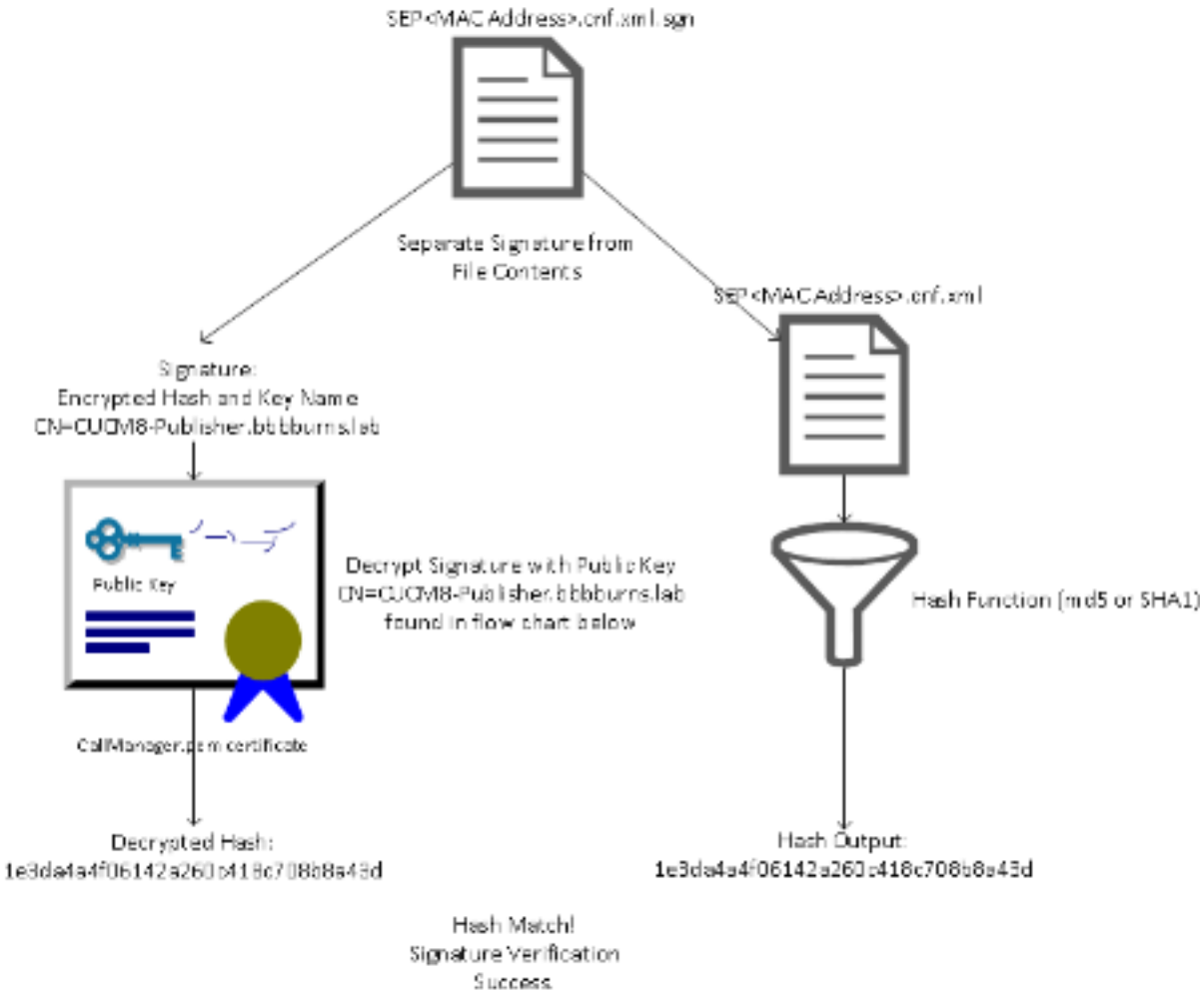


Está aqui um diagrama que mostre como a chave privada é usada junto com um algoritmo de message digest (MD)5 ou algoritmo de mistura segura (função de mistura SHA)1 a fim criar o arquivo assinado.



A verificação de assinatura inverte este processo com o uso da chave pública essa fósforos a fim decifrar a mistura. Se pica o fósforo, mostra:

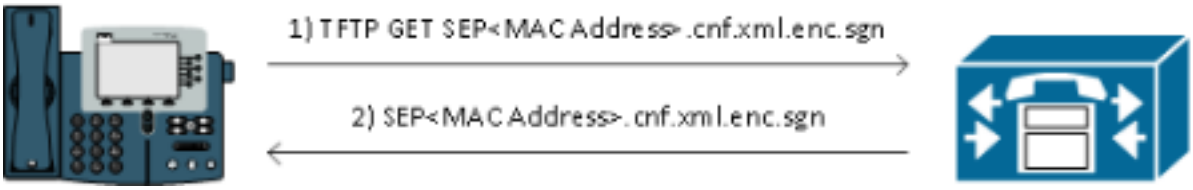
- Este arquivo não foi alterado no trânsito.
- Este arquivo vem do partido alistado na assinatura, desde que qualquer coisa decifrado com sucesso com a chave pública deve ter sido cifrado com a chave privada.



Criptografia do arquivo de configuração de TFTP

Se a criptografia opcional da configuração de TFTP é permitida no perfil de segurança associado do telefone, o telefone pede um arquivo de configuração cifrado. Este arquivo é assinado com a chave privada TFTP e cifrado com uma chave simétrica trocada entre o telefone e o CUCM (refira o guia da Segurança do gerente das comunicações unificadas de Cisco, liberam 8.5(1) para detalhes completos) de modo que seus índices não possam ser lidos com um rastreador de rede a menos que o observador tiver as chaves necessárias.

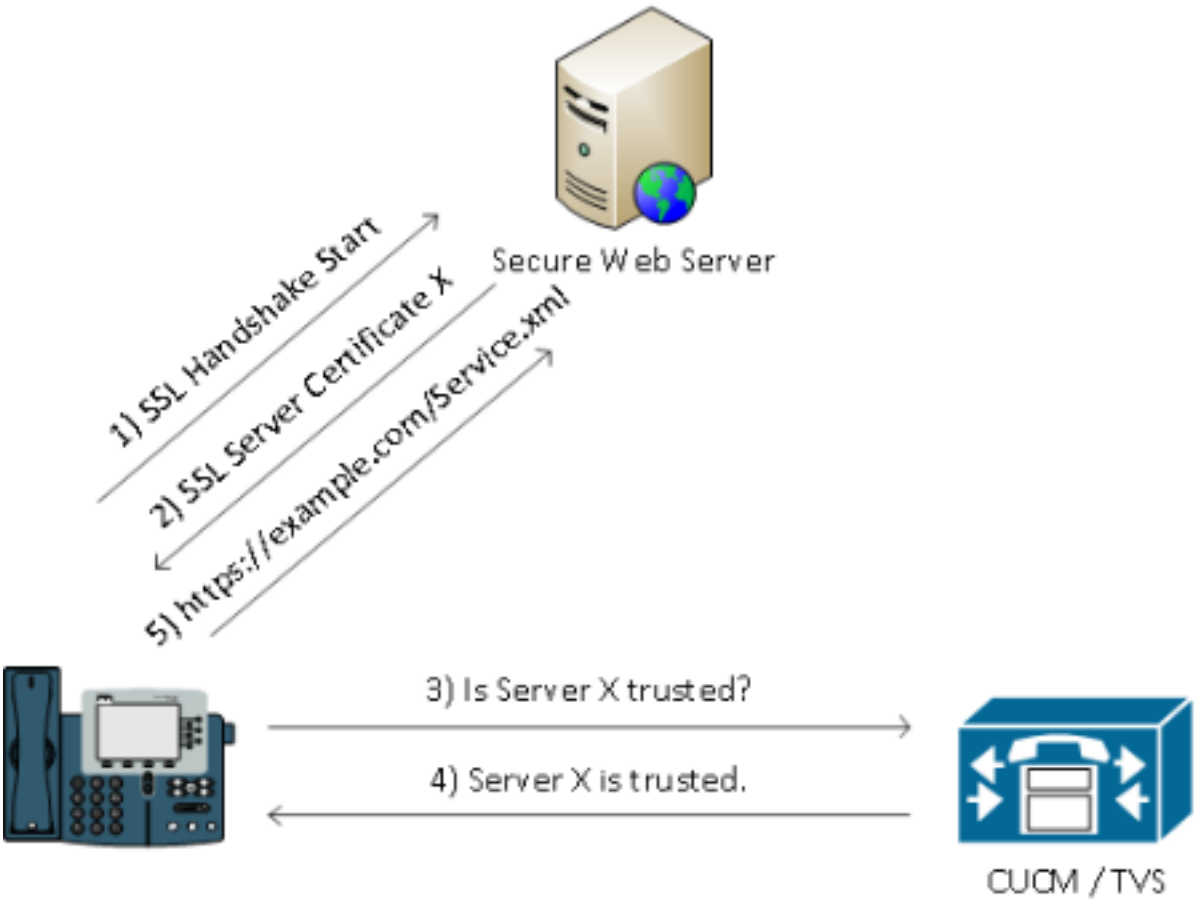
O telefone pede **SEP *< MAC address >.cnf.xml.enc.sgn* a fim** obter o arquivo cifrado assinado.



