



Certificate Management – UC Portfolio

Presenter – Vasanth Kumar K, Amit Sharma

Panelist – Manjunath Junnur

16th March 2016

Agenda

- Certificates Basics
- Cisco Video Infrastructure(Expressway, Jabber Guest, TPS, Conductor)
- Cisco Unified Communications Manager (PKI, TVS, certificate regenerations, Phone PKI)
- Cisco Unified IM and P server (Trust Store)
- Troubleshooting (Common Issues)



Cisco Video Infrastructure

(Expressway, Jabber Guest, TPS, Conductor)

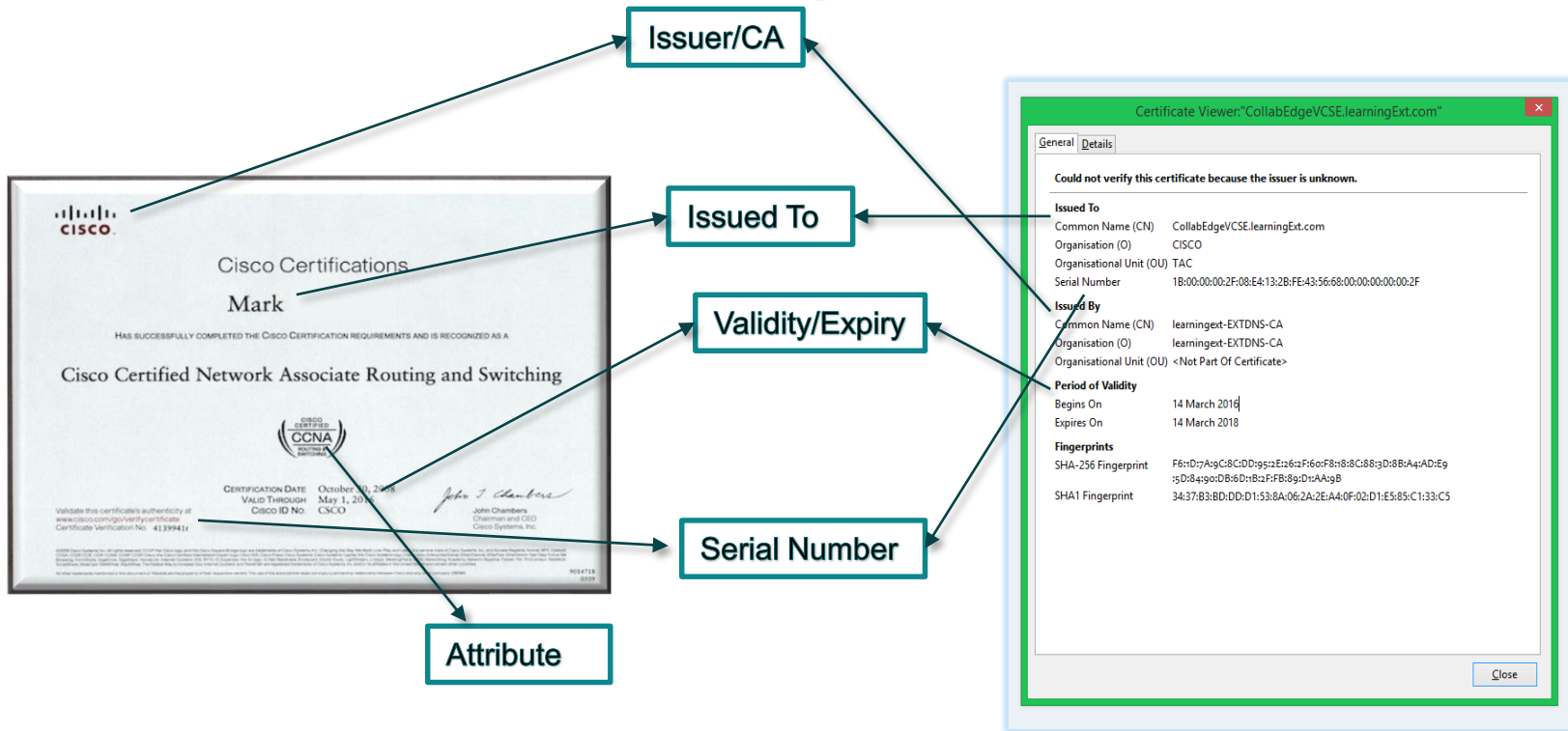
▪

Zoltan Kelemen, Amit Sharma

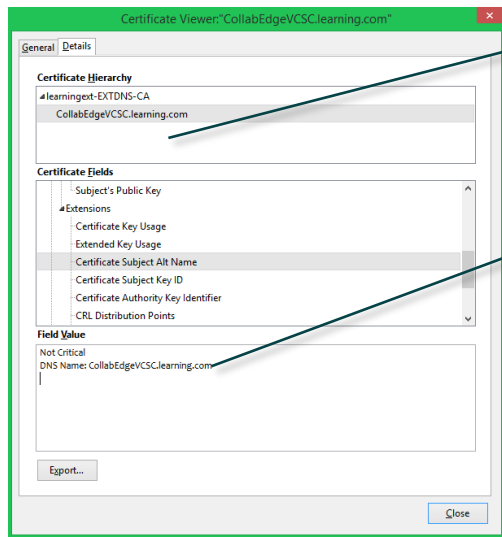
Agenda

- Certificates: What are they (*Basic Overview*)
- Certificates for Expressway: How to get them (*CSR generation/ uploading Certs*)
- Certificates on Other TP Devices
- Troubleshooting (*Common Issues*)

Certificates: What are they

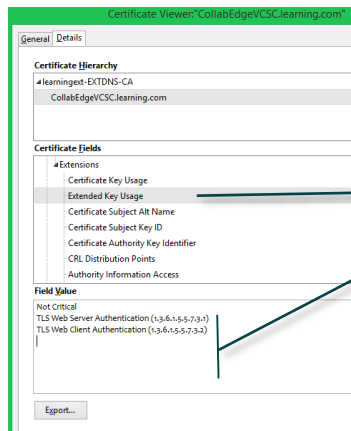


Certificates: What are they



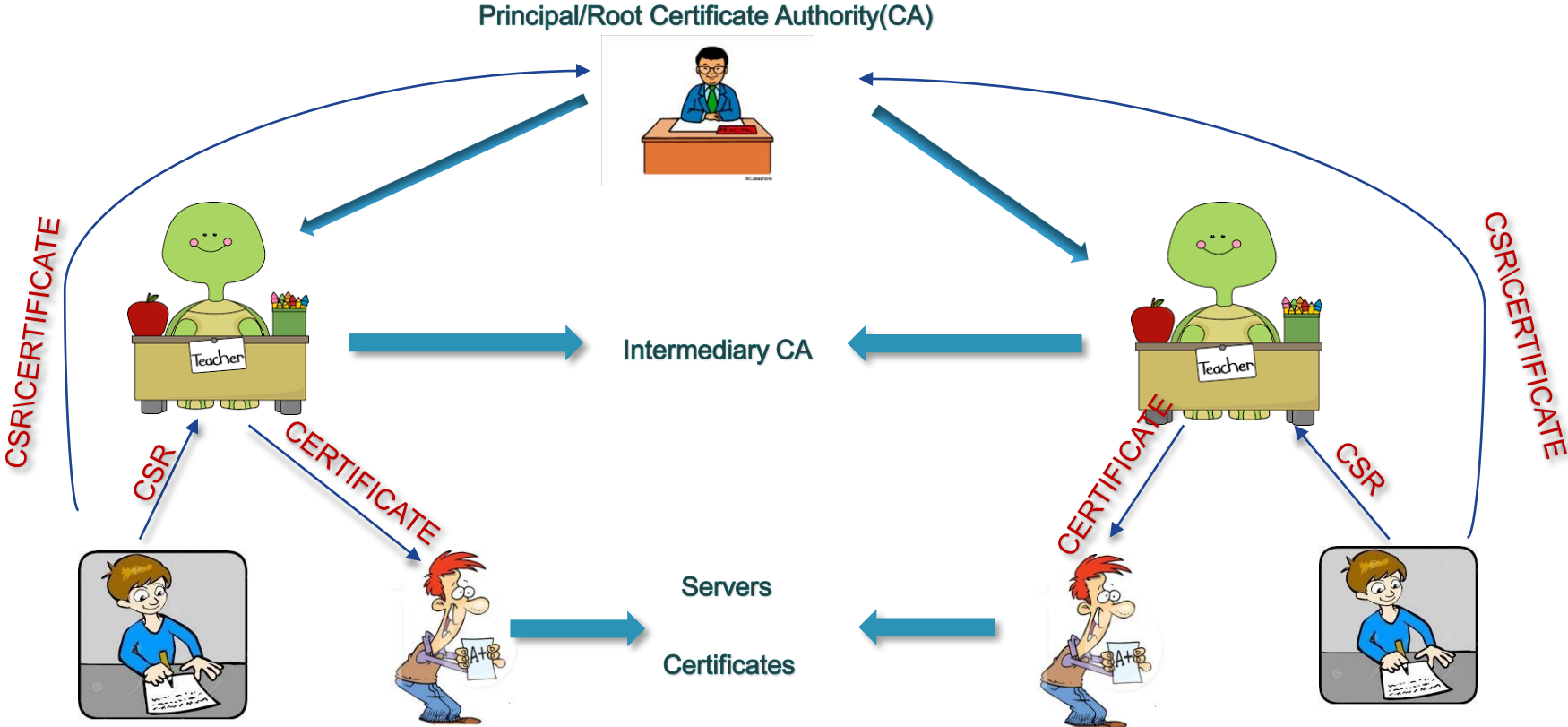
Hierarchy: who issued the certificate

SAN: Additional FQDNs/Domains to be put here. Put in as many information here(not more than 999 characters)



Attributes required in the certificate

Certificates: How to Get them



Obtaining Certificates: Who to Chose

- Two options:
 - Use in-house, “**enterprise CA**” (Microsoft / Linux)
 - Request a signed certificate from a “**public CA**”
- Technically both kinds are equivalent.
- The difference is
 - **Trust**: do your devices/end-users trust your internal CA?
 - **Cost**: internal certificates are usually free, public certificates have recurring costs associated with them
- Rule of thumb:
 - use **internal** certificates on internal devices (e.g. Expressway-C)
 - use **public** certificates on devices facing the public (Expressway-E)

Certificates in Telepresence.

It's not optional anymore

Certificates Expressway: WHY

- **Secured Communication:**

 - Secure HTTP with TLS (HTTPS) connectivity

 - TLS connectivity for SIP signaling, endpoints and neighbor zones

 - Connections to other systems such as Unified CM, Cisco TMS,LDAP servers etc.

- **MRA:**

 - Self Signed Certificates do not work

 - Traversal Zone between C and E must be secured.

 - Client communication with VCS-E must be encrypted.

 - Communication between VCS-C and CUCM should be over TLS (optional)

Certificates Expressway: HOW To Get Them contd..

Generate Certificate Signing Request

The screenshot shows the 'Maintenance' page in the Cisco Expressway interface. The 'Server certificate' section is active, and a dropdown menu is open, showing 'Server certificate' selected. The 'Generate CSR' button at the bottom left is highlighted with a red arrow.

- This will also generate a **private key that remains on Expressway**, it cannot be downloaded
- Only **one CSR request** at a time
- CSR can be **downloaded or viewed** in browser
- CSR **can be discarded**
- **Digest algorithm:SHA-256(Default)**, options:SHA-1, SHA-384, or SHA-512

The screenshot shows the 'Generate CSR' configuration page. The 'Common name' is set to 'FQDN of VCS cluster' and 'vcs-c.kelzotta.local'. The 'Alternative name' section is expanded, showing 'Subject alternative names' set to 'None' and 'Additional alternative names' set to 'vcs-c'. The 'Additional information' section is also expanded, showing 'Key length (in bits)' set to 4096, 'Digest algorithm' set to SHA-256, and various location and organizational details. The 'Generate CSR' button at the bottom left is highlighted with a red arrow.

Certificates Expressway: HOW To Get Them contd..

Fill in the required information in the CSR: SAN

Certificates must contain **several names** either in Subject CN or SAN fields depending on the feature

CSR SAN element	MRA	JabberGuest	XMPP federation
Cluster (if used) and node FQDN	Both	Both	Both
Public domain or collab-edge.<domain>	E only	X	X
Unified CM registration domains	E only	X	X
Unified CM phone security profile names	C only	X	X
XMPP federation domains	X	X	E only
IM&P chat node aliases (federated group chat)	X	X	Both

Certificates Expressway: HOW To Get Them contd..

Fill in the required information in the CSR: SAN

CUPADMIN > Messaging > Group Chat Server Alias Mapping

Generate CSR You are here: Maintenance > Security certificates > Generate CSR

Common name

Common name: FQDN of Expressway
Common name as it will appear: xwayc.coluc.com

Alternative name

Additional alternative names (comma separated):
IM and Presence chat node aliases: **conference-2-ecup9.coluc.com**
Unified CM phone security profile names: csf-secure
Alternative name as it will appear: xwayc.coluc.com,conference-2-ecup9.coluc.com,csf-secure

Additional information

Key length (in bits): 4096
Country: * BE
State or province: * BRABANT
Locality (town name): * DIEGEM
Organization (company name): * CISCO
Organizational unit: * TAC

[Generate CSR](#)

Primary Group Chat Server Aliases

Primary Group Chat Server Alias	Node Name
conference-2-ecup9.coluc.com	ecup.coluc.com

Group Chat Server Alias Rows per Page: 50

Find Group Chat Server Alias where Group Chat Server Alias begins with [Find](#) [Clear Filter](#) [+](#) [-](#)

No active query. Please enter your search criteria using the options above.

[Add New](#)

Group Chat Server Alias (1 - 1 of 1) Rows per Page: 50

<input type="checkbox"/>	Group Chat Server Alias	Node Name
<input type="checkbox"/>	conference-2-ecup9.coluc.com	ecup.coluc.com

[Add New](#) [Select All](#) [Clear All](#) [Delete Selected](#)

Certificates Expressway: HOW To Get Them contd..

Request Certificates from the CA

- Certificates must be in PEM format for use on the VCS.
- Wild Cards (*.example.com) is not supported by VCS. Less Secure
- Both Expressway certificates **must** have **Server and Client** Extended Key Usage

```
X509v3 extensions:  
X509v3 Key Usage: critical  
    Digital Signature, Key Encipherment  
X509v3 Extended Key Usage:  
    TLS Web Server Authentication, TLS Web Client Authentication  
X509v3 Subject Alternative Name:  
    DNS:exp-e.kelzolta.com, DNS:kelzolta.local, DNS:collab-edge.kelzolta.com, DNS:exp-e  
X509v3 Subject Key Identifier:  
    38:23:A8:84:42:CB:95:71:25:14:20:D4:29:69:81:3F:6A:3C:4A:6A
```

- Request for the Root/Intermediate CA certificates from the CA.

Certificates Expressway: HOW To Get Them contd..

Uploading Server Certificate

The screenshot displays the Cisco Expressway-E web interface. At the top, the Cisco logo and 'Cisco Expressway-E' are visible. The navigation menu includes Status, System, Configuration, Applications, Users, and Maintenance. The 'Maintenance' menu is expanded, showing options like Upgrade, Logging, Option keys, Tools, Security certificates (highlighted), Backup and restore, Diagnostics, Maintenance mode, Language, and Restart options. The 'Security certificates' sub-menu is also expanded, showing Trusted CA certificate, Server certificate (highlighted), CRL management, Client certificate testing, and Certificate-based authentication configuration. The main content area shows a 'Server certificate' section with a message: 'CSR creation successful: Certificate Signing Request saved.' Below this is a 'Server certificate data' section with a 'Reset to default server certificate' button. The 'Certificate signing request (CSR)' section shows the certificate request and the date it was generated (Mar 14 2016). The 'Upload new certificate' section has two 'Browse...' buttons for selecting the private key and certificate files. A blue arrow points to the 'Browse...' button for the certificate file.

