CISCO

You make **possible**

Introduction to Cisco UC Security

Rado Drabik– Technical Consulting Engineer
Laurent Pham – Technical Marketing Engineer

BRKCOL-2014

Barcelona | January 27-31, 2020

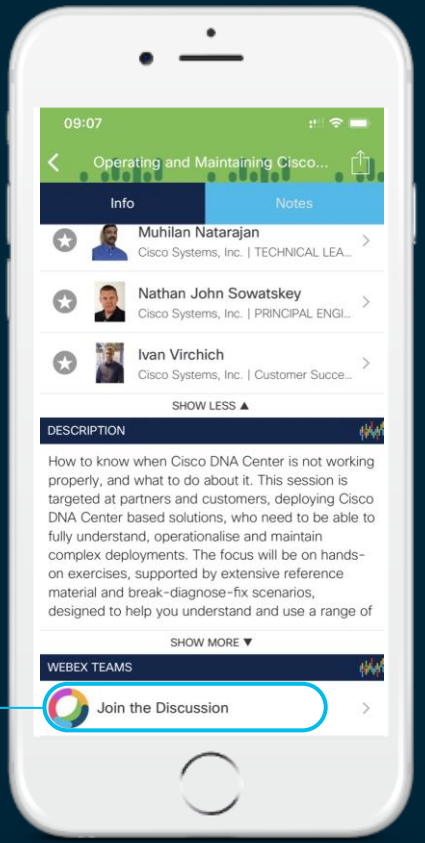
Cisco Webex Teams

Questions?

Use Cisco Webex Teams to chat with the speaker after the session

How

1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space



IP Telephony is a Wonderful Thing, but…

Denial of Service

Privacy

Replay

Eavesdropping

Impersonation

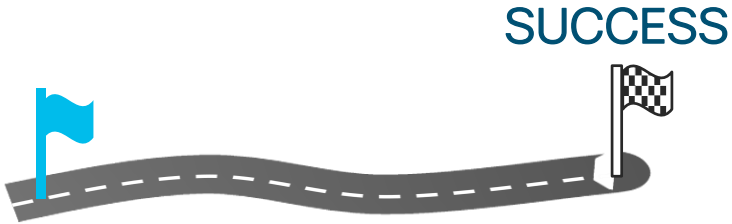
Stealing Credentials

Toll Fraud

Security is Critical

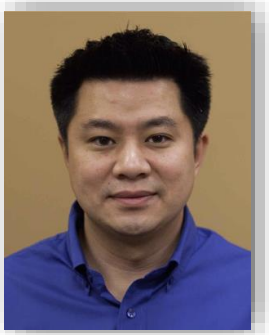
UC Security is a hassle...

but we are trying to make it easier...



Speakers

- **Rado Drabik**
  Technical Consulting Engineer
  11 years in Networking
  CCIE #49005



- **Laurent Pham**
  Technical Marketing Engineer
  21 years in Networking
  CCIE #11139

Agenda

- UC Security Overview
- PKI and Certificate Fundamentals
- TLS and Cryptography
- Securing UCM, Endpoints, CUBE
- Expressway Mobile and Remote Access

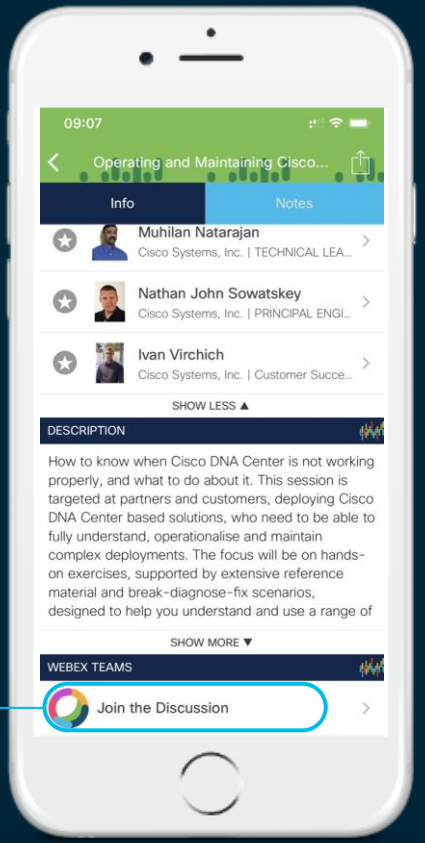
Cisco Webex Teams

Questions?

Use Cisco Webex Teams to chat with the speaker after the session

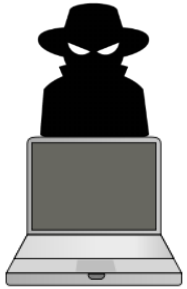
How

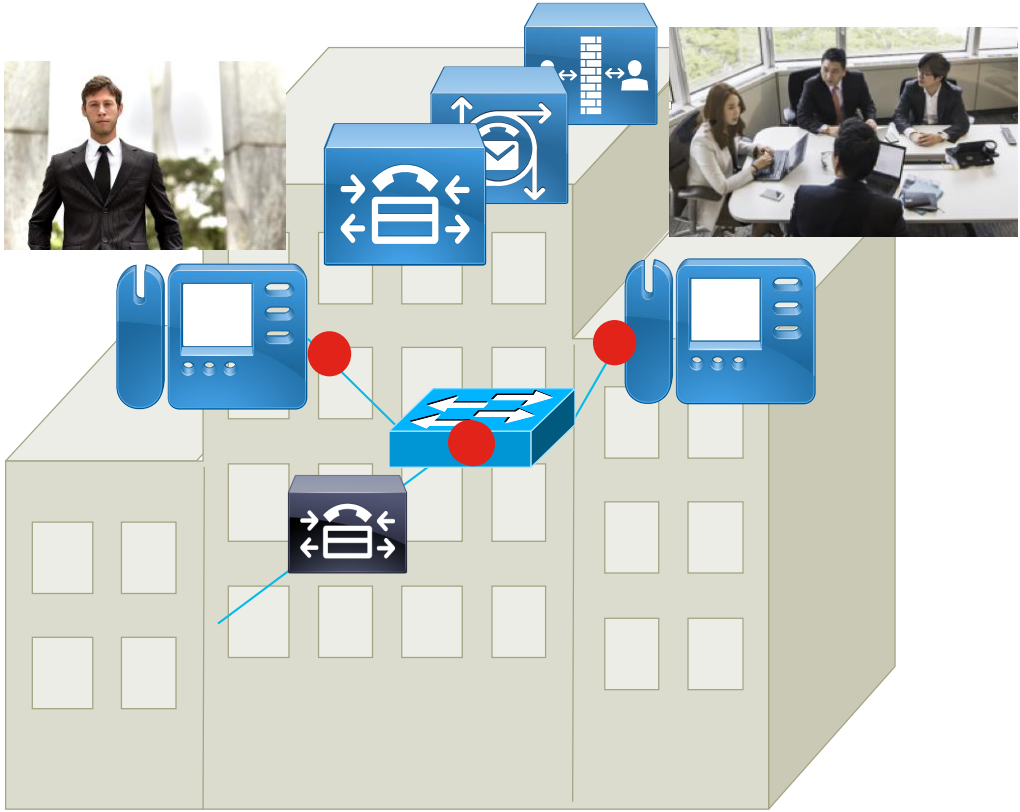
1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space



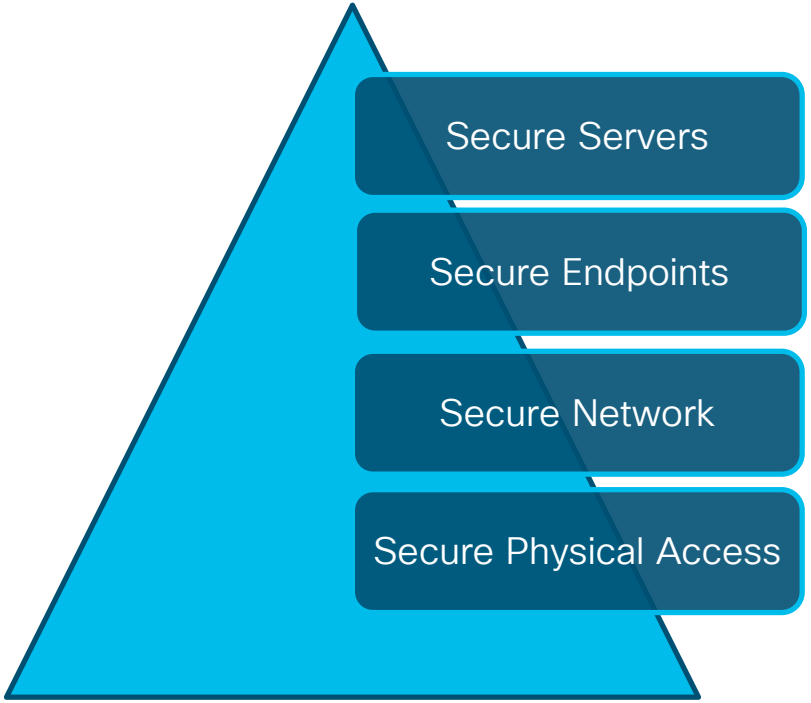
UC Security Overview

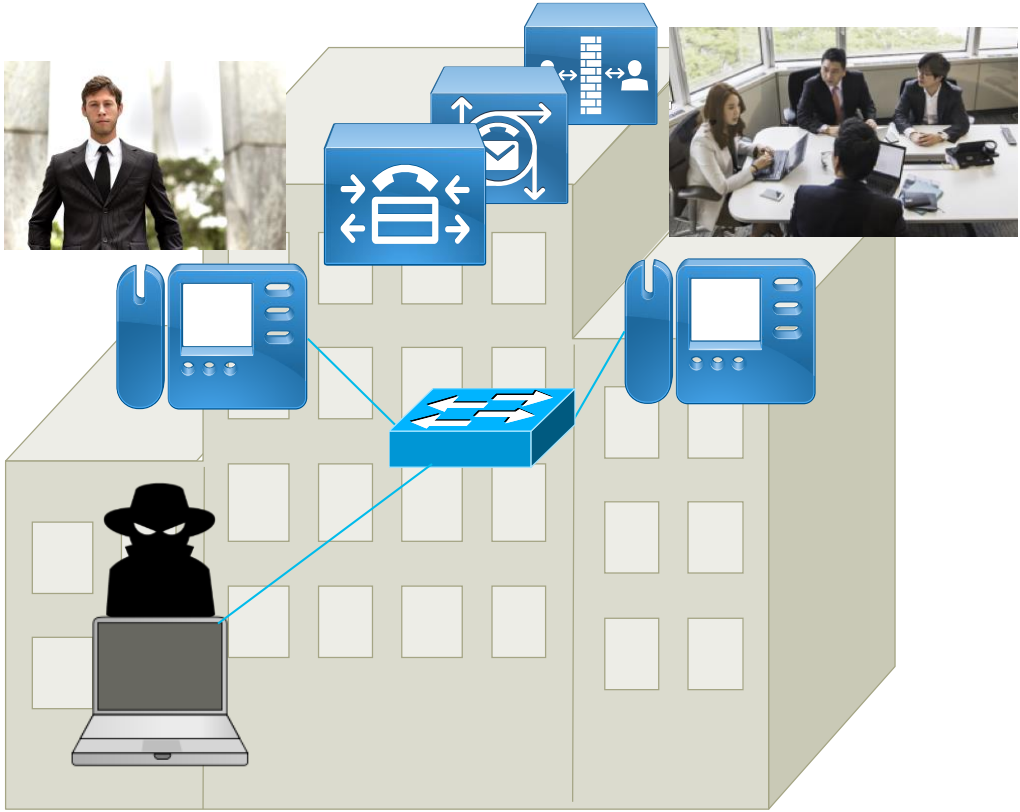
Attack Examples



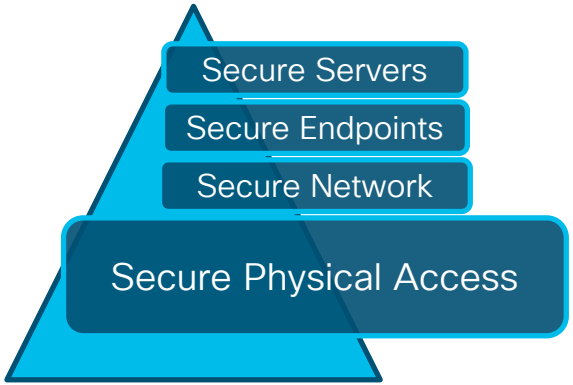


Multi-Layered Security





Secure Physical Access

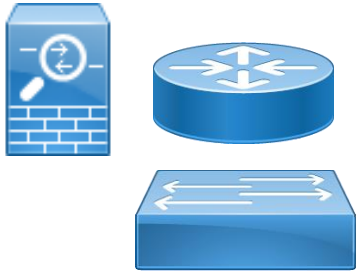


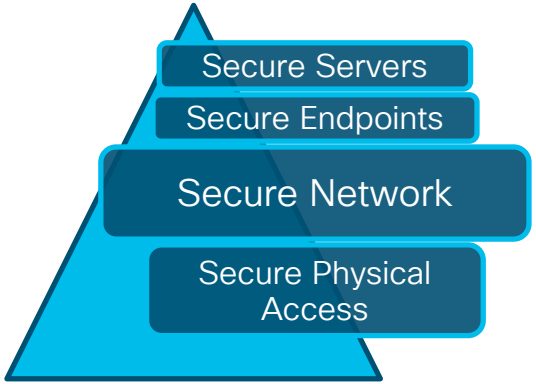
- **Secure physical access** to the Buildings, Data Centers, servers, network devices.