O arquivo de configuração cifrado tem a assinatura no início também, mas não há nenhum dados do texto simples após, simplesmente os dados criptografados (caráteres binários truncados neste editor de texto). A imagem mostra que o signatário é o mesmo que no exemplo anterior, assim que esta obrigação do signatário esta presente no arquivo ITL antes que o telefone aceite o arquivo. Mais, as chaves de descriptografia devem estar corretas antes que o telefone possa ler os índices do arquivo.

Serviço da verificação da confiança (verificação remota do certificado e de assinatura)

Os Telefones IP contêm uma quantidade limitada de memória, e pode igualmente haver um grande número telefones a controlar em uma rede. CUCM atua como uma loja remota da confiança através dos TV de modo que uma loja completa da confiança do certificado não tenha que ser colocada em cada telefone IP. Quando o telefone não pode verificar uma assinatura ou um certificado através dos arquivos CTL ou ITL, pede o servidor para verificação TV. Esta loja central da confiança é mais fácil de controlar do que se a loja da confiança estou presente em todos os Telefones IP.



Detalhe e informação de Troubleshooting SBD

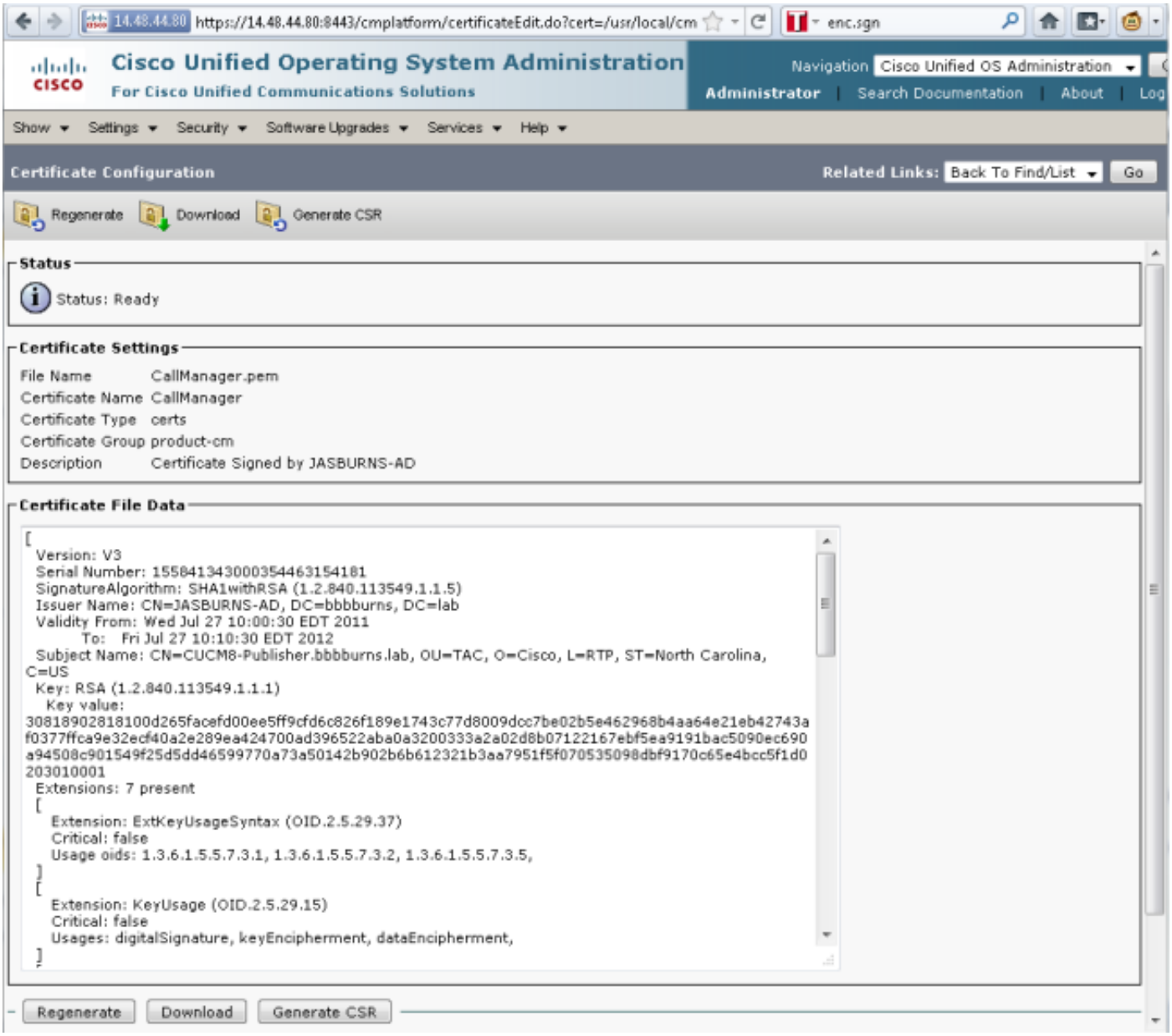
Esta seção detalha o processo SBD.

Arquivos e Certificados ITL atuais em CUCM

Primeiramente, há um número de arquivos que devem estam presente no server próprio CUCM. A parte a mais importante é o certificado TFTP e a chave privada TFTP. O certificado TFTP é ficado situado sob o **> gerenciamento de certificado do > segurança da administração do OS > o CallManager.pem.**

O server CUCM usa o certificado CallManager.pem privado e chaves públicas para o serviço TFTP (assim como para o serviço do Cisco Call Manager (CCM)). A imagem mostra que o certificado CallManager.pem está emitido a CUCM8-publisher.bbbburns.laband **assinado por** JASBURNS-AD**. Todos os** arquivos de configuração de TFTP são assinados pela chave privada abaixo.

Todos os telefones podem usar a chave pública TFTP no certificado CallManager.pem a fim decifrar todo o arquivo cifrado com a chave privada TFTP, assim como verificar qualquer arquivo assinado com a chave privada TFTP.



Além do que a chave privada do certificado CallManager.pem, o server CUCM igualmente armazena um arquivo ITL que seja apresentado aos telefones. **O comando do** showitl mostra os conteúdos completos deste arquivo ITL através do acesso do Shell Seguro (ssh) ao OS CLI do server CUCM.