Only one server certificate at a time
Restart of Expressway required

Certificates Expressway: HOW To Get Them contd..

Uploading Root/Intermediate certificates to Expressway

The screenshot shows the Cisco Expressway Maintenance interface. The 'Trusted CA certificate' section is active, displaying a table of certificates. The table has columns for Type, Issuer, Expiration date, Validity, and View. Below the table are buttons for 'Show all (decoded)', 'Show all (PEM file)', 'Delete', 'Select all', and 'Unselect all'. An 'Upload' section is visible with a 'Browse...' button. At the bottom, there are buttons for 'Append CA certificate' and 'Reset to default CA certificate', both highlighted with red arrows.

Type	Issuer	Expiration date	Validity	View
<input type="checkbox"/> Certificate	CN=learningS-EXTERNALDNS-CA	Aug 05 2019	Valid	View (decoded)
<input type="checkbox"/> Certificate	CN=learningExt-CA-SERVER-CA	Nov 15 2019	Valid	View (decoded)
<input type="checkbox"/> Certificate	CN=learningext-EXTDNS-CA			

- Can have **several certificates**
- **Trusted Root and intermediate** certificates go in this store, including the CA certificates signing the Expressways own certificate
- Root/Intermediate certificates signing the other Expressway's cert, CUCM's cert etc.

Certificates Expressway – External CSR

- Possible to use **externally requested** certificate
- If there's **no active CSR** on Expressway
- The **private key will need to be uploaded** together with the certificate
- Keys longer than **4096bits** should not be used

The screenshot displays the Cisco Expressway Certificate Management interface. It features two main sections: 'Certificate signing request (CSR)' and 'Upload new certificate'. The 'Certificate signing request (CSR)' section shows a 'Certificate request' field with the message 'There is no certificate signing request in progress' and a 'Generate CSR' button. The 'Upload new certificate' section is highlighted with a green border and contains two rows of file selection options: 'Select the server private key file' and 'Select the server certificate file'. Each row has a 'Browse...' button and the text 'No file selected.' To the right of each row is an information icon (i). Below the 'Upload new certificate' section is an 'Upload server certificate data' button.

Certificates on Other Telepresence Devices

Certificates : CONDUCTOR

- Certificate management almost **identical to Expressway**
- Since XC4.0 you can **add FQDNs to each virtual IP**
- These should be **added to SAN** for secure trunks with CUCM and Mutual TLS with TS

Cisco TelePresence Conductor

Status System Conference configuration Users Maintenance

Generate CSR

You are here: Maintenance

Common name

Common name FQDN of Con

Common name as it will appear CNDTR.learn

Alternative name

Additional alternative names (comma separated)

Alternative name as it will appear DNS:CNDTR.learning.com

Additional information

Key length (in bits) 4096

Country * BE

State or province * BRUSSELS

Locality (town name) * DIEGEM

Organization (company name) * Cisco

Organizational unit * TAC

Generate CSR

Alternative name

Additional alternative names :tor,conductor-rv.kelzolta.local,conductor-ah.kelzolta.local

(comma separated)

Alternative name as it will appear DNS:conductor.kelzolta.local
DNS:conductor
DNS:conductor-rv.kelzolta.local
DNS:conductor-ah.kelzolta.local

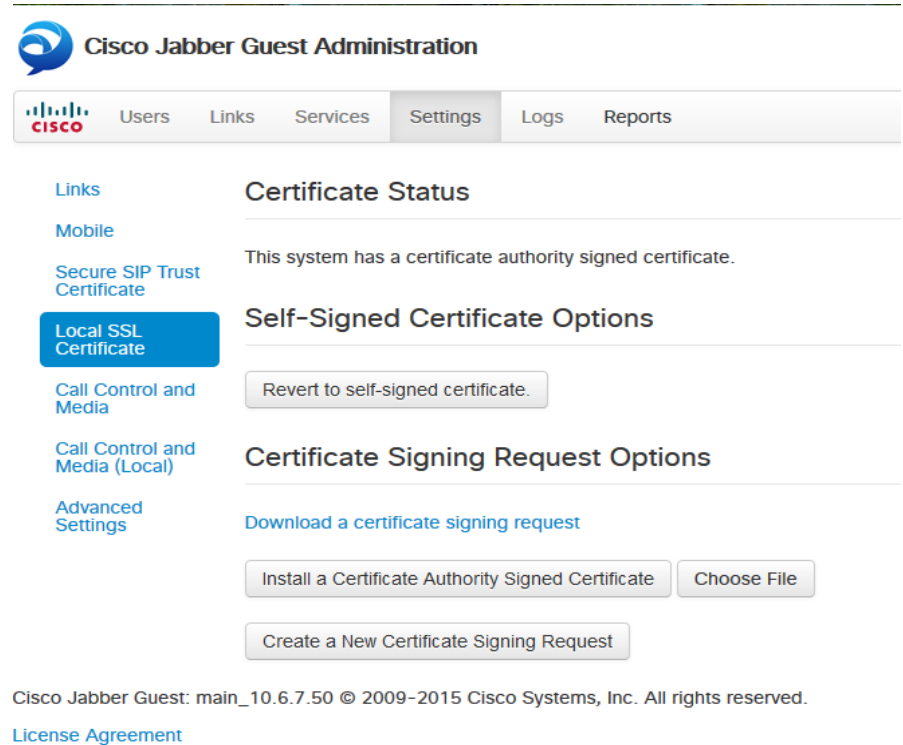
Certificates : Telepresence Server / MCU

- **Cannot generate its own CSR**
- All **trusted certificates** must be uploaded **in one file**, each upload overwrites the “trust store”
- Certificate verification by default turned off.

The screenshot displays the Cisco TelePresence Server web interface. The top navigation bar includes Status, Network, Configuration, Conferences, Users, and Logs. The main content area is titled "SSL certificates" and features a table with columns for Subject, Issuer, and Issued. A table entry shows a certificate issued on 20120524 09:17:43 by an issuer with the subject "/C=GB/ST=Berkshire/L=Langleigh/O=Unknown". Below the table, there are sections for "Local certificate configuration" with fields for Certificate, Private key, and Private key encryption password, each with a "Browse..." button and a "No file selected." message, and an "Upload certificate and key" button. The "Trust store" section shows "No trust store certificates present" and a "Delete trust store" button. The "Trust store configuration" section has a "Trust store" field with a "Browse..." button and a "No file selected." message, and an "Upload trust store" button. At the bottom, the "Certificate verification settings" section shows a dropdown menu set to "No verification" and an "Apply changes" button with a blue link that says "A trust store is required to enable certificate verification".

Certificates : Jabber Guest

- GUI offers only very **basic CSR**
- More advanced certificate management must be performed from **Linux CLI** (see Install Guide for details)
- All members of a cluster must have respective certificates



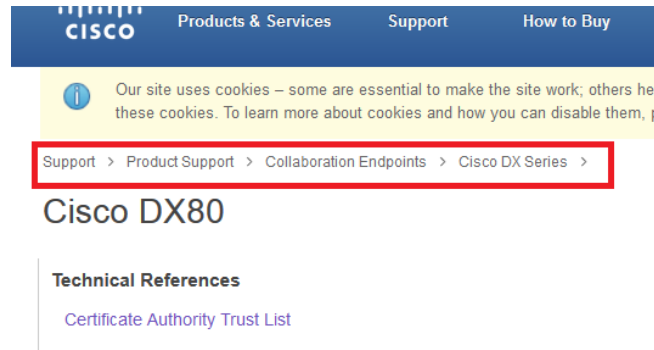
The screenshot displays the Cisco Jabber Guest Administration interface. At the top, the Cisco logo and the title "Cisco Jabber Guest Administration" are visible. Below the title is a navigation menu with tabs for "Users", "Links", "Services", "Settings" (which is selected), "Logs", and "Reports". On the left side, there is a sidebar menu with options: "Links", "Mobile", "Secure SIP Trust Certificate", "Local SSL Certificate" (highlighted in blue), "Call Control and Media", "Call Control and Media (Local)", and "Advanced Settings". The main content area is titled "Certificate Status" and contains the following information:

- Certificate Status**: This system has a certificate authority signed certificate.
- Self-Signed Certificate Options**: A button labeled "Revert to self-signed certificate."
- Certificate Signing Request Options**: A link "Download a certificate signing request" and three buttons: "Install a Certificate Authority Signed Certificate", "Choose File", and "Create a New Certificate Signing Request".

At the bottom of the page, the text reads: "Cisco Jabber Guest: main_10.6.7.50 © 2009-2015 Cisco Systems, Inc. All rights reserved." followed by a link for "License Agreement".

Certificates : DX Series / 78XX / 88XX

- If you plan to use DX series endpoints or 78XX/88XX phones across MRA, Expressway-E Certificates **must be signed by a public CA** in the pre-installed CA Trust List.
- Any other certificates will be disregarded by these devices.
- List can be downloaded from [cisco.com](https://www.cisco.com)



Certificates : TCS / TMS

- As both are Windows-based appliances, they both rely on the Windows Certificate stores and can be mostly managed through Windows certificate utilities.
<https://technet.microsoft.com/en-us/library/cc771377%28v=ws.10%29>
- TMS accounts will need read access to the private keys
- TMS Tools enables to check client certificate to be used when TMS authenticates itself to remote systems

Troubleshooting

common issues and how to solve them

Troubleshooting: Viewing Certificates

Click on the small lock

Click here

More Details

Click "More Information"

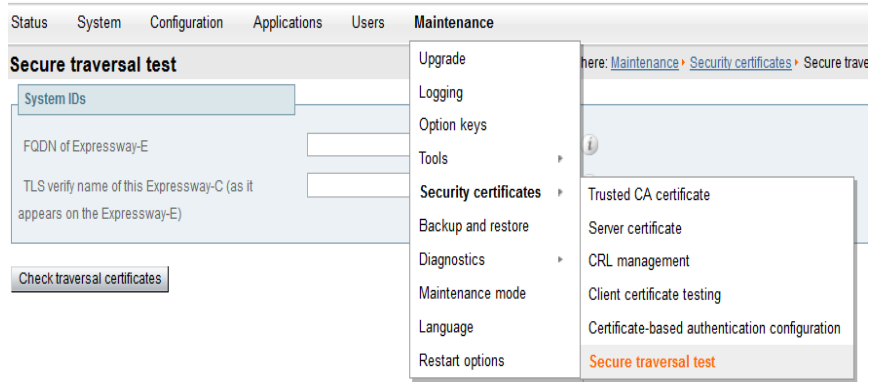
View Certificate

More Details

More Details

Troubleshooting: MRA/Traversal Zones Failing

- Expressway has a **built-in tool** for certificate verification:
- Secure Traversal Test** (Expressway-C / Expressway-C only). This utility tests whether a secure connection can be made from the Expressway-C to the Expressway-E



The screenshot shows the Cisco Expressway Maintenance menu. The 'Maintenance' tab is selected, and a dropdown menu is open. The 'Secure traversal test' option is highlighted in orange. The breadcrumb path is 'Maintenance > Security certificates > Secure traversal test'.

System IDs

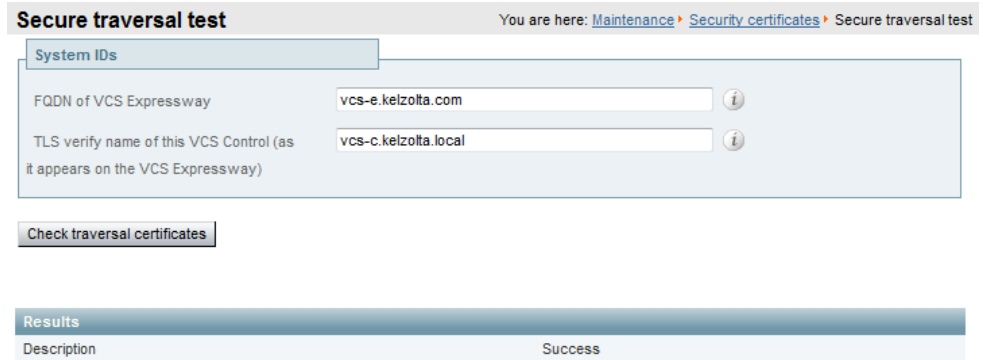
FQDN of Expressway-E

TLS verify name of this Expressway-C (as it appears on the Expressway-E)

Check traversal certificates

Maintenance

- Upgrade
- Logging
- Option keys
- Tools
- Security certificates
 - Trusted CA certificate
 - Server certificate
 - CRL management
 - Client certificate testing
 - Certificate-based authentication configuration
 - Secure traversal test**
- Backup and restore
- Diagnostics
- Maintenance mode
- Language
- Restart options



The screenshot shows the 'Secure traversal test' configuration page. The breadcrumb path is 'You are here: Maintenance > Security certificates > Secure traversal test'.

System IDs

FQDN of VCS Expressway: vcs-e.kelzolta.com

TLS verify name of this VCS Control (as it appears on the VCS Expressway): vcs-c.kelzolta.local

Check traversal certificates

Results

Description	Success

Troubleshooting: Common Issues

- Certificates not installed
- Certificates were created with Server Authentication only
- Trust store not populated with required intermediate and root certificates
- IP used instead of FQDN for neighbor peers
- FQDN entered in peer list and/or TLS verify hostname does not match Subject CN or SAN of certificate

Troubleshooting: Common Issues

- Certificate (externally requested) with a 8192 bit key length – this is not supported.
- Uploaded private key file missing a newline at the end of the file (may cause service issues with MRA)
- Unsupported OIDs in the certificates (ssh tunnels may fail) – please follow Certificate Creation and Use Guides for Expressway/Expressway
subject=CN=blahdeblah,OU=IT Security,O=BigBang,L=Washington,ST=District of Columbia,C=US,1.3.6.1.4.1.6449.1.2.1.5.1 = #060C2B06010401B2310102010501
- Wild cards not supported (*.example.com)


Troubleshooting: WebServer-Client Attribute Absent



Cisco Expressway-E

Status System Configuration Applications Users **Maintenance**

Server certificate

 **Invalid certificate:** The file provided does not have a client usage attribute. The certificate must be usable for both servers and clients for Unified Communications.