Available option to use **Self-Encrypting Drives**

- **Secure VMware**
  - Through VMware, can mount DVD and recover password
  - Access to VMDK and disk content

Secure Network





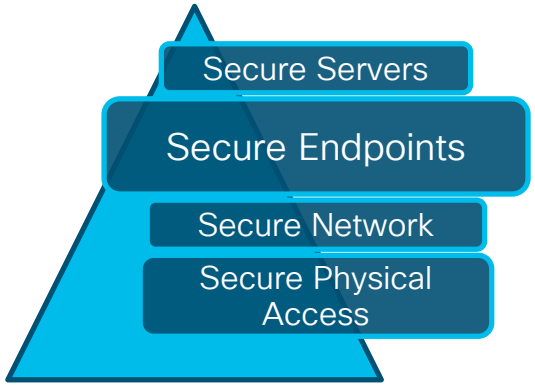
Layer 2/3 Security

- **Separate VLAN** for voice and data
- **Port Security** limits the number of MAC addresses allowed per port, against CAM table flooding
- **DHCP Snooping** against rogue DHCP, DHCP starvation, also creates binding table
- **IP Source Guard** against spoofed IP addresses
- **Dynamic ARP Inspection** (DAI) examines ARP & GARP for violations (against ARP spoofing)
- **802.1x** limits network access to authenticate devices on assigned VLANs (phones do support 802.1x)
- **QoS** helps during Denial of Service attacks

Perimeter Security

- Cisco NGFW – Next Generation Firewall

Secure Endpoints



Default Security Features

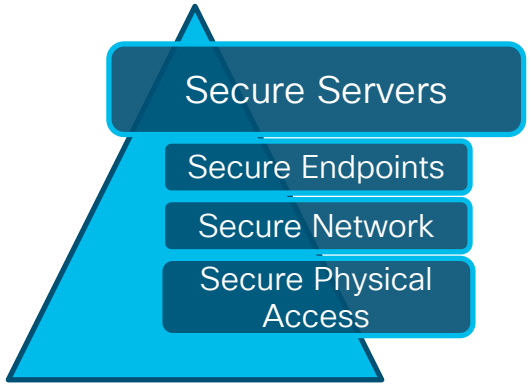
- Signed firmware
- Secure boot (selected models)
- Manufacturer Installed Certificate (MIC)
- Signed configuration files

Additional Security Features

- **Encrypt IP Phone Services** (HTTPS), e.g. EM
- Issue **LSC** (Locally Significant Certificates) from CAPF or Microsoft CA (new online mode in 12.5)
- **Encrypt config files**
- **Encrypt Media and Signaling**
- **Disable settings** if not used: PC port, PC Voice VLAN Access, Gratuitous ARP, Web Access, Settings button, SSH, console…

White Paper: Cisco IP Phone 7800 and 8800 Series Security Overview

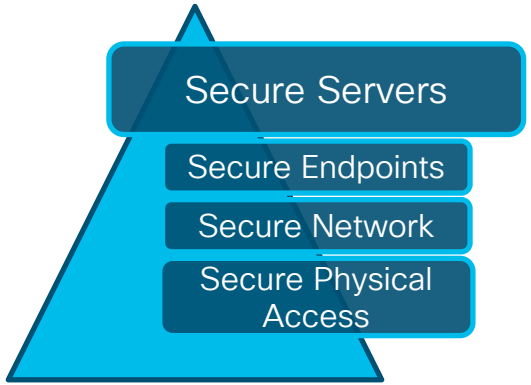
Secure Servers – Platform



Platform Security

- SELinux – Security Policies for access control
- IPTables – Host based firewall
- No 3rd party software allowed
- **Root account disabled**
- Signed upgrade software
- Secure management protocols

Secure Servers – Unified CM

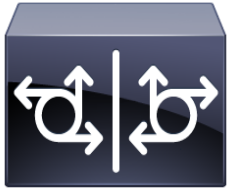


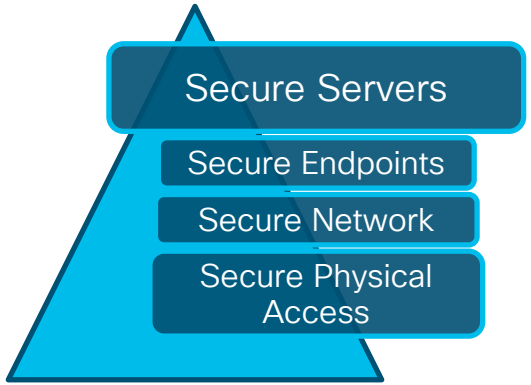
Security Features

- **Encryption** for network links available (LDAP, SIP…)
- TLS version control, granular cipher control
- Provides many security features for the endpoints
  - **Built-in Certificate Authority (CAPF)**
  - **Encryption of media and signaling**
  - **SIP OAuth** for Jabber (to be expanded to some phones in the future)
- Encrypted Backups (always enabled)
- Multi-Level Administration
- **Audit Logging**

Secure Servers – CUBE

```
voice service voip
  ip address trusted list
    ipv4 10.1.1.10
    ipv4 66.66.66.66
```

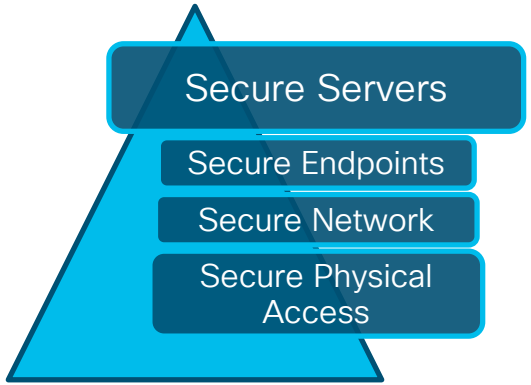




CUBE Security Features

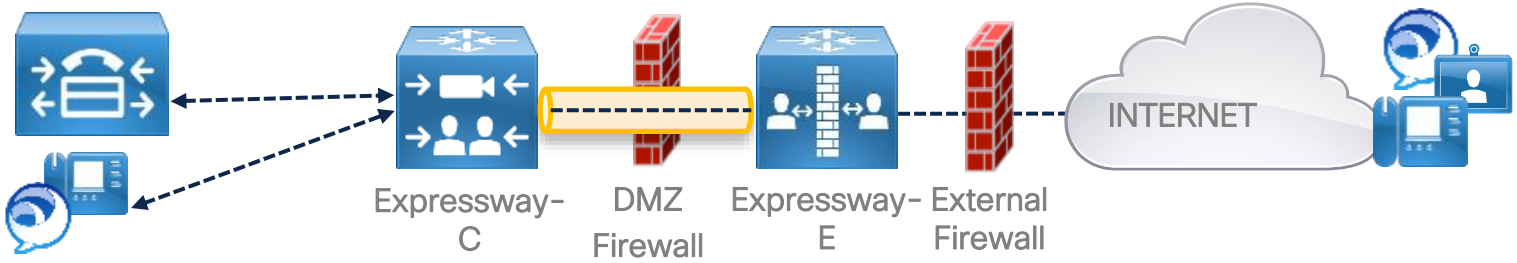
- **Encryption** with Next Generation Encryption cipher suites and TLS 1.2
- **RTP/SRTP Interworking**
- **IP Trust List**: Don't respond to any SIP INVITEs if not originated from an IP address specified in this trust list
- **Call Threshold**: Protect against CPU, Memory & Total Call spike
- **Call Spike Protection**: Protect against spike of INVITE messages within a sliding window
- **Bandwidth Based CAC**: Protect against excessive media
- **Voice Policies**: Identify patterns of valid phone calls that might suggest potential abuse

Secure Servers - Expressway

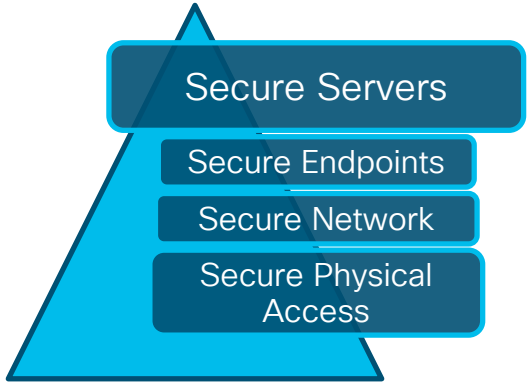


Expressway Security Benefits

- Used for internet connectivity
- Firewall Traversal
- Mobile & Remote Access
- Secure business-to-business (B2B) audio/vide communications
- Secure Instant Messaging and Presence Federation



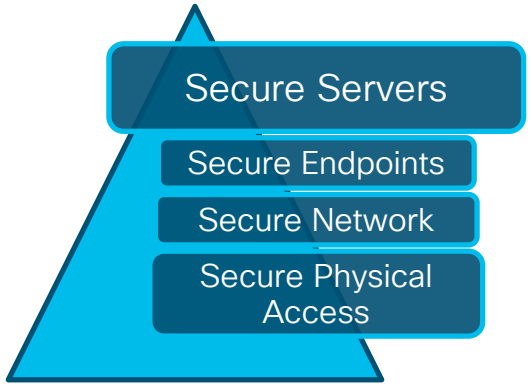
Secure Servers – Toll Fraud



Cisco UCM Toll Fraud Prevention

- **Partitions** and **Calling search spaces** provide dial plan segmentation and access control
- **"Block offnet to offnet transfer"** (CallManager service parameter)
- "**Drop Ad hoc Conferences**" (CallManager service parameter)
- Device Pool "Calling Search Space for **Auto-registration**" to limit access to dial plan
- Employ **Time of day routing** to deactivate segments of the dial plan after hours
- Require **Forced Authentication Codes** on route patterns to restrict access on long distance or international calls.
- Monitor **Call Detail Records**

Secure Servers – Toll Fraud



Unity Connection

- Threat: Unity Connection could be used to transfer a call
- Use **restriction tables** to allow or block call patterns
- Change the **Rerouting CSS** on the trunk in the **Cisco UCM** side

CUBE

- Use **IP Trust List**

Expressway

- Call Policy Rules (CPL)
- Search History

Balancing Risk

Cost - Complexity - Resources - Performance - Manpower - Overhead

Low Easy or Default	Medium Moderate and Reasonable	High Advanced or Not Integrated
Hardened Platform	Secure Directory Integration (SLDAP)	UC-Aware Firewall (Inspection)
SELinux - Host Based Intrusion Protection	OAuth with Refresh Token	802.1x & NAC
iptables - Integrated Host Firewall	TLS & SRTP for Jabber w/ SIP OAuth	IPsec
Signed Firmware & Configuration	TLS & SRTP for Phones & Gateways	Rate Limiting
HTTPS	QoS Packet Marking	Managed VPN (Remote Worker)
Separate Voice & Data VLANs	DHCP Snooping	Network Anomaly Detection
STP, BPDU Guard, SmartPorts	Dynamic ARP Inspection	Scavenger Class QoS
Basic Layer 3 ACL's (Stateless)	IP Source Guard	TLS & SRTP for Jabber w/o SIP OAuth
Phone Security Settings	Port Security	Encrypted Configuration

Cisco Secure Development Lifecycle

www.cisco.com/go/csdl

- **CSDL**

  Repeatable and measurable process designed to increase Cisco product resiliency and trustworthiness.

