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)

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco Video Infrastructure

(Expressway, Jabber Guest, TPS, Conductor)

.

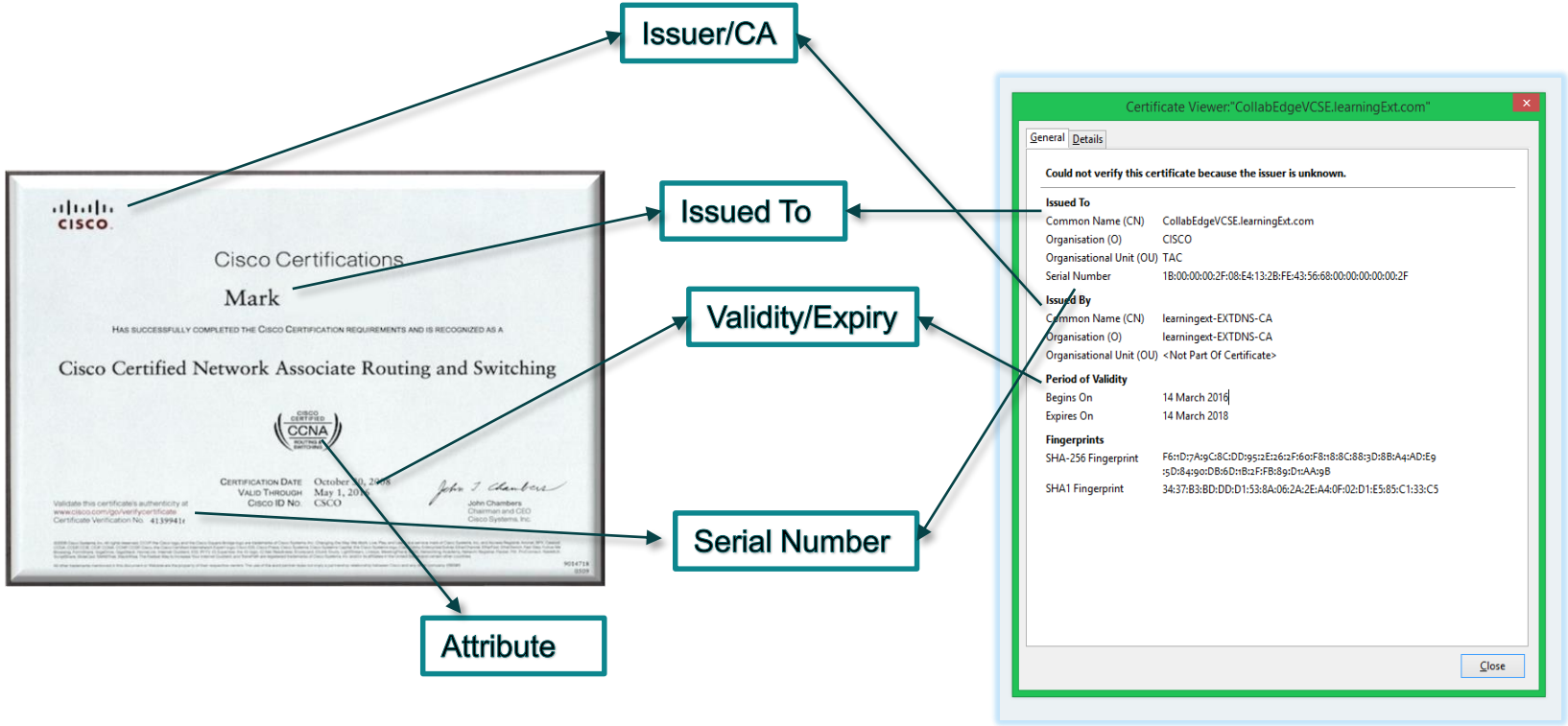
Zoltan Kelemen, Amit Sharma

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)*

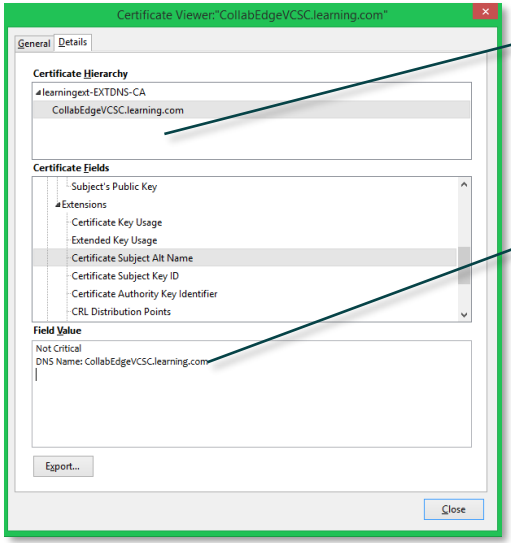
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Certificates: What are they



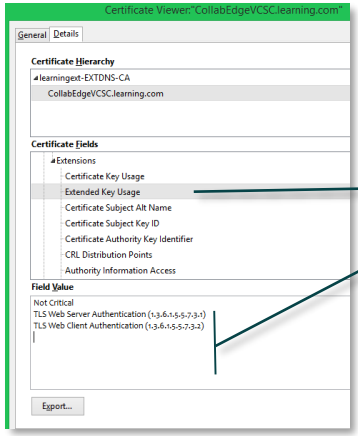
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Certificates: What are they



Hierarchy: who issued the certificate

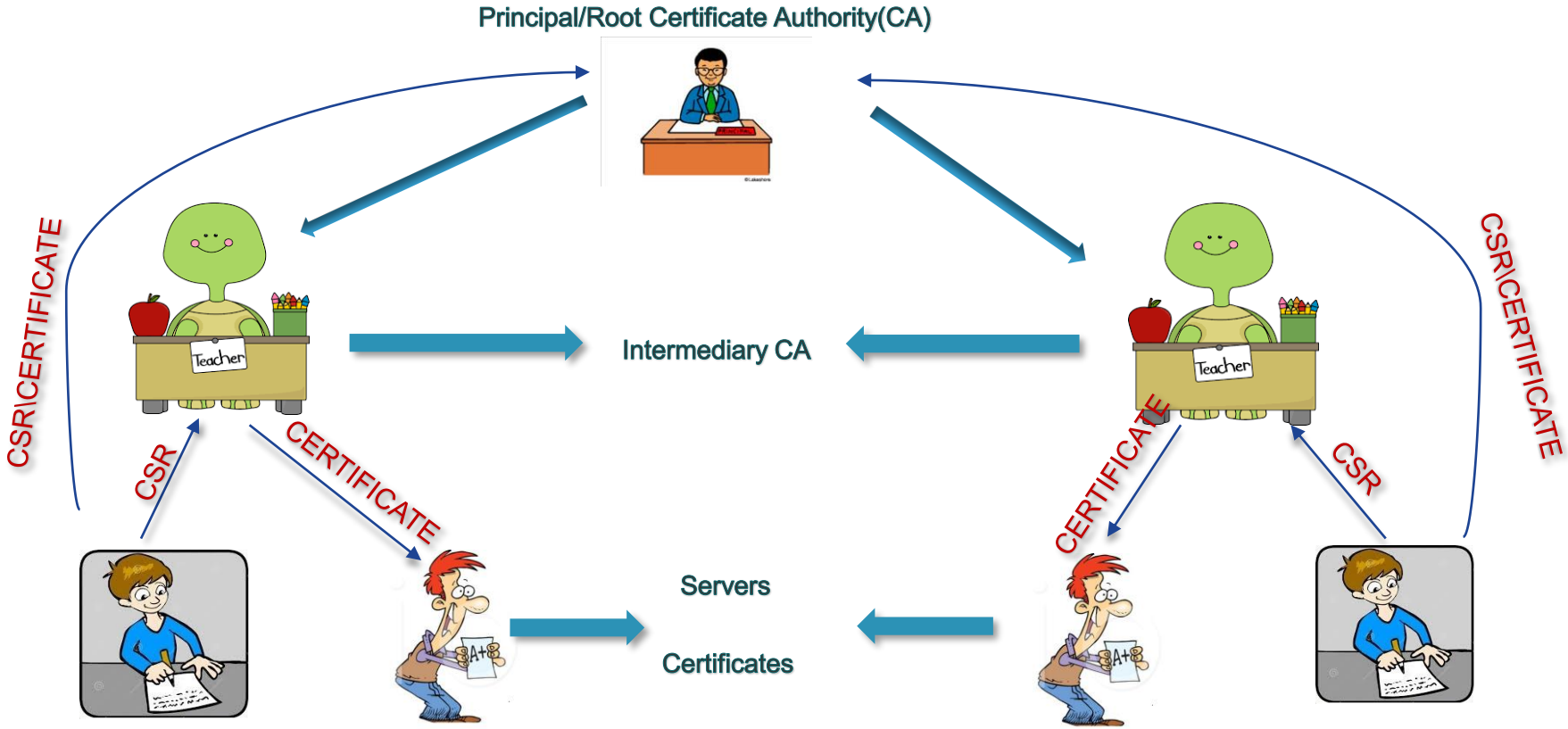
SAN: Additional FQDNs/Domains to be put here. Put in as many information here(not more than 999 characters)



Attributes required in the certificate

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Certificates: How to Get them



© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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)

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Certificates in Telepresence.

It's not optional anymore

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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**:

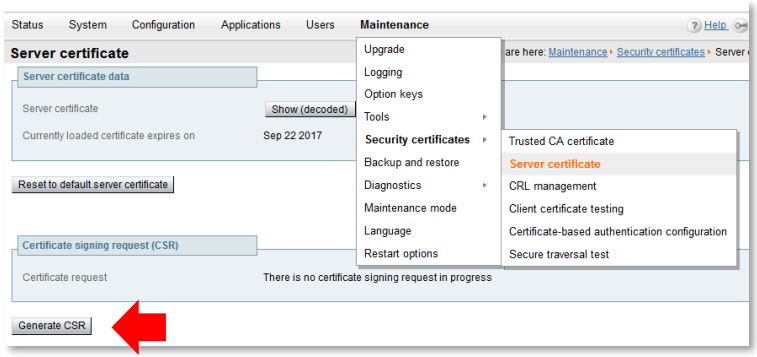
  Self Signed Certificates do not work

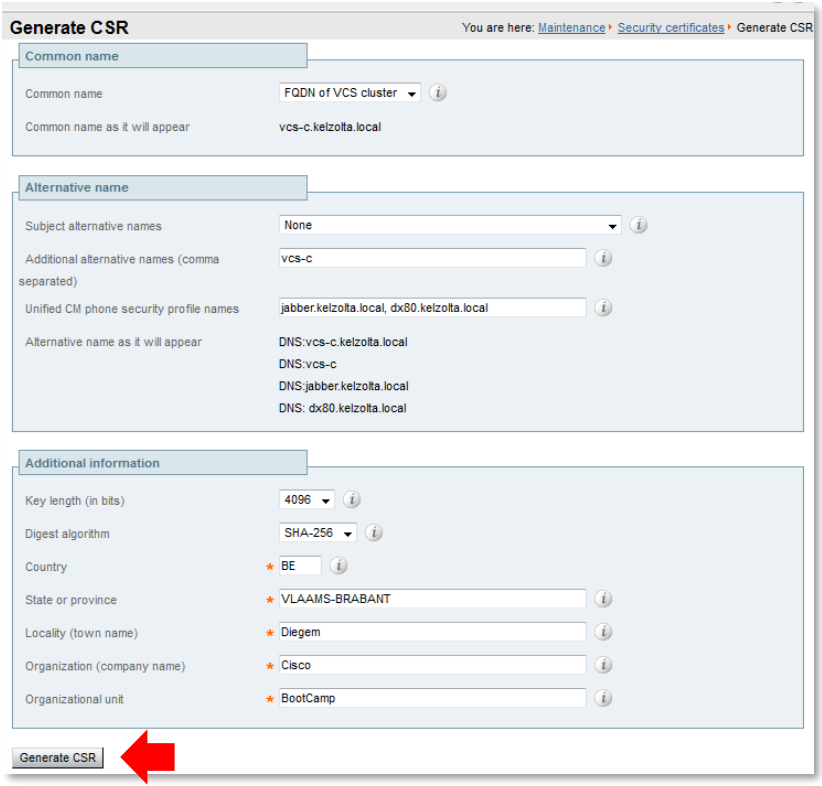
  Traversal Zone between C and E must be secured.
  Client communication with VCS-E must be encrypted.
  Communication between VCS-C and CUCM should be over TLS (optional)

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Certificates Expressway: HOW To Get Them contd..