Server certificate data

Server certificate

[Show \(decoded\)](#) [Show \(PEM file\)](#)


Currently loaded certificate expires on

Sep 22 2017

[Reset to default server certificate](#)

[Certificate signing request \(CSR\)](#)

Server certificate

 **Invalid certificate:** The file provided does not have a server usage attribute

Server certificate data

Server certificate

[Show \(decoded\)](#) [Show](#)

Troubleshooting: Root/Intermediate CA cert not uploaded

Status	System	Configuration	Applic
Overview			
Alarms			
System	>		
Calls	>		
Search history			
Local Zone			
Zones			
Bandwidth	>		
Policy services			
Unified Communications		ssh: Event="sshd"	
Applications	>	-15 21:38:48"	
Hardware		ssh: Event="sshd"	
Logs	>	=2016-03-15 21:38	
		Event Log	
		Configuration Log	
		Network Log	
2016-03-15T22:38:48+01:00		ssh: event="sshd"	
2016-03-15T22:38:48+01:00		-15 21:38:48"	

xwayc tvcs: Event="Outbound TLS Negotiation Error" Service="SIP" Src-ip="10.48.55.98" Src-port="25016" Dst-ip="10.48.55.99" **Dst-port="7001"** Detail="tlsv1 alert unknown ca" Protocol="TLS" Common-name="xwayc.coluc.com" Level="1" UTCtime="2014-03-24 17:33:30,872"

Results

2014-03-24T17:36:30+00:00

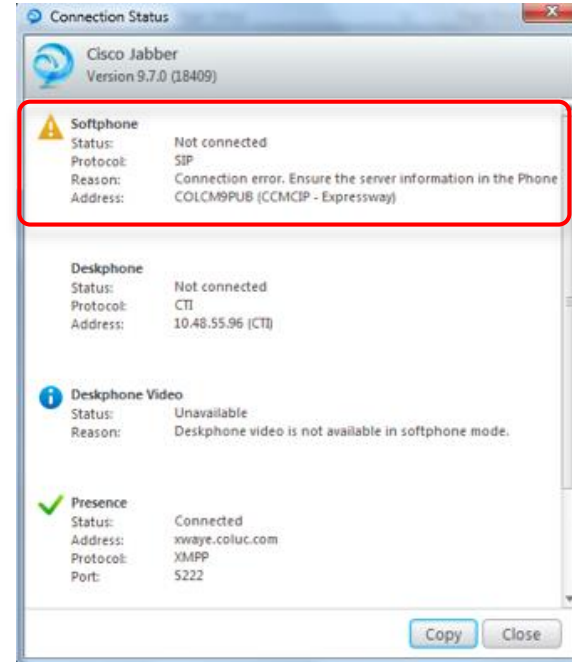
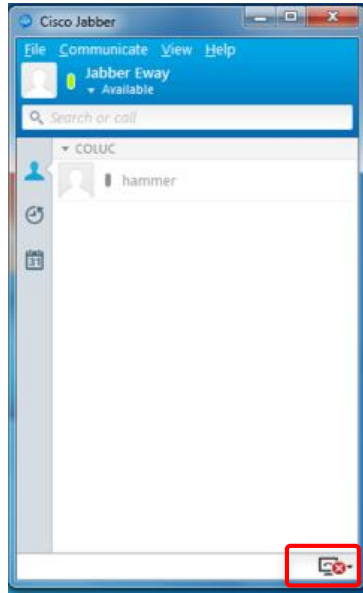
tvcs: Event="Outbound TLS Negotiation Error" Service="SIP" Src-ip="10.48.55.98" Src-port="25025" Dst-ip="10.48.55.99" Dst-port="7001" Detail="tlsv1 alert unknown ca" Protocol="TLS" Common-name="xwayc.coluc.com" Level="1" UTCtime="2014-03-24 17:36:30,872"

Troubleshooting: Certificate Presented does not match FQDN

```
2016-03-15T22:27:33+01:00 CollabEdgeVCSC management: UTCTime="2016-03-15 21:27:33,709"
Module="developer.management.cucmconfig" Level="WARN" CodeLocation="ucqueryrun(100)" Detail="Certificate
validation failed" Host="pub10.learning.com" Error="Server presented certificate that does not match host
pub10.learning.com: {'crlDistributionPoints': (u'ldap:///CN=learningext-EXTDNS-
CA,CN=EXTDNS,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=learningext,DC=com
?certificateRevocationList?base?objectClass=cRLDistributionPoint',), 'subjectAltName': (('DNS', 'learning.com'),),
'notBefore': u'Sep 29 21:39:35 2015 GMT', 'calssuers': (u'ldap:///CN=learningext-EXTDNS-
CA,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=learningext,DC=com?cACertificate?
base?objectClass=certificationAuthority',), 'serialNumber': u'1B0000000F30A1FC854C3F21DE00000000000F',
'notAfter': 'Sep 29 21:49:35 2017 GMT', 'version': 3L, 'subject': (((('countryName', u'BE'),), (('stateOrProvinceName',
u'Brussels'),), (('localityName', u'Diegem'),), (('organizationName', u'Cisco'),), (('organizationalUnitName', u'TAC'),),
(('commonName', u'pub.learning.com'),)), 'issuer': (((('domainComponent', u'com'),), (('domainComponent',
u'learningext'),), (('commonName', u'learningext-EXTDNS-CA'),))})"
```

Troubleshooting: Security Profile not listed in Expressway-C SAN

- Softphone Registration fails (other will work) when endpoint security settings are authenticated or encrypted



Troubleshooting: Certificate Expiry

CISCO Cisco Expressway-E

Status System Configuration Applications Users **Maintenance**

Server certificate

Server certificate data

Server certificate

Show (decoded)

Show (PEM file)

Currently loaded certificate expires on

Sep 22 2017

Reset to default server certificate



CISCO Cisco Expressway-E

Status System Configuration Applications Users **Maintenance**

[Help](#) [Logout](#)

Trusted CA certificate

You are here: [Maintenance](#) > [Security certificates](#) > Trusted CA certificate

Failed: Expired certificates or CRLs detected in trusted CA file

Type	Issuer	Subject	Expiration date	Validity	View
Certificate	O=Temporary CA 35f12f8-7456-41e3-a387-005056974a0d, OU=Temporary CA 35f12f8-7456-41e3-a387-005056974a0d, CN=Temporary CA 35f12f8-7456-41e3-a387-005056974a0d	Matches Issuer	Jan 13 2019	Valid	View (decoded)
Certificate	CN=MCDEAN	Matches Issuer	Sep 25 2006	Expired	View (decoded)

[Show all \(decoded\)](#) [Show all \(PEM file\)](#) [Delete](#) [Select all](#) [Download all](#)

Troubleshooting: Extract Certificates from Wireshark

Filter the packets on the secured port

Right Click → Decode As → SSL

No.	Time	Source	Destination	Protocol	Length	Info
2	2016-03-14 10:00:20.473082	10.48.80.47	10.48.36.101	TCP	74	25010 → 7001 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=429250218 TSecr=0
3	2016-03-14 10:00:20.474343	10.48.36.101	10.48.80.47	TCP	74	7001 → 25010 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1380 SACK_PERM=1 TSval=...
4	2016-03-14 10:00:20.474384	10.48.80.47	10.48.36.101	TCP	66	25010 → 7001 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=429250218 TSecr=421144501
5	2016-03-14 10:00:20.489789	10.48.80.47	10.48.36.101	TLSv1.2	292	Client Hello
6	2016-03-14 10:00:20.490318	10.48.36.101	10.48.80.47	TCP	66	7001 → 25010 [ACK] Seq=1 Ack=227 Win=30080 Len=0 TSval=421144517 TSecr=429250234
7	2016-03-14 10:00:20.505488	10.48.36.101	10.48.80.47	TLSv1.2	1434	Server Hello
8	2016-03-14 10:00:20.505520	10.48.80.47	10.48.36.101	TCP	66	25010 → 7001 [ACK] Seq=227 Ack=1369 Win=32128 Len=0 TSval=429250249 TSecr=42114...
9	2016-03-14 10:00:20.505550	10.48.36.101	10.48.80.47	TCP	1434	[TCP segment of a reassembled PDU]
10	2016-03-14 10:00:20.505566	10.48.80.47	10.48.36.101	TCP	66	25010 → 7001 [ACK] Seq=227 Ack=2737 Win=35072 Len=0 TSval=429250249 TSecr=42114...
11	2016-03-14 10:00:20.505570	10.48.36.101	10.48.80.47	TLSv1.2	971	Certificate
12	2016-03-14 10:00:20.505582	10.48.80.47	10.48.36.101	TCP	66	25010 → 7001 [ACK] Seq=227 Ack=2737 Win=35072 Len=0 TSval=429250249 TSecr=42114...
13	2016-03-14 10:00:20.506093	10.48.80.47	10.48.36.101	TLSv1.2	73	Alert (Level: Fatal, Description: Unknown CA)
14	2016-03-14 10:00:20.506102	10.48.36.101	10.48.80.47	TCP	66	7001 → 25010 [FIN, ACK] Seq=3642 Ack=235 Win=30080 Len=0 TSval=421144534 TSecr=...
15	2016-03-14 10:00:20.507175	10.48.36.101	10.48.80.47	TCP	66	7001 → 25010 [FIN, ACK] Seq=3642 Ack=235 Win=30080 Len=0 TSval=421144534 TSecr=...
16	2016-03-14 10:00:20.507197	10.48.80.47	10.48.36.101	TCP	66	25010 → 7001 [ACK] Seq=235 Ack=3643 Win=37760 Len=0 TSval=429250251 TSecr=42114...
453	2016-03-14 10:00:40.473483	10.48.80.47	10.48.36.101	TCP	74	25013 → 7001 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=429270217 T...
454	2016-03-14 10:00:40.473989	10.48.36.101	10.48.80.47	TCP	74	7001 → 25013 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1380 SACK_PERM=1 TSval=...
455	2016-03-14 10:00:40.474031	10.48.80.47	10.48.36.101	TCP	66	25013 → 7001 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=429270218 TSecr=421164501
456	2016-03-14 10:00:40.486918	10.48.80.47	10.48.36.101	TCP	292	25013 → 7001 [PSH, ACK] Seq=1 Ack=1 Win=29312 Len=226 TSval=429270231 TSecr=421...

Frame 13: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)
Ethernet II, Src: Vmware_99:23:cb (00:50:56:99:23:cb), Dst: CiscoInc_29:96:c8 (00:1b:54:29:96:c8)
Internet Protocol Version 4, Src: 10.48.80.47, Dst: 10.48.36.101
Transmission Control Protocol, Src Port: 25010 (25010), Dst Port: 7001 (7001), Seq: 227, Ack: 3642, Len: 7
Secure Sockets Layer
 * TLSv1.2 Record Layer: Alert (Level: Fatal, Description: Unknown CA)
 Content Type: Alert (21)
 Version: TLS 1.2 (0x0303)
 Length: 2
 * Alert Message
 * Alert (Fatal) (3)
 Description: Unknown CA (48)

Offset	Destination	Protocol	Length	Info
0	10.48.36.101	TCP	74	25010 → 7001 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=429250218 TSecr=0
8	10.48.80.47	TCP	74	7001 → 25010 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1380 SACK_PERM=1 TSval=...
16	10.48.36.101	TCP	66	25010 → 7001 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=429250218 TSecr=421144501
24	10.48.80.47	TLSv1.2	292	Client Hello
32	10.48.36.101	TCP	66	7001 → 25010 [ACK] Seq=1 Ack=227 Win=30080 Len=0 TSval=421144517 TSecr=429250234
40	10.48.80.47	TLSv1.2	1434	Server Hello
48	10.48.36.101	TCP	66	25010 → 7001 [ACK] Seq=227 Ack=1369 Win=32128 Len=0 TSval=429250249 TSecr=42114...
56	10.48.80.47	TCP	1434	[TCP segment of a reassembled PDU]
64	10.48.36.101	TCP	66	25010 → 7001 [ACK] Seq=227 Ack=2737 Win=35072 Len=0 TSval=429250249 TSecr=42114...
72	10.48.80.47	TLSv1.2	971	Certificate
80	10.48.36.101	TCP	66	25010 → 7001 [ACK] Seq=227 Ack=2737 Win=35072 Len=0 TSval=429250249 TSecr=42114...
88	10.48.80.47	TLSv1.2	73	Alert (Level: Fatal, Description: Unknown CA)
96	10.48.36.101	TCP	66	7001 → 25010 [FIN, ACK] Seq=3642 Ack=235 Win=30080 Len=0 TSval=421144534 TSecr=...
104	10.48.80.47	TCP	66	25010 → 7001 [ACK] Seq=235 Ack=3643 Win=37760 Len=0 TSval=429250251 TSecr=42114...
112	10.48.36.101	TCP	74	25013 → 7001 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=429270217 T...
120	10.48.80.47	TCP	74	7001 → 25013 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1380 SACK_PERM=1 TSval=...
128	10.48.36.101	TCP	66	25013 → 7001 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=429270218 TSecr=421164501
136	10.48.80.47	TCP	292	25013 → 7001 [PSH, ACK] Seq=1 Ack=1 Win=29312 Len=226 TSval=429270231 TSecr=421...



Troubleshooting: Extract Certificates from Wireshark *contd..*

If port not known, try filtering using SSL protocol

The screenshot shows the Wireshark interface with a packet capture filtered by 'ssl'. The packet list pane displays the following data:

No.	Time	Source	Destination	Protocol	Length	Info
5	2016-03-14 10:00:20.489789	10.48.80.47	10.48.36.101	TLSv1.2	292	Client Hello
7	2016-03-14 10:00:20.505488	10.48.36.101	10.48.80.47	TLSv1.2	1434	Server Hello
11	2016-03-14 10:00:20.505570	10.48.36.101	10.48.80.47	TLSv1.2	971	Certificate
13	2016-03-14 10:00:20.506093	10.48.80.47	10.48.36.101	TLSv1.2	73	Alert (Level: Fatal, Description: Unknown CA)
20	2016-03-14 10:00:20.835510	144.254.7.92	10.48.80.47	TCP	60	[TCP segment of a reassembled PDU]
23	2016-03-14 10:00:21.245408	10.48.80.47	144.254.7.92	TLSv1.2	107	Encrypted Alert
65	2016-03-14 10:00:25.841451	10.48.80.47	144.254.7.92	TLSv1.2	107	Encrypted Alert
71	2016-03-14 10:00:26.315922	10.48.80.47	144.254.7.92	TLSv1.2	1019	Application Data
72	2016-03-14 10:00:26.320402	144.254.7.92	10.48.80.47	TLSv1.2	699	Application Data
75	2016-03-14 10:00:26.586083	10.48.80.47	144.254.7.92	TLSv1.2	2814	Application Data, Application Data
76	2016-03-14 10:00:26.586042	10.48.80.47	144.254.7.92	TLSv1.2	2509	Application Data
78	2016-03-14 10:00:26.586782	10.48.80.47	144.254.7.92	TLSv1.2	1459	Application Data
83	2016-03-14 10:00:26.602672	10.48.80.47	144.254.7.92	TLSv1.2	2814	Application Data, Application Data
84	2016-03-14 10:00:26.602722	10.48.80.47	144.254.7.92	TLSv1.2	1581	Application Data
86	2016-03-14 10:00:26.602929	10.48.80.47	144.254.7.92	TLSv1.2	1523	Application Data
91	2016-03-14 10:00:26.621765	10.48.80.47	144.254.7.92	TLSv1.2	2814	Application Data, Application Data
92	2016-03-14 10:00:26.621798	10.48.80.47	144.254.7.92	TLSv1.2	615	Application Data
95	2016-03-14 10:00:26.741690	144.254.7.92	10.48.80.47	TLSv1.2	779	Application Data
97	2016-03-14 10:00:26.748971	144.254.7.92	10.48.80.47	TLSv1.2	763	Application Data

The packet details pane for the selected packet (No. 11) shows the following structure:

- Transmission Control Protocol, Src Port: 7001 (7001), Dst Port: 25010 (25010), Seq: 2737, Ack: 227, Len: 905
- [3 Reassembled TCP Segments (2750 bytes): #7(1310), #9(1368), #11(72)]
- Secure Sockets Layer
 - TLSv1.2 Record Layer: Handshake Protocol: Certificate
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 2745
 - Handshake Protocol: Certificate
 - Handshake Type: Certificate (11)
 - Length: 2741
 - Certificates Length: 2738
 - Certificates (2738 bytes)
 - Certificate Length: 1833
 - Certificate: 308207253082060da00302010202113b000000ccd344ca8... (id-at-commonName=CollabEdgeVCE.learningExt.com,id-at-organizationalUnitName=TAC,id-at-organizationName=CISCO,id-at-organizationalUnitName=CISCO)
 - Certificate Length: 899
 - Certificate: 3082037f30820267a00302010202103ff2e799f2c453b246... (id-at-commonName=learningext-EXTDNS-CA,dc=learningext,dc=com)