- **Product Security Baseline**

  Internal Requirements on important security components (credential and key management, cryptography standards, sensitive data disposal…).

Government Certifications

- Core Certifications
  - **FIPS 140-2** (Federal Information Processing Standard)
  - **CC & CSfC** (Common Criteria & Commercial Solutions for Classified)
  - **DoDIN APL** (Department of Defense Information Network Approved Product List)
  - **FedRAMP** (Federal Risk and Authorization management Program)
- Next Generation Encryption (NGE), NSA Suite B Cryptography

- More information at: https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications.html

Cisco PSIRT has your back

Product Security Incident Response Team (PSIRT) - www.cisco.com/go/psirt

- Dedicated, global team managing security vulnerability information related to Cisco products and networks
- Responsible for Cisco Security Advisories, Responses and Notices
- Interface with security researchers and hackers
- Assist Cisco product teams in securing products

Quick Search unified communications

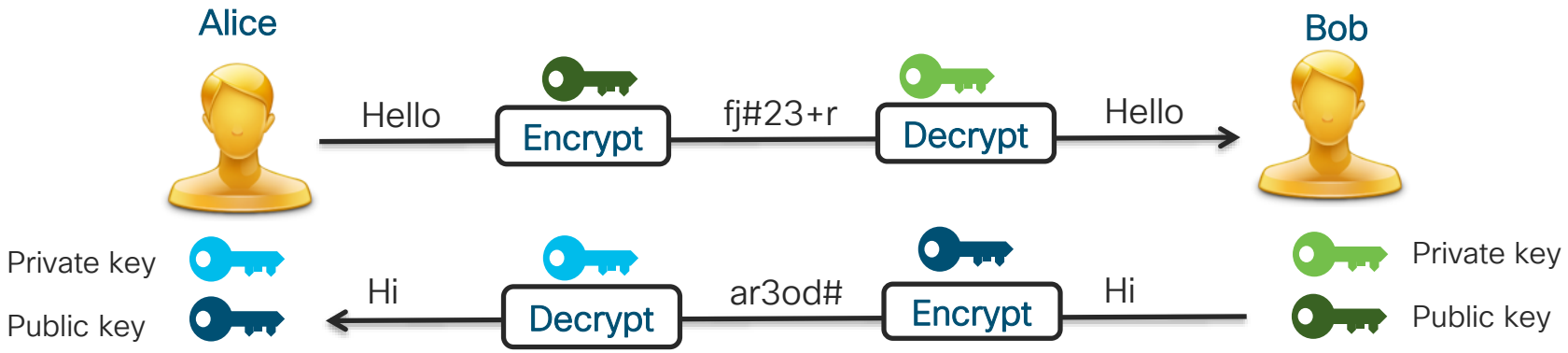
Advanced Search

ADVISORY	IMPACT	CVE	LAST UPDATED	VERSION
Search Advisory Name	*All*	*Search CVE*	*Most Recent*	
Cisco Unified Communications Manager Cross-Site Request Forgery Vulnerability	Medium	CVE-2020-3135	2020 Jan 22	1.0
Cisco Unified Communications Manager Information Disclosure Vulnerability	Medium	CVE-2019-15963	2020 Jan 22	1.0
Cisco Secure Boot Hardware Tampering Vulnerability	High	CVE-2019-1649	2019 Nov 20	1.17
Cisco Unified Communications Domain Manager Persistent Cross-Site Scripting Vulnerability	Medium	CVE-2019-15968	2019 Nov 20	1.0
Cisco Unified Communications Manager SQL Injection Vulnerability	Medium	CVE-2019-15972	2019 Nov 20	1.0
Cisco Unified Communications Manager Security Bypass Vulnerability	Medium	CVE-2019-15272	2019 Oct 23	1.1
Cisco Unified Communications Manager XML External Expansion Vulnerability	Medium	CVE-2019-12711	2019 Oct 23	1.1
Multiple Cisco Unified Communications Products Cross-Site Request Forgery Vulnerability	High	CVE-2019-1915	2019 Oct 15	1.1
Cisco IOS and IOS XE Software Session Initiation Protocol Denial of Service Vulnerability	High	CVE-2019-12654	2019 Oct 04	1.1
Cisco Unified Communications Manager Cross-Site Scripting Vulnerability	Medium	CVE-2019-12716	2019 Oct 02	1.0
Cisco Unified Communications Manager Cross-Site Scripting Vulnerability	Medium	CVE-2019-12715	2019 Oct 02	1.0
Multiple Cisco Unified Communications Products Cross-Site Scripting Vulnerability	Medium	CVE-2019-12707	2019 Oct 02	1.0

PKI and Certificate Fundamentals

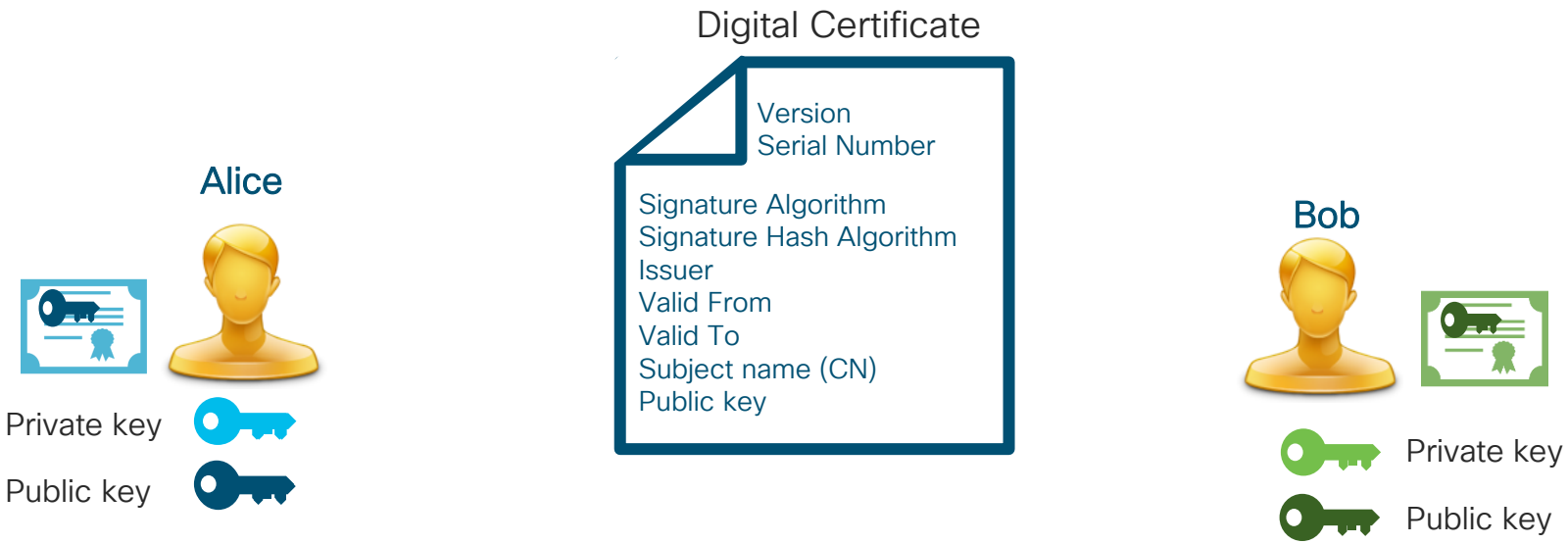
Symmetric and Asymmetric Encryption

- Encryption allows to transform a message to a cipher text
- In the Symmetric encryption, the same key (secret key) is used to both encrypt and decrypt the text
- In the Asymmetric encryption (depicted below), each party generate a key pair (public and private key) which is used for encryption



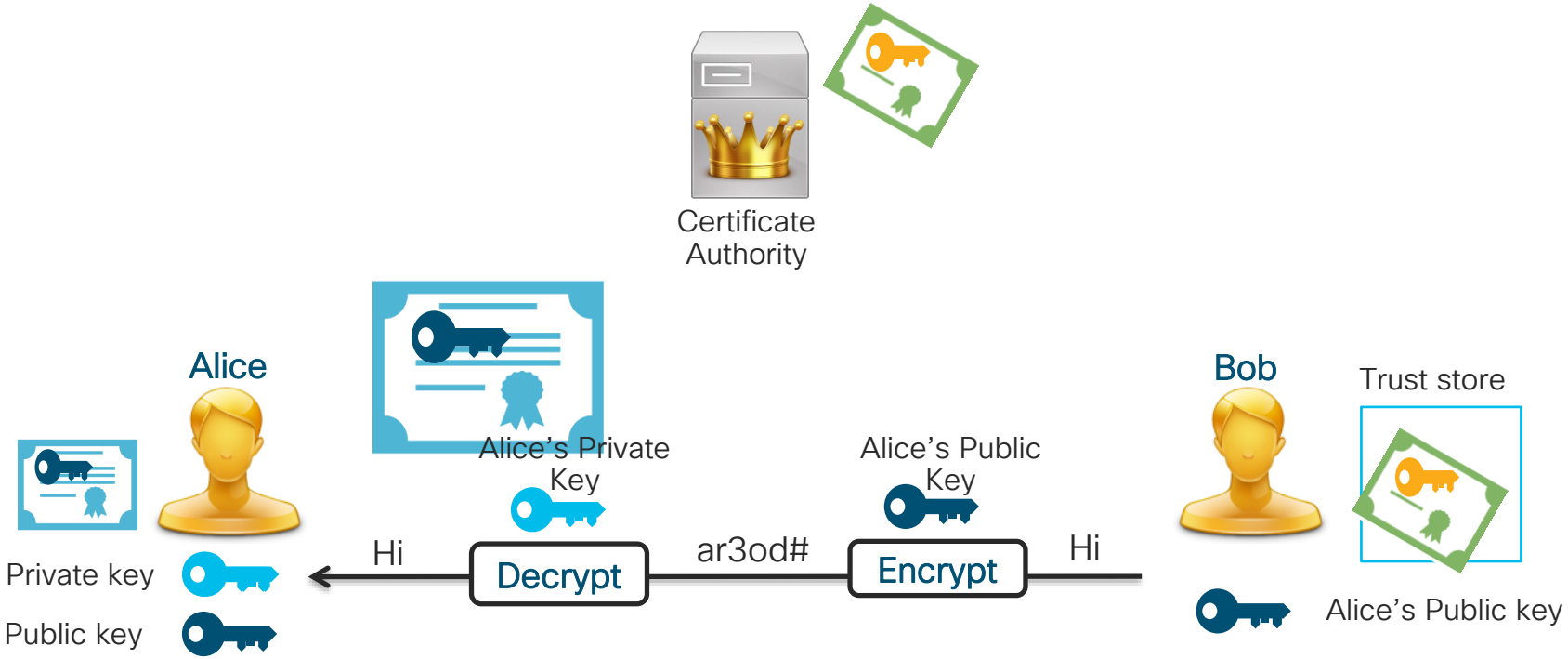
Digital Certificates

- Electronic document that is used to identify an individual, a server, a company, or some other entity, and to associate that identity with a public key
- Standard x.509 defines the format