Generate Certificate Signing Request





- 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

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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

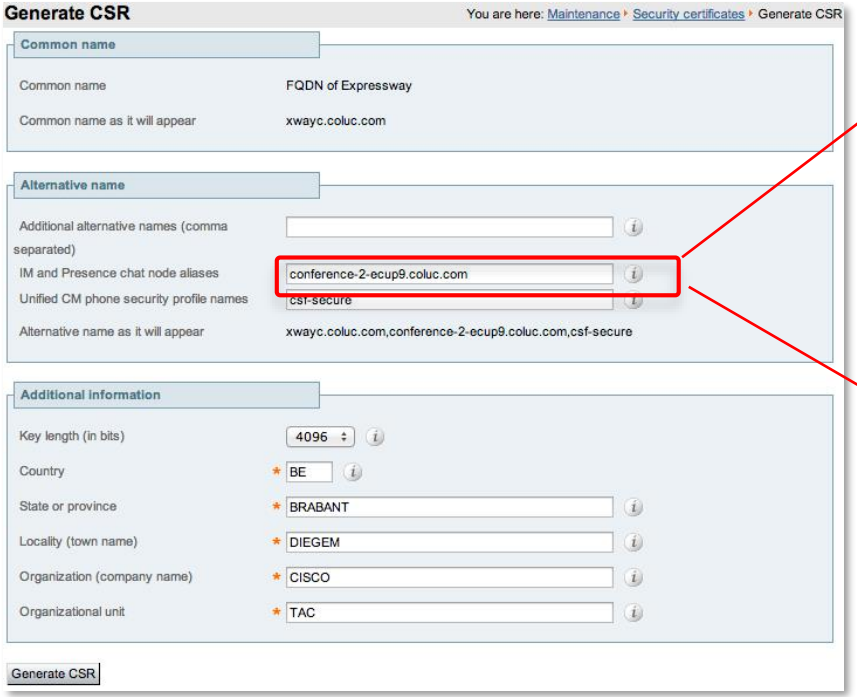
CSR SAN element	MRA	JabberGuest	XMPP federation
Cluster (if used) and node FQDN	Both	Both	Both
Public domain or collab-edge.<domain>	E only	✗	✗
Unified CM registration domains	E only	✗	✗
Unified CM phone security profile names	C only	✗	✗
XMPP federation domains	✗	✗	E only
IM&P chat node aliases (federated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

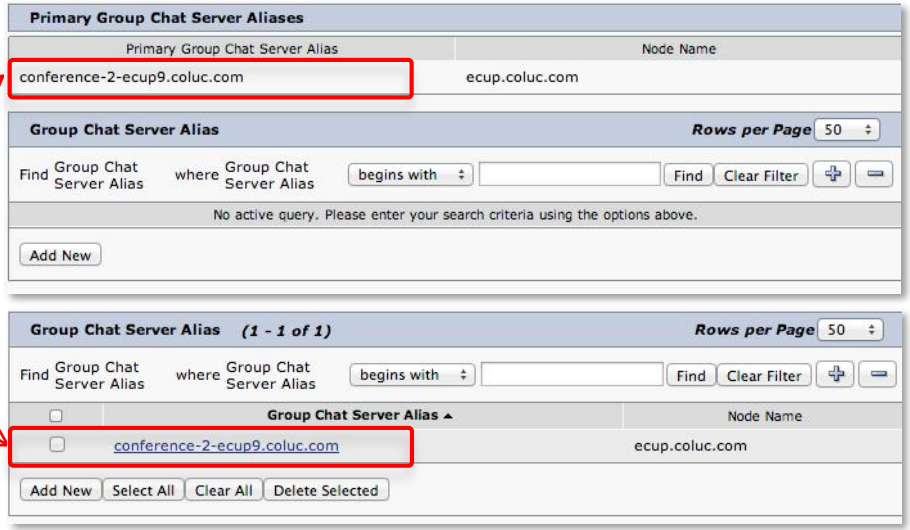
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Certificates Expressway: HOW To Get Them contd..

Fill in the required information in the CSR: SAN

CUPADMIN > Messaging > Group Chat Server Alias Mapping

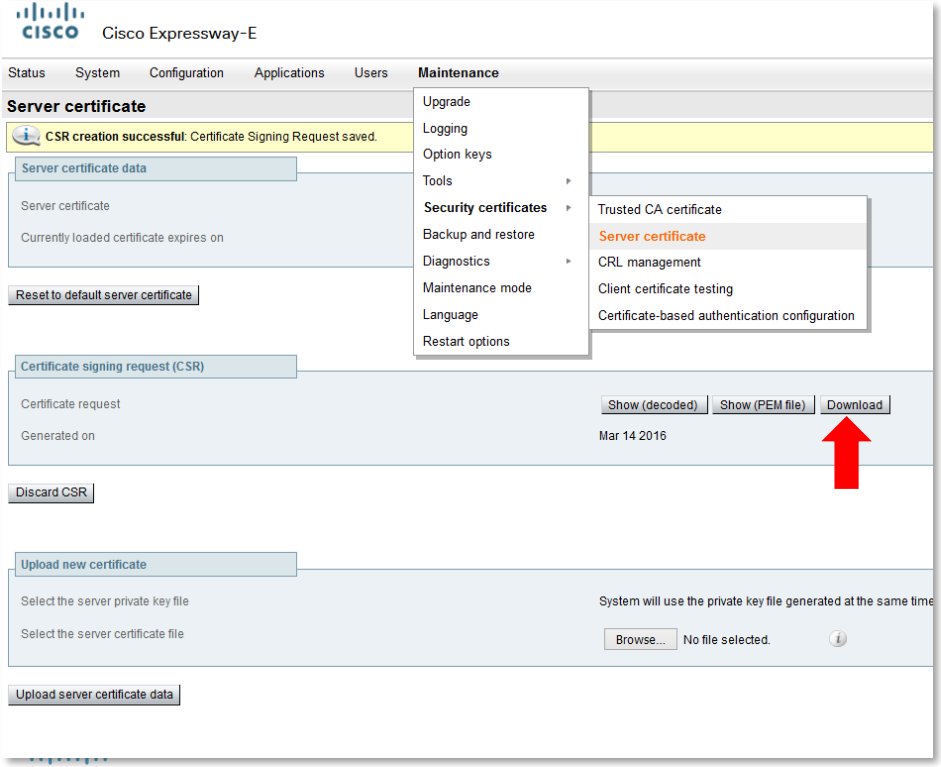




© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Certificates Expressway: HOW To Get Them contd..

Generate CSR, Download, Send it to the CA



Example CSR

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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