Further reading

Further reading

- Certificate Creation and Use Deployment Guide for Expressway/Expressway
<https://tools.cisco.com/squish/CCFb3>
- Microsoft TechNet: Manage Certificates (for TMS and TCS)
<https://technet.microsoft.com/en-us/library/cc771377%28v=ws.10%29>
- Jabber Guest Server Installation and Configuration Guide
<https://tools.cisco.com/squish/4E445>



Cisco UC Infrastructure

(CUCM, IP Phone Endpoint, IMP)

▪

Vasanth Kumar, Manjunath Junnur

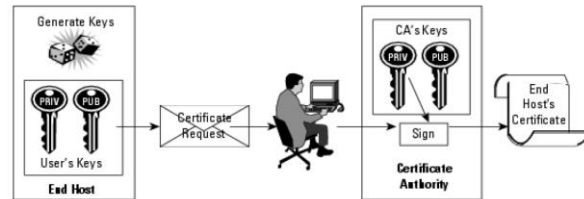
Unified Communications - Agenda

1. UCM Public Key Infrastructure
2. IP Phone PKI
3. Trust Verification Service
4. Certificate Monitor Daemon
5. Certificate Regeneration and ITL Recovery
6. IM and Presence Certificates
7. Troubleshooting Scenario (Some known Caveats) and further Reading

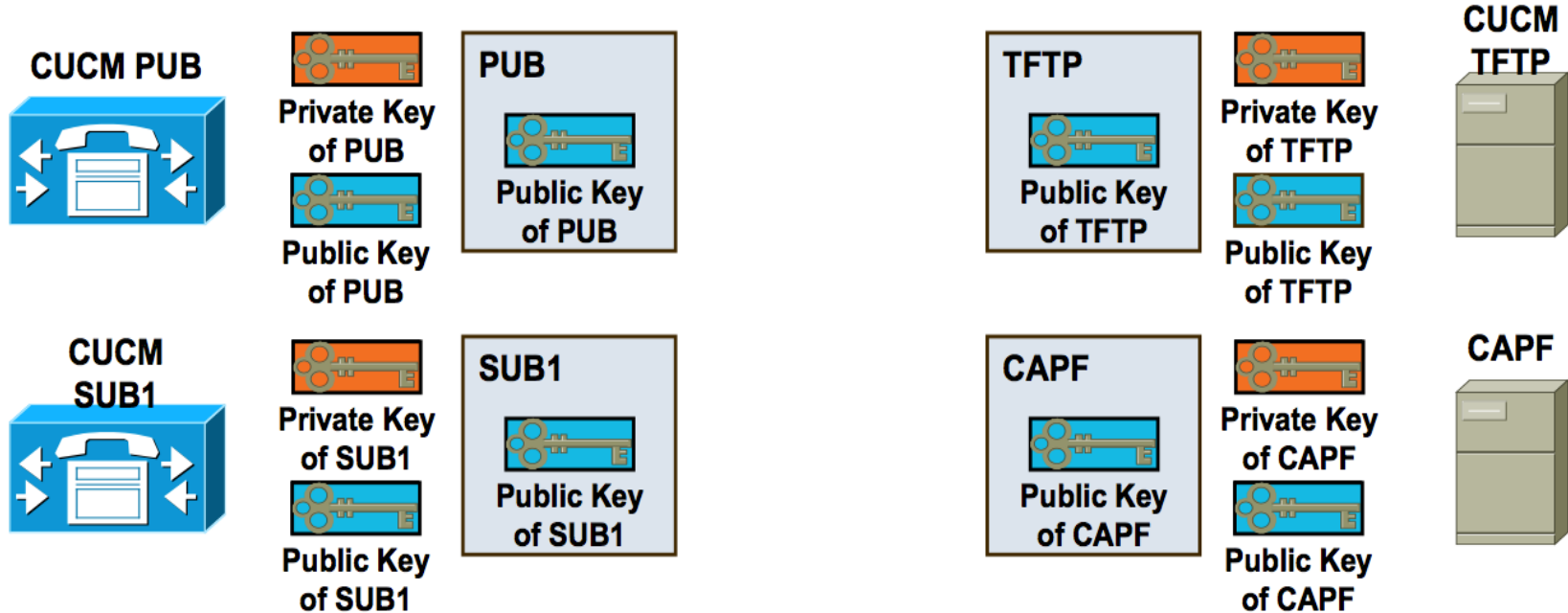
UCM Public Key Infrastructure

Encryption with the public key is decrypted with the private key and vice versa

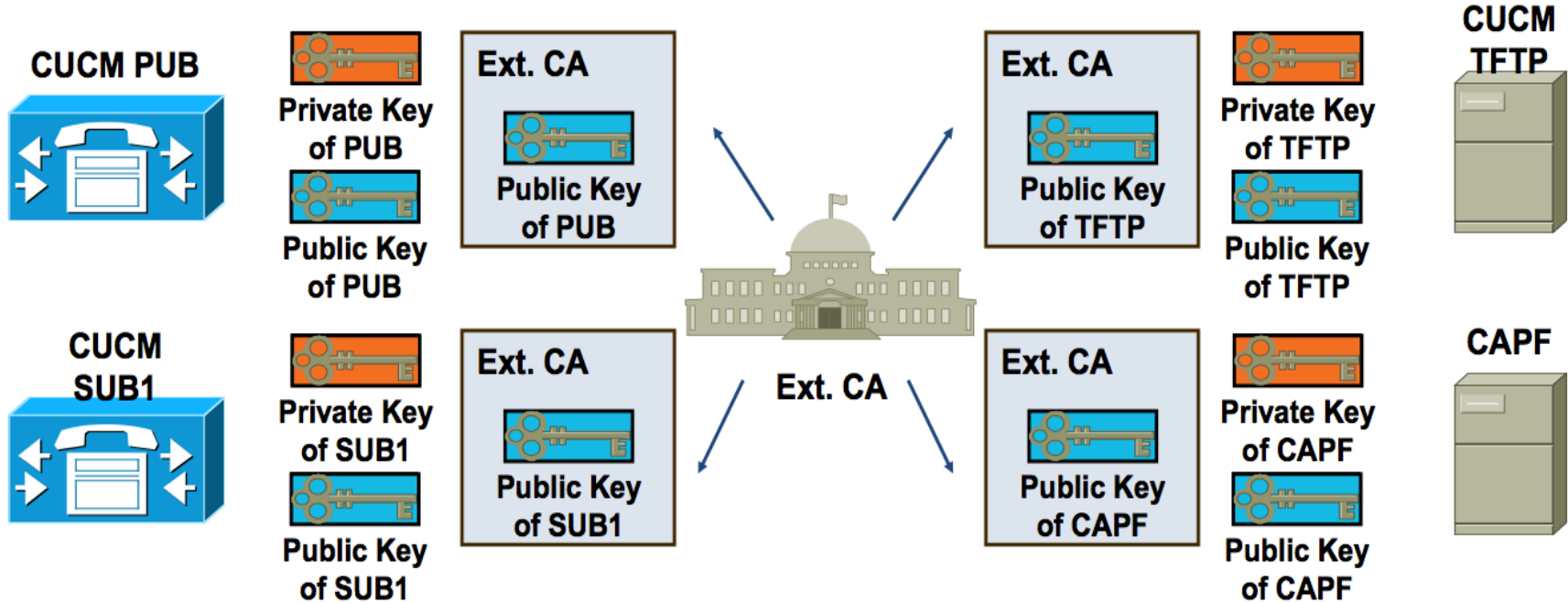
Each server has a public key, private key, and certificate signed by the Certificate Authority



UC Server Certificates in CUCM



UC Externally Signed CA Architecture



Services and Certificate

- Cisco Tomcat (Network) – tomcat/tomcat-trust
- Cisco DRF Master/Local (Network) – ipsec/ipsec-trust
- Cisco CallManager (Feature Service) – callmanager/callmanager-trust
- Cisco TFTP (Feature Service) - callmanager/callmanager-trust
- Cisco CAPF (Feature Service) capf/capf-trust
- Cisco Trust Verification Service (Network Service) – tvs/tvs-trust

Self – Signed Certificates

```
admin:show cert list own
```

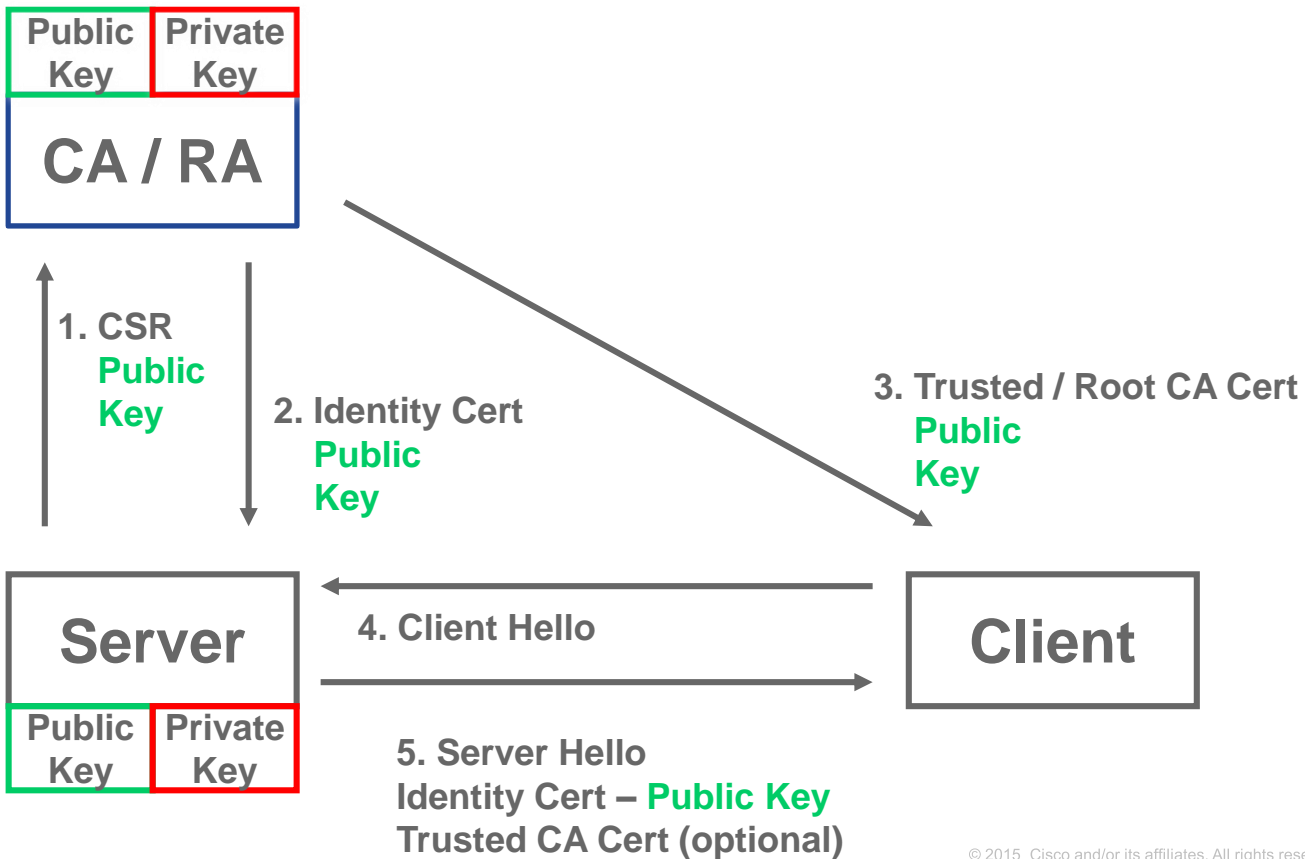
```
tomcat/tomcat.pem: Self-signed certificate generated by system  
ipsec/ipsec.pem: Self-signed certificate generated by system  
CallManager/CallManager.pem: Self-signed certificate generated by system  
CAPF/CAPF.pem: Self-signed certificate generated by system  
TVS/TVS.pem: Self-signed certificate generated by system
```

```
LA2\LA2.bew: Self-signed certificate generated by system
```

- Certificates Validity of 5 Years
- CallManager , CAPF, ipsec certificates are generated using 1024 bit RSA Key (UCM 10 onwards 2048 bit RSA Key)
- Tomcat and TVS are generated using 2048 bit RSA Key
- CSR for the services used to get it signed by 3rd party CA

Certificate Signing Request – Use with CA

- Cisco Unified Communications Operating System supports certificates that a third-party CA issues with PKCS#10 Certificate Signing Request (CSR).
- Cisco Unified Communications Manager supports
 - Privacy Enhanced Mail (PEM) Base64 encoded format of X.509 certificate (only one PEM certificate in a file), Distinguished Encoding Rules (DER) format of X509 Certificate
 - DER format of PKCS#7 (Public-Key Cryptography Standards) Certificate Chain. The system does not support PEM format of PKCS#7 Certificate Chain.



CA Requirements for Signing CSR

- Key Size of CA
- Additional of Attributes by CA
- Extended Key Usage : ServerAuthentication, ClientAuthentication
- Key Usage : DigitalSignature, keyEncipherment, DataEncipherment, keyCertSign.
- Key Usage with critical attribute set to true

Service Trust-Store

```
admin:show cert list trust

tomcat-trust/cm9sub.pem: Trust Certificate
tomcat-trust/cm9.pem: Trust Certificate
tomcat-trust/VeriSign_Class_3_Secure_Server_CA_-_G3.pem: Trust Certificate
ipsec-trust/cm9.pem: Trust Certificate
CallManager-trust/CAPF-be0b40de.pem: Trust Certificate
CallManager-trust/cm9sub.pem: Trust Certificate
CallManager-trust/Leaf3.vasank.com.pem: Signed Certificate
CallManager-trust/CAPF-f21b4acd.pem: Signed Certificate
CallManager-trust/CAP-RTP-002.pem: Trust Certificate
CallManager-trust/Cisco_Manufacturing_CA.pem: Signed Certificate
CallManager-trust/iosra.pem: Signed Certificate
CallManager-trust/CAP-RTP-001.pem: Signed Certificate
CallManager-trust/SKIGW2414BB5BDF_CN_00_24_14_BB_5B_DF.pem: Signed Certificate
CallManager-trust/Cisco_Root_CA_2048.pem: Signed Certificate
CAPF-trust/CAPF-f21b4acd.pem:
CAPF-trust/CAP-RTP-002.pem:
CAPF-trust/Cisco_Manufacturing_CA.pem:
CAPF-trust/CAP-RTP-001.pem:
CAPF-trust/Cisco_Root_CA_2048.pem:
Phone-VPN-trust/10.105.131.60.pem: Signed Certificate
```

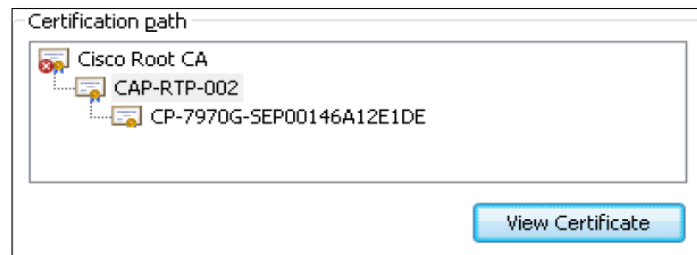
Trust Store Description

Trust Store Name	Common Usage
tomcat-trust	3rd party CA certificates, LDAP Directory Server certificate or CA cert chain, Other CUCM cluster Tomcat certificates for EMCC or ILS
ipsec-trust	IOS Signed or 3 rd party CA Signed Network Device Certificate for certificate based ipsec tunnel between CUCM and gateway
callmanager-trust	Cisco Root and MFG CA certs to trust MICs (included by default), CAPF certificate to trust Phone's LSC issued by CAPF allowing for TLS secured signaling (included by default), MCU, IOS, ASA, IME, etc.. self-signed certificate (or CA cert chain) to allow for TLS,
tvsv-trust	Only used if TVSV certificate is signed by 3rd Party CA
phone-vpn-trust	IOS or ASA self-signed certificates (or CA cert chain) used for VPN Phone feature
capf-trust	Cisco Root and Mfg CA certs to trust MICs (included by default), 3rd party CA certificates