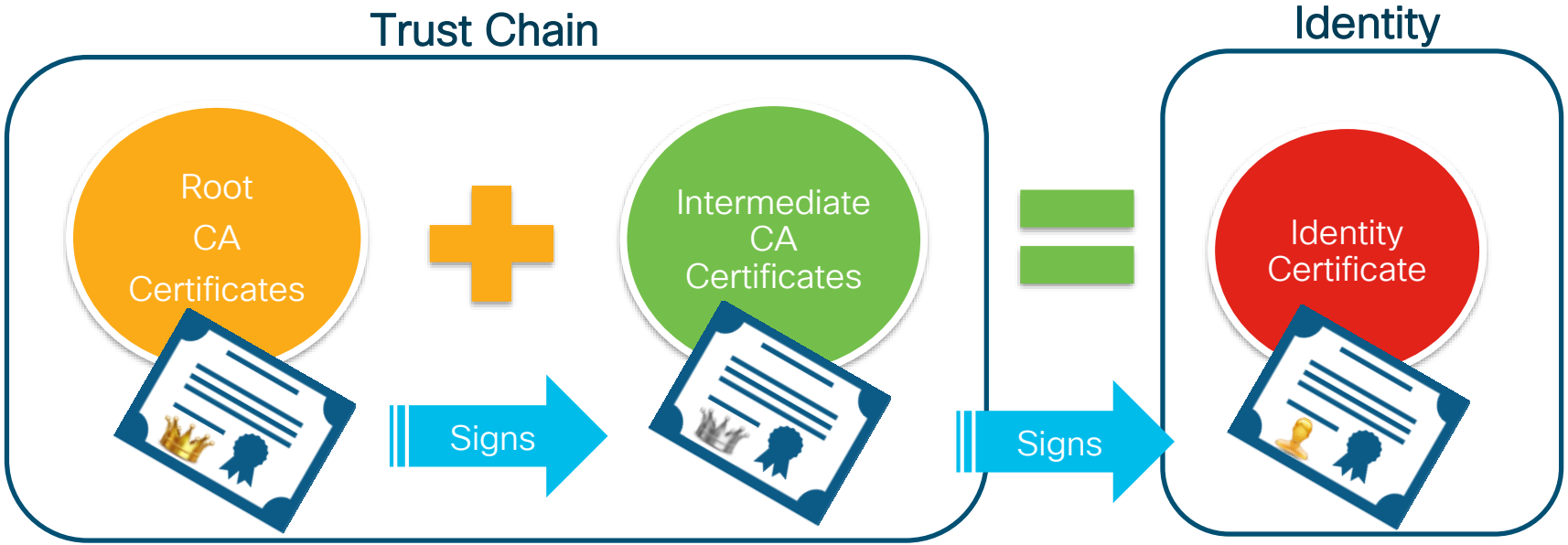


Public Key Infrastructure

- Provides a uniform way for different organizations to identify people or other entities through X.509 identity certificates containing public keys



Types of Certificates and Trust Chain



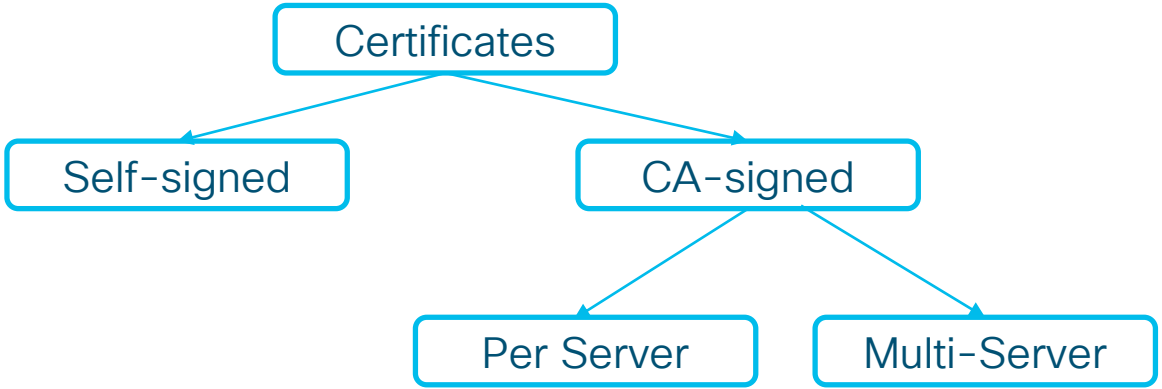
Self-Signed certificates used by Certificate Authorities to sign other certificates.

Certificates signed by a Root CA and in turn can sign other identity certificates.

Certificates issued to a specific entity (a device) and signed or issued by a root CA and sometimes also by intermediate CAs.

Note: Root CA Public Certificates Must be stored in Clients' Trust Store(s).

Types of certificates on UC products



Multi-Server certificates support

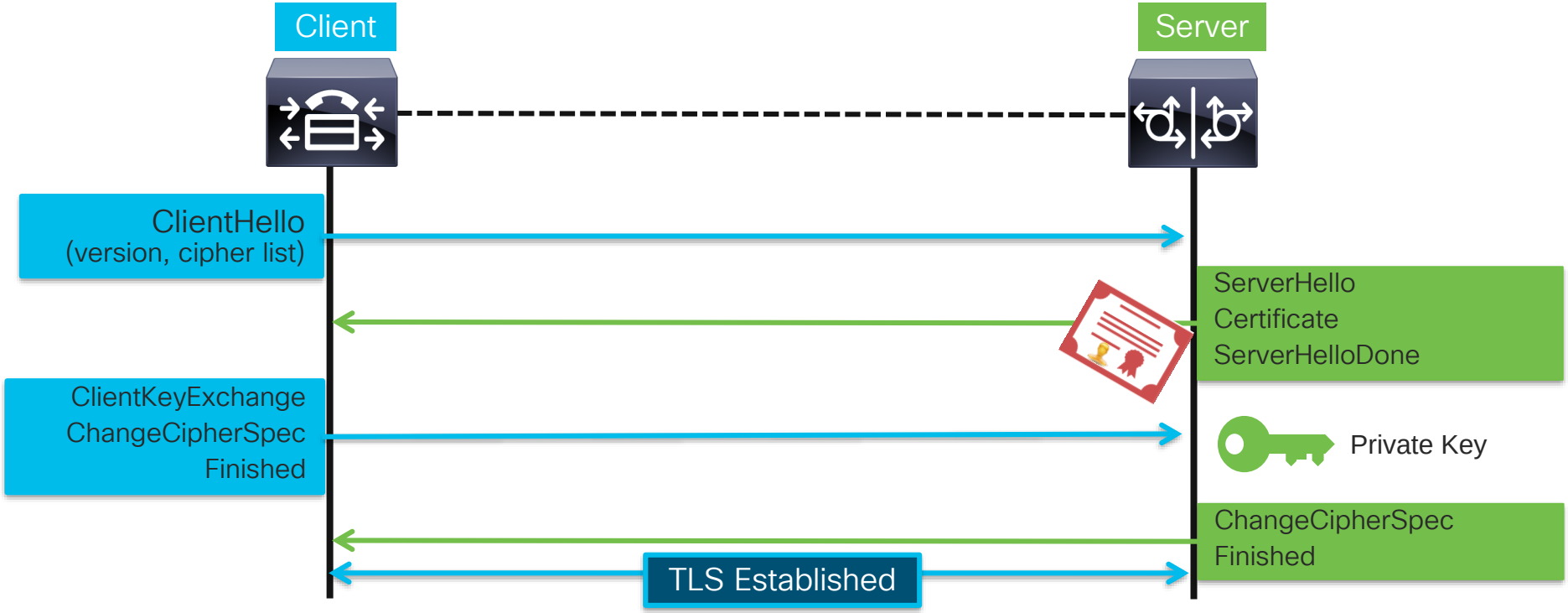
- To simplify certificate management in clustered environments
- One single CA-signed certificate used across all the nodes in a cluster (private key pushed automatically across all nodes in a cluster)
- Each cluster node's FQDN included as Subject Alternative Name (SAN) in a single certificate, custom SANs can also be included

Recommendation:
Use Multi-Server certificates wherever available: Tomcat/Tomcat-ECDSA for Unified CM/IM&P and CUC, CallManager for Unified CM, CUP-XMPP, CUP-XMPP-S2S for IM&P.

Transport Layer Security and Ciphers

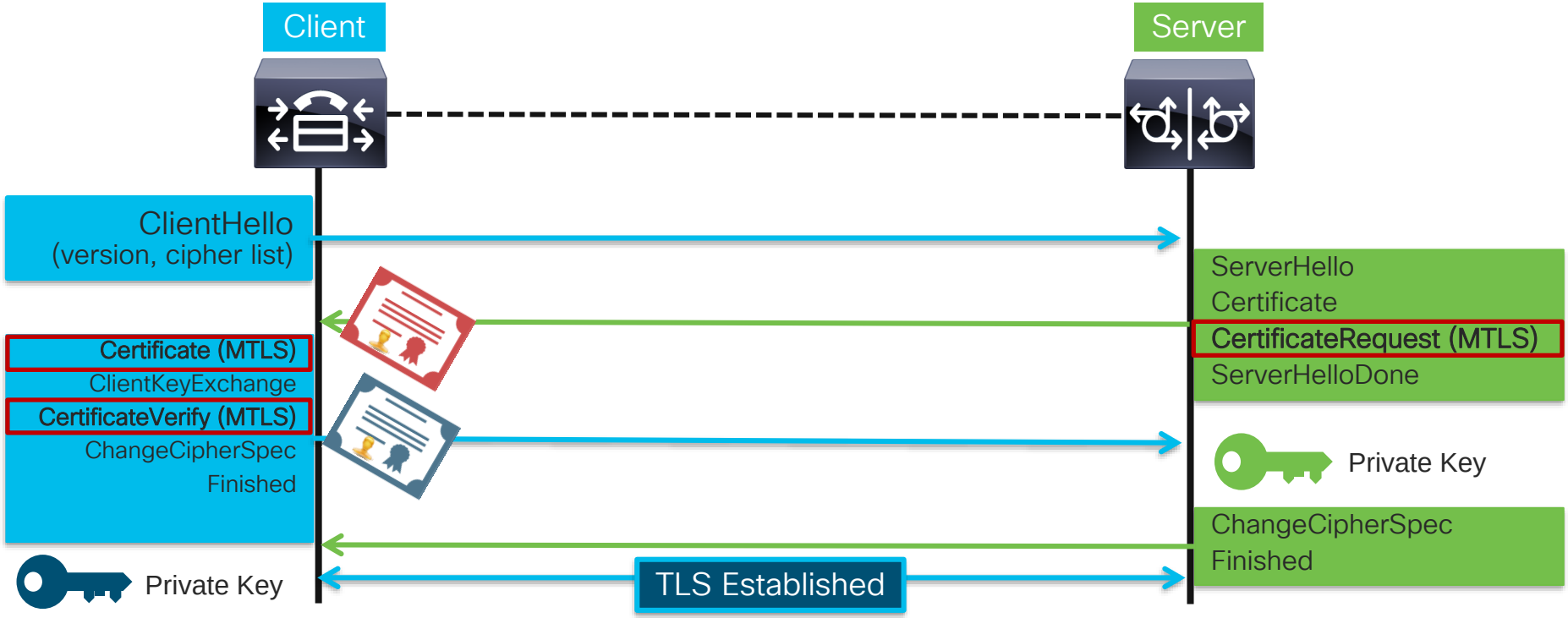
TLS Session Establishment

* RSA Key Exchange



TLS Session Establishment – Mutual TLS

* RSA Key Exchange



TLS 1.2

- TLS 1.2 more secure than SSL3, TLS 1.0, TLS 1.1
- Supports stronger ciphers
- May be required for security or compliance reasons (e.g. PCI)