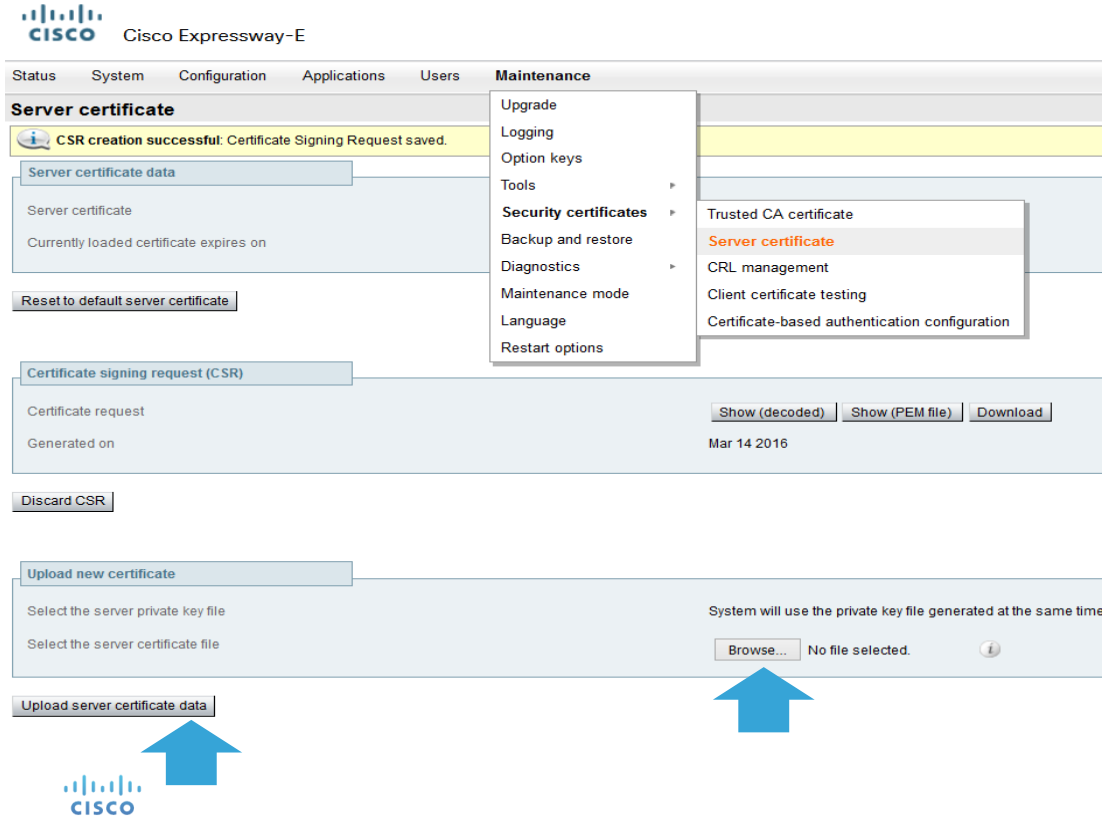
```
X509v3 extensions:
    X509v3 Key Usage: critical
        Digital Signature, Key Encipherment
    X509v3 Extended Key Usage:
        TLS Web Server Authentication, TLS Web Client Authentication
    X509v3 Subject Alternative Name:
        DNS:exp-e.kelzolta.com, DNS:kelzolta.com, DNS:kelzolta.local, 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.

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Certificates Expressway: HOW To Get Them contd..

Uploading Server Certificate



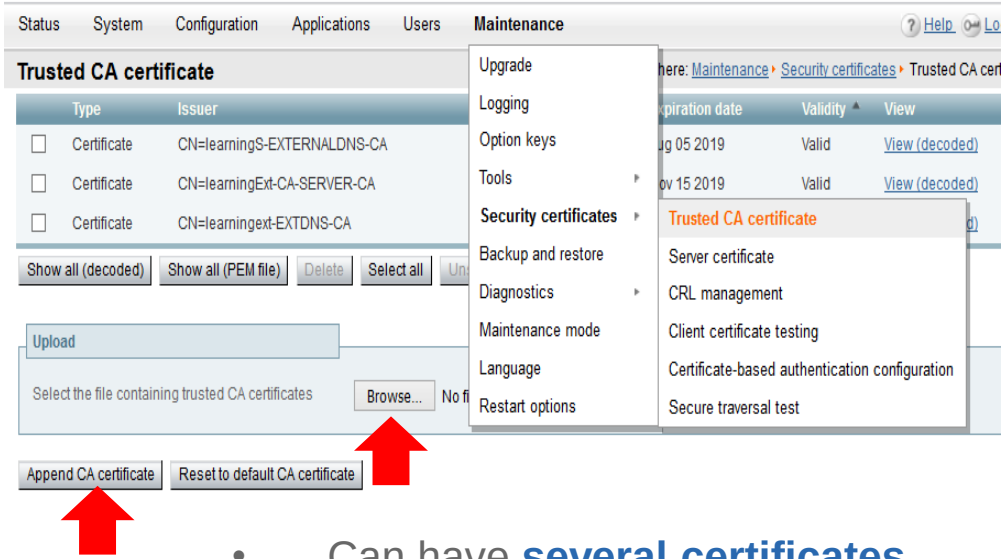
Only one server certificate at a time

Restart of Expressway **required**

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Certificates Expressway: HOW To Get Them contd..

Uploading Root/Intermediate certificates to Expressway

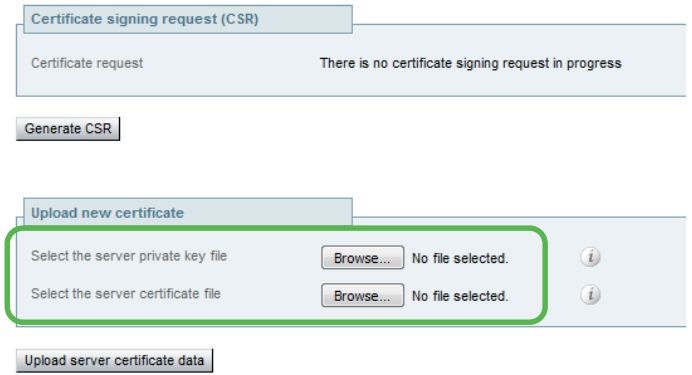


- Can have **several certificates**
- **Trusted Root and intermediate** certificates go in this store, including the CA certificates signing the Expressways own certificate
- Root/Intermediate certificates signing the other Expressway's cert, CUCM's cert etc.

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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 that **4096bits** should not be used



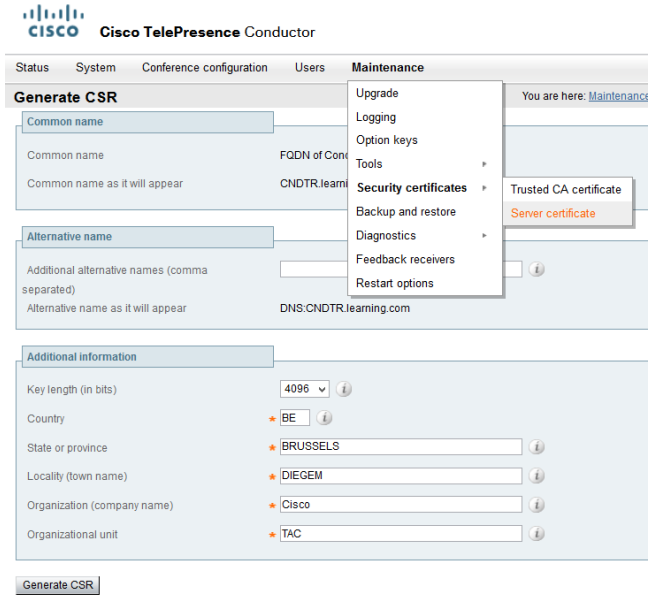
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

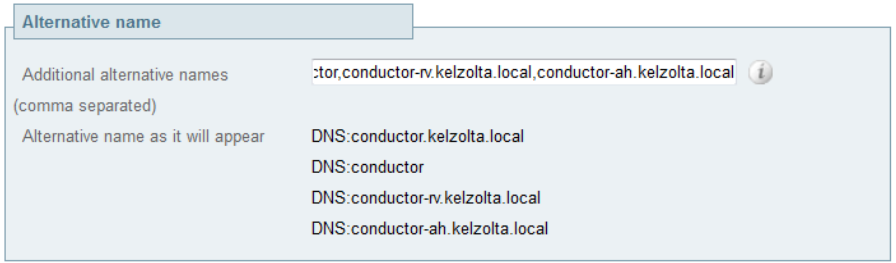
Certificates on Other Telepresence Devices

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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

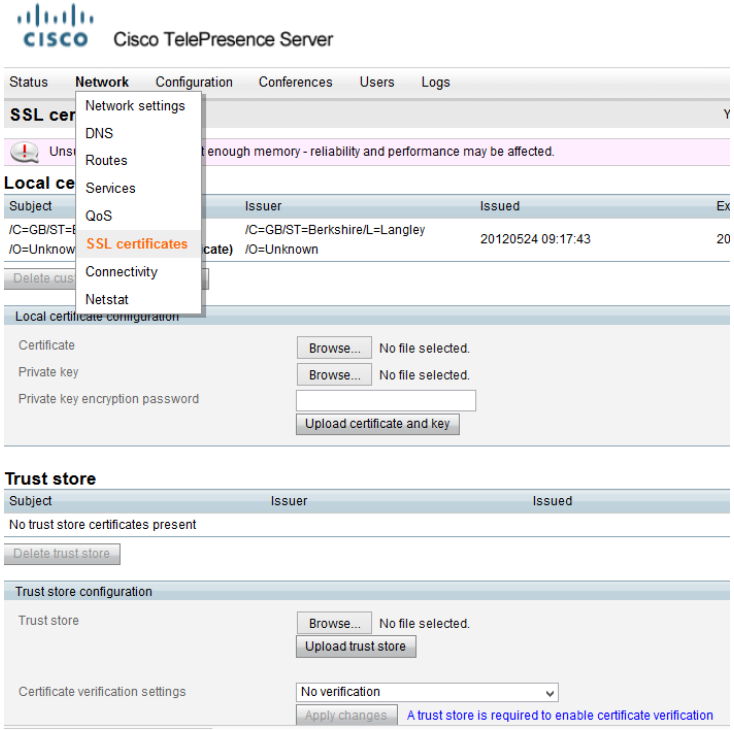




© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Certificates : Telepresence Server / MCU

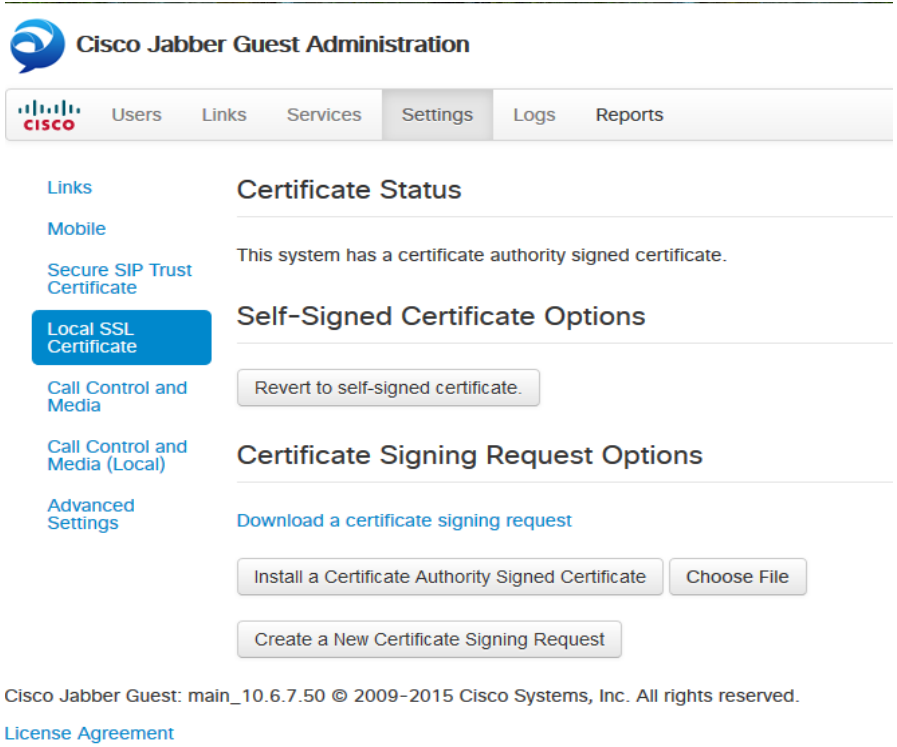
- **Cannot generate its own CSR**
- All **trusted certificates** must be uploaded **in one file**, each upload overwrites the “trust store”
- Certificate verification by default turned off.



© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Certificates : Jabber Guest

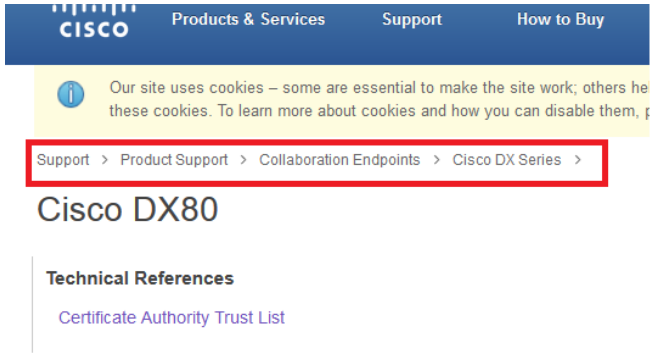
- GUI offers only very **basic CSR**
- More advanced certificate management must be performed from **Linux CLI** (see Install Guide for details)
- All members of a cluster must have respective certificates



© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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



© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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

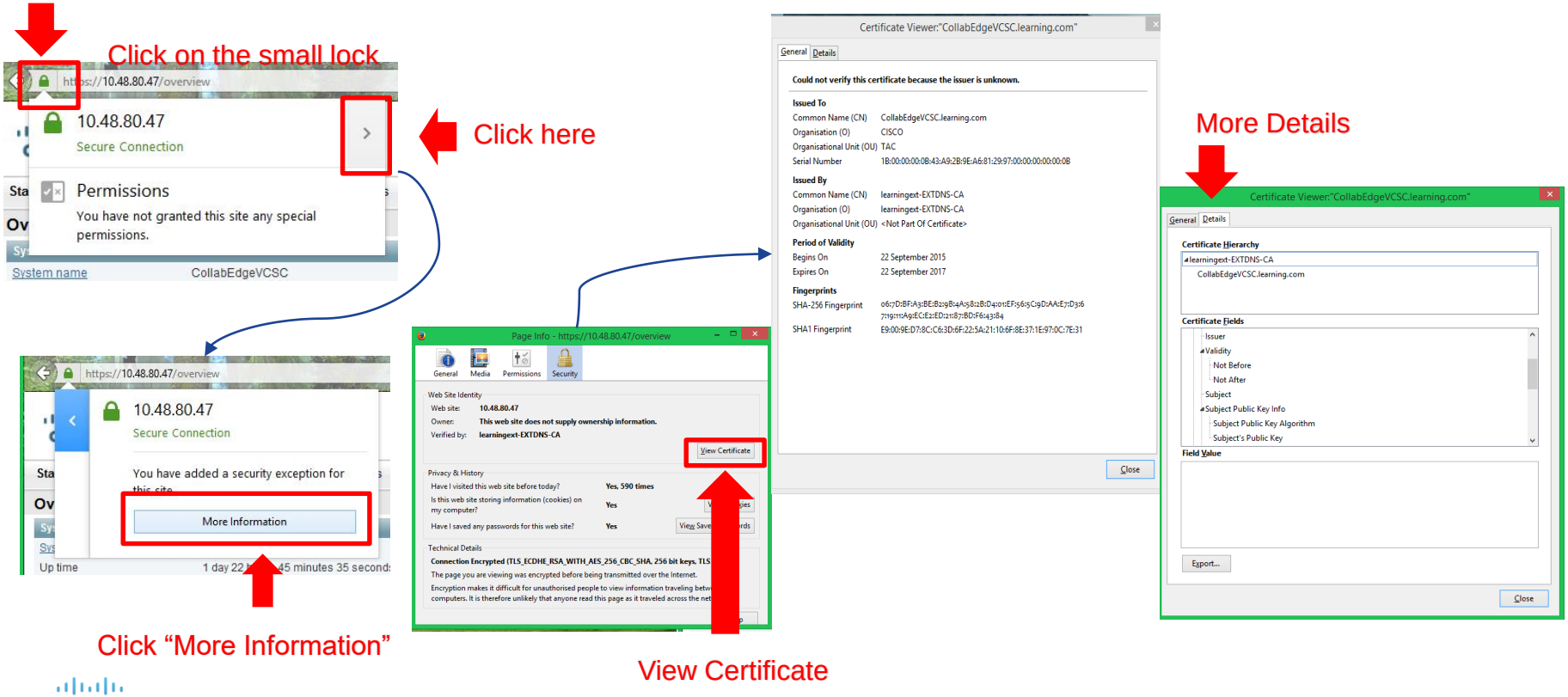
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Troubleshooting

common issues and how to solve them

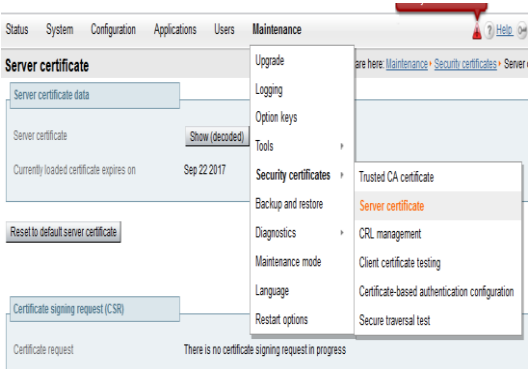
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

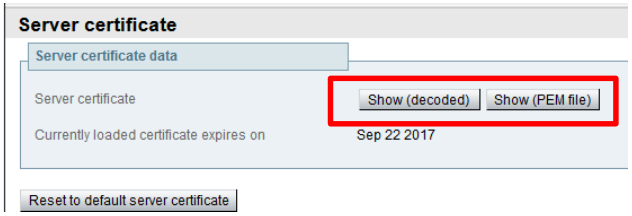
Troubleshooting: Viewing Certificates



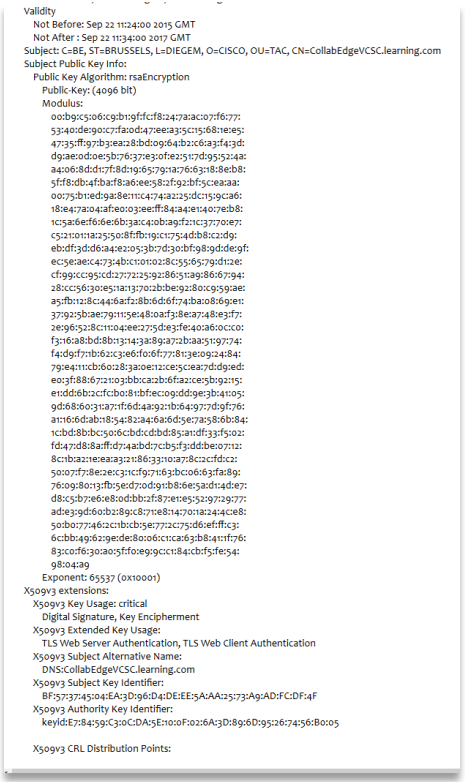
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Troubleshooting: Viewing Certificates

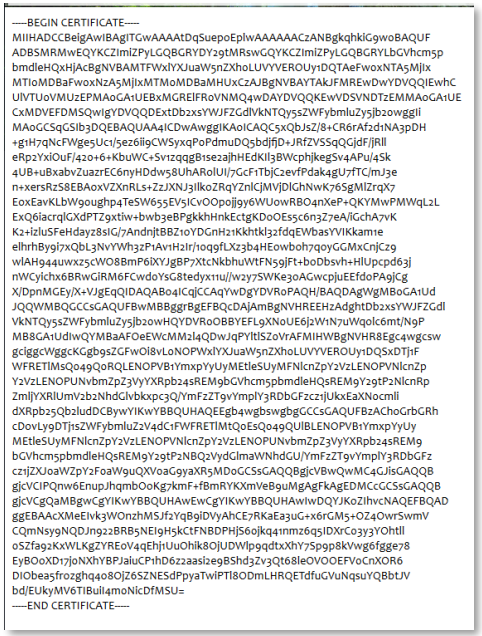




Show Decoded



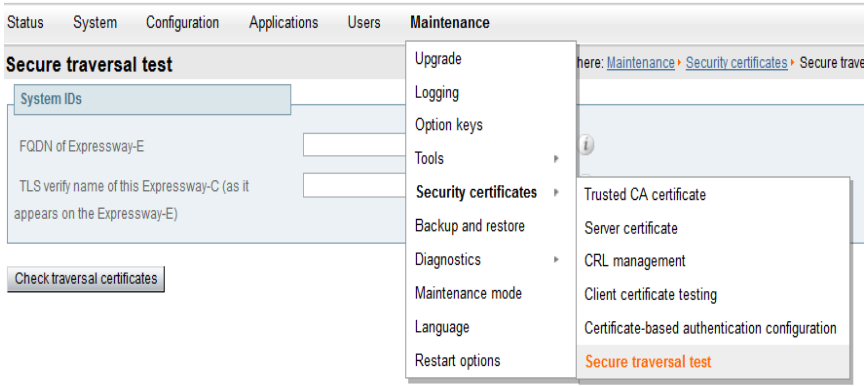
Show PEM

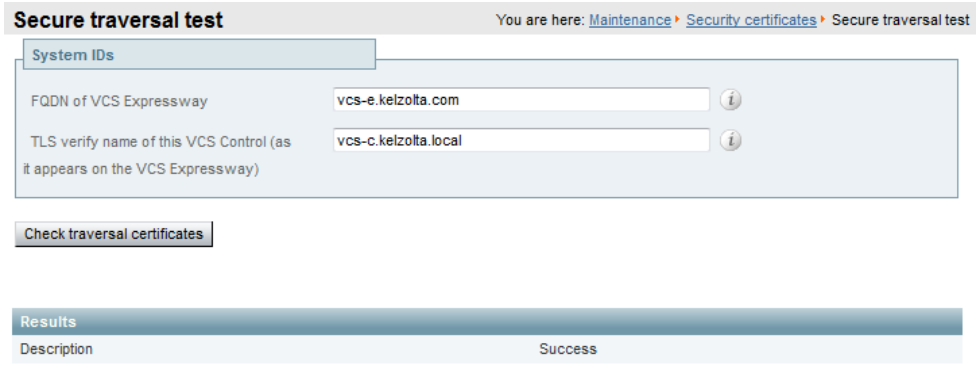


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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





© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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