UC – IP Phone PKI

IP Phone Certificates - MIC

- Cisco IP Phones ship from the factory with a unique MIC preinstalled
- MIC are signed by Cisco CA
- Certificate is Valid for 10 Years
- 2048 bit RSA



Issued to: CP-7970G-SEP00146A12E1DE

Issued by: CAP-RTP-002

Valid from 6/ 8/ 2005 **to** 6/ 8/ 2015

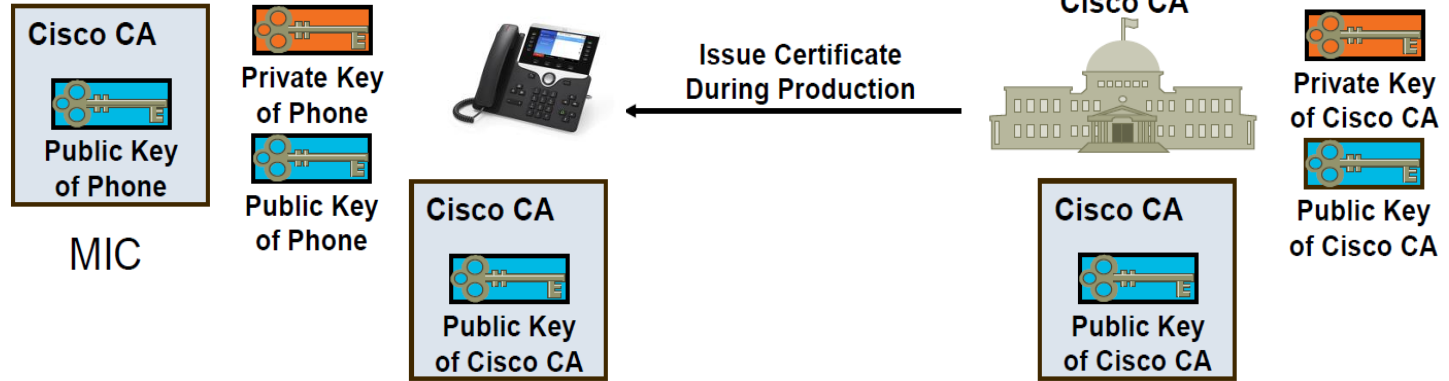
MIC – Best Practices

- Ideal use for building initial LSC for phone
- MIC is installed during manufacturing of phone and cannot be revoked
- LSC takes precedence when both MIC and LSC are present
- Certificates installed to trust MIC is listed below in the screenshot

CAPF-trust/Cisco_Manufacturing_CA.pem:
CAPF-trust/CAP-RTP-001.pem:
CAPF-trust/ACT2_SUDI_CA.pem:
CAPF-trust/Cisco_Root_CA_2048.pem:
CAPF-trust/Cisco_Root_CA_M2.pem:
CAPF-trust/CAP-RTP-002.pem:
CAPF-trust/Cisco_Manufacturing_CA_SHA2.pem:



MIC PKI Topology in CUCM



Locally Significant Certificate

- Certificates Issued to Phone, Jabber Clients and Telepresence Units
- Certificate is Signed by CAPF
- Valid for 5 Years
- RSA Key Size can vary between 512 bytes, 1024 bytes or 2048 bytes

CAPF – Certificate Authority Proxy Function

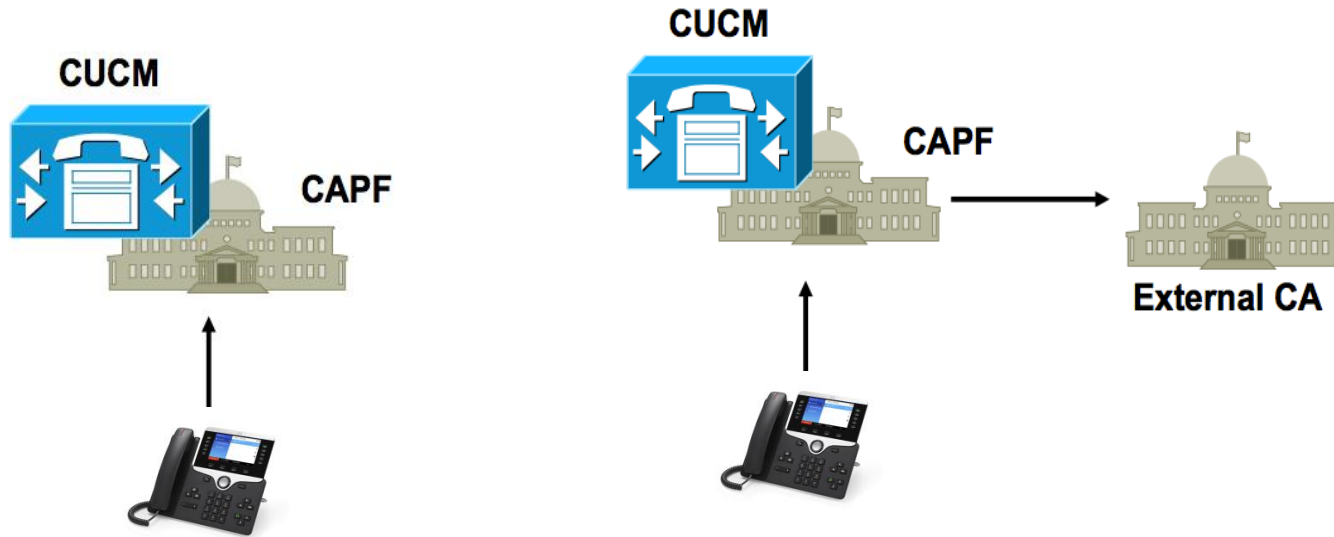
- CAPF Service runs on publisher only (Listening on port 3804)
- Responsible for issuing LSC to phones, clients, etc.
- Multiple options for phones to authenticate with CAPF:

Certificate Authority Proxy Function (CAPF) Information

Certificate Operation*	No Pending Operation
Authentication Mode*	No Pending Operation
Authentication String	Install/Upgrade Delete Troubleshoot
Generate String	<input type="button" value="Generate String"/>
Key Size (Bits)*	1024
Operation Completes By	2014 7 6 12 (YYYY:MM:DD:HH)

Certificate Operation Status: Upgrade Success
Note: Security Profile Contains Addition CAPF Settings.

LSC PKI Topology



LSC is issued by CAPF acting as Root CA

CAPF has certificate issued by external CA

LSC is still issued by CAPF Certificate

IP Telephony Authentication

- Phone contains the CTL and ITL file served by TFTP server
- Phone requests signed configuration file from TFTP server
- TFTP server signs the configuration using the Private Key
- Phone validates the Signed Configuration file
- SEP<MAC>.cnf.xml is parsed and Phone attempts registration

Trust Verification Service

Phones Security drawbacks

- Built around the CTL paradigm: all trusted certificates bundled in a digitally signed file (CTL File). CTL File is downloaded by phones.
- **Issues:**
 - Not scalable: CTL File does not scale well with the growing number of certificates that a phone might need to trust.
 - Not flexible: Every time a new certificate needs to be trusted, CTL File needs to be rebuilt, signed and downloaded to phones. Similarly, every time a certificate should not be trusted anymore, the CTL File needs to be rebuilt, signed and downloaded to phones.
 - Security features that are not media and signaling related (configuration file signing/encryption, https support) cannot be enabled separately.

TVS (Trust Verification Service)

- TVS service provides that security with:
 - Scalability: phones resources are not impacted by the number of certificates to trust.
 - Flexibility: addition or removal of trust certificates are automatically reflected in the system.
 - Non-media and signaling security features are part of the default installation and don't require user intervention.

Note: Enabling secure signaling and media still requires the CTL Client.

TVS Deployment Model

- TVS servers co-exist with each CM node
- Number of TVS servers equals to CM nodes
- Same TVS server distribution scheme for CM servers
- Up to 3 TVS servers configured per phone (primary, secondary and tertiary)
- No support when failover to SRST by phone

TVS Basic Concepts

- TVS runs on the CUCM server and authenticates certificates on behalf of the phone.
- Instead of downloading all the trusted certificates, phones need only to trust TVS.
- The TVS certificates and a few key certificates are bundled in a new file: ITL File (Identity Trust List).
- The ITL File is generated automatically without user intervention.
- The ITL File is downloaded by phones and trust flows from there.

TVS Information

- ITL file contains all TVS credentials:
 - certificates or hashes of certificates
- TVS server information (address, port and priority) is in configuration file
 - Up to 3 TVS servers information
- Only IPv4 support only

Locating TVS information

ITL Record #:8

BYTEPOS	TAG	LENGTH	VALUE
1	RECORDLENGTH	2	739
2	DNSNAME	2	
3	SUBJECTNAME	70	CN=cs-ccm-sub.vasank.com;OU=TAC;O=Cisco;L=Bangalore;ST=Karnataka;C=IN
4	FUNCTION	2	TVS
5	ISSUENAME	70	CN=cs-ccm-sub.vasank.com;OU=TAC;O=Cisco;L=Bangalore;ST=Karnataka;C=IN
6	SERIALNUMBER	16	6D:EE:FF:0E:66:E6:36:93:61:18:C4:05:65:38:C0:CF
7	PUBLICKEY	270	
8	SIGNATURE	256	
11	CERTHASH	20	3D 8D 47 C1 DE 21 70 2B 59 6A 2F 41 BD F2 A8 16 A7 DA D7 46
12	HASH ALGORITHM	1	SHA-1

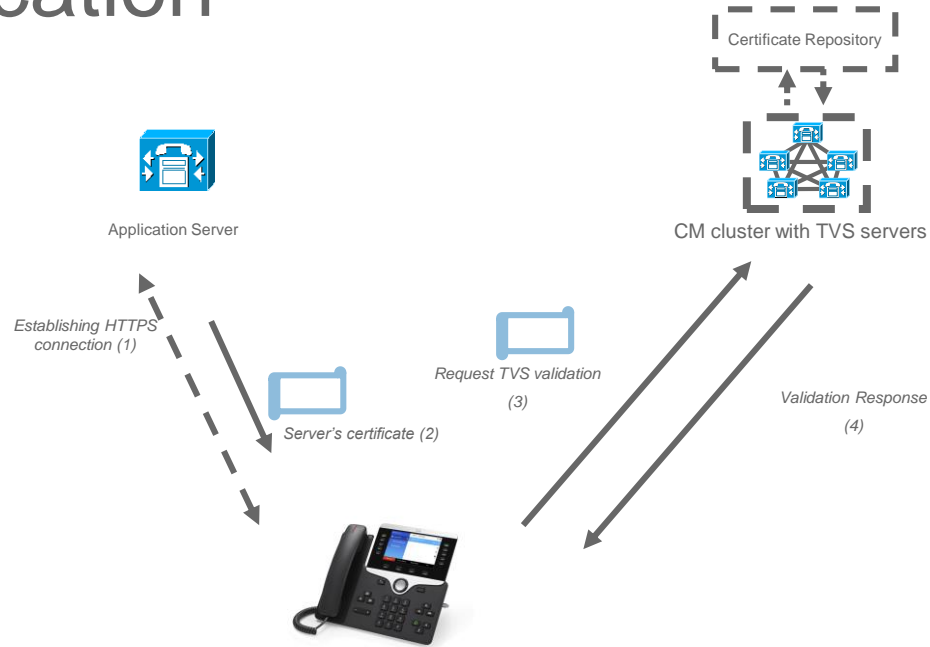
```
<TVS>
  <members>
    <member priority="0">
<port> 2445</port>
      <address> address </address>
    </member>

    ... Up to 2 more members >
  </members>
</TVS>
```

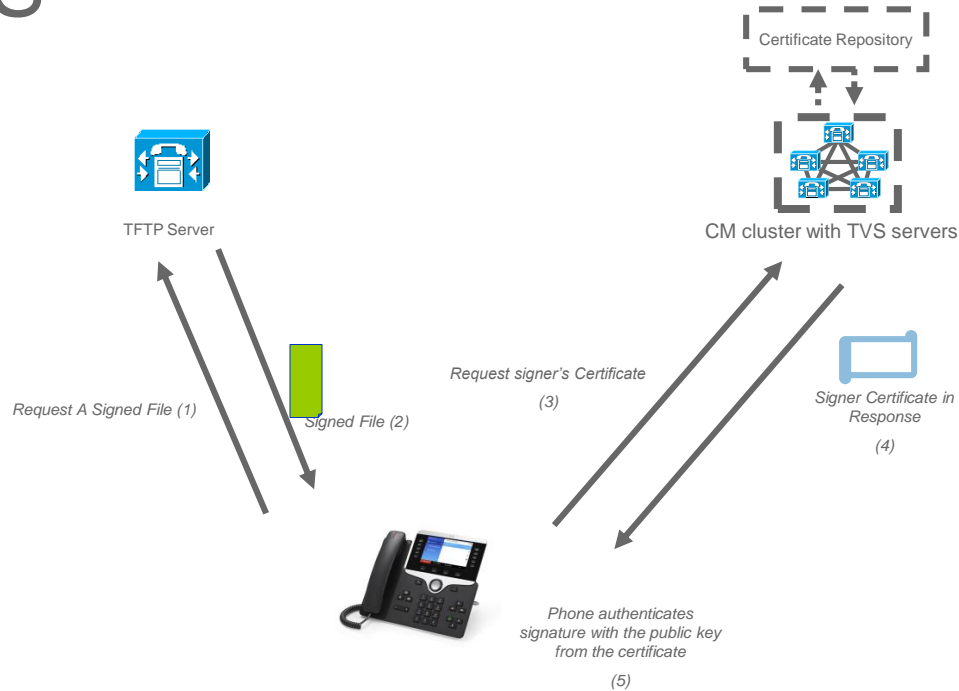
TVS Protocol

- TLS with server authentication only
- Stateless transaction base (request and response)
- Non - persistent connection
- Support multiple requests per TLS session
- 2 Types of Request:
 - Validate a certificate
 - Request a certificate