Esta seção divide o arquivo ITL peça por peça, porque tem um número de componentes importantes que o telefone usa.

A primeira parcela é a informação de assinatura. Mesmo o arquivo ITL é um arquivo assinado. Esta saída mostra que está assinada pela chave privada TFTP que é associada com o certificado precedente CallManager.pem.

```
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*
```

As próximas seções cada um contêm sua finalidade dentro de um parâmetro da função especial. A primeira função é o token de segurança do administrador de sistema. Esta é a assinatura da chave 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.
```

A função seguinte é CCM+TFTP. Esta é outra vez a chave pública TFTP que serve para autenticar e decifrar arquivos de configuração de TFTP transferidos.

```
        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)
```

A função seguinte é TV. Há uma entrada para a chave pública de cada server TV a que o telefone conecta. Isto permite que o telefone estabeleça uma sessão do secure sockets layer (SSL) ao server TV.

```
        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
```

A função final incluída no arquivo ITL é a função do proxy do Certificate Authority (CAPF). Este certificado permite que os telefones estabeleçam uma conexão segura ao serviço CAPF no server CUCM de modo que o telefone possa instalar ou atualizar a localmente - o certificado significativo (LSC). Este processo será coberto em um outro documento que deva ser liberada ainda.

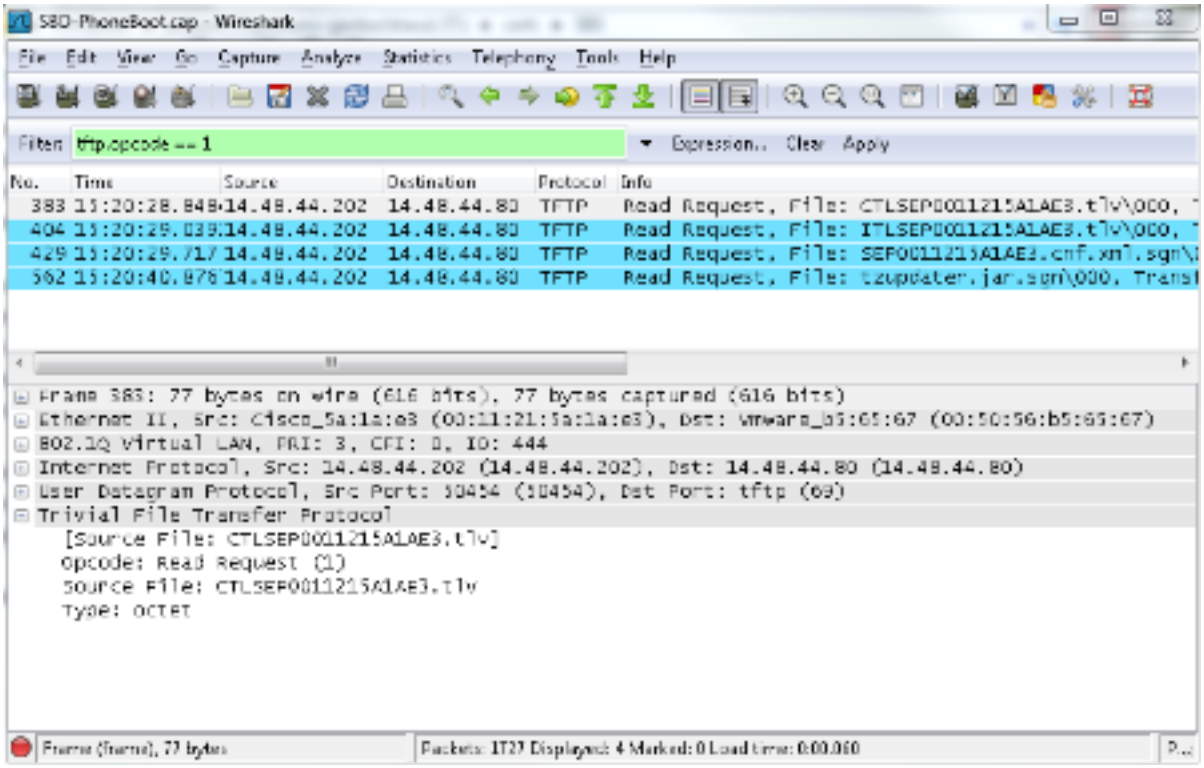
```
        ITL Record #:4
                 ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       455
2       DNSNAME         2
3       SUBJECTNAME     61      CN=CAPF-9c4cba7d;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US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

As tampas da próxima seção exatamente o que acontece quando um telefone carreg.

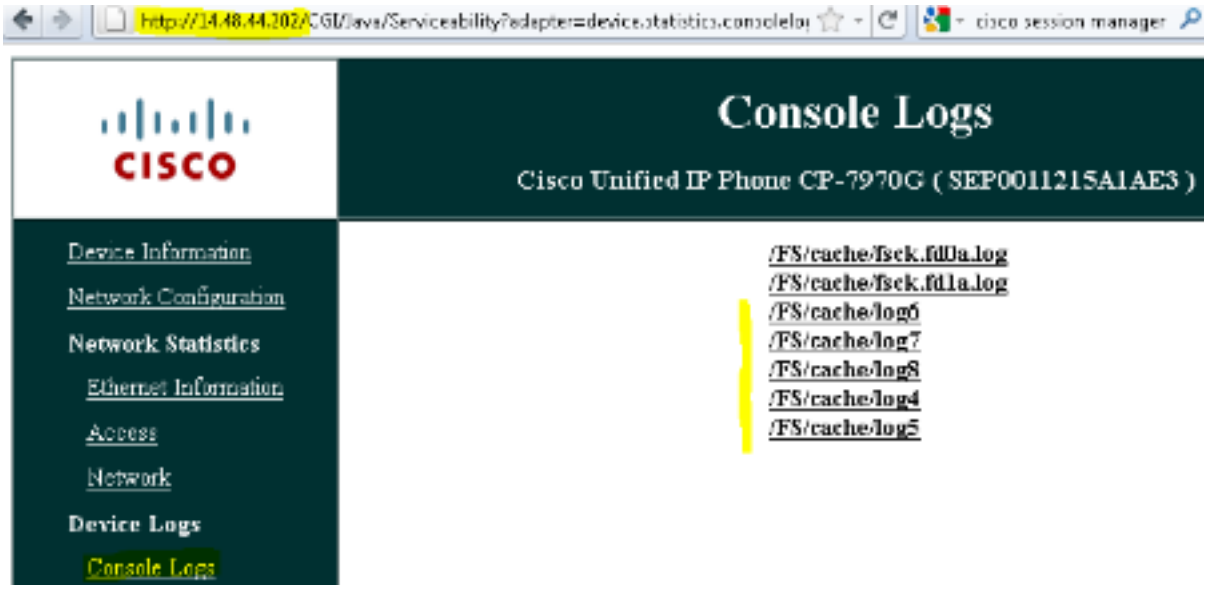
O telefone transfere a ITL e o arquivo de configuração

Depois que o telefone carreg e obtém um endereço IP de Um ou Mais Servidores Cisco ICM NT assim como o endereço de um servidor TFTP, pede o CTL e os arquivos ITL primeiramente.