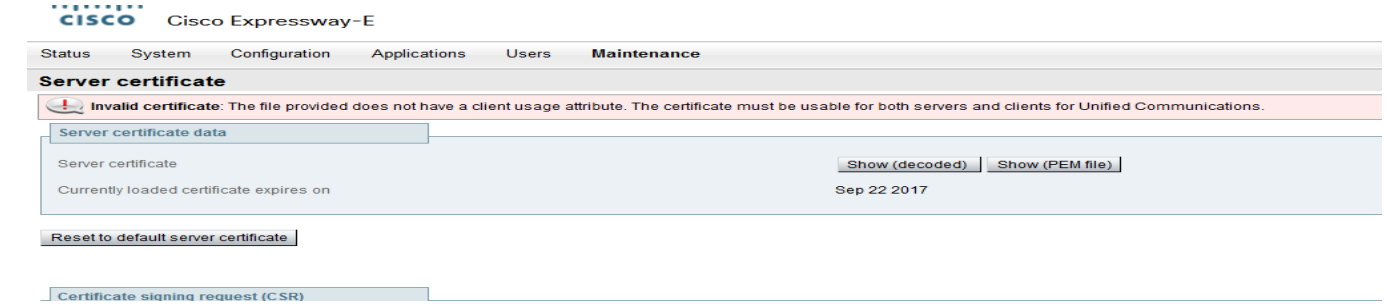
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

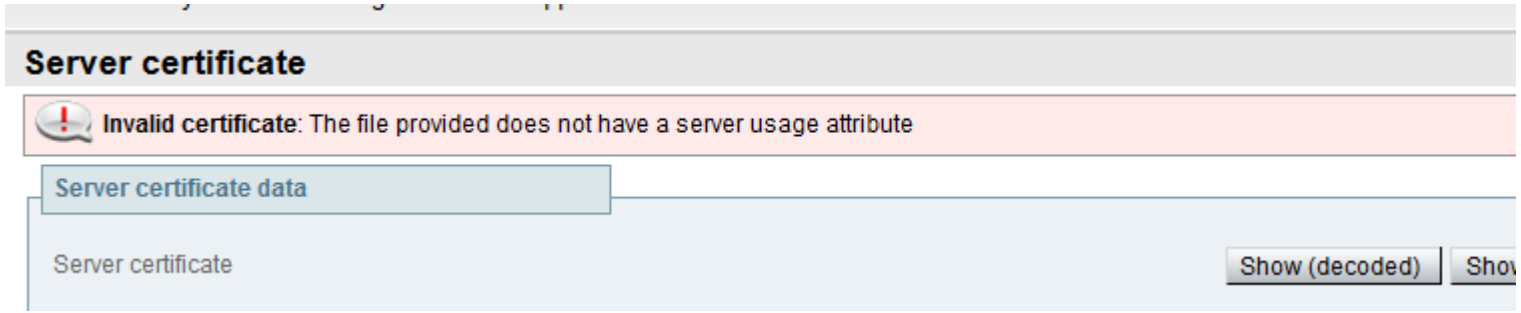
Troubleshooting: Common Issues

- 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)

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

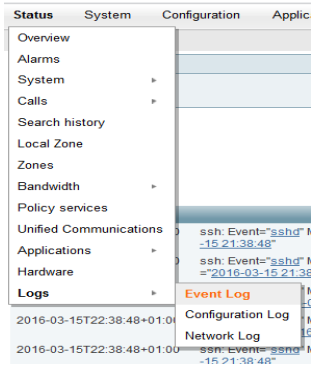
Troubleshooting: WebServer-Client Attribute Absent





© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Troubleshooting: Root/Intermediate CA cert not uploaded



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="xwaye.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="xwaye.coluc.com" Level="1" UTCTime="2014-03-24 17:36:30,872"

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

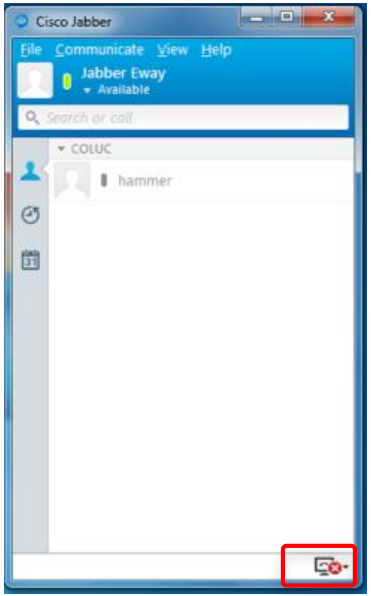
Troubleshooting: Certificate Presented does not match FQDN

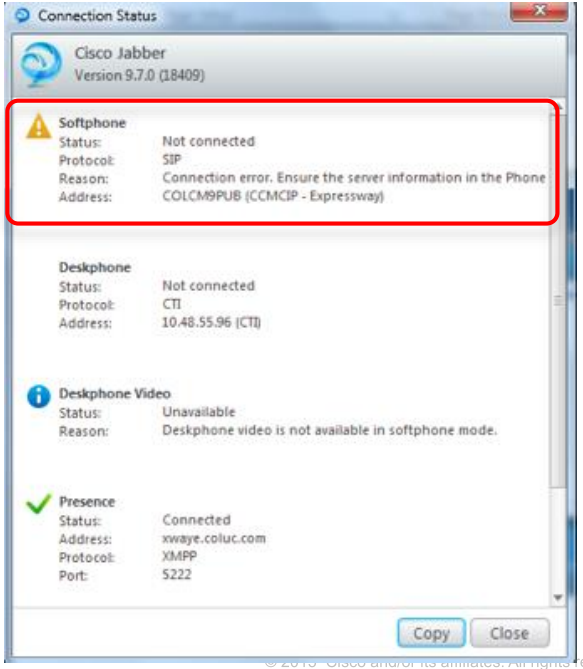
2016-03-15T22:27:33+01:00 CollabEdgeVCSC management: UTCTime="2016-03-15 21:27:33,709" Module="developer.management.cucmconfig" Level="WARN" CodeLocation="ucqueryrun(100)" Detail="Certificate validation failed" Host="pub10.learning.com" Error="Server presented certificate that does not match host pub10.learning.com: {'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', 'caIssuers': (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'),))}"

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

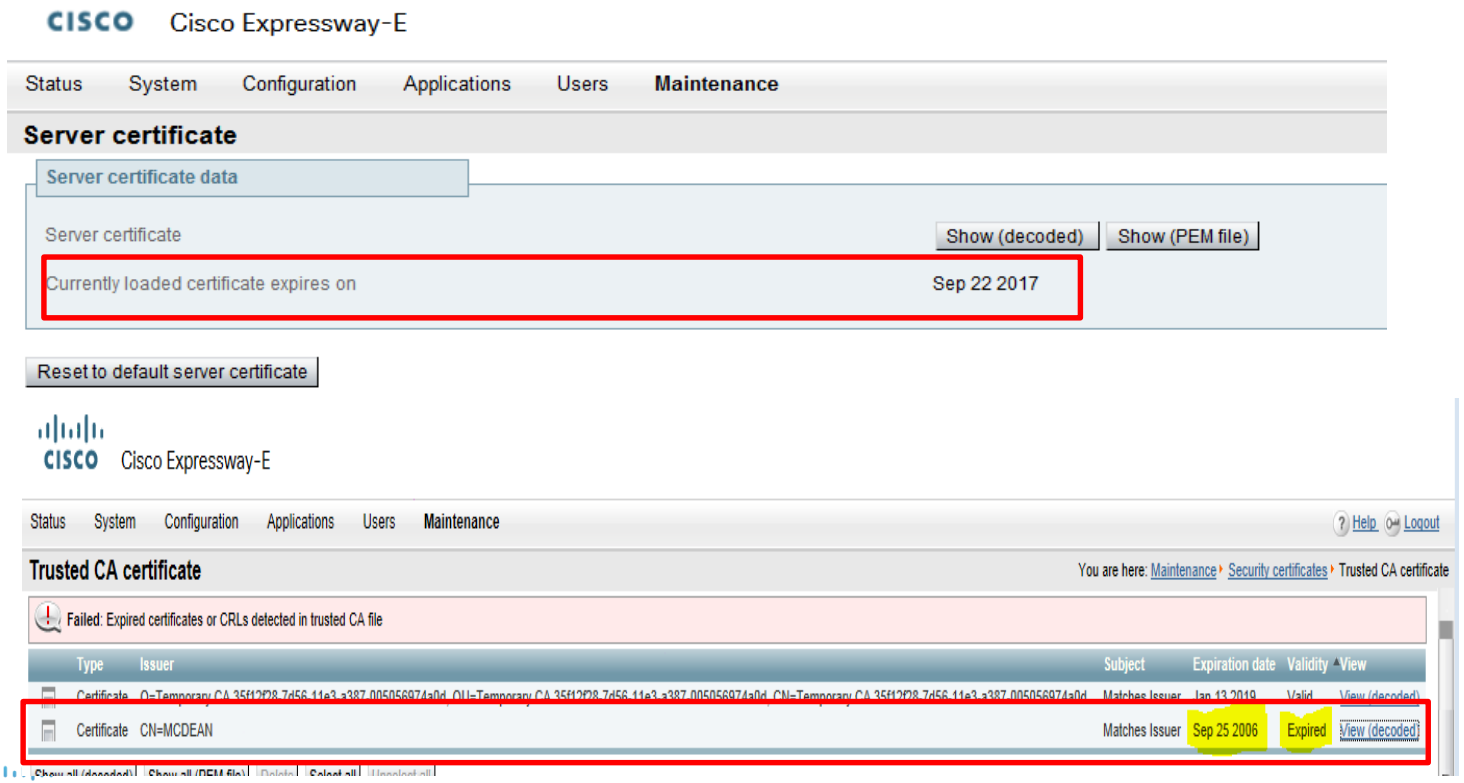
Troubleshooting: Security Profile not listed in Expressway-C SAN

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





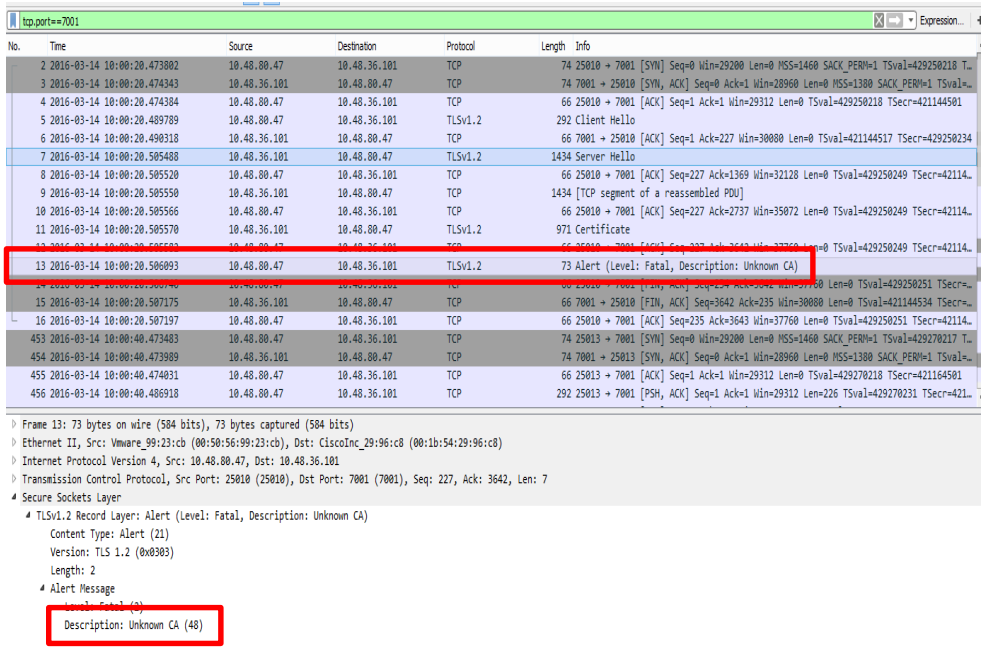
Troubleshooting: Certificate Expiry



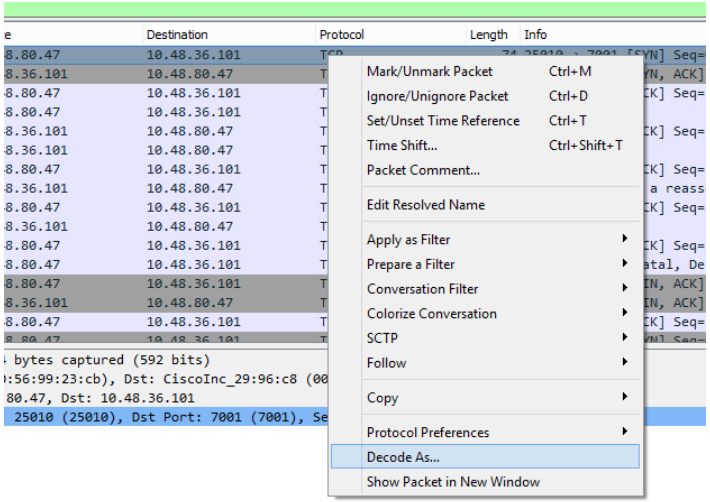
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Troubleshooting: Extract Certificates from Wireshark

Filter the packets on the secured port



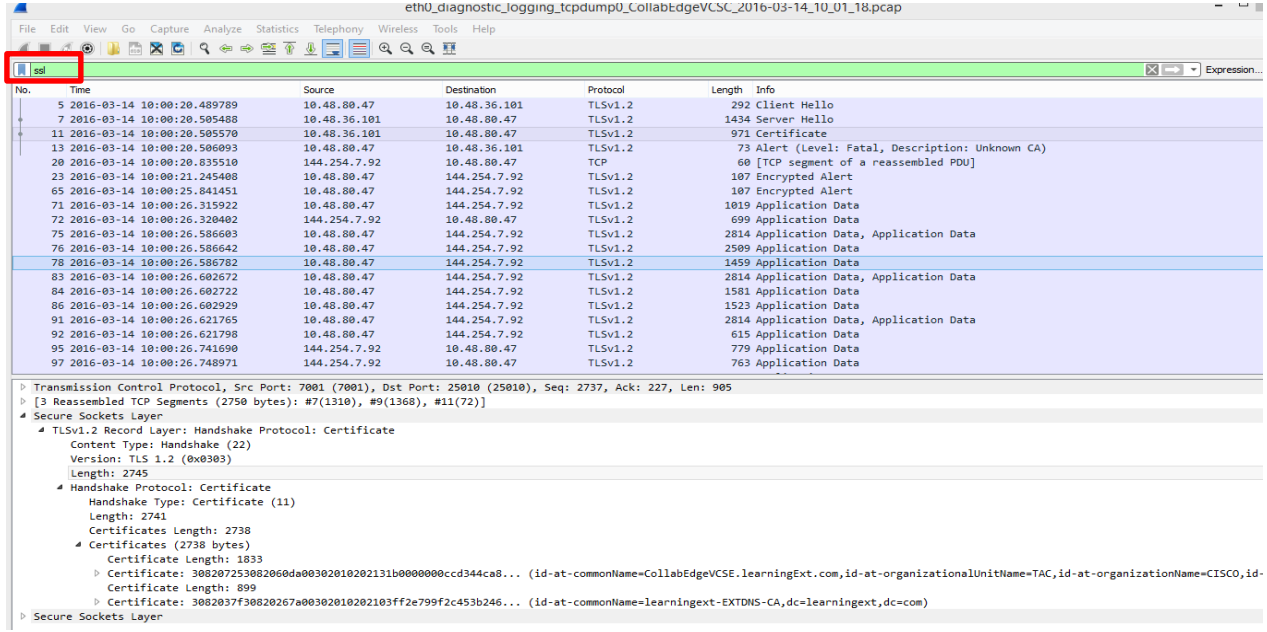
Right Click → Decode As → SSL



© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

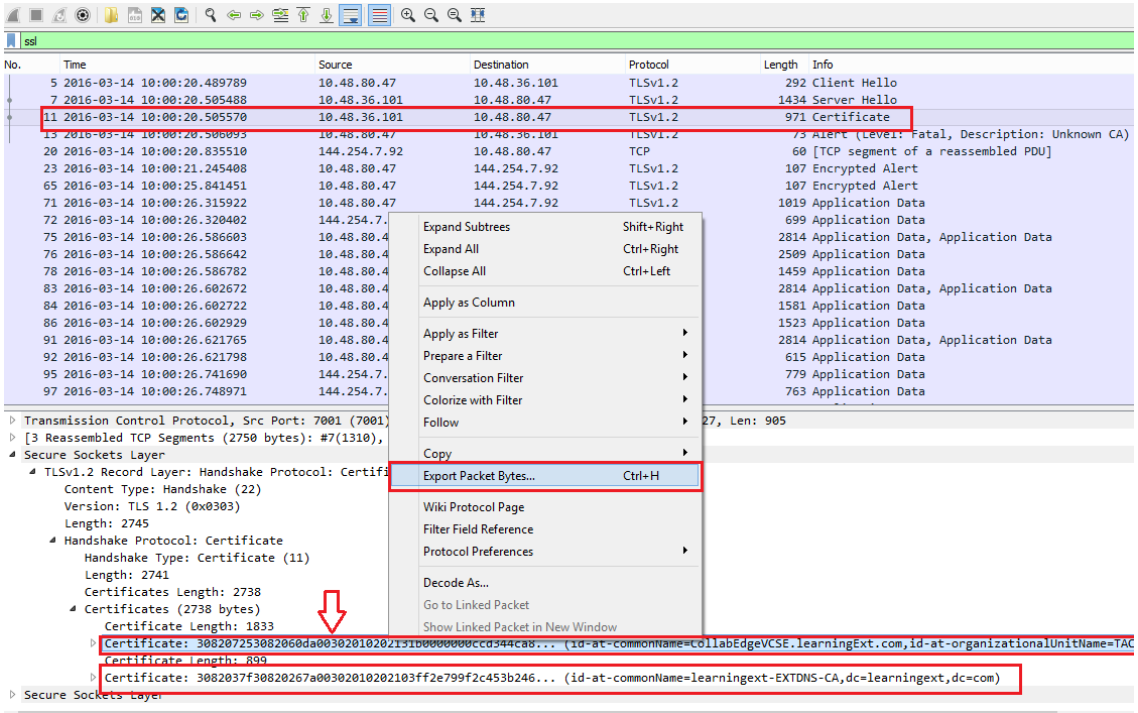
Troubleshooting: Extract Certificates from Wireshark contd..

If port not known, try filtering using SSL protocol

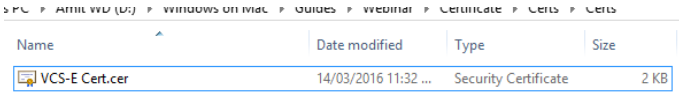


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

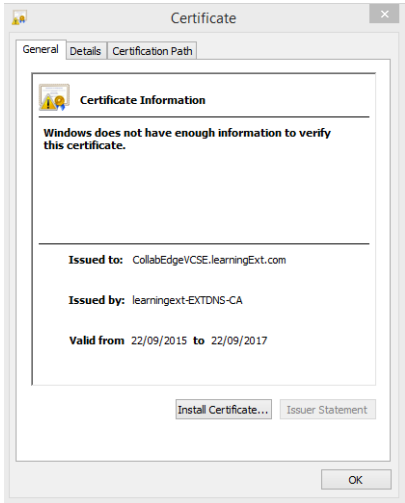
Troubleshooting: Extract Certificates from Wireshark contd..



Save the exported file



Open the certificate



© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Further reading

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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

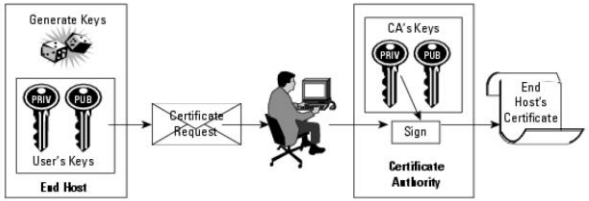
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

UCM Public Key Infrastructure

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

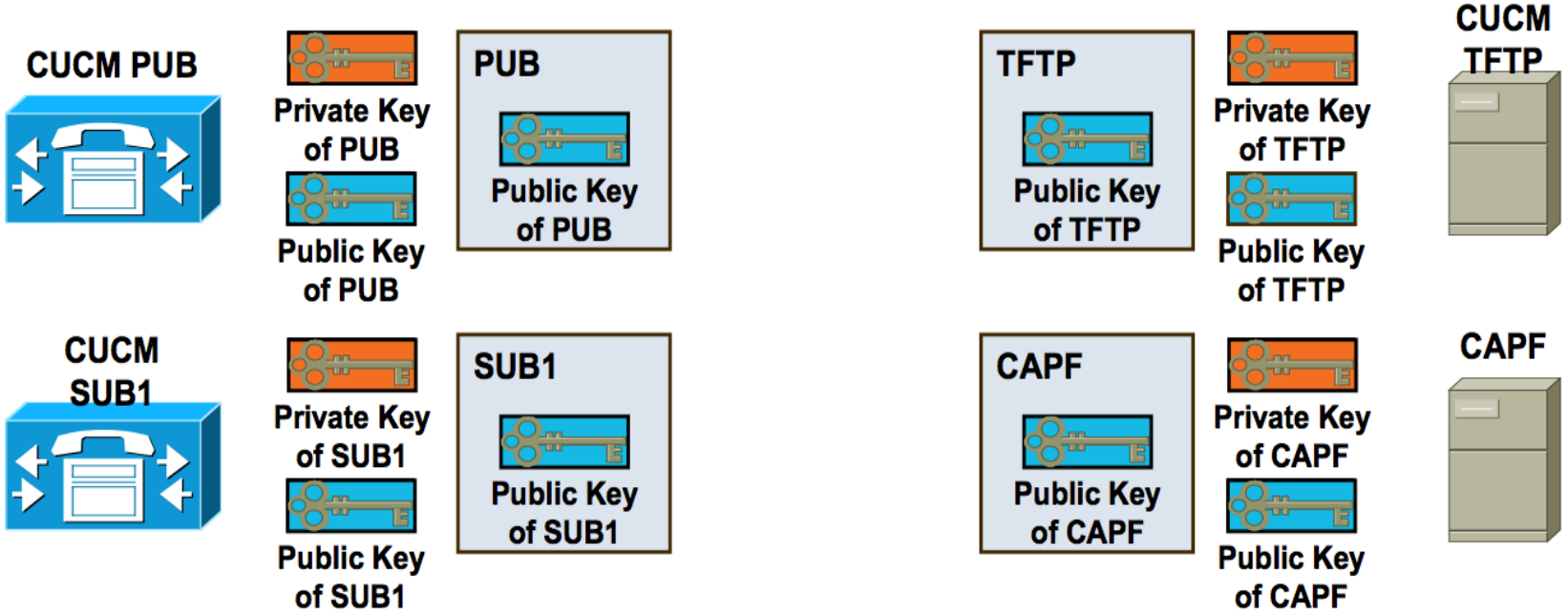
Encryption with the public key is decrypted with the private key and vice versa

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



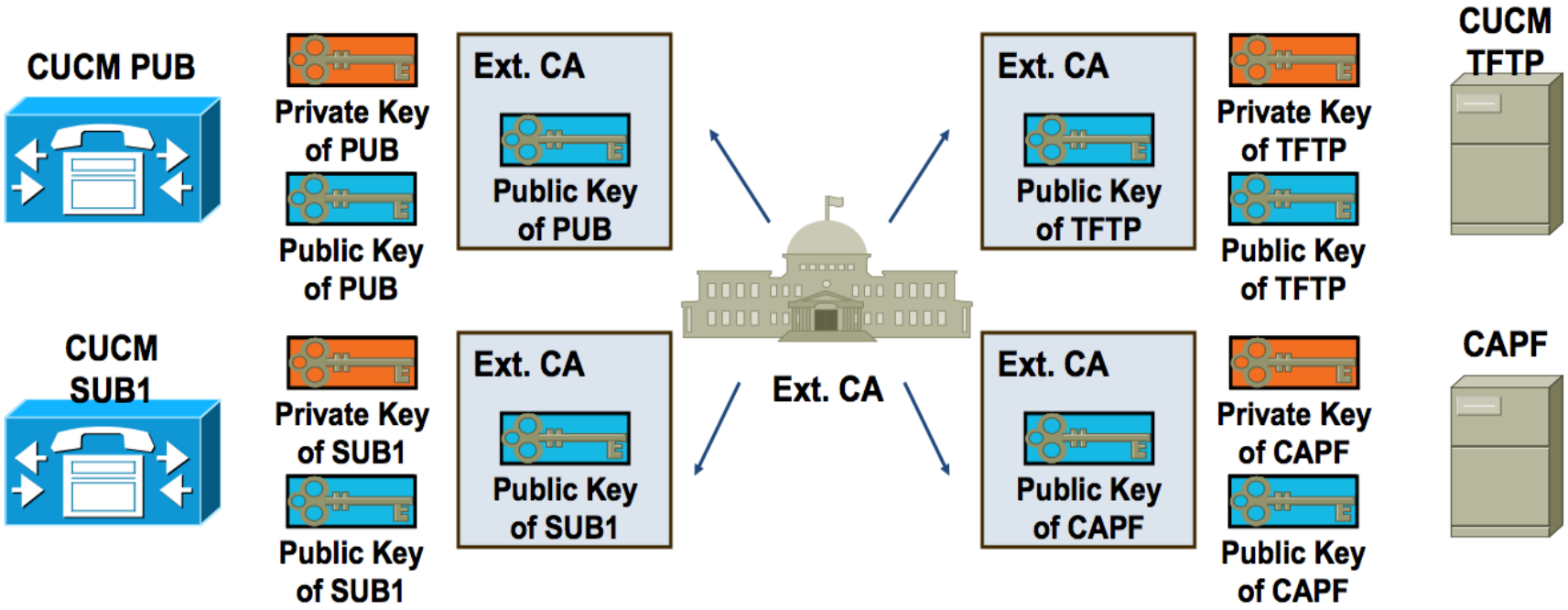
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

UC Server Certificates in CUCM



© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

UC Externally Signed CA Architecture



© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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
```