- Two main requirements:

1. TLS v1.2 Support
2. Ability to disable lower TLS versions (disable TLS 1.0, TLS 1.1)

TLS 1.2 Support

Product	Support			
	Supports TLS 1.2	Disable TLS 1.0	Disable TLS 1.1	Notes
UCM/IM&P, UCxn, CER, PLM*, PCD, TMS, secure CUBE (G2/G3)				System Release 12 (and 11.5(1)SU3+)
Other infrastructure (CMS, Conductor, TP Server, Expressway, Contact Center, PCP, secure SIP PSTN GW/CUBE/MTP/CFB G2/G3, secure SRST G3, secure analog VG)				System Release 12
CE Endpoints (DX70/80, MX 200/300 G2, MX 700/800, SX, IX 5000				9.1.3
78xx/88xx				12.1(1)
Newer TC endpoints (could run CE) (MX 200/300 G2, MX 700/800, SX)	☑	☑	☒	Can SW upgrade to CE
Legacy TC endpoints (C-series, EX, MX 200/300 G1, Profile)	☑	☑	☒	End of Sale
Legacy Immersive (TX 9000 series, CTS)	☑	☒	☒	End of Sale
Older IP phones (e.g., 79xx series, 69xx, 99xx, 89xx, DX on Android, IP Communicator)	☒	☒	☒	No support or partial support

TLS 1.2 Compatibility Matrix

TLS 1.2 Support (Interop)

Disabling TLS 1.0/1/1 (PCI Compliance)

Product	Minimum recommended version that supports TLS 1.2[1]	Minimum version that can disable TLS version 1.0 and 1.1	Link to product support documentation
Call Control			
Cisco Unified Communications Manager and IM and Presence Service	11.5(1)SU3 CTL client does not support TLS 1.2.	11.5(1)SU3	Support
Cisco Unified Survivable Remote Site Telephony	12.1 (IOS 16.7.1)	12.1 (IOS 16.7.1)	Support
Conferencing			
Cisco Meeting Server	2.0	2.3	Support
Cisco Meeting App	1.9	Not applicable for clients.	Support

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/unified/communications/system/Compatibility/TLS/TLS1-2-Compatibility-Matrix.html

Deconstructing the Cipher Suite

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Key Exchange

- { }: RSA
- ECDHE/DHE: (Elliptic Curve) Diffie-Hellman Ephemeral

10.5(2)

Signature Algorithm

- RSA
- ECDSA

SIP 11.0

HTTPS 11.5

Phones 12.5

Message Authentication Code

- SHA1
- SHA2 with key size

10.5(2)

Bulk Encryption

- AES: Advanced Encryption Standard
- AES GCM: AES Galois Counter Mode

10.5(2)

3DES: Removed in 11.5(1)SU4 and 12.0(1)SU2

Cipher Management Control in Unified CM and phones (12.5)

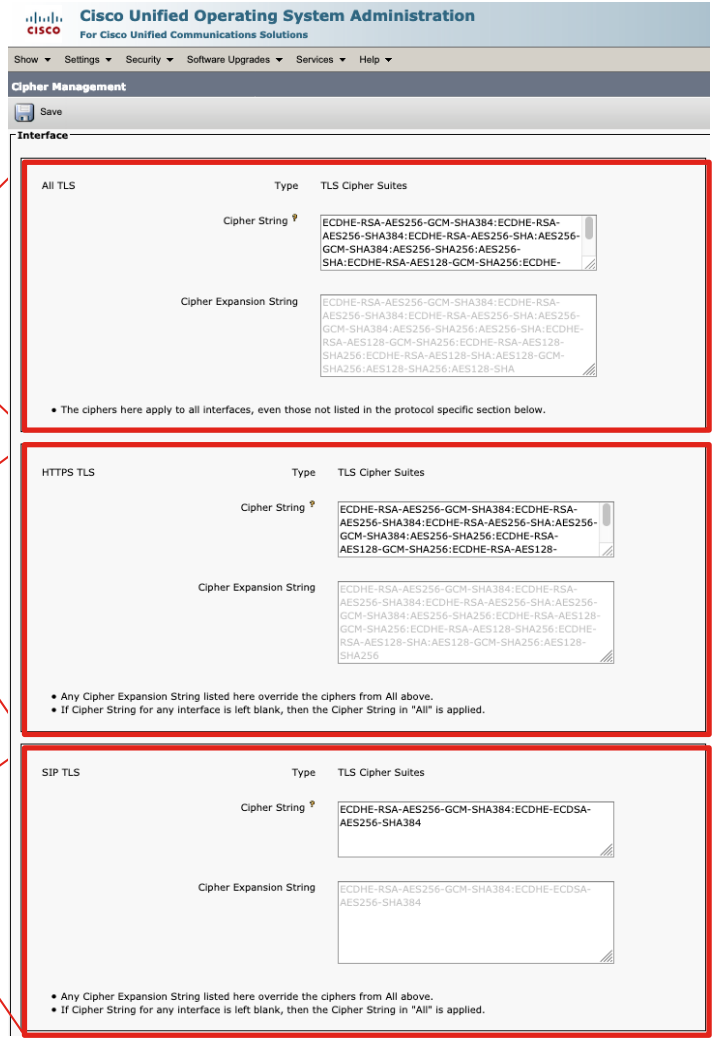
Interface	Prior to 12.5	12.5+
HTTPS	ECDSA disable/enable	Can be customized
SIP/CTI	Strongest, Medium, All - ECDSA or RSA preferred	
Other TLS Interfaces	None	
SSH		
7800/8800		

Cipher Management Control

ALL TLS

HTTPS TLS

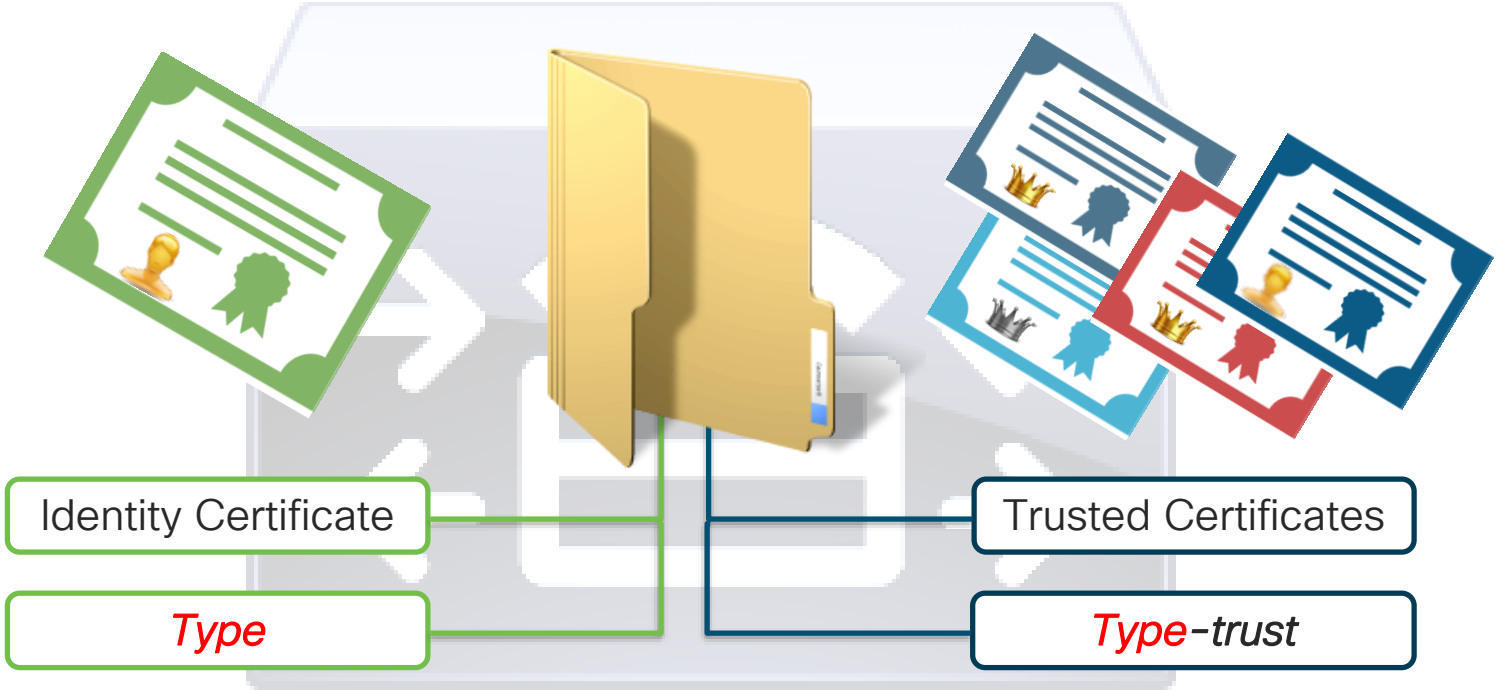
SIP TLS



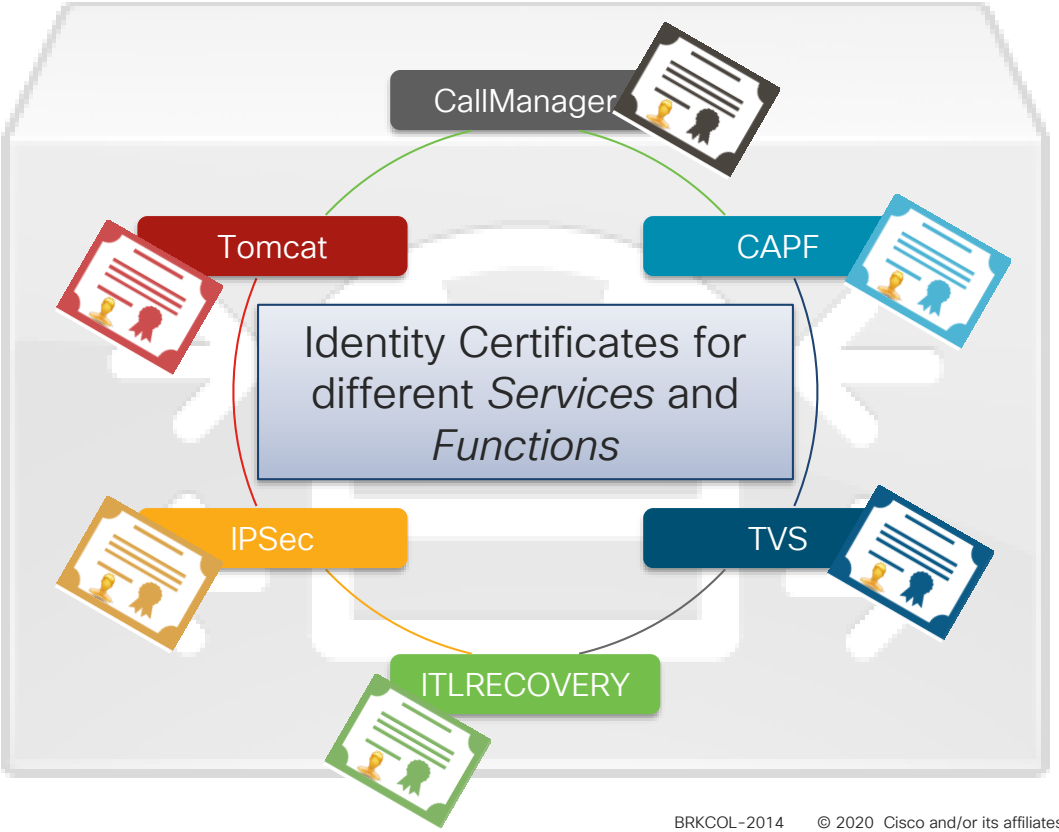
*Also available in Expressway

Unified CM Certificates and Trust Stores

UCM Certificate Trust Stores



UCM Certificate Types



UCM Certificate Truststores

UCM Certificate Truststores

IDENTITY	TRUST
CallManager	CallManager-Trust
CallManager-ECDSA	Tomcat-Trust
Tomcat	CAPF-Trust
Tomcat-ECDSA	TVS-Trust
CAPF	IPSec-Trust
TVS	Phone-VPN-Trust
IPSec	Phone-CTL-Trust
authz (12.0+)	Phone-CTL-ASA-Trust (12.0+)
ITLRecovery	Phone-SAST-Trust
	Phone-Trust
	UserLicensing-Trust