Esta captura de pacote de informação mostra um pedido do telefone para o arquivo ITL. Se você filtra no **== 1 tftp.opcode, você** vê cada TFTP ler o pedido do telefone:



Desde que o telefone recebeu arquivos CTL e ITL do TFTP com sucesso, o telefone pede um arquivo de configuração assinado. Os logs do console do telefone que mostram este comportamento estão disponíveis da interface da WEB do telefone:



Primeiramente o telefone pede um arquivo CTL, que suceda:

```
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
```

Em seguida o telefone igualmente pede um arquivo ITL:

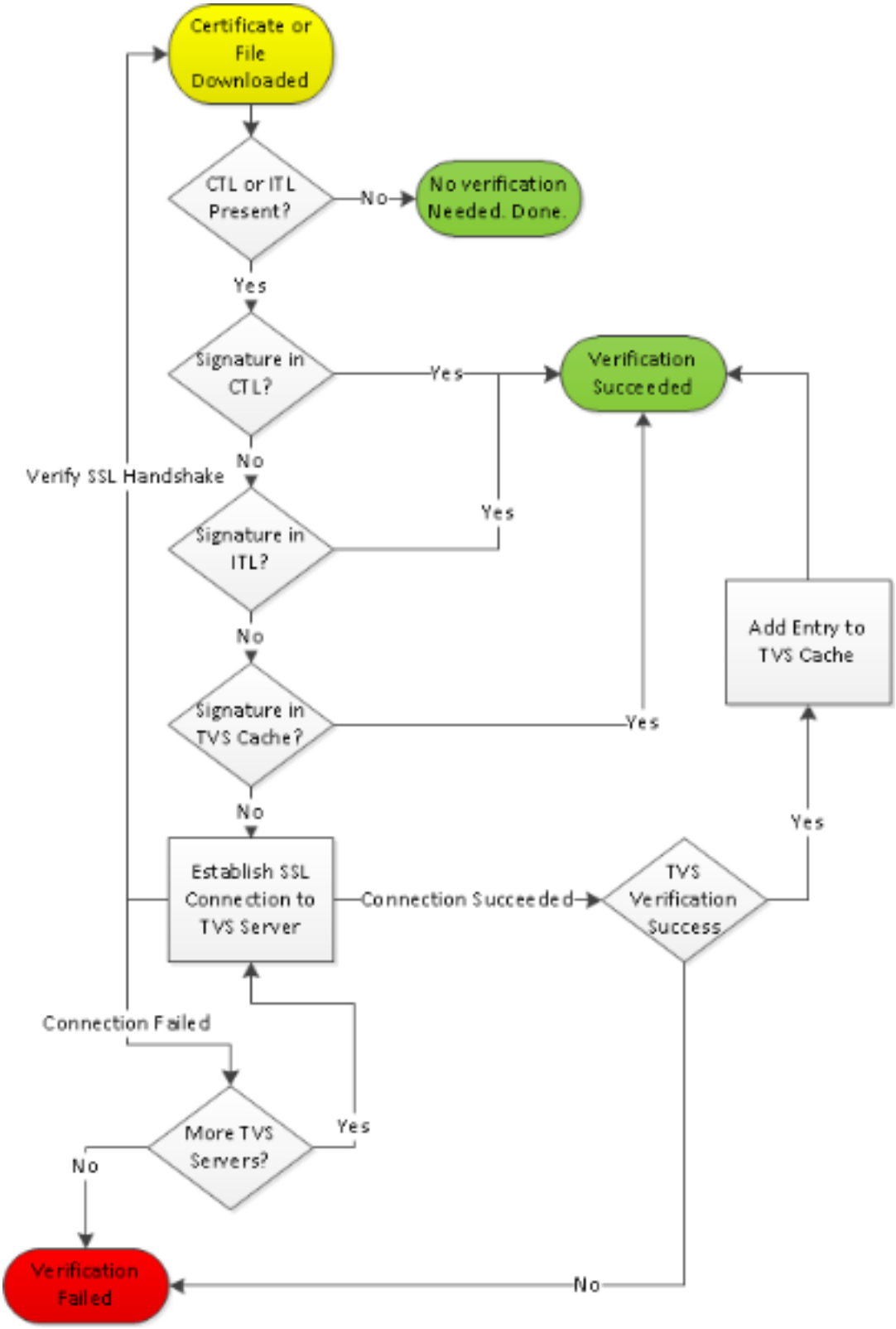
```
868: NOT 09:13:17.860613 TFTP: [28]:Requesting ITLSEP0011215A1AE3.tlv from
14.48.44.80
869: NOT 09:13:17.875059 TFTP: [28]:Finished --> rcvd 5438 bytes
```

O telefone verifica a ITL e o arquivo de configuração

Depois que o arquivo ITL é transferido, deve-se verificar. Há um número de estados que um telefone pode estar dentro neste momento, assim estes as capas de documento eles todos.

- O telefone não tem presente de nenhum arquivo CTL ou ITL ou a ITL está vazia devido ao conjunto da preparação para o Rollback ao parâmetro pre 8.0. neste estado, o telefone cegamente confia o arquivo seguinte CTL ou ITL transferido e usa esta assinatura doravante.
- O telefone já não tem um CTL mas nenhuma ITL. Neste estado, o telefone confia somente uma ITL se pode ser verificado pela função CCM+TFTP no arquivo CTL.
- O telefone já tem um CTL e um arquivo ITL. Neste estado, o telefone verifica que recentemente os arquivos baixados combinam a assinatura no server CTL, ITL, ou TV.

Está aqui um fluxograma que descreva como o telefone verifica arquivos assinados e Certificados HTTPS:



Neste caso, o telefone pode verificar a assinatura nos arquivos ITL e CTL. O telefone já tem um CTL e a ITL assim que verificou simplesmente contra eles e encontrou a assinatura correta.

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

Desde que o telefone transferiu os arquivos CTL e ITL, a partir daqui pede SOMENTE arquivos de configuração assinados. Isto ilustra que a lógica do telefone é determinar que o servidor TFTP é seguro, com base na presença de CTL e de ITL, e para pedir então um arquivo assinado:

```
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
```

Uma vez que o arquivo de configuração assinado é transferido, o telefone deve autenticá-lo contra a função para CCM+TFTP dentro da ITL:

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

O telefone contacta TV para certificado desconhecido

O arquivo ITL fornece uma função TV que contenha o certificado do serviço TV que é executado na porta TCP 2445 do server CUCM. Os TV são executado em todos os server onde o serviço do CallManager é ativado. O serviço TFTP CUCM usa o grupo do CallManager configurado a fim construir uma lista de server que TV o telefone deve contactar no arquivo de configuração telefônica.

Alguns laboratórios usam somente um único server CUCM. Em um conjunto do multi-nó CUCM, pode haver até três entradas TV para um telefone, um para cada CUCM no grupo CUCM do telefone.

Este exemplo mostra o que acontece quando o botão Directories Button no telefone IP é pressionado. Os diretórios URL são configurados para o HTTPS, assim que o telefone é presentado com o certificado da Web de Tomcat do server dos diretórios. Este certificado da Web de Tomcat (tomcat.pem na administração do OS) não é carregado no telefone, assim que no telefone deve contactar TV a fim autenticar o certificado.

Refira o diagrama de vista geral precedente TV para uma descrição da interação. Está aqui a perspectiva do console log do telefone:

Primeiramente você encontra o diretório 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
```

Esta é uma sessão de HTTP segura da Segurança da camada SSL/Transport (TLS) que exija a verificação.

```
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
```

O telefone verifica primeiramente que o certificado apresentado pelo server SSL/TLS esta presente no CTL. Então os olhares do telefone nas funções na ITL arquivam a fim considerar se encontra um fósforo. Este Mensagem de Erro diz “o CERT HTTPS não no CTL,” que significa “que a certificação não pode ser encontrada no CTL ou na 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>
```

Depois que os índices diretos do arquivo CTL e ITL são verificados para ver se há o certificado, a coisa seguinte as verificações do telefone é o esconderijo TV. Isto está feito a fim reduzir no tráfego de rede se o telefone tem pedido recentemente o server TV o mesmo certificado. Se o certificado HTTPS não é encontrado no esconderijo do telefone, você pode fazer uma conexão de TCP ao server TV própria.

```
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.
```

Recorde que a conexão aos TV própria é SSL/TLS (HTTP seguro, ou HTTPS), assim que é igualmente um certificado que precise de ser autenticado contra a ITL do ot CTL. Se tudo vai corretamente, o certificado de server TV deve ser encontrado na função TV do arquivo ITL. Veja a ITL gravar #3 no arquivo ITL do exemplo anterior.

```
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>
```

Sucesso! O telefone tem agora uma conexão segura ao server TV. A próxima etapa é pedir o server TV “olá!, faz confiança I este certificado de servidor dos diretórios?”