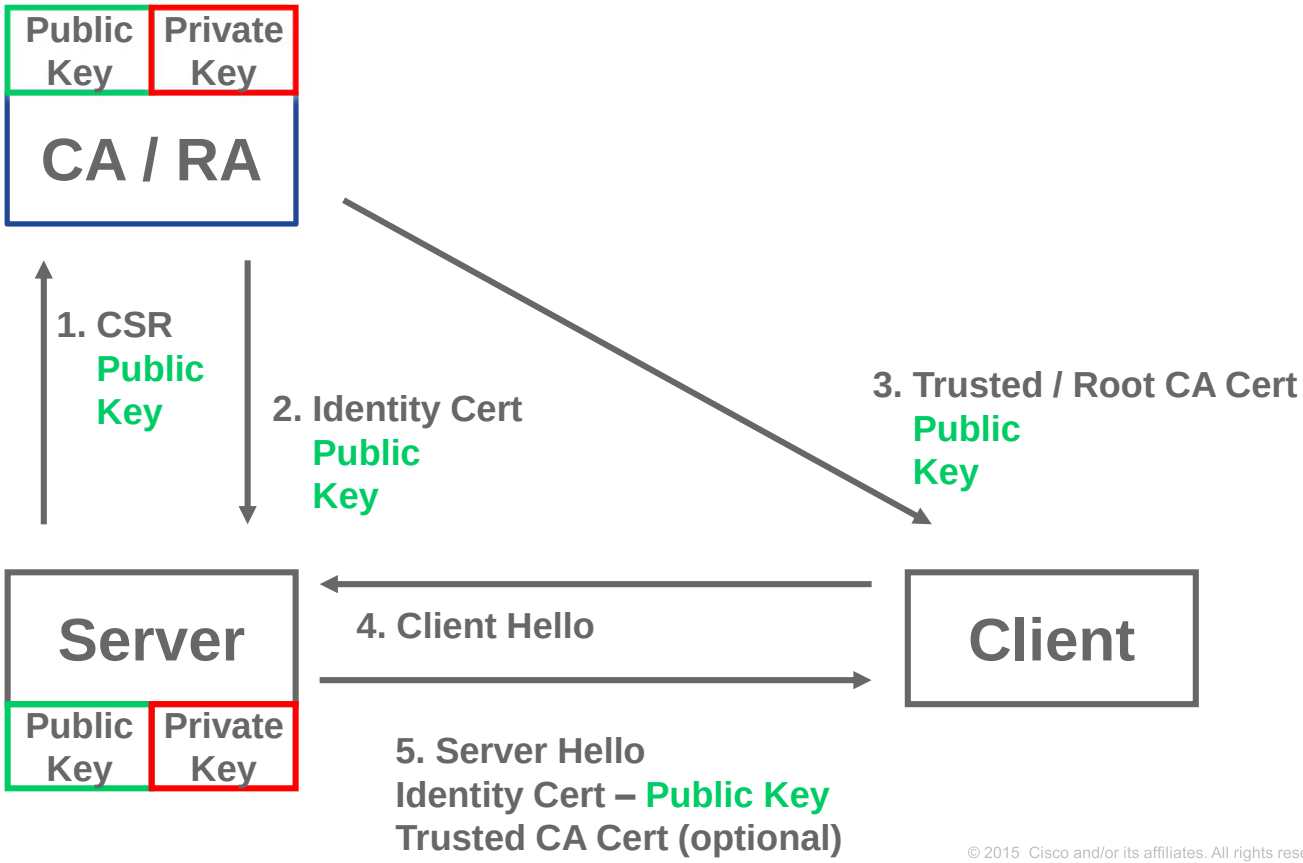
- Certificates Validity of 5 Years
- CallManager , CAPF, ipsec certificates are generated using 1024 bit RSA Key (UCM 10 onwards 2048 bit RSA Key)
- Tomcat and TVS are generated using 2048 bit RSA Key
- CSR for the services used to get it signed by 3rd party CA