CAUTION - SUBJECT TO CHANGE

Certificate Reduction Preview

Planned for future UCM release

More than 80% reduction in certificates to manage

Scenario 1 (Worst case): 8 node cluster with all self-signed certificates

Certificate	UCM 12.5	Future release
Tomcat	8	1
Tomcat-ECDSA	8	1
CallManager	8	0*
CallManager-ECDSA	8	0*
TVS	8	1
CAPF	8	1
IPSec	8	0**
ITLRecovery	1	1
TOTAL	57	5

Scenario 2 (Best case): 8 node cluster with Multi-server Tomcat and Call Manager CA signed certificates

Certificate	UCM 12.5	Future release
Tomcat	1	1
Tomcat-ECDSA	1	1
CallManager	1	0*
CallManager-ECDSA	1	0*
TVS	8	1
CAPF	8	1
IPSec	8	0**
ITLRecovery	1	1
TOTAL	29	5

* CallManager / CallManager-ECDSA can reuse Tomcat and Tomcat-ECDSA certificate

** IPSec certificate does not need to be managed if IPSec is configured with Pre-Shared Key or if IPSec is not used.

CAUTION - SUBJECT TO CHANGE

Centralized Certificate Management

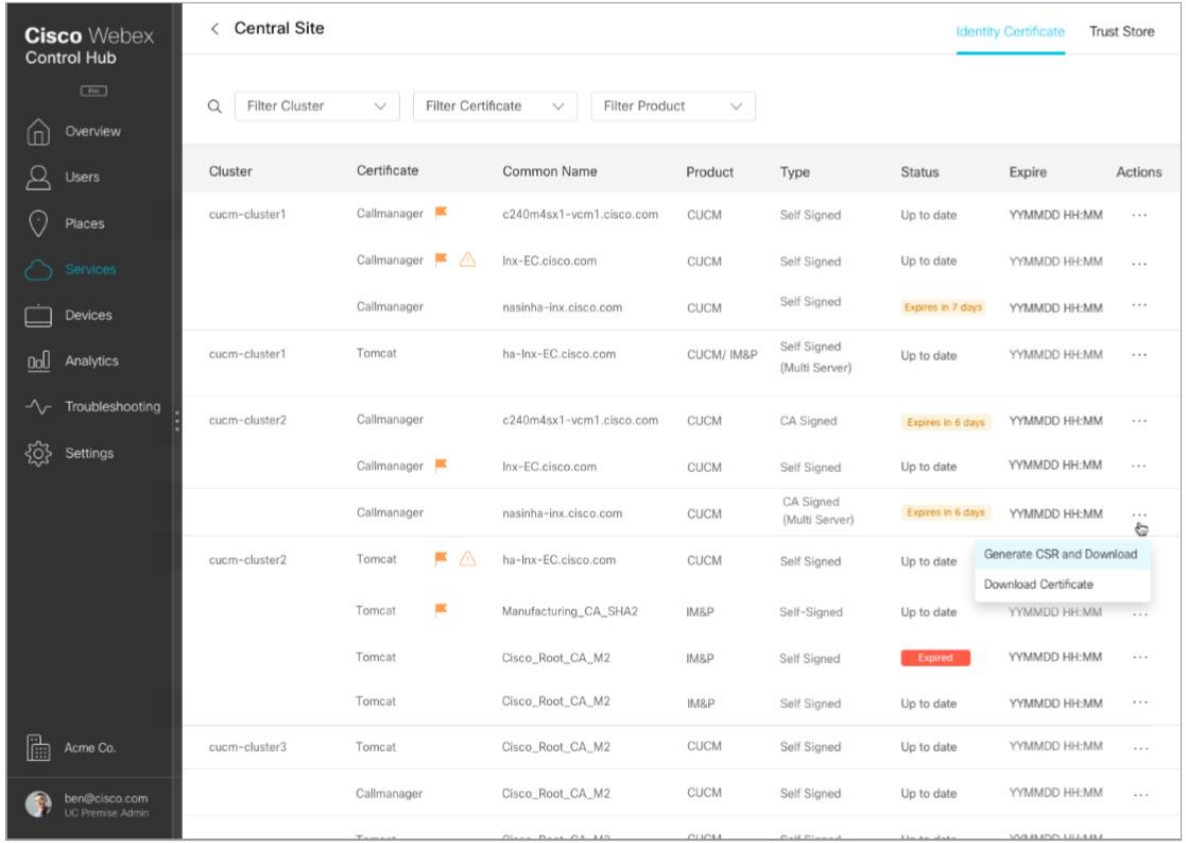
Planned for future UCM release

Centralized Certificate Management

- Cloud-based centralized UI to manage certificates across multiple clusters and UC Apps
- Rest APIs driven
- Single place to manage certificates across the deployment (by cluster, by UC App, etc.)

Cloud Offering

APIs for Dev Partners

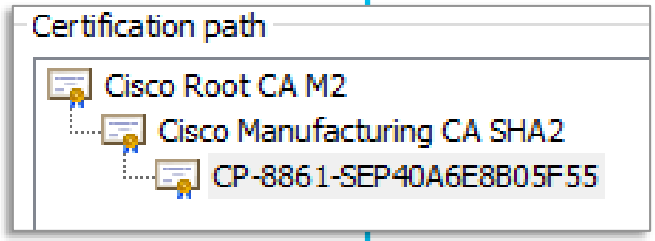


Phone Certificates and Trust Lists

Phone Certificate Types

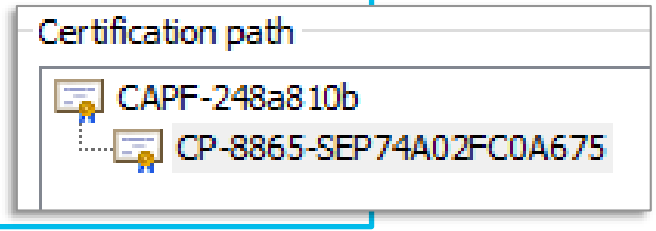
Manufacturer-Installed Certificate (MIC)

- Signed by Cisco Manufacturing CA
- Automatically installed in supported phone models
- Used to authenticate with CAPF for LSC installation or downloading an encrypted configuration file
- Cannot be overwritten or deleted or revoked



Locally Significant Certificate (LSC)

- Used for authentication and encryption
- Signed by **CAPF** service or **other CA**
- Takes precedence over MIC



Recommended

CAPF (Certificate Authority Proxy Function)

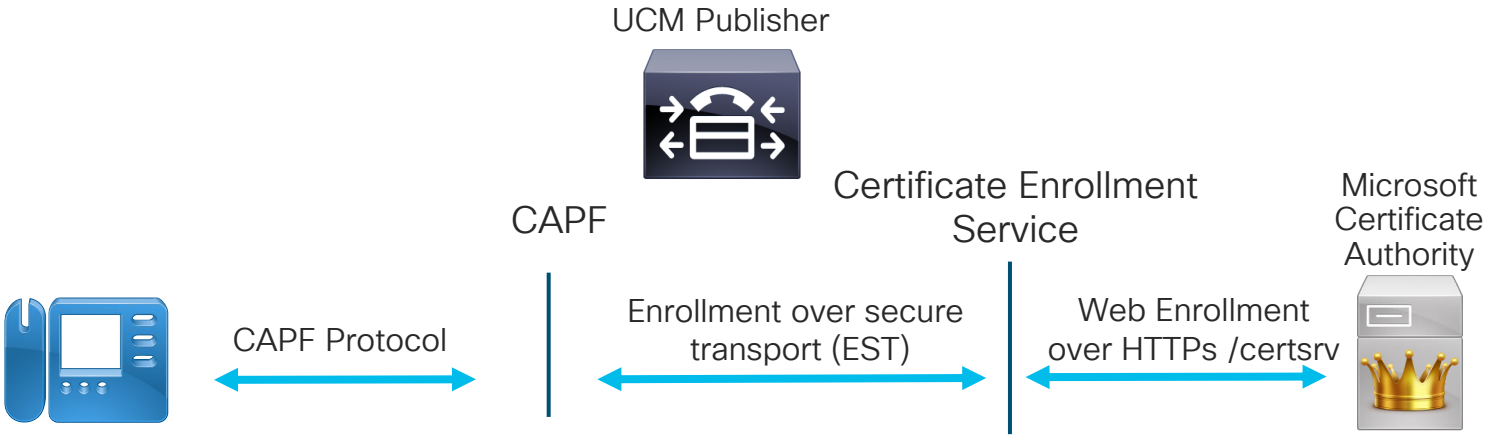
- Scalable solution to easily generates LSCs for thousand of phones
- CAPF is a service on UCM publisher which acts like a CA for the phones
- Automates the entire process of issuing certificates to the phones
- When 802.1x in use, publisher's CAPF certificate being uploaded onto RADIUS server

LSC signing options

LSC
Locally Significant Certificate

- Signed by CAPF
- Signed by external CA
  - Offline CA
    - ☒ Manual Process
  - Online CA (UCM 12.5+)
    - ☑ Easy Enrollment
    - ☒ Microsoft CA only

CAPF Online CA - concept

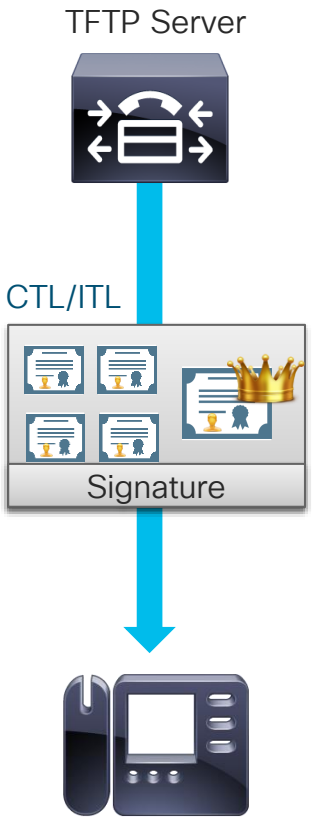


- IP Phone generates CSR and sends it to CAPF service that is running on UCM PUB
- CAPF later on 'talks' to new service called **Cisco Certificate Enrollment Service** and this service is responsible for sending CSR to CA in order to get is signed
- Signed LSC is being sent back to UCM and finally CAPF is pushing that LSC to IP Phone

How Do Endpoints Trust Servers?

- When an endpoint boots/resets, it requests the files from UCM TFTP:
  - **CTL file** (Certificate Trust List)*
  - **ITL file** (Initial Trust List)**
- CTL and ITL files are signed files that contain a list of certificates that the endpoint can trust
- Endpoints verify the signature of the CTL/ITL

* Only available in Mixed mode
** No support with Cisco Jabber.