Este exemplo mostra a resposta a essa pergunta - uma resposta de 0 qual significa o sucesso (nenhum erro).

```
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
```

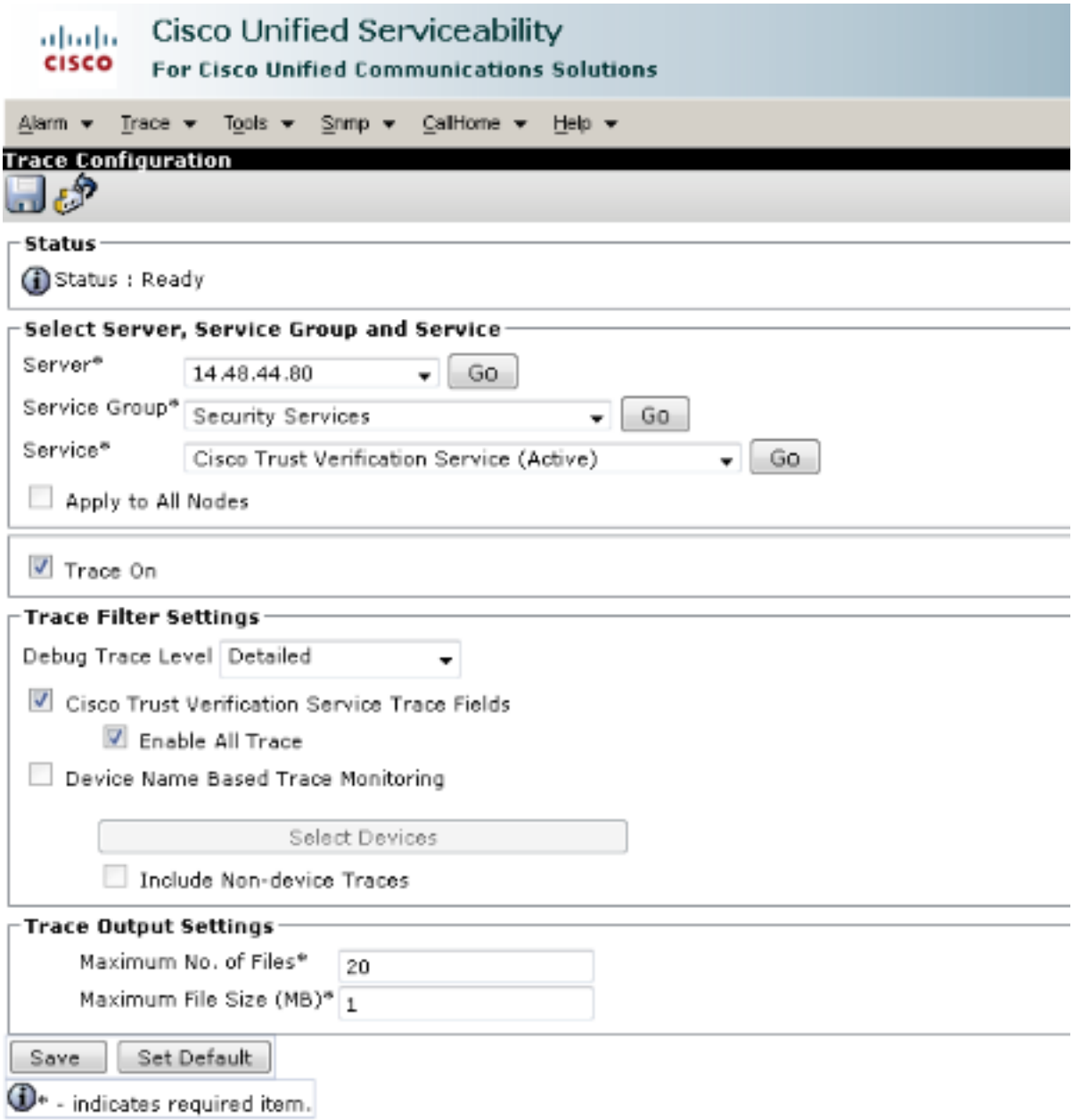
Desde que há uma resposta bem sucedida dos TV, os resultados para esse certificado salvar no esconderijo. Isto significa que, se você pressiona o **botão Directories Button** outra vez dentro dos próximos 86,400 segundos, você não precisa de contactar o server TV a fim verificar o certificado. Você pode simplesmente alcançar o cache local.

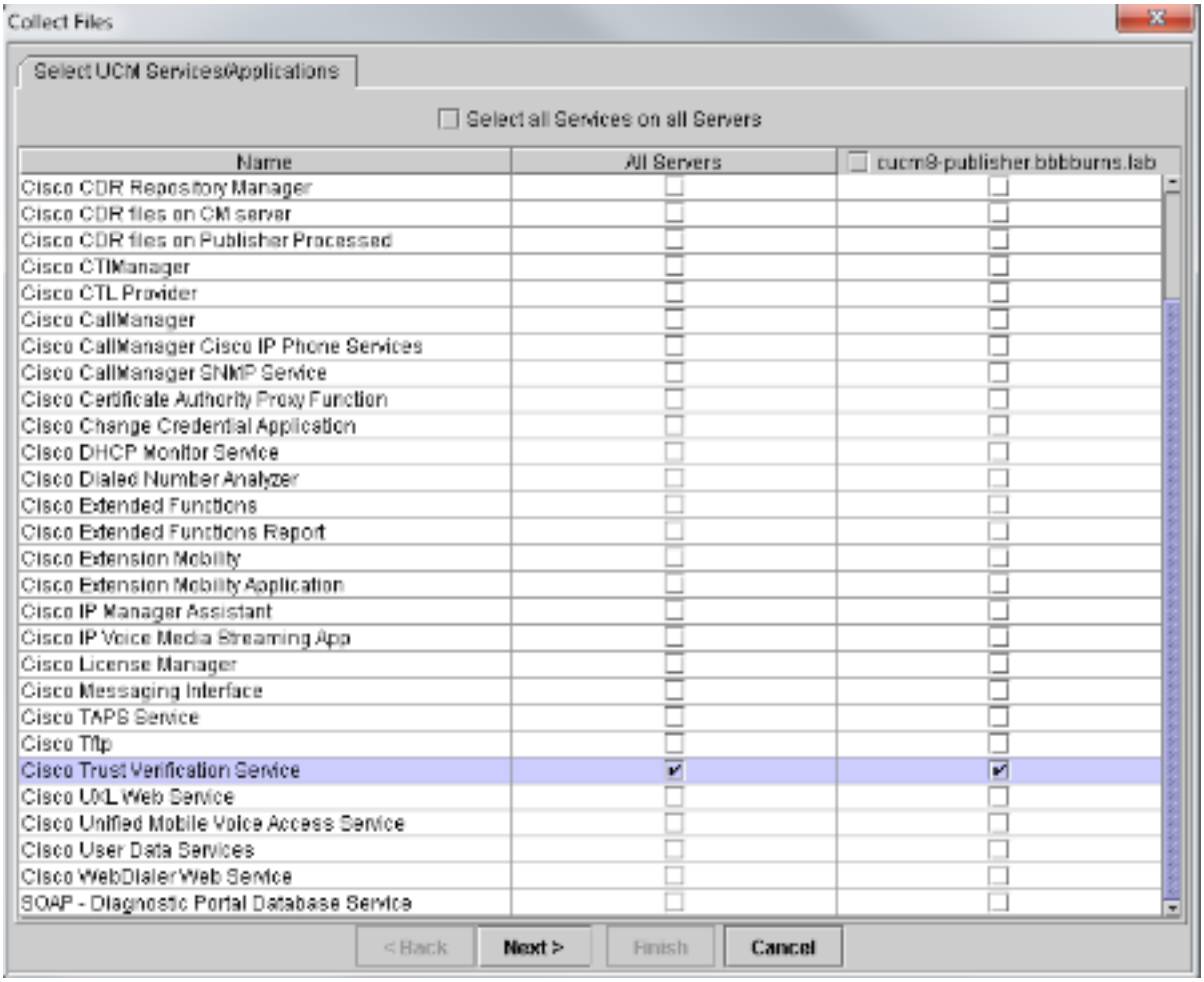
```
1279: NOT 15:20:59.837086 SECD: saveCertToTvsCache: Saving certificate
in TVS cache with default time-to-live value: 86400 seconds
1287: ERR 15:20:59.859993 SECD: Authenticated the HTTPS conn via TVS
```