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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.

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential



© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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
```

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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 3rd 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,
tvs-trust	Only used if TVS 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

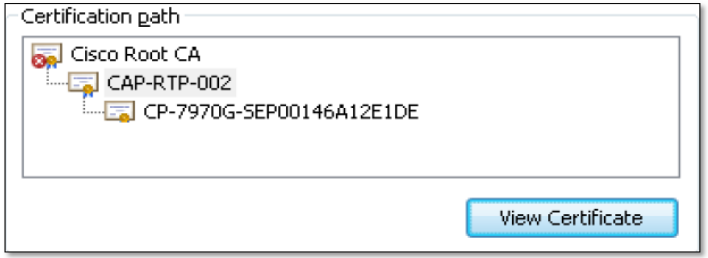
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

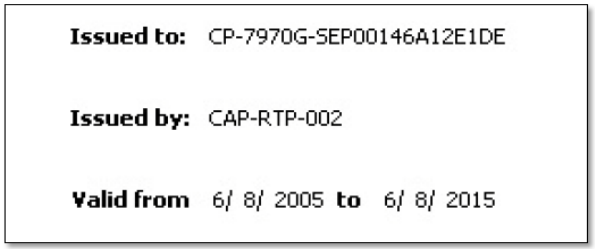
UC – IP Phone PKI

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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





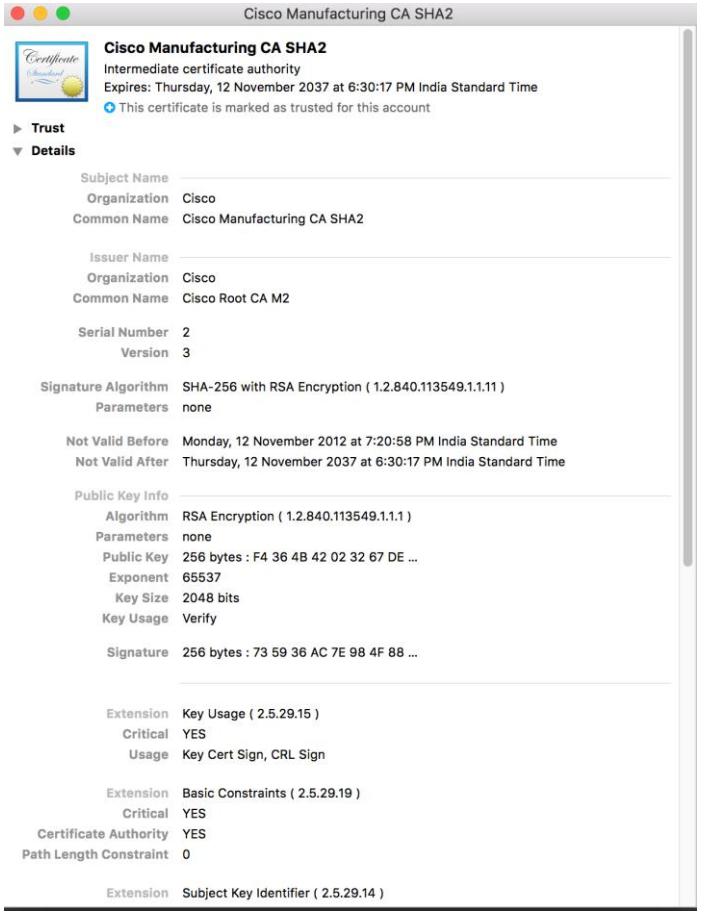
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

MIC – Best Practices

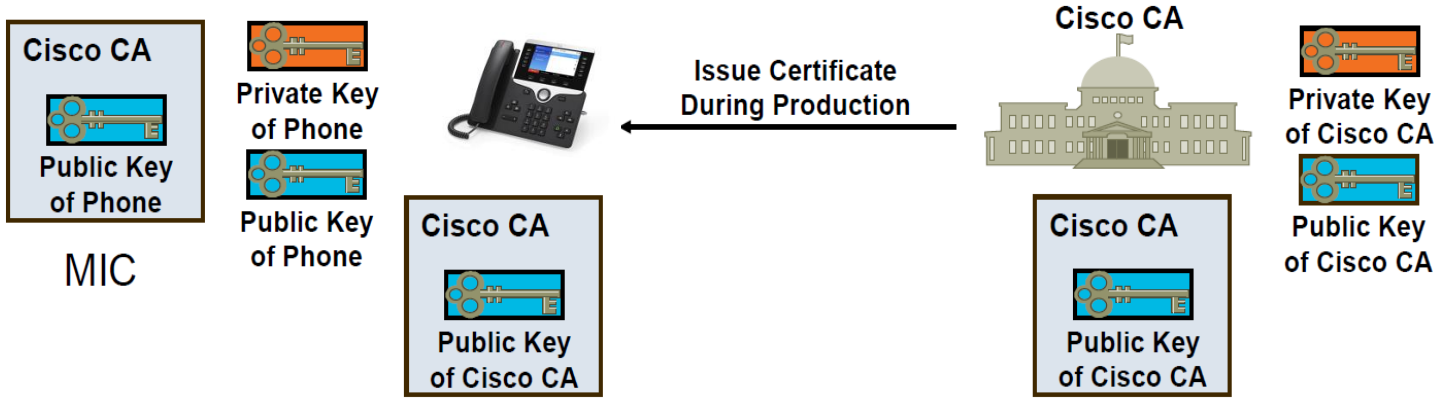
- Ideal use for building initial LSC for phone
- MIC is installed during manufacturing of phone and cannot be revoked
- LSC takes precedence when both MIC and LSC are present
- Certificates installed to trust MIC is listed below in the screenshot

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:

CMCA2



MIC PKI Topology in CUCM



© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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

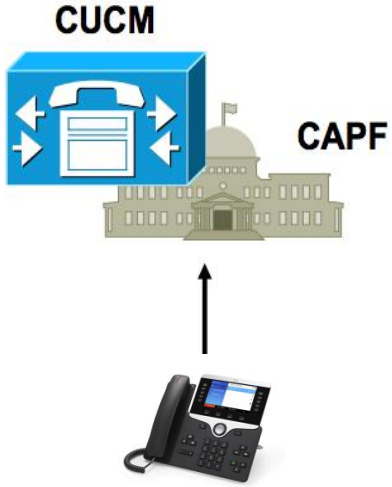
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

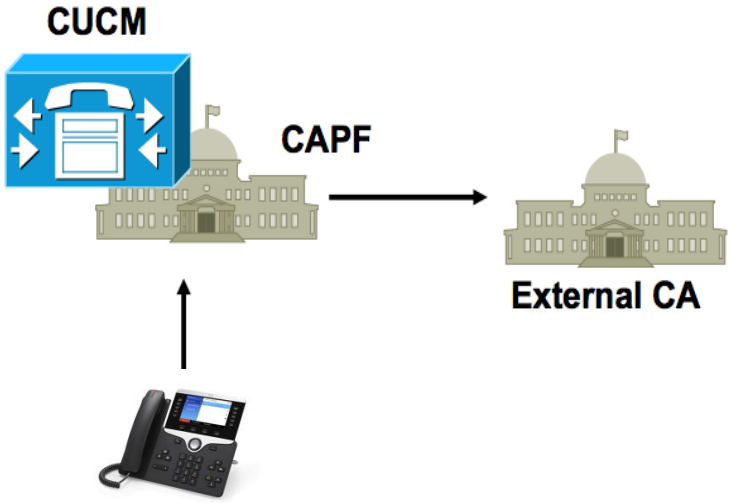
CAPF – Certificate Authority Proxy Function

- 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:

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Trust Verification Service

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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.

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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.

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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.

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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	ISSUERNAME	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>
```

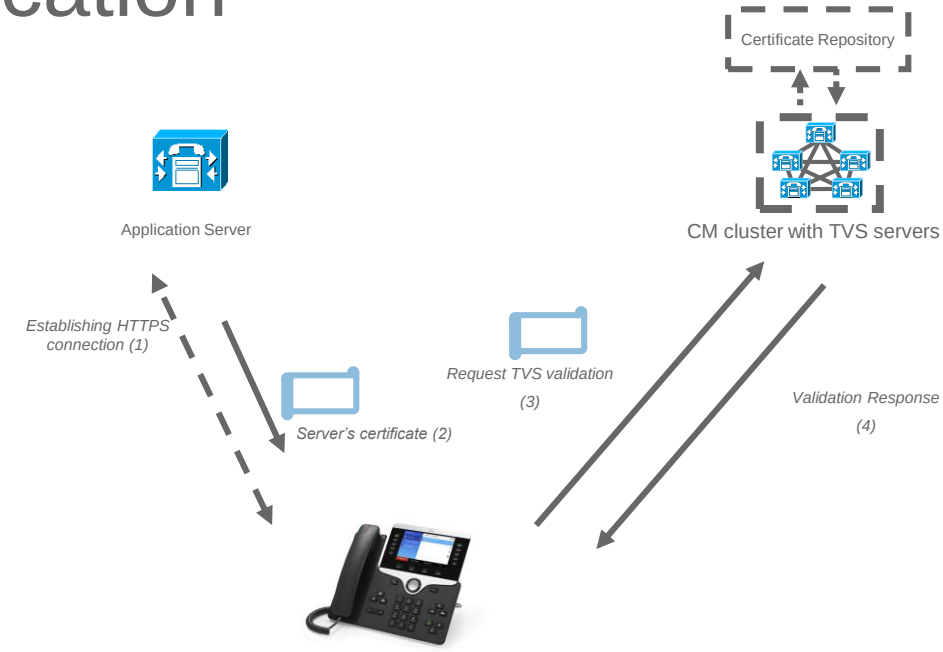
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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

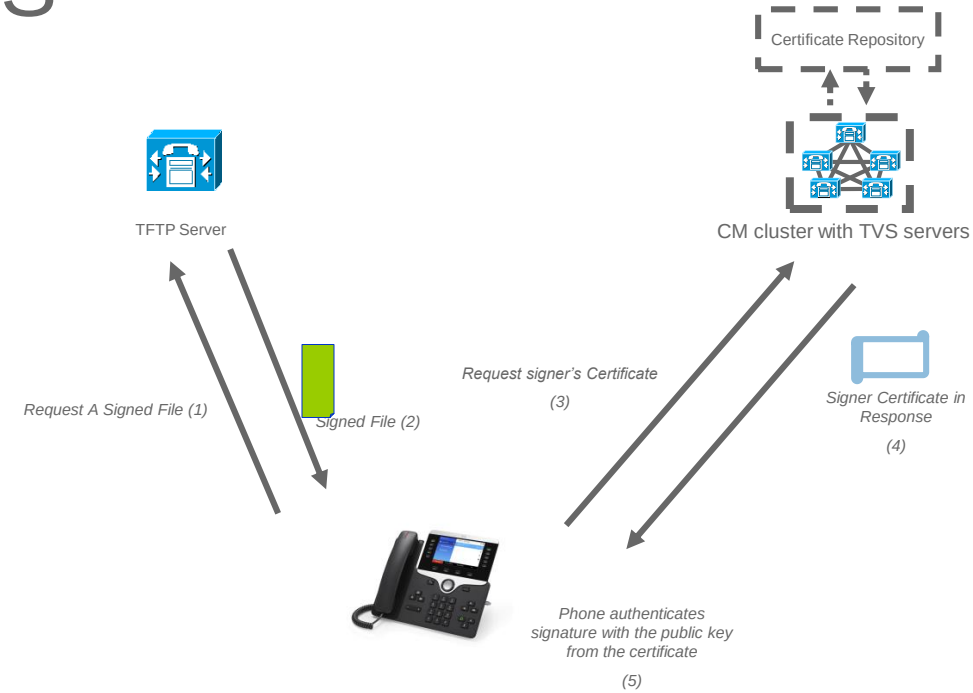
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