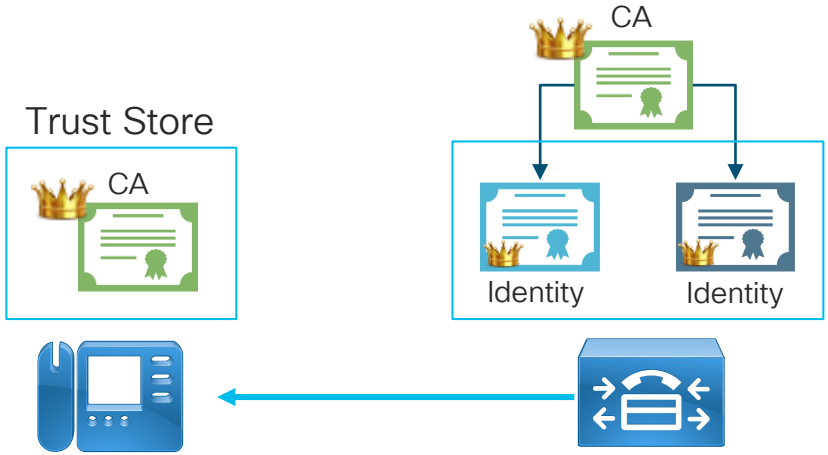
CAUTION - SUBJECT TO CHANGE

PKI – Certificate Chain Validation by Phones

Planned for a future UCM release

- ✓ Lowers TCO* by decreasing admin effort
- ✓ Reduces chances of losing of trust
- ✓ Easy to migrate across clusters
- ✓ Reduces dependency on ITL/CTL/TVS

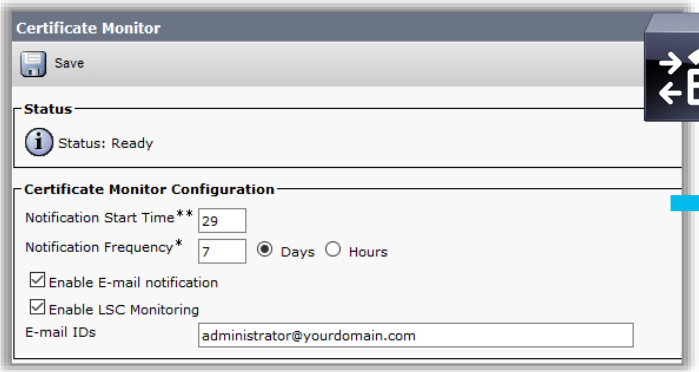
- Phones would be able to:
  - Download a CA certificate
  - Validate identity certificate (that was not found in ITL/CTL file) by verifying the certificate chain

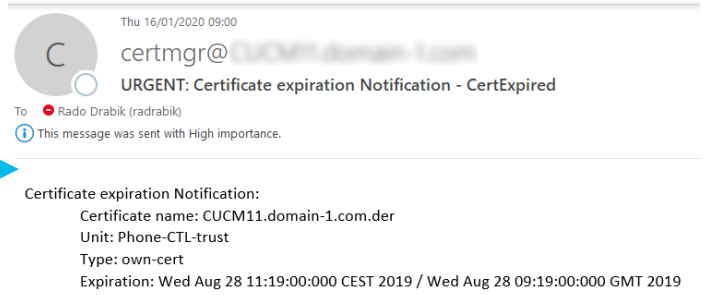


*Total Cost of Ownership

Monitoring Certificate Expiration

- Syslog/RTMT/Email notifications for expiring/expired certificates (Server and LSC certificates)





- LSC Status & CAPF report

Device Name(Line)	LSC Status	LSC Expires	LSC Issued By	LSC Issuer Expires By
SEP74A02FC0A675	None	06/05/2018	CAPF-2ab21620	06/06/2018
SEP24B65744EBFE	Upgrade Success	06/05/2018	CAPF-2ab21620	06/06/2018
SEP001F6C81118B	Upgrade Success	06/05/2018	CAPF-2ab21620	06/06/2018
SEP001F9EAD32E6	Upgrade Success	06/05/2018	CAPF-2ab21620	06/06/2018

New in 11.5(1)

Unified CM
Non-Secure Mode

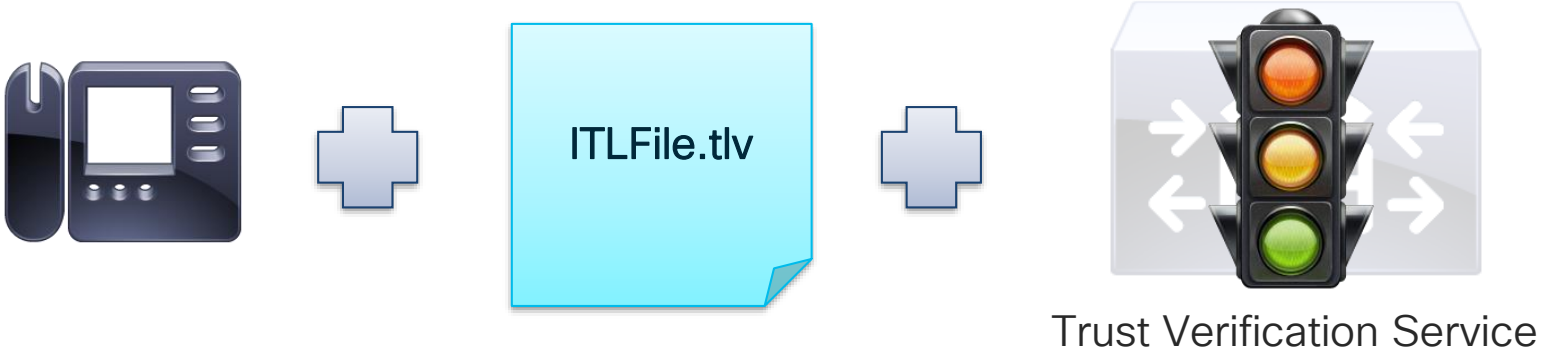
Security By Default

Feature	Non Secure Cluster
Auto-registration	✓
Signed Phone Firmware	✓
Signed & Encrypted Phone Configs	✓
Secure Phone Services (HTTPS)	✓
CAPF + LSC	✓
IP VPN Phone	✓
Encrypted SIP Trunk	✓
Secure Jabber (TLS & SRTP)	✓
Secure Endpoints (TLS & SRTP)	✗

New in 12.5 with SIP OAuth

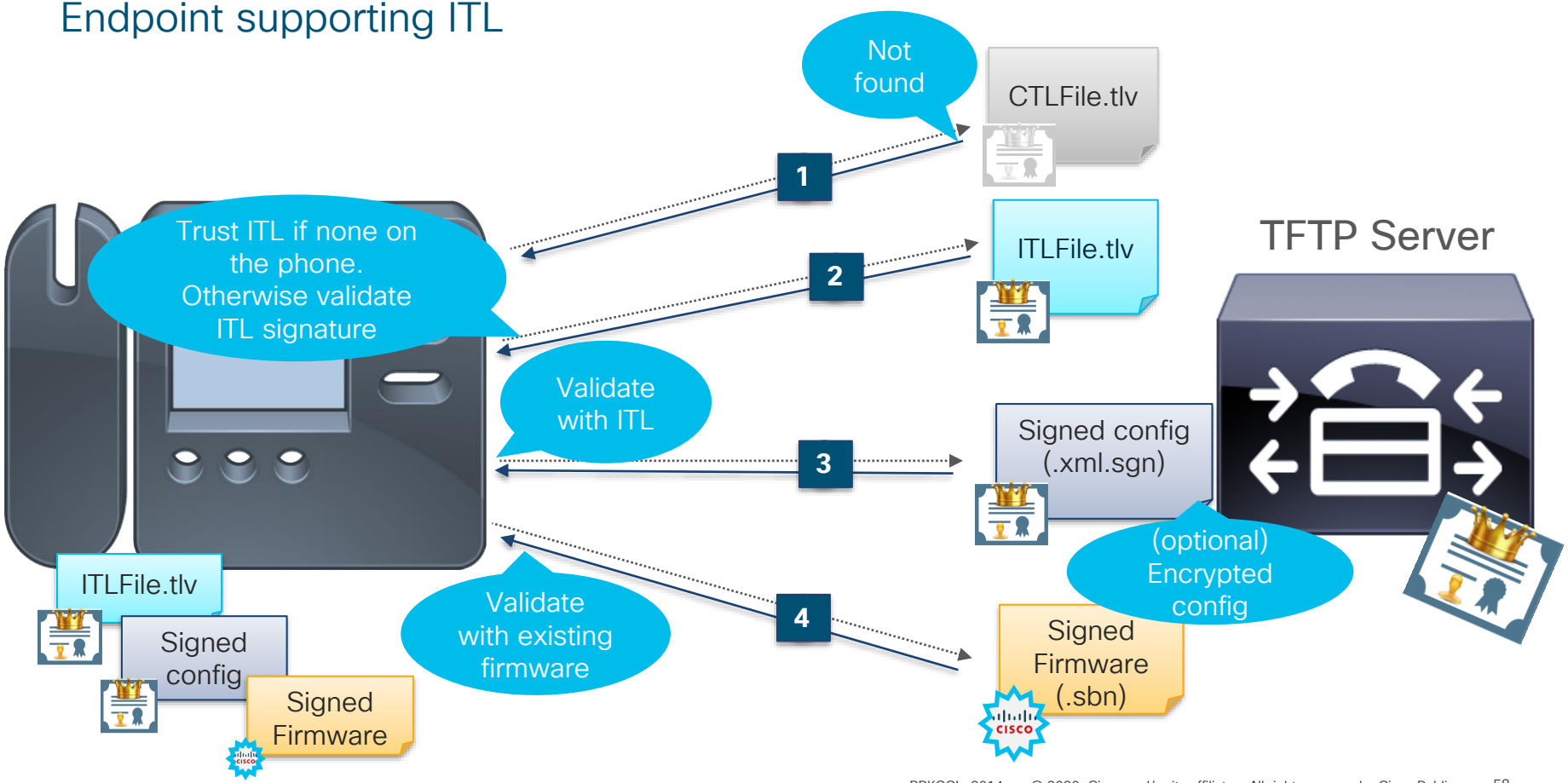
Planned in future release with SIP OAuth

Security by Default



UCM non-secure

Endpoint supporting ITL



Contents of the ITL and Trust Anchor

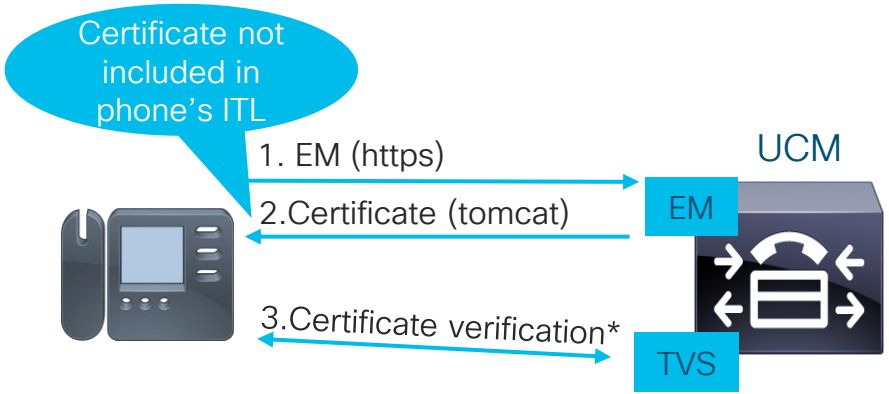
Certificate	ITLFile.tlv
CallManager	☑ from TFTP only, all nodes 12.0+
CallManager EC	☑ from TFTP only, all nodes 12.0+
TVS	☑ all nodes
CAPF	☑ pub only, if activated
ITLRECOVERY	☑ UCM 10.0+
Signer of ITL File	☑ CallManager Certificate (TFTP) ☑ ITLRECOVERY

Before 12.0

As of 12.0

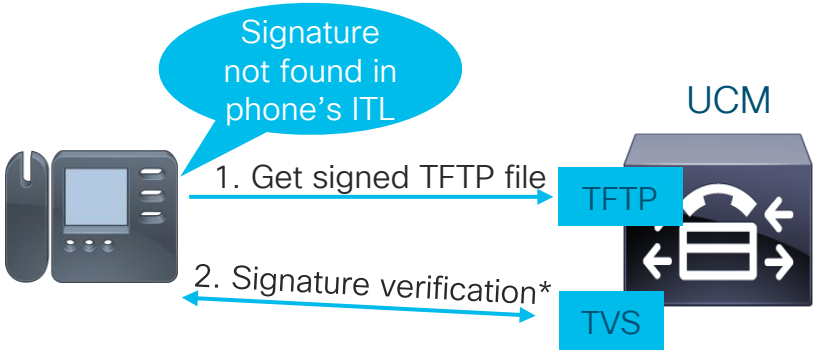
Trust Verification service (TVS)