Finalmente, você verifica que sua conexão ao server dos diretórios sucedeu.

```
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
```

Está aqui um exemplo do que acontece no server CUCM aonde os TV são executado. Você pode recolher logs TV com a ferramenta unificada Cisco do monitoramento em tempo real (RTMT).





Os logs CUCM TV mostram que você saudação de SSL com o telefone, o telefone pede TV sobre o certificado de Tomcat, a seguir TV responde para indicar que o certificado está combinado na loja do certificado TV.

```
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
```

A loja do certificado TV é uma lista de todos os Certificados contidos no página da web do **administração > gerenciamento de certificado do OS**.

Verifique manualmente essa ITL dos fósforos CUCM ITL do telefone

Uma concepção errada comum vista quando pesquisar defeitos se referir à tendência suprimir do arquivo ITL com a esperança que resolverá um problema da verificação do arquivo. O supressão do arquivo ITL é exigido às vezes, mas pôde haver uma maneira melhor.

O arquivo ITL precisa somente de ser suprimido quando TODAS estas circunstâncias são estadas conformes.

- A assinatura do arquivo ITL no telefone não combina a assinatura do arquivo ITL no servidor TFTP CM.
- A assinatura TV no arquivo ITL não combina o certificado apresentado por TV.
- O telefone mostrar a “verificação” quando ele attemps não é transferido o arquivo ou arquivos de configuração ITL.
- Nenhum backup existe da chave privada velha TFTP.

Éaqui como você verifica as primeiros duas destas circunstâncias.

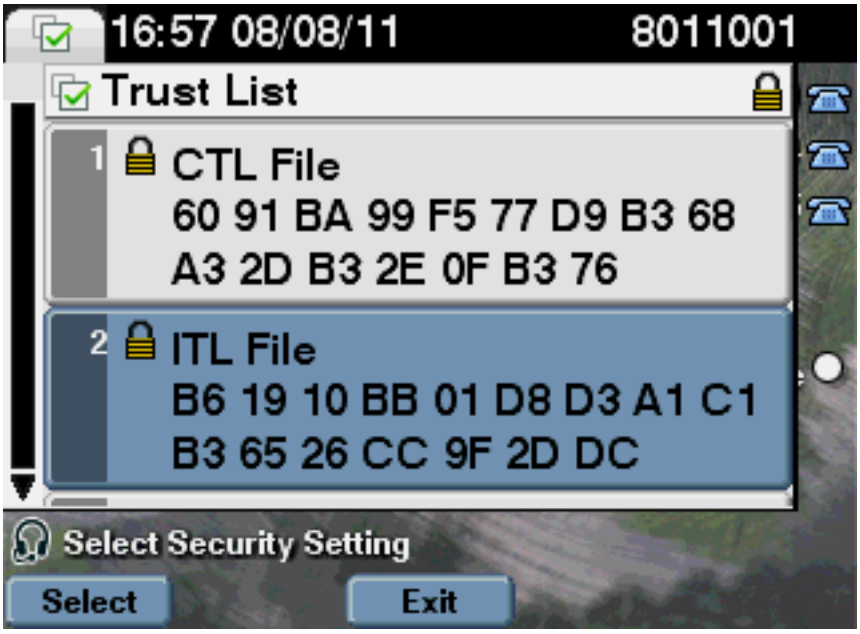
Primeiramente, você pode comparar a soma de verificação do arquivo ITL atual em CUCM com o arquivo ITL da soma de verificação do telefone. Não há atualmente nenhuma maneira de olhar o MD5sum do arquivo ITL em CUCM de CUCM próprio até que você execute uma versão com o reparo para esta identificação de bug Cisco CSCto60209.

No ínterim, execute isto com seu favorito GUI ou programas CLI:

```
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
```

Isto mostra que o MD5sum do arquivo ITL em CUCM é **b61910bb01d8d3a1c1b36526cc9f2ddc**.

Agora você pode olhar o telefone próprio a fim determinar a mistura do arquivo ITL carregado lá: **Configuração do > segurança dos ajustes > lista da confiança**.