TVS Protocol – Server Certificate Authentication



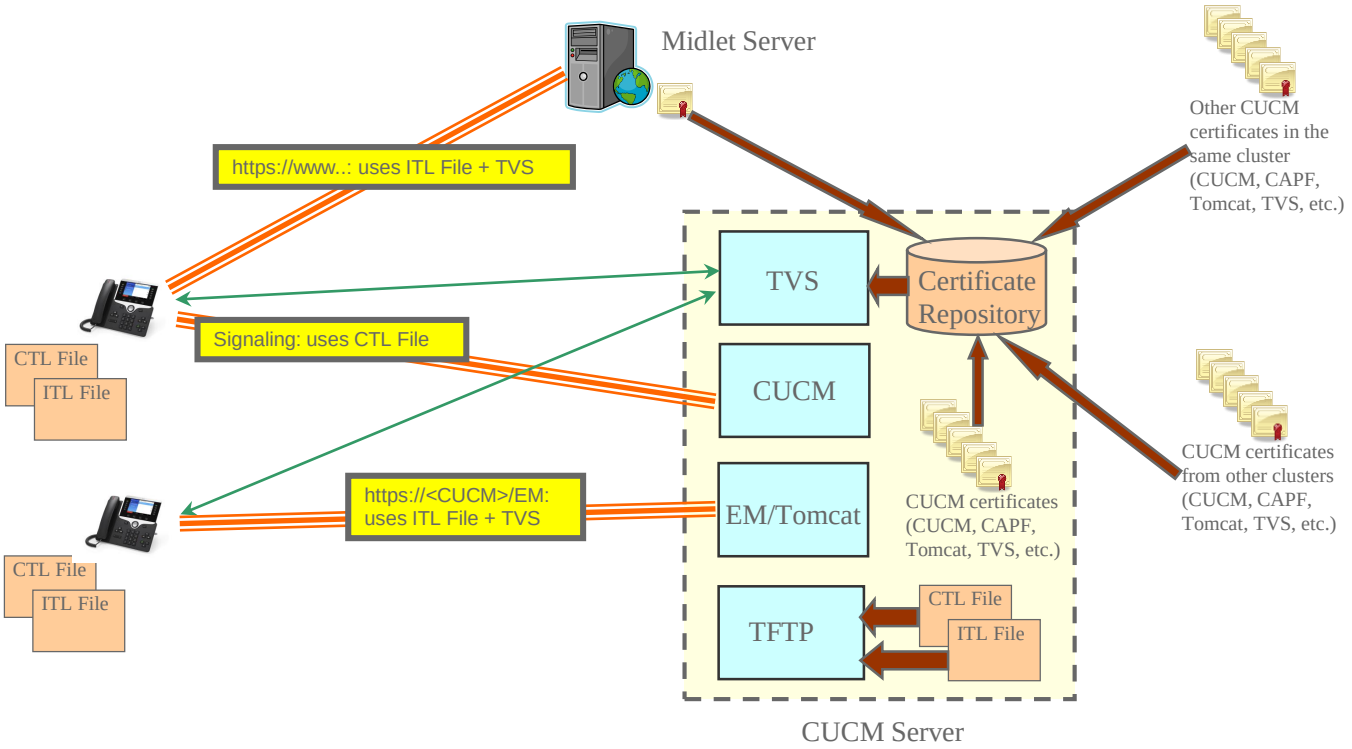
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

TVS Protocol – Signed File Authentication with TVS



© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The Big Picture



© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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+)

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Certificate Monitor Daemon

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Certificate Monitor Alarm Catalog

Alarm Message Definitions

Search Options

Find alarms where CallManager Alarm Catalog Equals* CertMonitorAlarmCatalog Enter Alarm Name [ ] Find

Status:

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

Search Results

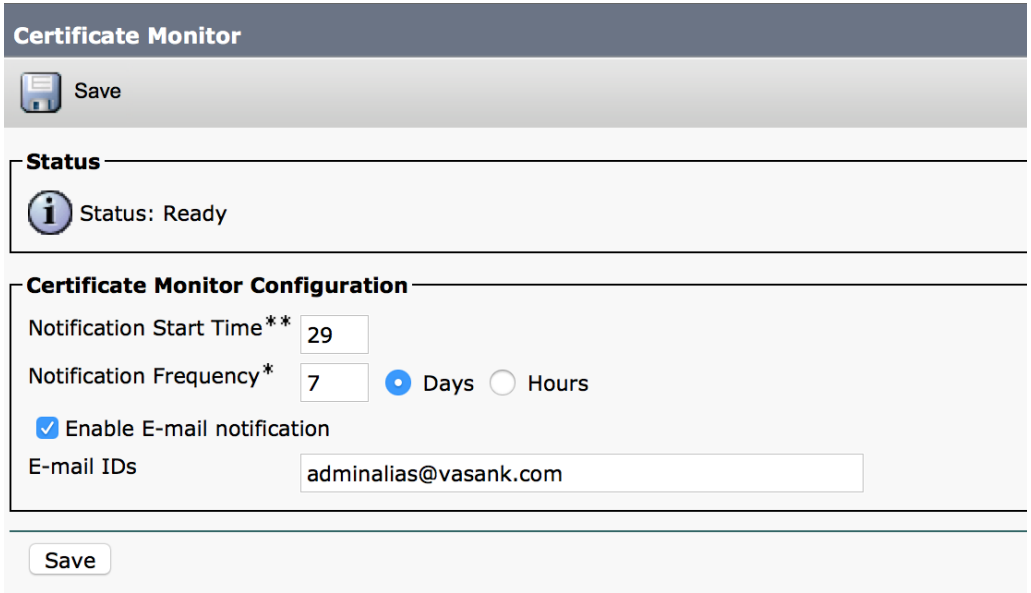
Alarm Name	Description	Recommended Action
CertValidLessthanADa...	Certificate is about to Expire...	Re-generate the certificate th...
CertValidfor7days	Alarm to indicate that Certifi...	Re-generate the certificate th...
CertValidityOver30Da...	Alarm to Indicate certificate ...	Re-generate the certificate 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 10 Page 1 of 2

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Certificate Monitor Feature

Cisco Unified OS Administration > Security > Certificate Monitor



© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Certificate Regeneration

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

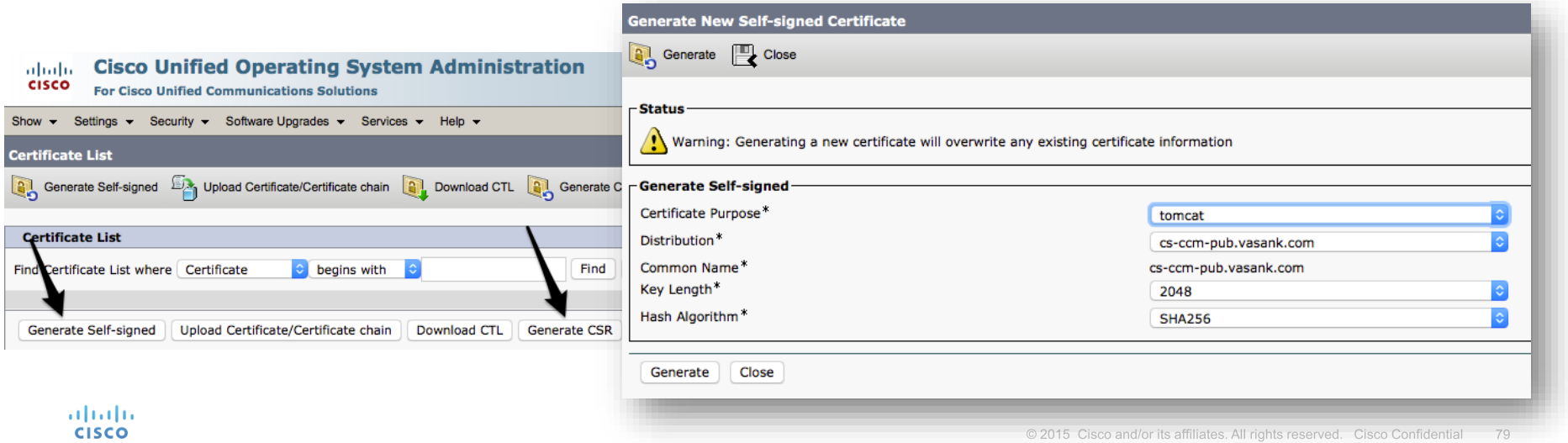
Scenarios

- 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)

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Regenerate tomcat certificate

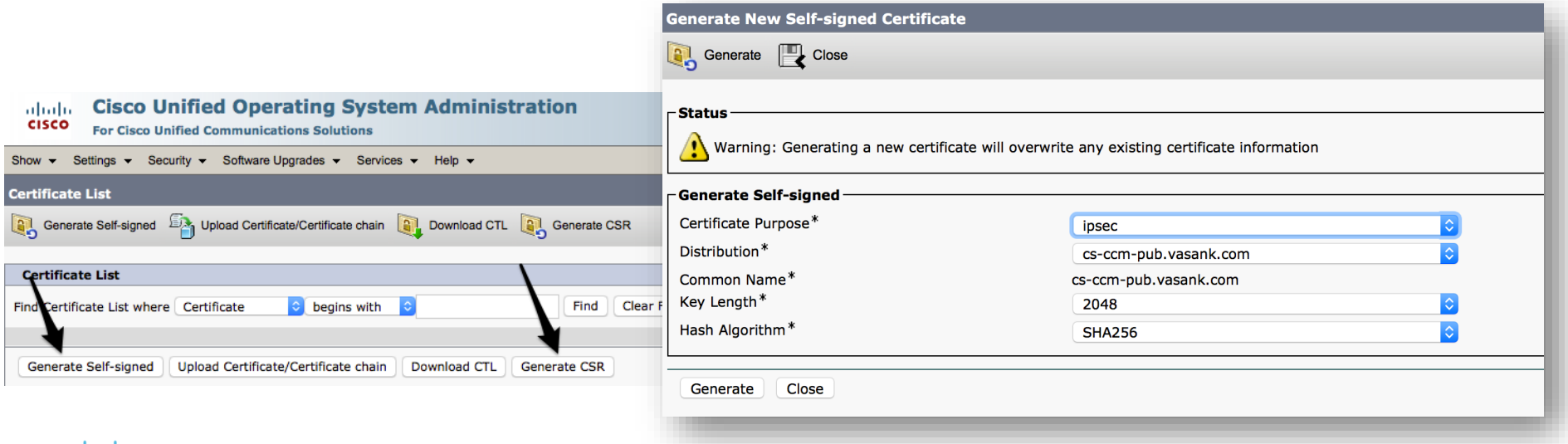
- Minimal service impact
- Requires restart of Cisco Tomcat Service for the new certificate to take effect.
- Verify if the UCM server has any external integration with AXL, CCMCIP, UDS



© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Regenerate ipsec certificate

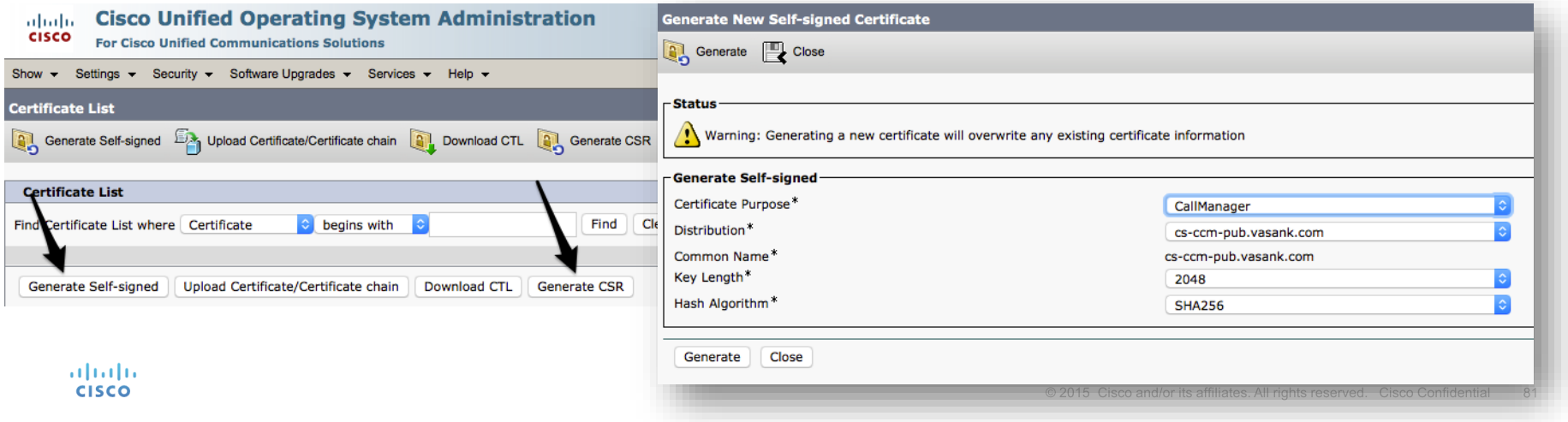
- Requires restart of DRF (Master) and Local service on the node
- DRF backup Failure (expired or corrupt certificate)



© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Regenerate ccm certificate

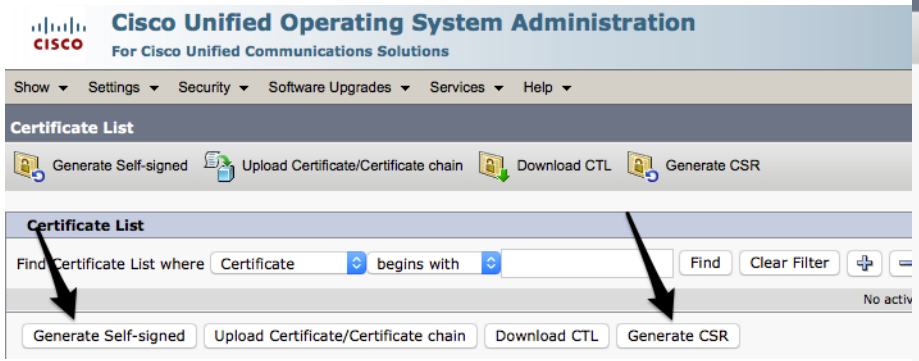
- If the node is TFTP server all phones will be restarted to update ITL file.
- Unregistered phones will be able to update ITL file and will request the new TFTP certificate using TVS service to validate the configuration file.