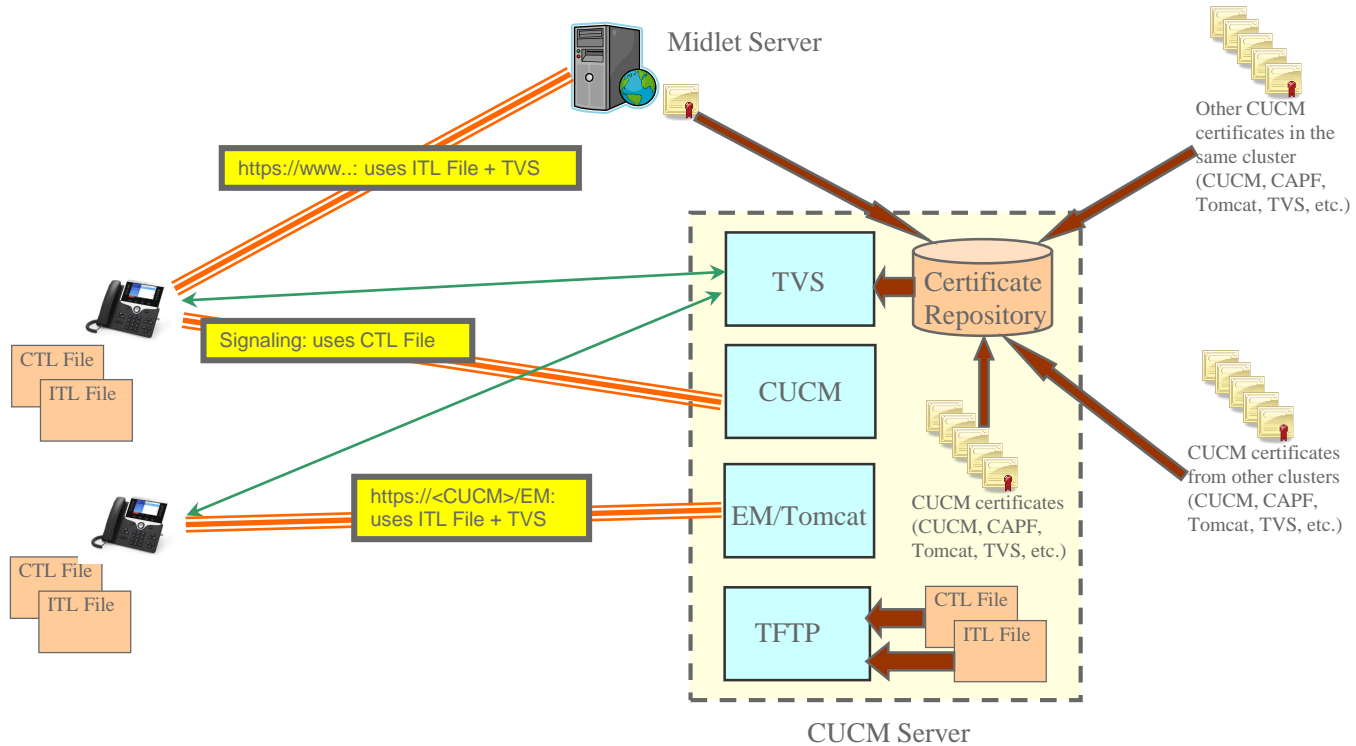
TVS Protocol – Server Certificate Authentication



TVS Protocol – Signed File Authentication with TVS



The Big Picture



SBD (Security by Default)

- SBD refers to security features other than securing call-control signaling and media:
 - Signing of the phone configuration files.
 - Phone configuration file encryption.
 - https with Tomcat and other Web services (Midlets)
- These security features are provided by default in 8.0+ without running the CTL Client.
- Secure Signaling and Media will still require running the CTL Client and using the hardware e-Tokens or Enhanced CTL Method which uses Soft-Token (Introduced in 10.0+)

Certificate Monitor Daemon


Certificate Monitor Alarm Catalog

Alarm Message Definitions

Search Options

Find alarms where Equals* Enter Alarm Name

Status:

 Matching record(s) 1 to 10 of 12 for "CertMonitorAlarmCatalog"

Search Results

Alarm Name	Description	Recommended Action
CertValidLessthanADa...	Certificate is about to Expire...	Re-generate the certificate th...
CertValidfor7days	Alarm to indicate that Certifi...	Re-generate the certificate th...
CertValidityOver30Da...	Alarm to Indicate certificate ...	Re-generate the certificate th...
CertValidLessThanMon...	Alarm that indicates Certifica...	Re-generate the certificate th...
TomcatCertRegen	Alarm that indicates the tomca...	Restart the tomcat service for...
CertificateRevoked	Alarm indicates that recently ...	Delete revoked trust certifica...
CertificateRevokatio...	Alarm indicates that CUCM coul...	Evaluate reason of certificate...
ITLRecoveryCertBacku...	This cluster has an ITLRecover...	Use the CLI command "file get ...
CertExpiryApproachin...	This alarm is Obsolete.	Re-generate the certificate th...
CertExpired	This alarm is Obsolete.	Re-generate the certificate th...




Rows Per Page

Page of 2


Certificate Monitor Feature

Cisco Unified OS Administration > Security > Certificate Monitor

Certificate Monitor

 Save

Status

 Status: Ready

Certificate Monitor Configuration

Notification Start Time**

Notification Frequency* Days Hours

Enable E-mail notification

E-mail IDs

Certificate Regeneration

Scenarios

- Non-Secure Cluster (Certificates are used for Signing purposes and TVS takes care of HTTPS communication)
- Secure Cluster (Certificates are used for Encryption/Decryption and CTL is a must, TVS is still needed for HTTPS communication)

Regenerate tomcat certificate

- Minimal service impact
- Requires restart of Cisco Tomcat Service for the new certificate to take effect.
- Verify if the UCM server has any external integration with AXL, CCMCIP, UDS

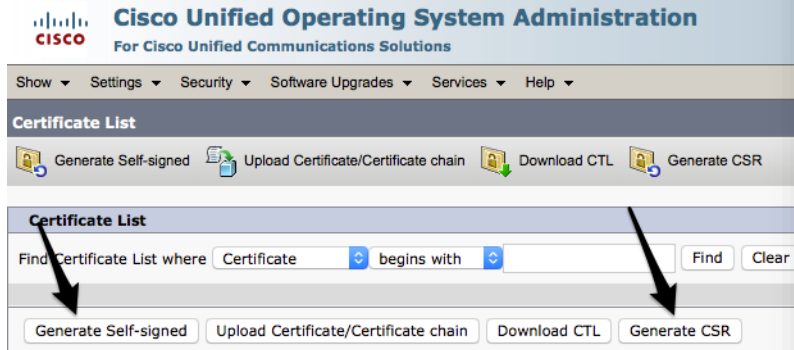
The screenshot displays the Cisco Unified Operating System Administration interface. The main window shows the 'Certificate List' section with a search bar and several action buttons: 'Generate Self-signed', 'Upload Certificate/Certificate chain', 'Download CTL', and 'Generate CSR'. Two black arrows point from the 'Generate Self-signed' and 'Generate CSR' buttons in the main window to the corresponding buttons in the 'Generate New Self-signed Certificate' dialog box. The dialog box has a title bar 'Generate New Self-signed Certificate' and a 'Warning: Generating a new certificate will overwrite any existing certificate information' message. Below the warning, there are several fields for certificate configuration:

Field	Value
Certificate Purpose*	tomcat
Distribution*	cs-ccm-pub.vasank.com
Common Name*	cs-ccm-pub.vasank.com
Key Length*	2048
Hash Algorithm*	SHA256

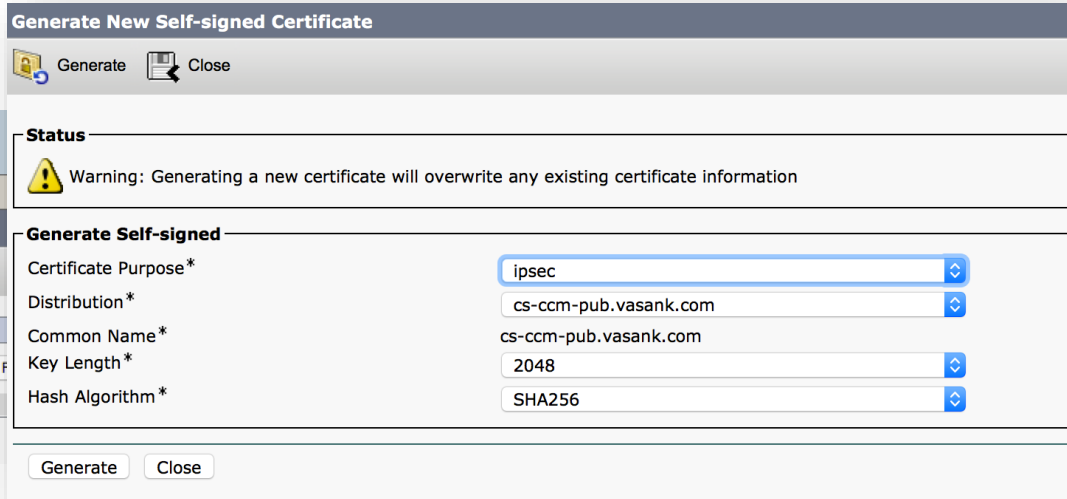
At the bottom of the dialog box, there are 'Generate' and 'Close' buttons.

Regenerate ipsec certificate

- Requires restart of DRF (Master) and Local service on the node
- DRF backup Failure (expired or corrupt certificate)



The screenshot shows the Cisco Unified Operating System Administration interface. The top navigation bar includes "Cisco Unified Operating System Administration" and "For Cisco Unified Communications Solutions". Below this are menu items: "Show", "Settings", "Security", "Software Upgrades", "Services", and "Help". The main content area is titled "Certificate List" and contains several action buttons: "Generate Self-signed", "Upload Certificate/Certificate chain", "Download CTL", and "Generate CSR". A search bar is visible with the text "Find Certificate List where Certificate begins with" and "Find" and "Clear" buttons. Two black arrows point from the search bar area to the "Generate Self-signed" button.



The screenshot shows the "Generate New Self-signed Certificate" dialog box. It has a title bar with "Generate" and "Close" buttons. The "Status" section contains a warning icon and the text: "Warning: Generating a new certificate will overwrite any existing certificate information". The "Generate Self-signed" section contains the following fields:

Certificate Purpose*	ipsec
Distribution*	cs-ccm-pub.vasank.com
Common Name*	cs-ccm-pub.vasank.com
Key Length*	2048
Hash Algorithm*	SHA256

At the bottom of the dialog box are "Generate" and "Close" buttons.

Regenerate ccm certificate

- If the node is TFTP server all phones will be restarted to update ITL file.
- Unregistered phones will be able to update ITL file and will request the new TFTP certificate using TVS service to validate the configuration file.

The screenshot displays the Cisco Unified Operating System Administration interface. The main window is titled "Cisco Unified Operating System Administration" and "For Cisco Unified Communications Solutions". The navigation menu includes "Show", "Settings", "Security", "Software Upgrades", "Services", and "Help". The "Certificate List" section is active, showing a search bar and buttons for "Generate Self-signed", "Upload Certificate/Certificate chain", "Download CTL", and "Generate CSR". Two arrows point from the "Generate Self-signed" button in the main window to the "Generate New Self-signed Certificate" dialog box.

The "Generate New Self-signed Certificate" dialog box has a "Generate" button and a "Close" button. It displays a warning: "Warning: Generating a new certificate will overwrite any existing certificate information". The "Generate Self-signed" section contains the following fields:

Field	Value
Certificate Purpose*	CallManager
Distribution*	cs-ccm-pub.vasank.com
Common Name*	cs-ccm-pub.vasank.com
Key Length*	2048
Hash Algorithm*	SHA256

At the bottom of the dialog box, there are "Generate" and "Close" buttons.

Regenerate tvs certificate

- All the registered phones with callmanager group containing the node will be restarted to update the ITL file.
- Unregistered phone will update ITL using TVS service.

The screenshot shows the Cisco Unified Operating System Administration interface. The top navigation bar includes 'Show', 'Settings', 'Security', 'Software Upgrades', 'Services', and 'Help'. The main content area is titled 'Certificate List' and contains several action buttons: 'Generate Self-signed', 'Upload Certificate/Certificate chain', 'Download CTL', and 'Generate CSR'. Below the buttons is a search filter section with the text 'Find Certificate List where Certificate begins with' and a 'Find' button. Two black arrows point from the 'Generate Self-signed' and 'Generate CSR' buttons in the main area to the corresponding buttons in the bottom navigation bar.

The screenshot shows the 'Generate New Self-signed Certificate' dialog box. It has a title bar with 'Generate' and 'Close' buttons. Below the title bar is a 'Status' section with a warning icon and the text: 'Warning: Generating a new certificate will overwrite any existing certificate information'. The main section is titled 'Generate Self-signed' and contains several fields with dropdown menus: 'Certificate Purpose*' (set to TVS), 'Distribution*' (set to cs-ccm-pub.vasank.com), 'Common Name*' (set to cs-ccm-pub.vasank.com), 'Key Length*' (set to 2048), and 'Hash Algorithm*' (set to SHA256). At the bottom of the dialog are 'Generate' and 'Close' buttons.

Regenerate CAPF certificate

- If the CAPF service is activated then all phones will restart to update the ITL File and LSC should be re-issued
- No impact if CAPF service not activated

The screenshot shows the Cisco Unified Operating System Administration interface. The top navigation bar includes 'Show', 'Settings', 'Security', 'Software Upgrades', 'Services', and 'Help'. The main content area is titled 'Certificate List' and contains several buttons: 'Generate Self-signed', 'Upload Certificate/Certificate chain', 'Download CTL', and 'Generate CSR'. Below the buttons is a search section with the text 'Find Certificate List where Certificate begins with' and a 'Find' button. Two black arrows point from the 'Generate Self-signed' and 'Generate CSR' buttons in the main content area to the corresponding buttons in the 'Generate New Self-signed Certificate' dialog box shown on the right.

The dialog box is titled 'Generate New Self-signed Certificate' and has a 'Generate' button and a 'Close' button. Below the buttons is a 'Status' section with a warning icon and the text: 'Warning: Generating a new certificate will overwrite any existing certificate information'. The main section is titled 'Generate Self-signed' and contains the following fields:

Certificate Purpose*	CAPF
Distribution*	cs-ccm-pub.vasank.com
Common Name*	cs-ccm-pub.vasank.com
Key Length*	2048
Hash Algorithm*	SHA256

At the bottom of the dialog box are 'Generate' and 'Close' buttons.

Certificate Deletion from Trust Store


CSCus28550

- Prior to 11.0 - Stop “Cisco Certificate Change Notification Service”
- Post 11.0 – Replication Logic still exists along with deletion from one node deletes from ALL.