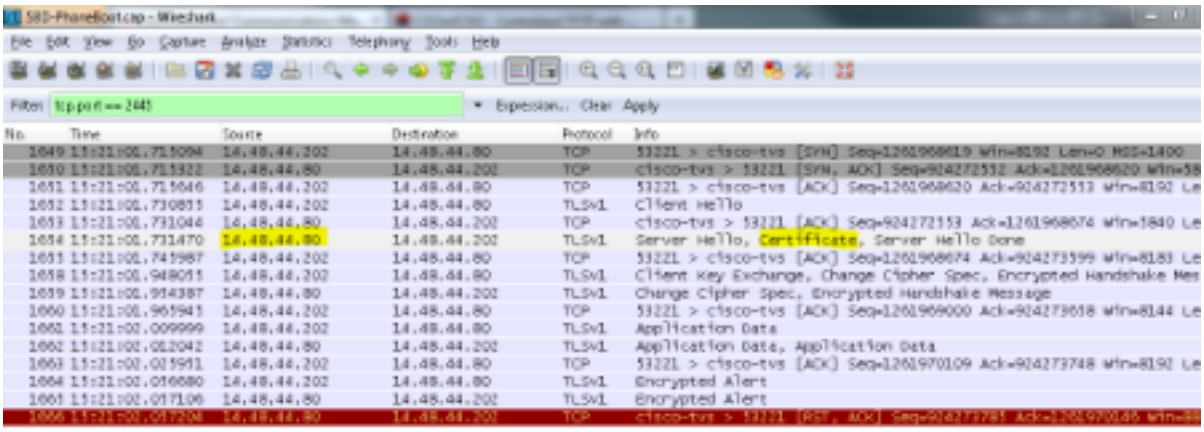


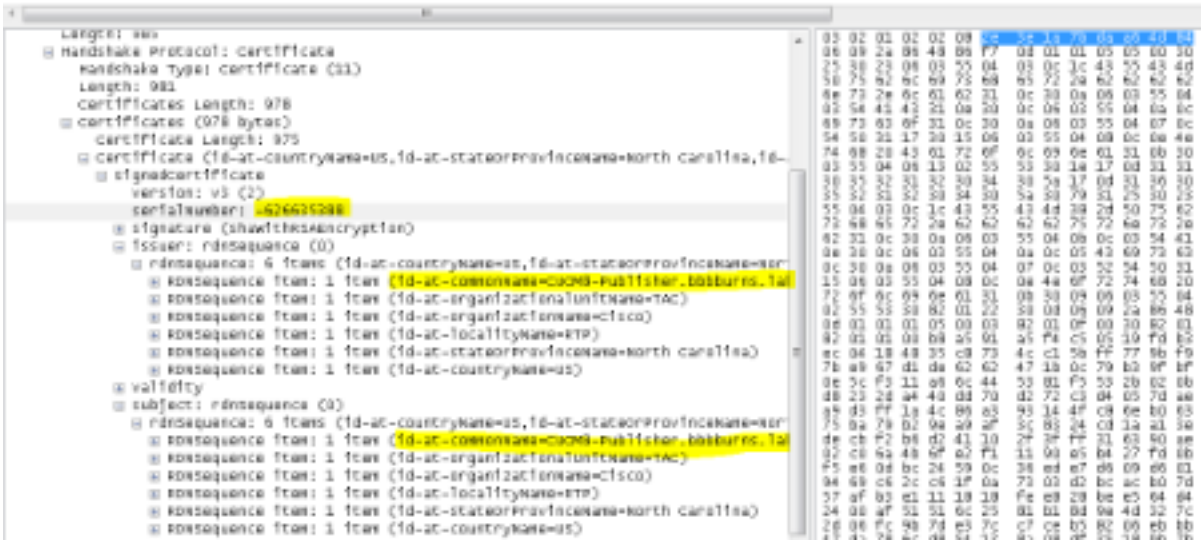
Isto mostra a isso o fósforo MD5sums. Isto significa que o arquivo ITL no telefone combina o arquivo no CUCM, assim que não precisa de ser suprimido.

Se combina, você precisa de transportar-se sobre à operação seguinte - determine mesmo se o certificado TV na ITL combina o certificado apresentado por TV. Esta operação é um pouco mais involvida.

Primeiramente, olhar na captura de pacote de informação do telefone que conecta aos TV o server na porta TCP 2445.

Clicar com o botão direito em todo o pacote neste córrego em Wireshark, o clique **descodifica como**, e seleciona o **SSL**. Encontre o certificado de servidor que olha como este:





Olhe o certificado TV contido dentro do arquivo precedente ITL. Você deve ver uma entrada com o número de série **2E3E1A7BDAA64D84**.

```
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
```

O sucesso, o **TVS.pem dentro do** arquivo ITL combina o certificado TV apresentado na rede. Você não precisa de suprimir da ITL, e os TV apresentam o certificado correto.

Se a autenticação do arquivo ainda falha, verifique o resto do fluxograma precedente.

Limitações e interações

Certificados regenerados/reconstrução um conjunto/expiração do certificado

O certificado o mais importante é agora o certificado CallManager.pem. A chave privada deste certificado é usada a fim assinar todos os arquivos de configuração de TFTP, que inclui o arquivo ITL.

Se o arquivo CallManager.pem é regenerado, um certificado novo CCM+TFTP está gerado com uma chave privada nova. O arquivo ITL é assinado adicionalmente agora por esta chave nova CCM+TFTP.

Depois que você regenera CallManager.pem e reinicia os TV e o serviço TFTP, este acontecer quando botas de um telefone.

1. As tentativas do telefone de transferir o arquivo novo ITL assinado pelo CCM+TFTP novo do servidor TFTP. O telefone tem somente o arquivo velho ITL neste momento, e as chaves novas não estão no arquivo ITL atual no telefone.
2. Desde que o telefone não poderia encontrar a assinatura nova CCM+TFTP na ITL velha, tenta contactar o serviço TV.
   Nota: Esta parte é extremamente importante. O certificado TV do arquivo velho ITL deve ainda combinar. Se os CallManager.pem e TVS.pem são regenerados no mesmo tempo exato, os telefones não podem transferir nenhuns arquivos novos sem suprimir da ITL do telefone manualmente.
3. Quando o telefone contacta TV, o server CUCM que executa TV tem o certificado novo CallManager.pem na loja do certificado do OS.
4. O sucesso dos retornos do server TV e o telefone carregam o arquivo novo ITL na memória.
5. O telefone tenta agora transferir um arquivo de configuração, que seja assinado pela chave nova CallManager.pem.
6. Desde que a ITL nova foi carregada, o arquivo de configuração recentemente assinado é verificado com sucesso pela ITL na memória.

Pontos chaves:

- Nunca regenere os Certificados CallManager.pem e TVS.pem ao mesmo tempo.
- Se TVS.pem ou CallManager.pem são regenerados, os TV e o TFTP devem ser reiniciados e telefonam à restauração a fim obter os arquivos novos ITL. Umas versões mais novas de CUCM seguram este telefone restaurado automaticamente e advertem o usuário no tempo da regeneração do certificado.
- Se mais de um server TV existe (mais de um server no grupo do CallManager), os server adicionais podem autenticar o certificado novo CallManager.pem.

Mova telefones entre conjuntos

Quando você move telefones de um conjunto para outro com ITLs no lugar, a chave privada ITL e TFTP deve ser levada em consideração. Todo o arquivo de configuração novo apresentado ao telefone DEVE combinar uma assinatura no CTL, na ITL, ou em uma assinatura no serviço atual TV do telefone.

Este documento explica como certificar-se que o arquivo e os arquivos de configuração ITL do conjunto novo podem ser confiados pelo arquivo atual ITL no telefone.

https://supportforums.cisco.com/docs/DOC-15799.

Alternativo e restauração

O certificado e a chave privada CallManager.pem são suportados através do sistema da Recuperação de desastres (DR). Se um servidor TFTP é reconstruído, DEVE ser restaurado do backup de modo que a chave privada possa ser restaurada. Sem a chave privada CallManager.pem no server, os telefones com ITLs atual que usam a chave velha não confiam arquivos de configuração assinados.

Se um conjunto é reconstruído e não restaurado do backup, é exatamente como "telefones moventes entre o documento dos conjuntos". Isto é porque um conjunto com uma chave nova é um cluster diferente tanto quanto os telefones.

Há um defeito sério associado com o alternativo e a restauração. Se um conjunto é susceptível à identificação de bug Cisco CSCtn50405, os backup DR não contêm o certificado CallManager.pem. Isto causa todo o server restaurado deste backup para gerar arquivos corrompidos ITL até que um CallManager.pem novo esteja gerado. Se há não outros servidores TFTP funcionais que não atravessaram a operação alternativa e da restauração, este pôde significar que todos os arquivos ITL precisam de ser suprimidos dos telefones.

A fim verificar se seu arquivo CallManager.pem precisa de ser regenerado, incorpore o **comando do** showitl seguido por:

```
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
```

Na saída ITL, os erros chaves a procurar são:

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

e

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

As buscas precedentes da pergunta da língua de consulta estruturada (SQL) para os Certificados que têm um papel da "authentication e autorização." O certificado CallManager.pem na pergunta precedente do base de dados que tem o papel da authentication e autorização deve IGUALMENTE esta presente no página da web do gerenciamento certificado da administração do OS. Se o defeito precedente é encontrado, há uma má combinação entre os Certificados CallManager.pem na pergunta e no página da web do OS.

Mude nomes de host ou Domain Name

Se você muda o hostname ou o Domain Name de um server CUCM, regenera todos os Certificados imediatamente nesse server. A seção da regeneração do certificado explicou que a regeneração do TVS.pem e de CallManager.pem é "uma coisa ruim."

Há algumas encenações onde uma mudança do hostname falha, e algumas onde trabalha sem problemas. Esta seção cobre todo e liga-os de volta ao o que você já sabe sobre TV e ITL deste documento.