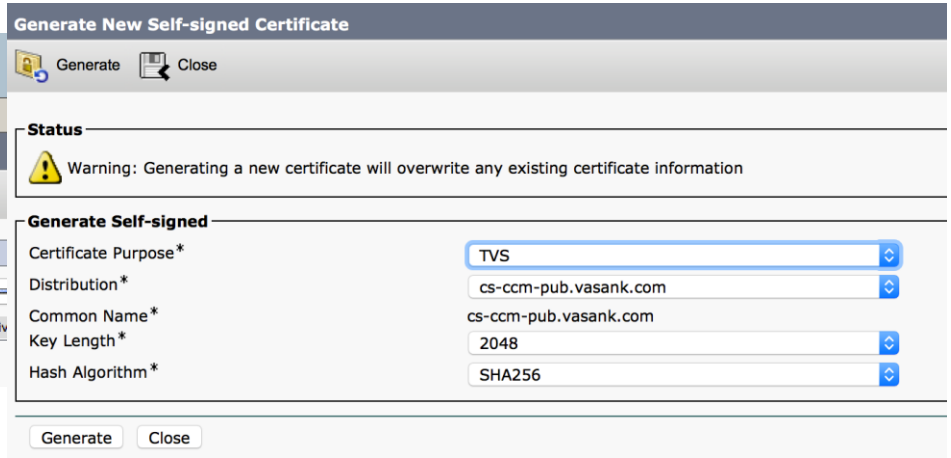


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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.

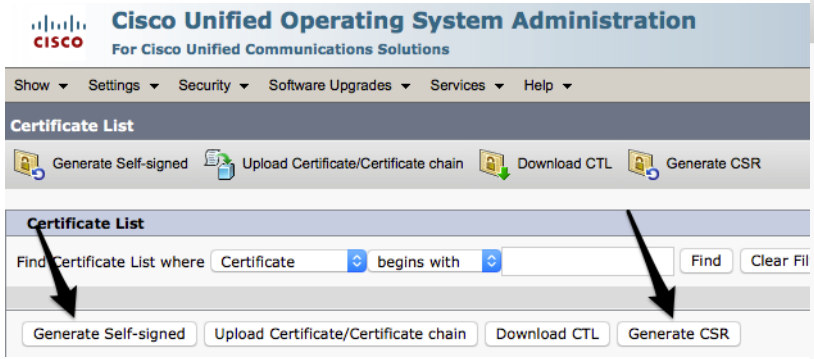


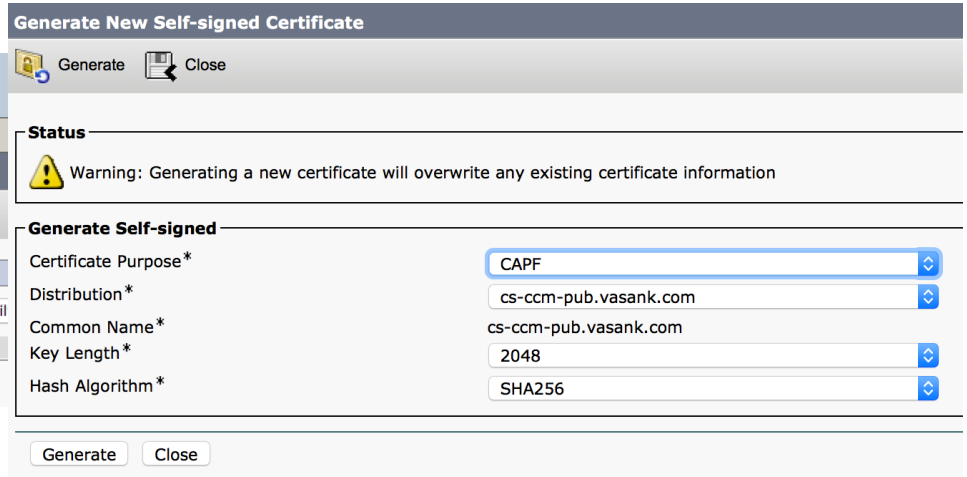


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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





© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Certificate Deletion from Trust Store

CSCus28550

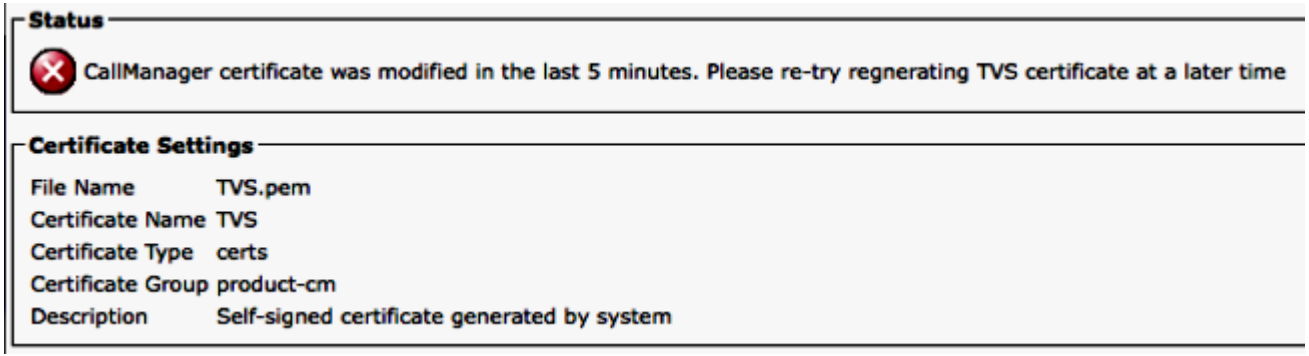
- Prior to 11.0 - Stop “Cisco Certificate Change Notification Service”

- Post 11.0 – Replication Logic still exists along with deletion from one node deletes from ALL.

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Avoiding phone trust list update failure

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



© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

ITL Recovery Method

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

CSCux73531

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.........
```

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

IM and Presence Certificates

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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.

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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.

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

cup-xmpp-s2s Certificate

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

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Troubleshooting

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Certificate Impact on Services

- If Tomcat certificate is expired or keystore is corrupt.
- Serviceability Page Communication between nodes in Trace Confiugration 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

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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

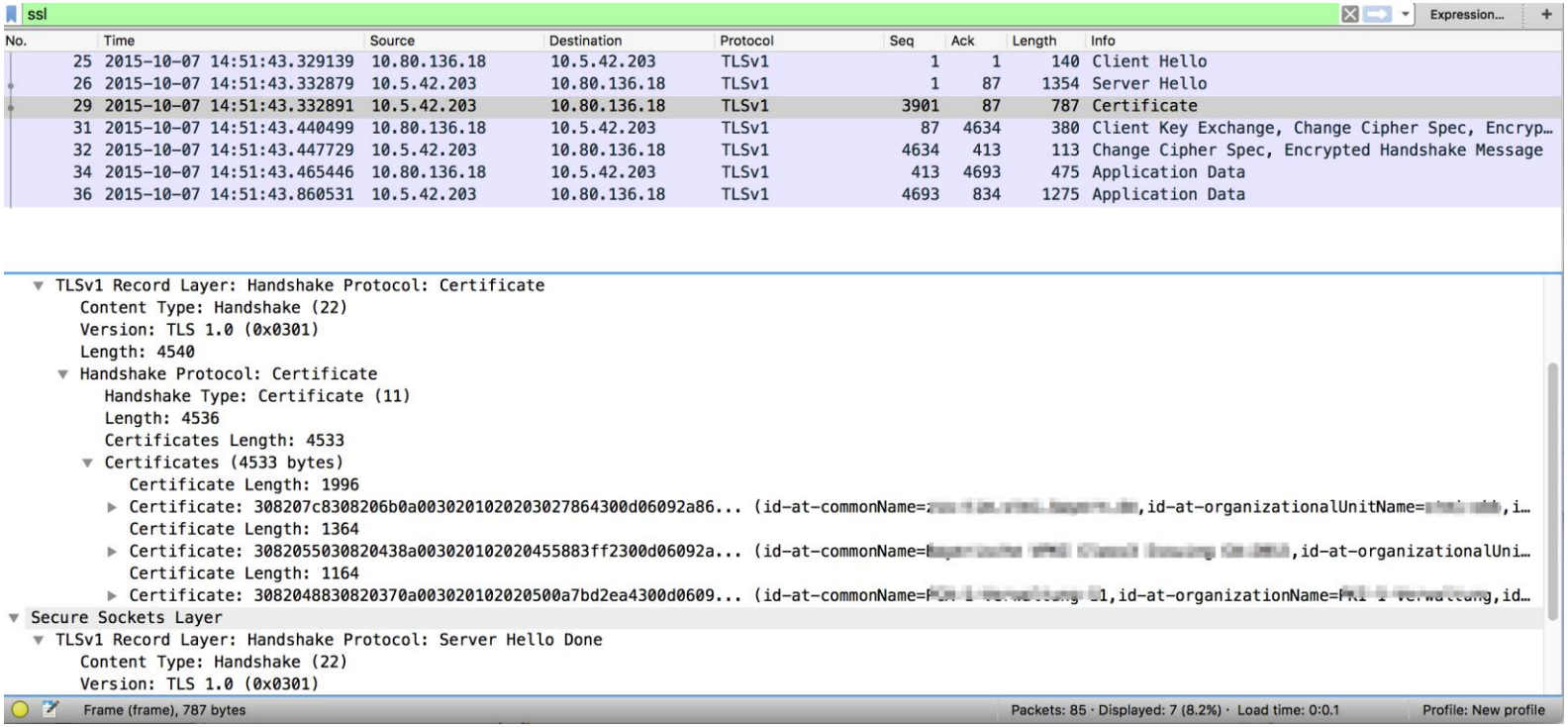
16:02:10.765 | debug tvsHandleCertVerificationReq

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

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

SSL Handshake



© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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=labserver1, IPv4=10.106.97.178, IPv6=, issuerName=L=BGL,ST=KA,CN=labserver1.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=labserver1,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

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Certificate Regeneration – TVS Service

00006935.001 |16:15:38.433 |AppInfo |ProcessCnf Y: certificate U 5e4594df-e935-494a-3549-6db7ffb89c1d, size(2634) serialnumber(6907c5548780e470b9e3cb3164b12c00/5c9a187f6bfcfbbcffc673ee1b4bd001)
00006935.002 |16:15:38.433 |AppInfo |Certificate CNF. ProcessDbChangeNotify - (certificate, action=2) Cert pkid=5e4594df-e935-494a-3549-6db7ffb89c1d. DEBOUNCED (: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=<>

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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
                                        e9oskH6wwv9faBNJO4RusiR5PE+/yIxRqmS5dVMwC8ig6ueg1oFEiNb1OcKUZw3l
                                        Iim0fgqrw1CnmgvJWdpdIV+OJmzu5v/zQGFdPQODhZw7lOqREEXAUspcF/uIT2v2
                                        p4KQjE0CKEkAKVaQyL85L1NAhpYC5G0B0zM6UGVyvBug6xFqKJqaBVQQq1DC+dd/
                                        uhRECYCZlsZP3Ea3L8cSyBA5fsk8rNSWwPZQsDpYc+1/RhXPfjO/mJzH+e9oqL1r
                                        FWNGJPo8T0UEt8i2Pf+4vix/VSfZ4lx9oQIDAQAB
                                        -----END RSA PUBLIC KEY-----
SEPB83861583B73      2                  NULL
```

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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----- MIIBCgKCAQEAkgfWRcugYmCE+JTDmyAXuiY4KKWG+adWCCev0Loy9sZQjaA4t9ox e9oskH6wwv9faBNJO4RusiR5PE+/yIxRqmS5dVMwC8ig6ueg1oFEiNb1OcKUZw3l Iim0fgqrw1CnmgvJWdpdIV+OJmzu5v/zQGFdPQODhZw7lOqREEXAUspcF/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+5SXdB1mcvCi4w4I3Nwe8f4YROC6U2Y4jmeJoZzJ/6C+HwUvkSaCxCU g0d6MTT15bA2mAADOaHD6/acCkXhfoWMspHNPJ5uqr0DxxeuVGB7MkQePE3Vrqfo N4pMXhadSIMBWXsCg4hkvcugI5PijwPb5h4odPGJ5xEgcSsnQ1s/a61+4ouv1pf6 pRSmk+xLMi29MZJa2o0Urny+qbafJd3YcIEB50FXZh9+lFNdt5mkStF/muvsWjt2 FAyxmXup1iKjomJ5rxJEQTtojaJZ7Bf6cQIDAQAB -----END RSA PUBLIC KEY-----

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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_CRENDENTIALS
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/Timedout	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_CRENDENTIALS
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/Timedout	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_CRENDENTIALS
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/Timedout	CERT_STATUS_TROUBLESHOOT_FAIL_LATE_REQUEST

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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 Algortihm 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", } }

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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) -

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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 subsriber during install time
-

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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)

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Further reading

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

- 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 Maintanence Guide List – Major Version Release
- IM and P Maintainence Guide List – Major Version Release

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential


CISCO