Avoiding phone trust list update failure

- DON'T Regenerate both ccm+tfoot, tvs certificate together in a single node cluster
- Track phone(s) not registered to the cluster before regenerating ccm+tfoot, tvs certificate

Status

 CallManager certificate was modified in the last 5 minutes. Please re-try regenerating TVS certificate at a later time

Certificate Settings

File Name TVS.pem
Certificate Name TVS
Certificate Type certs
Certificate Group product-cm
Description Self-signed certificate generated by system

ITL Recovery Method

ITL Recovery from Server

- Phones download ITL with additional entry of ITLRecovery which never changes in the server unless regenerated
- Signing of the ITL file using ITLRecovery private key
- Phone trusts the ITL file as it contains ITLRecovery entry in it's current ITL

```
admin:utils itl reset
      utils itl reset localkey
      utils itl reset remotekey

admin:utils itl reset localkey
Enter CCM Administrator password :

Locating active Tftp servers in the cluster.....

Following is the list of Active tftp servers in the cluster

['cs-ccm-pub', 'cs-ccm-sub']
The reset ITL file was generated successfully

Transferring new reset ITL file to the TFTP server nodes in the cluster.....
```

IM and Presence Certificates

Trust Store Description

Trust Store Name	Replication Within Cluster	Common Usage
cup-trust	True	SIP Proxy TLS Communication, Presence Engine CA certificate MS Exchange CA certificate and Certificates needed for Microsoft Lync or SIP Federation
cup-xmpp-trust	True	The trust certificates for cup-xmpp-s2s are stored in cup-xmpp-trust along with the general XMPP trust certificates.

cup-xmpp certificate – Installing CA Signed

- Restart of Cisco Intercluster SyncAgent after uploading CA certificate to cup-xmpp-trust
- Install the certificate on each node of IMP server.
- Restart of Cisco XCP Router Service
- Jabber will loose connectivity to Chat Server.

cup-xmpp-s2s Certificate

- Only needed on nodes running Federation service
- Installed as cup-xmpp after installing CA certificate as cup-xmpp-trust

Troubleshooting

Serviceability Features

- IPT Platform CertMgr Logs (CertMgmt000xy.log)
- Cisco Certificate Change Notification Logs(certCN000xy.log)
- Cisco Trust Verification Service Logs (tvs0000xy.log)
- IPT Platform Cert Monitor Logs (CertM000xy.log)
- Packet Captures (<name>.pcap)
- OpenSSL to test connection with UCM Server

Certificate Impact on Services

- If Tomcat certificate is expired or keystore is corrupt.
- Serviceability Page Communication between nodes in Trace Configuration and Service Activate Fail.
- External Web Client using AXL fail if Strict CertValidation is enabled. (Ex. /axl/, /perfmonservice etc.)
- TLS Handshake Failure
- Having Expired Certificate is Dangerous



TVS Certificate Verification Failure

16:02:10.271 | debug tvsIdleTLSEstablished
16:02:10.271 | debug Starting Timer after SSL Negotiation

Phone sends a TVS Certificate Verification Request

16:02:10.765 | debug tvsHandleCertVerificationReq

TVS looks for Certificate using a unique combination of Serial Number of Certificate and Issuer Certificate Subject CN

16:02:10.765 | debug CertificateDBCACHE::getCertificateInformation - Looking up the certificate cache using Unique MAP ID : 027865CN=VASANK-DC1-CA ;OU=BGL ;O=TAC;C=IN
16:02:10.765 | debug ERROR:CertificateDBCACHE::getCertificateInformation - Cannot find the certificate in the cache
16:02:10.765 | debug CertificateCTLCACHE::getCertificateInformation - Looking up the certificate cache using Unique MAP ID : 027865CN=VASANK-DC1-CA;OU=BGL;O=TAC;C=IN
16:02:10.765 | debug ERROR:CertificateCTLCACHE::getCertificateInformation - Cannot find the certificate in the cache
16:02:10.765 | debug getCertificateInformation(cert) : certificate not found
16:02:10.765 | debug 93:UNKNOWN:No associated roles found for the certificate in cache

SSL Handshake

No.	Time	Source	Destination	Protocol	Seq	Ack	Length	Info
25	2015-10-07 14:51:43.329139	10.80.136.18	10.5.42.203	TLSv1	1	1	140	Client Hello
26	2015-10-07 14:51:43.332879	10.5.42.203	10.80.136.18	TLSv1	1	87	1354	Server Hello
29	2015-10-07 14:51:43.332891	10.5.42.203	10.80.136.18	TLSv1	3901	87	787	Certificate
31	2015-10-07 14:51:43.440499	10.80.136.18	10.5.42.203	TLSv1	87	4634	380	Client Key Exchange, Change Cipher Spec, Encryp...
32	2015-10-07 14:51:43.447729	10.5.42.203	10.80.136.18	TLSv1	4634	413	113	Change Cipher Spec, Encrypted Handshake Message
34	2015-10-07 14:51:43.465446	10.80.136.18	10.5.42.203	TLSv1	413	4693	475	Application Data
36	2015-10-07 14:51:43.860531	10.5.42.203	10.80.136.18	TLSv1	4693	834	1275	Application Data

- ▼ TLSv1 Record Layer: Handshake Protocol: Certificate
 - Content Type: Handshake (22)
 - Version: TLS 1.0 (0x0301)
 - Length: 4540
 - ▼ Handshake Protocol: Certificate
 - Handshake Type: Certificate (11)
 - Length: 4536
 - Certificates Length: 4533
 - ▼ Certificates (4533 bytes)
 - Certificate Length: 1996
 - ▶ Certificate: 308207c8308206b0a0030201020203027864300d06092a86... (id-at-commonName=..., id-at-organizationalUnitName=..., i...
 - Certificate Length: 1364
 - ▶ Certificate: 3082055030820438a003020102020455883ff2300d06092a... (id-at-commonName=..., id-at-organizationalUni...
 - Certificate Length: 1164
 - ▶ Certificate: 3082048830820370a003020102020500a7bd2ea4300d0609... (id-at-commonName=..., id-at-organizationName=..., id...
- ▼ Secure Sockets Layer
 - ▼ TLSv1 Record Layer: Handshake Protocol: Server Hello Done
 - Content Type: Handshake (22)
 - Version: TLS 1.0 (0x0301)

Frame (frame), 787 bytes Packets: 85 · Displayed: 7 (8.2%) · Load time: 0:0:1 Profile: New profile

ipsec certificate Issue

DRF LA/MA Logs in Debug Level

```
2015-01-17 11:05:15,114 DEBUG [NetServerWorker] - drfNetServer.run: Received Client Socket request from /10.106.97.178:54697
2015-01-17 11:05:15,114 DEBUG [NetServerWorker] - Validating if client request is from a Node within the Cluster
2015-01-17 11:05:15,115 DEBUG [NetServerWorker] - Validated Client. IP = 10.106.97.178 Hostname = UCMC2S2.vasank.com. Request is from a
Node within the Cluster
2015-01-17 11:05:15,115 DEBUG [NetServerWorker] - drfNetServerWorker.drfNetServerWorker: Socket Object OutputStream to be created
2015-01-17 11:05:15,116 ERROR [NetServerWorker] - drfNetServerWorker.drfNetServerWorker: Unable to create input/output stream to client
Received fatal alert: certificate_unknown
2015-01-17 11:05:21,125 DEBUG [NetServerWorker] - drfNetServer.run: Received Client Socket request from /10.106.97.178:54702
2015-01-17 11:05:21,125 DEBUG [NetServerWorker] - Validating if client request is from a Node within the Cluster

2015-01-17 11:05:21,125 DEBUG [NetServerWorker] - Validated Client. IP = 10.106.97.178 Hostname = UCMC2S2.vasank.com.
Request is from a Node within the Cluster
2015-01-17 11:05:21,125 DEBUG [NetServerWorker] - drfNetServerWorker.drfNetServerWorker: Socket Object OutputStream to be created
2015-01-17 11:05:21,126 ERROR [NetServerWorker] - drfNetServerWorker.drfNetServerWorker: Unable to create input/output stream to client
Received fatal alert: certificate_unknown
2015-01-17 11:05:26,137 DEBUG [NetServerWorker] - drfNetServer.run: Received Client Socket request from /10.106.97.178:54704
2015-01-17 11:05:26,137 DEBUG [NetServerWorker] - Validating if client request is from a Node within the Cluster
2015-01-17 11:05:26,137 DEBUG [NetServerWorker] - Validated Client. IP = 10.106.97.178 Hostname = UCMC2S2.vasank.com. Request is from a
Node within the Cluster
2015-01-17 11:05:26,137 DEBUG [NetServerWorker] - drfNetServerWorker.drfNetServerWorker: Socket Object OutputStream to be created
2015-01-17 11:05:26,139 ERROR [NetServerWorker] - drfNetServerWorker.drfNetServerWorker: Unable to create input/output stream to client
Received fatal alert: certificate_unknown
```

Certificate Regeneration CCM

CertMgmt.log

2016-02-07 14:51:46,338 INFO [main] - decode

2016-02-07 14:51:46,339 INFO [main] - op:regenerate

2016-02-07 14:51:46,339 INFO [main] - unit:CallManager

2016-02-07 14:51:46,339 INFO [main] - cert-

dir:%2Fusr%2Flocal%2Fcm%2F.security%2FCallManager%2Fcerts%2FCallManager

2016-02-07 14:51:46,339 INFO [main] - key-dir:%2Fusr%2Flocal%2Fcm%2F.security%2FCallManager%2Fkeys

Certificate Regeneration – No Device Restart

```
00015365.000 |17:10:49.483 |SdlSig |CcmDbTableChangeNotify |wait |CcmDbChangeNotify(2,100,41,1)
|CcmDbChangeNotify(2,100,41,1) |2,100,41,1.38^*^* |[[T:N-H:0,N:0,L:0,V:0,Z:0,D:0]
00015366.000 |17:10:49.483 |SdlStat |Period: 6s #Lines: 13 #Bytes: 3338 Total Number of Buffers: 10000 Free LWM: 9995 Free LWM(total): 9770
00015365.001 |17:10:49.483 |AppInfo |DB: CFastAccess(certificate)
00015365.002 |17:10:49.483 |AppInfo |DB: SQL1[select * from certificate where pkid = '05aa6785-b756-c9ac-804f-17e92c44b016'];]
00015365.003 |17:10:49.606 |AppInfo |DB: SQL2[select * from certificate where pkid = '05aa6785-b756-c9ac-804f-17e92c44b016'];]
00015365.004 |17:10:49.606 |AppInfo |DB: ~CFastAccess(certificate)
00015365.005 |17:10:49.607 |AppInfo |Cnf Received: certificate U 05aa6785-b756-c9ac-804f-17e92c44b016, size(2634)
serialnumber(5ee1fd6f66b94ec43ca2c32e3ce90e78/63c8ff45bfa7fd34b6e2505bdeb83d1f)
00015367.000 |17:10:49.607 |SdlSig |DbTableChangeNotify |wait |DbChangeNotify(2,100,207,1) |CcmDbChangeNotify(2,100,41,1)
|2,100,41,1.38^*^* |[[T:N-H:0,N:0,L:0,V:0,Z:0,D:0] certificate U 05aa6785-b756-c9ac-804f-17e92c44b016
00015367.001 |17:10:49.608 |AppInfo |ProcessCnf N: certificate U 05aa6785-b756-c9ac-804f-17e92c44b016, size(2634)
serialnumber(5ee1fd6f66b94ec43ca2c32e3ce90e78/63c8ff45bfa7fd34b6e2505bdeb83d1f)
00015367.002 |17:10:49.608 |AppInfo |doGroupReset: checking for group reset on table certificate
00015367.003 |17:10:49.608 |AppInfo |Certificate CNF. ProcessDbChangeNotify - (certificate, action=2) Cert pkid=05aa6785-b756-c9ac-804f-17e92c44b016.
(:2320)
00015367.004 |17:10:49.608 |AppInfo |finish cnf on table certificate
```

Certificate Regeneration – Device **Restart**

```
03879286.001 |23:12:52.497 |AppInfo |ProcessCnf Y: certificate U 4480fa34-e3dd-de75-f26d-ea39c9daa99a, size(2634)
serialnumber(4c859863d5943db0631de8d37816129d/49623cfd4ce571daa9da49d9f792d334)
03879286.002 |23:12:52.497 |AppInfo |Certificate CNF. ProcessDbChangeNotify - (certificate, action=2) Cert pkid=4480fa34-e3dd-de75-f26d-
ea39c9daa99a. DEBOUNCED (:2320)
03879286.003 |23:12:52.497 |AppInfo |Certificate CNF. ProcessDbChangeNotify - Cert pkid=4480fa34-e3dd-de75-f26d-ea39c9daa99a,
serverName=labsrver1, IPv4=10.106.97.178, IPv6=, issuerName=L=BGL,ST=KA,CN=labsrver1.vasank.com,OU=TAC,O=Cisco,C=IN. Process it.
(:1318)
03879286.004 |23:12:52.556 |AppInfo |Certificate CNF. CertificateProcessNodeMap List has: pkid=83d76f5c-775a-4c89-a110-
a7b7e98bd104,servername=labsrver1,fkprocessnode=22b42762-9ae4-4ffc-9917-a8cd6fc213be (:1373)
03879286.005 |23:12:52.556 |AppInfo |Certificate CNF. Processing CertServiceCertMap pkid=ce8841e9-4902-4ae2-8f8c-746ca4a0b6bc,
tkcertificateservice=3/ fkCert=4480fa34-e3dd-de75-f26d-ea39c9daa99a. (:1413)
03879286.006 |23:12:52.556 |AppInfo |Certificate CNF. isITLRelatedRole=SERVICE_CALLMANAGER leads to an active TFTP node (:1260)
03879286.007 |23:12:52.566 |AppInfo |Cnf group reset: SQL1[execute procedure dbSelectAllRelatedDevices('CALLMANAGER', 'd4bfc995-72a1-
46af-a607-c0988cdd1be5')]
03879286.008 |23:12:52.567 |AppInfo |DB: CFastAccess(Group Reset)
03879286.009 |23:12:52.567 |AppInfo |DB: SQL1[execute procedure dbSelectAllRelatedDevices('CALLMANAGER', 'd4bfc995-72a1-46af-a607-
c0988cdd1be5')]
03879286.010 |23:12:52.652 |AppInfo |DB: SQL2[execute procedure dbSelectAllRelatedDevices('CALLMANAGER', 'd4bfc995-72a1-46af-a607-
c0988cdd1be5')]03879286.011 |23:12:52.652 |AppInfo |-->DB: MoveNext()
03879286.012 |23:12:52.924 |AppInfo |DB: MoveNext(): FALSE
```

Certificate Regeneration – TVS Service

```
00006935.001 |16:15:38.433 |AppInfo |ProcessCnf Y: certificate U 5e4594df-e935-494a-3549-6db7ffb89c1d, size(2634)
serialnumber(6907c5548780e470b9e3cb3164b12c00/5c9a187f6bfcfbcbfc673ee1b4bd001)
00006935.002 |16:15:38.433 |AppInfo |Certificate CNF. ProcessDbChangeNotify - (certificate, action=2) Cert pkid=5e4594df-e935-494a-3549-6db7ffb89c1d. DEBOUNDED (:2320)
00006935.003 |16:15:38.433 |AppInfo |Certificate CNF. ProcessDbChangeNotify - Cert pkid=5e4594df-e935-494a-3549-6db7ffb89c1d, serverName=labserver2, IPv4=10.106.97.179, IPv6=,
issuerName=L=BGL,ST=KA,CN=labserver2.vasank.com,OU=TAC,O=Cisco,C=IN. Process it. (:1318)
00006935.004 |16:15:38.433 |AppInfo |Certificate CNF. CertificateProcessNodeMap List has: pkid=e3048581-1c9e-4710-a101-f3599de6dcd0,servername=labserver2,fkprocessnode=1401da6f-79ea-32f3-
deca-bc664c0b0c12 (:1373)
00006935.005 |16:15:38.433 |AppInfo |Certificate CNF. Processing CertServiceCertMap pkid=cb200b81-8c15-49db-85ae-54b2c48f98f9, tkcertificateservice=11/ fkCert=5e4594df-e935-494a-3549-
6db7ffb89c1d. (:1413)
00006935.006 |16:15:38.433 |AppInfo |Certificate CNF. isITLRelatedRole=CERTIFICATE_SERVICE_TVS and CertProcessNodeMap pkid=e3048581-1c9e-4710-a101-f3599de6dcd0. (:1179)
00006935.007 |16:15:38.433 |AppInfo |Certificate CNF. Leads to CallManager pkid=d4bfc995-72a1-46af-a607-c0988cdd1be5. Name=CM_labserver2. (:1197)
00006935.008 |16:15:38.433 |AppInfo |Cnf group reset: SQL1[execute procedure dbSelectAllRelatedDevices('CALLMANAGER', 'd4bfc995-72a1-46af-a607-c0988cdd1be5')]
00006935.009 |16:15:38.433 |AppInfo |DB: CFastAccess(Group Reset)
00006935.010 |16:15:38.433 |AppInfo |DB: SQL1[execute procedure dbSelectAllRelatedDevices('CALLMANAGER', 'd4bfc995-72a1-46af-a607-c0988cdd1be5')]
00006935.011 |16:15:38.436 |AppInfo |DB: SQL2[execute procedure dbSelectAllRelatedDevices('CALLMANAGER', 'd4bfc995-72a1-46af-a607-c0988cdd1be5')]
00006935.012 |16:15:38.436 |AppInfo |-->DB: MoveNext()
00006935.013 |16:15:38.442 |AppInfo |DB: MoveNext(): FALSE
00006935.014 |16:15:38.442 |AppInfo |Cnf group reset: SQL2[execute procedure dbSelectAllRelatedDevices('CALLMANAGER', 'd4bfc995-72a1-46af-a607-c0988cdd1be5')], ccmPkid[d4bfc995-72a1-46af-
a607-c0988cdd1be5]
00006935.015 |16:15:38.442 |AppInfo |DB: IsEOF(): FALSE
00006935.016 |16:15:38.442 |AppInfo |<--DB: Int[tkmodel]=[645]
00006935.017 |16:15:38.442 |AppInfo |<--DB: Str[pkid]=[21b83701-7d88-479f-b885-0cf40956b5a3]
00006935.018 |16:15:38.442 |AppInfo |<--DB: Str[name]=[Sample Device Template with TAG usage examples]
00006935.019 |16:15:38.442 |AppInfo |<--DB: Str[fkcallmanager1]=[d4bfc995-72a1-46af-a607-c0988cdd1be5]
00006935.020 |16:15:38.442 |AppInfo |<--DB: Str[fkcallmanager2]=[
00006935.021 |16:15:38.442 |AppInfo |Sending device reset(2) for pkid=21b83701-7d88-479f-b885-0cf40956b5a3, name=Sample Device Template with TAG usage examples, tkmodel=645 cache=Y
fk1=<d4bfc995-72a1-46af-a607-c0988cdd1be5> fk2=<>
```