Conjunto do nó único com somente ITL (use o cuidado, este quebra sem preparação)

- Com um desenvolvimento do server ou do editor-somente da edição do negócio, os CallManager.pem e TVS.pem estão regenerados ao mesmo tempo quando você muda nomes de host.
- Se o hostname é mudado em um conjunto do nó único sem primeiramente usar o parâmetro empresarial do Rollback coberto aqui, os telefones não podem verificar que o arquivo novo ou os arquivos de configuração ITL contra sua ITL atual arquivam. Adicionalmente, não podem conectar aos TV porque o certificado TV é confiado igualmente já não.
- Os telefones indicam um erro sobre da "a verificação da lista confiança falhada," nenhuma alteração de configuração nova toma o efeito, e o serviço seguro URL falha.
- A única solução se a precaução em etapa 2 não é primeira tomada é suprimir manualmente da ITL de cada telefone.

Conjunto do nó único com o CTL e a ITL (este pode temporariamente se quebrar, mas facilmente ser fixado)

- Depois que você é executado com o rebatismo dos server, torne a colocar em funcionamento o cliente CTL. Isto coloca o certificado novo CallManager.pem no arquivo CTL esse as transferências do telefone.
- Os arquivos de configuração novos, que incluem os arquivos novos ITL, podem ser confiados basearam na função CCM+TFTP no arquivo CTL.
- Isto trabalha porque o arquivo actualizado CTL é confiado baseou em um USB eToken a chave privada que permanece a mesma.

Conjunto do Multi-nó com somente ITL (este trabalha geralmente, mas pode permanentemente se quebrar se feito a toda pressa)

- Porque um conjunto do multi-nó tem server múltiplos TV, todo o servidor único pode ter seus Certificados regenerados sem um problema. Quando o telefone for presentado com este novo, assinatura estranha, pede outros dos server TV para verificar o certificado de servidor novo.
- Há dois problemas principais que podem fazer com que este falhe:
  Se todos os server são rebatizados e recarregados ao mesmo tempo, nenhuns dos server TV são alcançáveis com Certificados conhecidos quando os server e os telefones vêm apoio.Se um telefone tem somente um servidor único no grupo do CallManager, os server adicionais TV não fazem nenhuma diferença. Veja do "a encenação do conjunto nó único" a fim resolver isto, ou adicionar um outro server ao grupo do CallManager do telefone.

Conjunto do Multi-nó com o CTL e a ITL (este não pode permanentemente se quebrar)

- Depois que você é executado com rebatiza, o serviço TV autentica os Certificados novos.
- Mesmo se todos os server TV são não disponíveis por qualquer motivo, o cliente CTL pode ainda ser usado a fim atualizar os telefones com os Certificados novos CallManager.pem CCM+TFTP.

TFTP centralizado

Quando um telefone com as botas ITL, ele pedir estes arquivos: **CTLSEP** ***< MAC address >.tlv***, **ITLSEP** ***< MAC address >.tlv***, e **SEP** ***< MAC address >.cnf.xml.sgn***.

Se o telefone não pode encontrar estes arquivos, pede o **ITLFile.tlv e o** CTLFile.tlv**, que um** servidor TFTP centralizado fornece a todo o telefone que o pedir.

Com TFTP centralizado, há um único conjunto TFTP esses pontos a um número outros de conjuntos secundários. Isto é feito frequentemente porque os telefones em CUCM múltiplo aglomeram a parte o mesmo escopo de DHCP, e deve consequentemente ter o mesmo servidor TFTP da opção de DHCP 150. Todo o ponto dos Telefones IP ao conjunto central TFTP, mesmo se se registram a outros conjuntos. Este servidor TFTP central pergunta os servidores de TFTP remotos sempre que recebe um pedido para um arquivo que não possa encontrar.

Devido a esta operação, o TFTP centralizado trabalha somente em um ambiente homogêneo ITL. Todos os server devem executar a versão 8.x ou mais recente CUCM, ou todos os server devem executar versões antes da versão 8.x.

Se um ITLFile.tlv é apresentado do servidor TFTP centralizado, os telefones não confiam nenhuns arquivos do servidor de TFTP remoto porque as assinaturas não combinam. Isto acontece em uma mistura heterogênea. Em uma mistura homogênea, o telefone pede ITLSEP **<MAC>.tlv que** é puxado do conjunto remoto correto.

Em um ambiente heterogêneo com uma mistura de 8.x pré-versão e de conjuntos da versão 8.x, “prepare o conjunto para o Rollback a pre 8.0" deve ser permitido no conjunto da versão 8.x como descrito na identificação de bug Cisco CSCto87262 e “nos parâmetros de URL fixados do telefone” configurados com o HTTP em vez do HTTPS. Isto desabilita eficazmente as funções ITL no telefone.

Perguntas mais freqüentes

Posso eu desligar o SBD?

Você pode somente desligar o SBD se os SBD e as ITL trabalham atualmente.

O SBD pode temporariamente ser desabilitado em telefones com o conjunto da preparação para o Rollback ao parâmetro empresarial de pre 8.0" e configurando “os parâmetros de URL fixados do telefone” com o HTTP em vez do HTTPS. Quando você ajusta o parâmetro do Rollback, cria um arquivo assinado ITL com as entradas vazias da função. O arquivo “vazio” ITL é assinado ainda, assim que o conjunto deve estar no estado funcional da Segurança a inteiramente - antes que este parâmetro possa ser permitido.

Depois que este parâmetro é permitido e o arquivo novo ITL com entradas vazias está transferido e verificado, os telefones aceitam todo o arquivo de configuração, não importa quem o assinou.

Não se recomenda deixar o conjunto neste estado, porque nenhumas das três funções metioned previamente (arquivos de configuração autenticados, arquivos de configuração cifrados, e HTTPS URL) estão disponíveis.

Posso eu facilmente suprimir do arquivo ITL de todos os telefones uma vez que o CallManager.pem é perdido?

Não há atualmente nenhum método para suprimir de todo o ITLs de um telefone fornecido remotamente por Cisco. É por isso os procedimentos e as interações descritos neste documento são tão importantes de levar em consideração.

Há atualmente um realce não resolvido à identificação de bug Cisco CSCto47052 que pede esta funcionalidade, mas não foi executada ainda.

No ínterim período, uns novos recursos foram adicionados através da identificação de bug Cisco CSCts01319 que pôde permitir que o centro de assistência técnica da Cisco (TAC) reverta à ITL previamente confiada se está ainda disponível no server. Isto trabalha somente em determinados exemplos onde o conjunto está em uma versão com esta solução do defeito, e onde a ITL precedente existe em um backup armazenado em um lugar especial no server. Veja o defeito para ver se sua versão tem o reparo. Contacte o tac Cisco a fim ser executado com o procedimento de recuperação potencial explicado no defeito.

Se o procedimento anterior não está disponível, os botões Phone Button devem ser empurrados manualmente no telefone a fim suprimir do arquivo ITL. Esta é as trocas que são feitas entre a Segurança e a facilidade da administração. Para que o arquivo ITL seja verdadeiramente seguro, ele não deve seja removido facilmente remotamente.

Mesmo com botão baseado num guião pressiona com objetos do simple object access protocol (SABÃO) XML, a ITL não pode remotamente ser removido. Isto é porque, neste momento, o acesso TV (e acesso seguro da autenticação a URL para validar assim o impulso entrante do botão do SABÃO XML objeta) é nonfunctional. Se a autenticação URL não é configurada como segura, pôde ser possível passar pelo processo de script as imprensas chaves a fim suprimir de uma ITL, mas este script não está disponível de Cisco.

Outros métodos a fim passar pelo processo de script imprensas chaves remotas sem usar a autenticação URL puderam estar disponíveis de uma terceira parte, mas estes aplicativos não são fornecidos por Cisco.

Mais frequentemente o método usado a fim suprimir da ITL é uma transmissão do email a todos os usuários do telefone que os instrua da sequência chave. Se o acesso dos ajustes é ajustado **restrito** ou **deficiente**, o telefone precisa de ser restauração da fábrica, porque os usuários não têm o acesso ao menu de configurações do telefone.