Unofficial Way – Track LSC Installation

```
admin:run sql select name,tkcertificatestatus,publickey from device where name like 'SEP%'
```

name	tkcertificatestatus	publickey
SEP885A92D977CA	3	-----BEGIN RSA PUBLIC KEY----- MIIBCgKCAQEAkGfWRcugYmCE+JTDmyAXuiY4KKWG+adWCCev0Loy9sZQjaA4t9ox e9oskH6www9faBNJO4RusiR5PE+/yIxRqmS5dVMwC8ig6ueg1oFEiNb1OcKUZw3l lim0fgqrw1CnmgvJWdpdIV+OJmzu5v/zQGFdPQODhZw7lOqREEXAUspcF/uIT2v2 p4KQjE0CKEkAKVaQyL85L1NAhpYC5G0B0zM6UGVyyvBug6xFqKJqaBVQQq1DC+dd/ uhRECYCZlsZP3Ea3L8cSyBA5fsk8rNSWwPZQsDpYc+1/RhXPfjO/mJzH+e9oqL1r FWNGJPo8T0UEt8i2Pf+4vix/VsfZ4lx9oQIDAQAB -----END RSA PUBLIC KEY-----
SEPB83861583B73	2	NULL

Unofficial Way – Track LSC Installation Contd..

```
admin:run sql select name,tkcertificatestatus,publickey from device where name like 'SEP%'
```

name	tkcertificatestatus	publickey
SEP885A92D977CA	3	-----BEGIN RSA PUBLIC KEY----- MIIBCgKCAQEAkqfWRcugYmCE+JTDmyAXuiY4KKWG+adWCCev0Loy9sZQjaA4t9ox e9oskH6www9faBNJO4RusiR5PE+/yIxRqmS5dVMwC8ig6ueg1oFEiNb1OcKUZw3l lim0fgqrw1CnmgvJWdpdIV+OJmzu5v/zQGFdPQODhZw7IOqREEXAUspcF/uIT2v2 p4KQjE0CKEkAKVaQyL85L1NAhpYC5G0B0zM6UGVyvBug6xFqKJqaBVQQq1DC+dd/ uhRECYCZlsZP3Ea3L8cSyBA5fsk8rNSWwPZQsDpYc+1/RhXPfjO/mJzH+e9oqL1r FWNGJPo8T0UEt8i2Pf+4vix/VsfZ4lx9oQIDAQAB -----END RSA PUBLIC KEY-----
SEPB83861583B73	3	-----BEGIN RSA PUBLIC KEY----- MIIBCgKCAQEAIlkiFXEYg5wxykHaxt9+5jRpH/RmT/CMvuCoPKAgLZiSHTiPn8JK mljbrA8nU+5SXdB1mcvCi4w4l3Nwe8f4YROC6U2Y4jmeJoZzJ/6C+HwUvkSaCxCU g0d6MTT15bA2mAADOaHD6/acCkXhfoWMspHNPJ5uqr0DxxeuVGB7MkQePE3Vrqq N4pMXhadSIMBWXsCg4hkvcugl5PijwPb5h4odPGJ5xEgcSsnQ1s/a61+4ouv1pf6 pRSmk+xLMi29MZJa2o0Urny+qbafJd3YcIEB50FXZh9+IFNdt5mkStF/muvsWjt2 FAyxmXup1iKjomJ5rxJEQTtojaJZ7Bf6cQIDAQAB -----END RSA PUBLIC KEY-----

Understand LSC Installation Status

enum name	moniker
1 None	CERT_STATUS_NONE
2 Operation Pending	CERT_STATUS_SCHEDULE
3 Upgrade Success	CERT_STATUS_UPGRADE_SUCCESS
4 Delete Success	CERT_STATUS_DELETE_SUCCESS
5 Troubleshoot Success	CERT_STATUS_TROUBLESHOOT_SUCCESS
6 Upgrade Failed	CERT_STATUS_UPGRADE_FAIL
7 Delete Failed	CERT_STATUS_DELETE_FAIL
8 Troubleshoot Failed	CERT_STATUS_TROUBLESHOOT_FAIL
9 Upgrade Failed: Invalid LSC	CERT_STATUS_UPGRADE_FAIL_INVALID_LSC
10 Upgrade Failed: Invalid Authentication String	CERT_STATUS_UPGRADE_FAIL_INVALID_AUTH_STR
11 Upgrade Failed: Invalid MIC	CERT_STATUS_UPGRADE_FAIL_INVALID_MIC
12 Upgrade Failed: Invalid Credentials	CERT_STATUS_UPGRADE_FAIL_INVALID_CREDENTIALS
13 Upgrade Failed: Phone Communication Failure	CERT_STATUS_UPGRADE_FAIL_PHONE_COMM_ERROR
14 Upgrade Failed: Key Generation Failed/Timeout	CERT_STATUS_UPGRADE_FAIL_OP_TIMED_OUT
15 Upgrade Failed: CA Communication Failure	CERT_STATUS_UPGRADE_FAIL_CA_COMM_ERROR
16 Upgrade Failed: CA Rejected Connection	CERT_STATUS_UPGRADE_FAIL_CA_REJECT
17 Upgrade Failed: User Initiated Request Late/Timeout	CERT_STATUS_UPGRADE_FAIL_LATE_REQUEST
18 Delete Failed: Invalid LSC	CERT_STATUS_DELETE_FAIL_INVALID_LSC
19 Delete Failed: Invalid Authentication String	CERT_STATUS_DELETE_FAIL_INVALID_AUTH_STR
20 Delete Failed: Invalid MIC	CERT_STATUS_DELETE_FAIL_INVALID_MIC
21 Delete Failed: Invalid Credentials	CERT_STATUS_DELETE_FAIL_INVALID_CREDENTIALS
22 Delete Failed: Phone Communication Failure	CERT_STATUS_DELETE_FAIL_PHONE_COMM_ERROR
23 Delete Failed: Key Generation Failed/Timeout	CERT_STATUS_DELETE_FAIL_OP_TIMED_OUT
24 Delete Failed: CA Communication Failure	CERT_STATUS_DELETE_FAIL_CA_COMM_ERROR
25 Delete Failed: CA Rejected Connection	CERT_STATUS_DELETE_FAIL_CA_REJECT
26 Delete Failed: User Initiated Request Late/Timeout	CERT_STATUS_DELETE_FAIL_LATE_REQUEST
27 Troubleshoot Failed: Invalid LSC	CERT_STATUS_TROUBLESHOOT_FAIL_INVALID_LSC
28 Troubleshoot Failed: Invalid Authentication String	CERT_STATUS_TROUBLESHOOT_FAIL_INVALID_AUTH_STR
29 Troubleshoot Failed: Invalid MIC	CERT_STATUS_TROUBLESHOOT_FAIL_INVALID_MIC
30 Troubleshoot Failed: Invalid Credentials	CERT_STATUS_TROUBLESHOOT_FAIL_INVALID_CREDENTIALS
31 Troubleshoot Failed: Phone Communication Failure	CERT_STATUS_TROUBLESHOOT_FAIL_PHONE_COMM_ERROR
32 Troubleshoot Failed: Key Generation Failed/Timeout	CERT_STATUS_TROUBLESHOOT_FAIL_OP_TIMED_OUT
33 Troubleshoot Failed: User Initiated Request Late/Timeout	CERT_STATUS_TROUBLESHOOT_FAIL_LATE_REQUEST

ITL Recovery

file get activelog cm/log/itlreset.log

```
Fri Mar 11 00:16:30 2016 itlreset INFO: Start Execution
Fri Mar 11 00:16:30 2016 itlreset DEBUG: Key location is local
Fri Mar 11 00:16:34 2016 itlreset DEBUG: Locating active Tftp servers in the cluster.....
Fri Mar 11 00:16:39 2016 itlreset INFO: Number of Active TFTP servers in the cluster : 1
Fri Mar 11 00:16:39 2016 itlreset INFO: Fetching App User ID from DB
Fri Mar 11 00:16:44 2016 itlreset INFO: rc is 0Fri Mar 11 00:16:44 2016 itlreset INFO: hostname is labserver1
Fri Mar 11 00:16:47 2016 itlreset INFO: (ServiceInformationResponse){ ReturnCode = "0" ReasonCode = -1 ReasonString = None ServiceInfoList = (ArrayOfServiceInformation){
item[] = (ServiceInformation){ ServiceName = "Cisco Tftp" ServiceStatus = "Started" ReasonCode = -1 ReasonCodeString = " " StartTime =
"Wed Feb 17 19:38:50 2016" UpTime = 1917476 }, }}
Fri Mar 11 00:16:47 2016 itlreset INFO: Cisco Tftp service started on host labserver1
Fri Mar 11 00:16:47 2016 itlreset DEBUG: Determining if the Live TFTP node is the self node or not
Fri Mar 11 00:16:47 2016 itlreset INFO: Live TFTP server is this pub node. So no need to sftp
Fri Mar 11 00:16:47 2016 itlreset DEBUG: Converting key to pkcs8
Fri Mar 11 00:16:47 2016 itlreset INFO: Converted key to pkcs8 format
Fri Mar 11 00:16:47 2016 itlreset DEBUG: Generating the reset ITL file.....Location of ITL = /usr/local/cm/tftp/ITLFile.tlv
Length of ITL File 7515
Header Length = 452
Printing the Cisco SAST signerNameL=BGL,ST=KA,CN=ITLRECOVERY_labserver1.vasank.com,OU=TAC,O=Cisco,C=IN
Printing the Cisco SAST issuerNameL=BGL,ST=KA,CN=ITLRECOVERY_labserver1.vasank.com,OU=TAC,O=Cisco,C=INSIGNERNAME
=CN=labserver1.vasank.com;OU=TAC;O=Cisco;L=BGL;ST=KA;C=IN
CANAME = CN=labserver1.vasank.com;OU=TAC;O=Cisco;L=BGL;ST=KA;C=IN SIGNATUREINFO = DIGESTALGORTITHM 1Digest Algorithm Tag read bytes is 19
SIGNATUREALGOINFO 2 810 SIGNATUREALGORTITHM 1 11 SIGNATUREMODULUS 1 Modulus : 2048 Printing the length of
the signature : 25612 SIGNATURE 256 hdrLength: 452Header tag not recognizedPrinting default header value read :24
Print the value of ITL new Header Length : 908
The new pITL file length is 7971got privKeySIG_BEGIN: 197
Fri Mar 11 00:16:49 2016 itlreset INFO: The reset ITL file was generated successfully
Fri Mar 11 00:16:49 2016 itlreset DEBUG: Transferring new reset ITL file to the TFTP server nodes in the cluster.....
Fri Mar 11 00:16:49 2016 itlreset INFO: On local node copying sftp recovery ITL file to TFTP directory
Fri Mar 11 00:16:49 2016 itlreset INFO: Copied successfullyFri Mar 11 00:16:49 2016 itlreset INFO: Restarting Cisco Tftp service on host labserver1
Fri Mar 11 00:16:49 2016 itlreset INFO: (ControlServiceRequest){ NodeName = "labserver1" ControlType = "Restart" ServiceList = (ArrayOfServices){ item[] = "Cisco
Tftp", }}
```



Certificate Deletion Enhancement Troubleshoot

Syslog Viewer/System Logs/messages

Jan 20 02:20:09 CuCM1-228 ilog_impl: Received request for platform-event (--no-wait **platform-event-clusterwide-certificate-delete**
HOSTNAME=CuCM1-223 UNIT=tomcat-trust TYPE=trust-certs NAME=**test1**)

CertMgmt Logs :

```
decode: true
op: delete
unit: tomcat-trust
keystoreUnit:tomcat-trust
logFile: /var/log/active/platform/log/cert-mgmt.log
resultFile: /var/log/active/platform/log/certde-info.xml
keyDir: /usr/local/platform/.security/tomcat/keys
certDir: /usr/local/platform/.security/tomcat/trust-certs/MyCertificate2.pem
```

The below log shows that the certificates are getting deleted from file system

```
2015-01-21 21:07:26,068 DEBUG [main] - deleteDERandPEM: sCertDir = /usr/local/platform/.security/tomcat/trust-certs --- sAlias = MyCertificate2
```

```
2015-01-21 21:07:26,068 INFO [main] - IN -- TomcatCertMgr.java - removeFromKeyStore(..) -
```

```
2015-01-21 21:07:26,068 INFO [main] - IN -- RSACryptoEngine.java - removeFromKeyStore(keystoreFile, keystorePass, alias) -
```

```
2015-01-21 21:07:26,068 INFO [main] - IN -- RSACryptoEngine.java - loadKeyStore(keystoreFile, keystorePass) -
```

```
2015-01-21 21:07:26,112 DEBUG [Thread-3] - pingPrimary returns[true]
```

```
2015-01-21 21:07:26,128 INFO [main] - OUT -- RSACryptoEngine.java - loadKeyStore -
```

```
2015-01-21 21:07:26,147 DEBUG [main] - Removing certificate from keystore : MyCertificate2
```

The below log shows that the certificates are getting deleted from data base

```
2015-01-21 21:07:24,488 INFO [main] - IN -- CertDBAction.java - deleteCertificateInDB(certInfo) -
```

Common known Caveats

- CSCur97909 - Uploading multiserver cert doesnot delete self signed certs in DB
- CSCur67631 – support for 4096 key size for CA signed certificate
- CSCuu59477 - SHA1 in CTL file with etoken is wrong if DER cert exceeds 2048 bytes
- CSCus47235 - CUCM 10.5.2 CN not duplicated into SAN for CSR
- CSCuh19734 - Uploading certs with same CN will overwrite old cert in Phone-VPN-trust
- CSCup28852 - phone reset every 7min due to cert update when using multi-server cert
- CSCuy21239 - remove CAPF certificate installation from subscriber during install time
-

Troubleshooting tools

- openssl req -text -in CallManager.csr
- openssl x509 -noout -text -in CallManager.pem
- openssl x509 -in CAPF.pem -hash -noout
- openssl verify -verbose -CApath . DOD_CA-27.pem
- openssl s_client -showcerts -connect <UCMIP> CallManager.pem -msg -debug
- Using [Wireshark to decrypt TLS 1.0 and 1.1 signaling](#). (TAC Case Mandatory)

Further reading

- [High Level View of Certificates and Authorities in CUCM](#)
- [CUCM Certificate Regeneration/Renewal Process](#)
- [How to Verify the CSR and Certificate Mismatch for UC](#)
- [Unified Communication Cluster Setup with CA-Signed Multi-Server Subject Alternate Name Configuration Example](#)
- [CUCM Third-Party CA-Signed LSCs Generation and Import Configuration Example](#)
- [UC Maintenance Guide List – Major Version Release](#)
- [IM and P Maintenance Guide List – Major Version Release](#)