Secure IP phones services (HTTPS)



*TVS gives the phone the ability to validate certificates which are not included in ITL (such as Tomcat certificate)

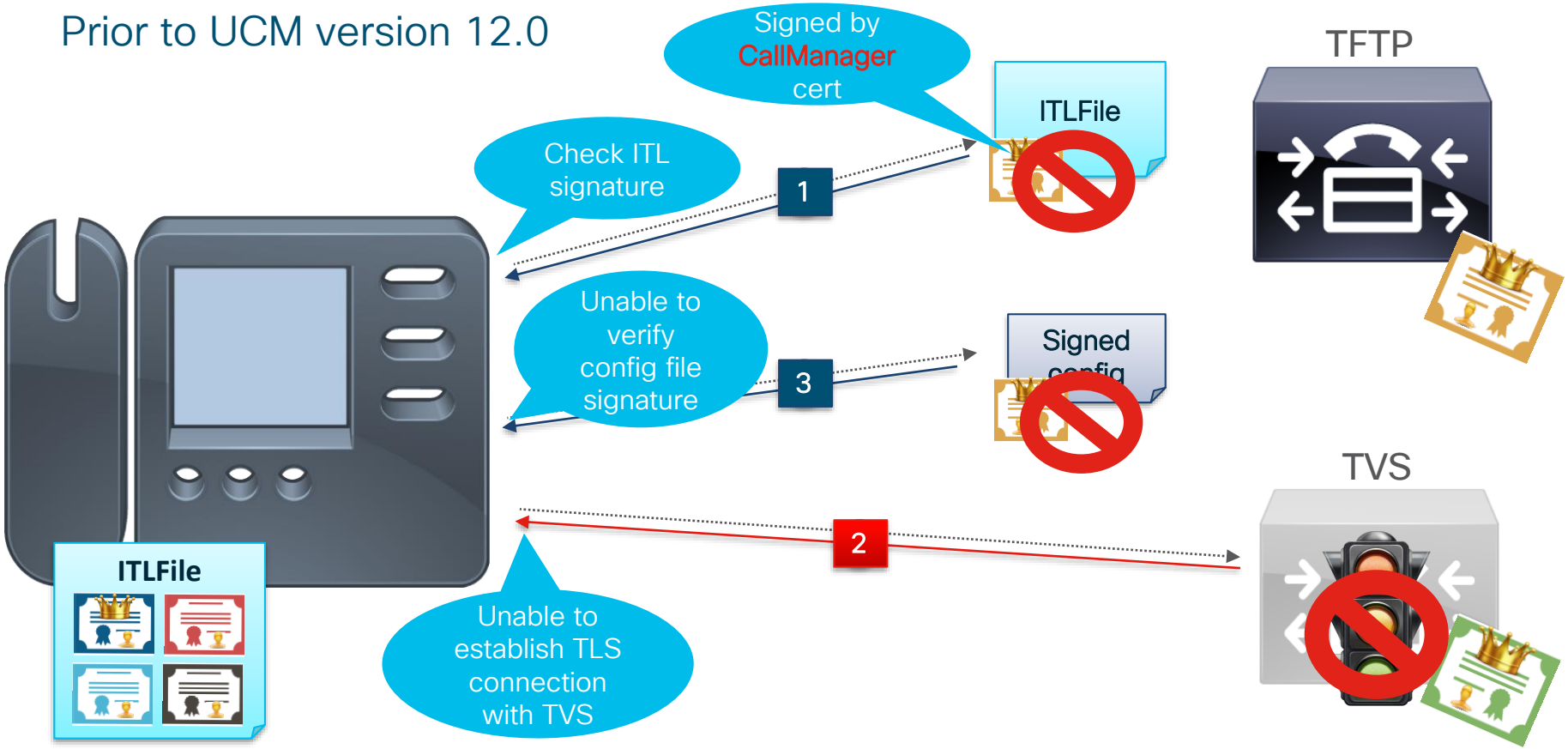
Signature verification of TFTP files (ITL, CTL, Config file, Locales..)*



*Applicable when the phone is not able to verify the signature against its trust store. Example – during certificate regeneration process. TVS process not engaged in normal operation.

Loss of Trust

Prior to UCM version 12.0



Fixing ITL mismatches

1. Perform Bulk Reset of ITL file*

   pub admin: ***utils itl reset localkey***

2. Contact TAC
3. Use 3rd party tools
4. Remove ITL file manually

- Least expensive
- Simple

- More expensive
- Complex

*Prior UCM 12.0 – ITL file temporarily signed by ITL Recovery key
UCM 12.0 onwards – ITL file signed by the CallManager key

Quiz

What is the purpose of the **CTL file** in non-secure cluster?

A) Used to verify certificates by endpoints

B) Allows encryption of TFTP configuration files

C) CTL file does not exist in non-secure cluster

D) Used to tell the future

Securing Media and Signaling (Mixed mode/SIP OAuth)

UCM Mixed mode

Feature	Non Secure Cluster	Mixed mode Cluster
Auto-registration	✓	✓
Signed Phone Firmware	✓	✓
Signed & Encrypted Phone Configs	✓	✓
Secure Phone Services (HTTPS)	✓	✓
CAPF + LSC	✓	✓
IP VPN Phone	✓	✓
Encrypted SIP Trunk	✓	✓
Secure Jabber (TLS & SRTP)	✓	✓
Secure Endpoints (TLS & SRTP)	✗	✓

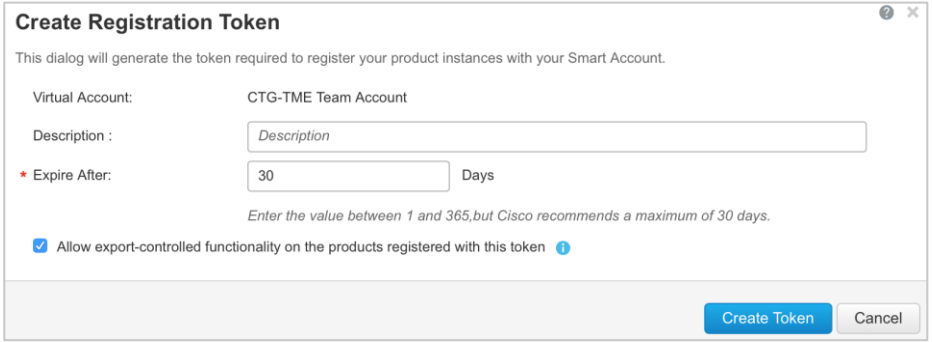
New in 11.5

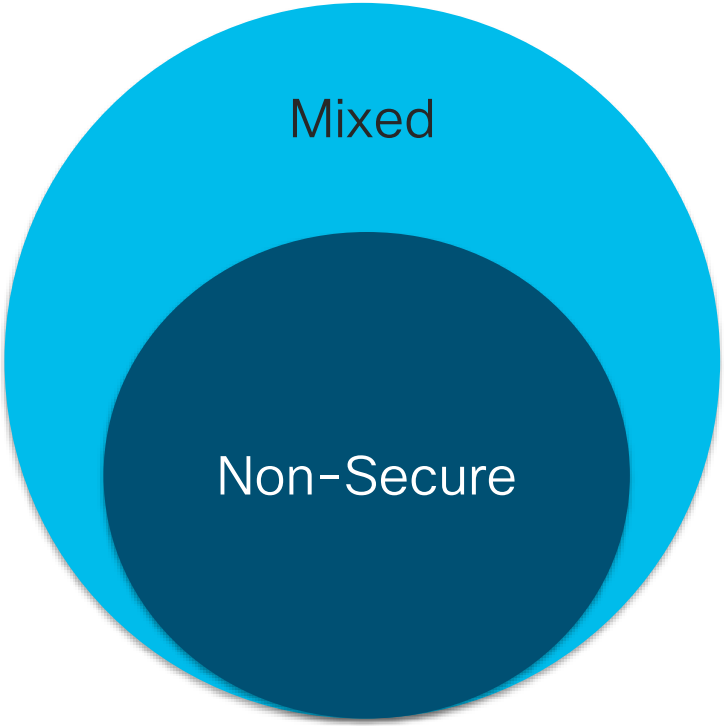
New in 12.5 with SIP OAuth

Planned in future release with SIP OAuth

UCM Cluster Security Mode

- Non-Secure or Mixed
  - NOT On/Off
- Mixed Mode Requirements:
  - Export Restricted version of UCM
  - 11.5(1)SU3+ Encryption License
    12.0+ Export-controlled Functionality allowed





UCM Mixed Mode and Generating CTL

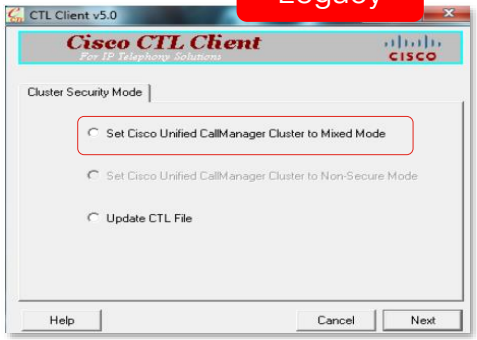
Tokenless method

10.5+ Recommended

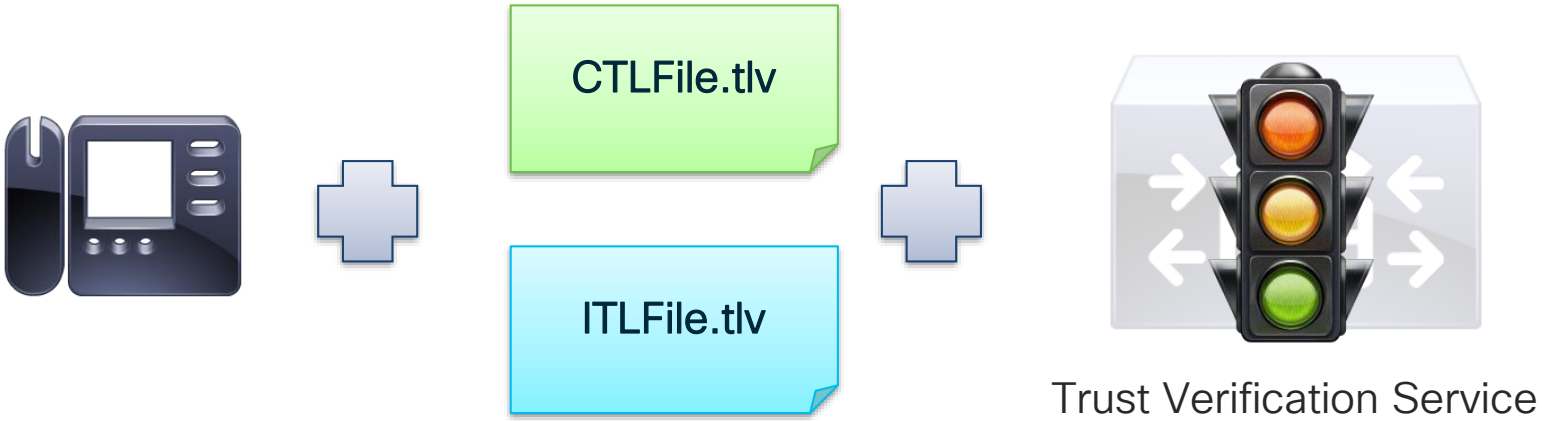
utils ctl set-cluster mixed-mode

Token based method

Legacy

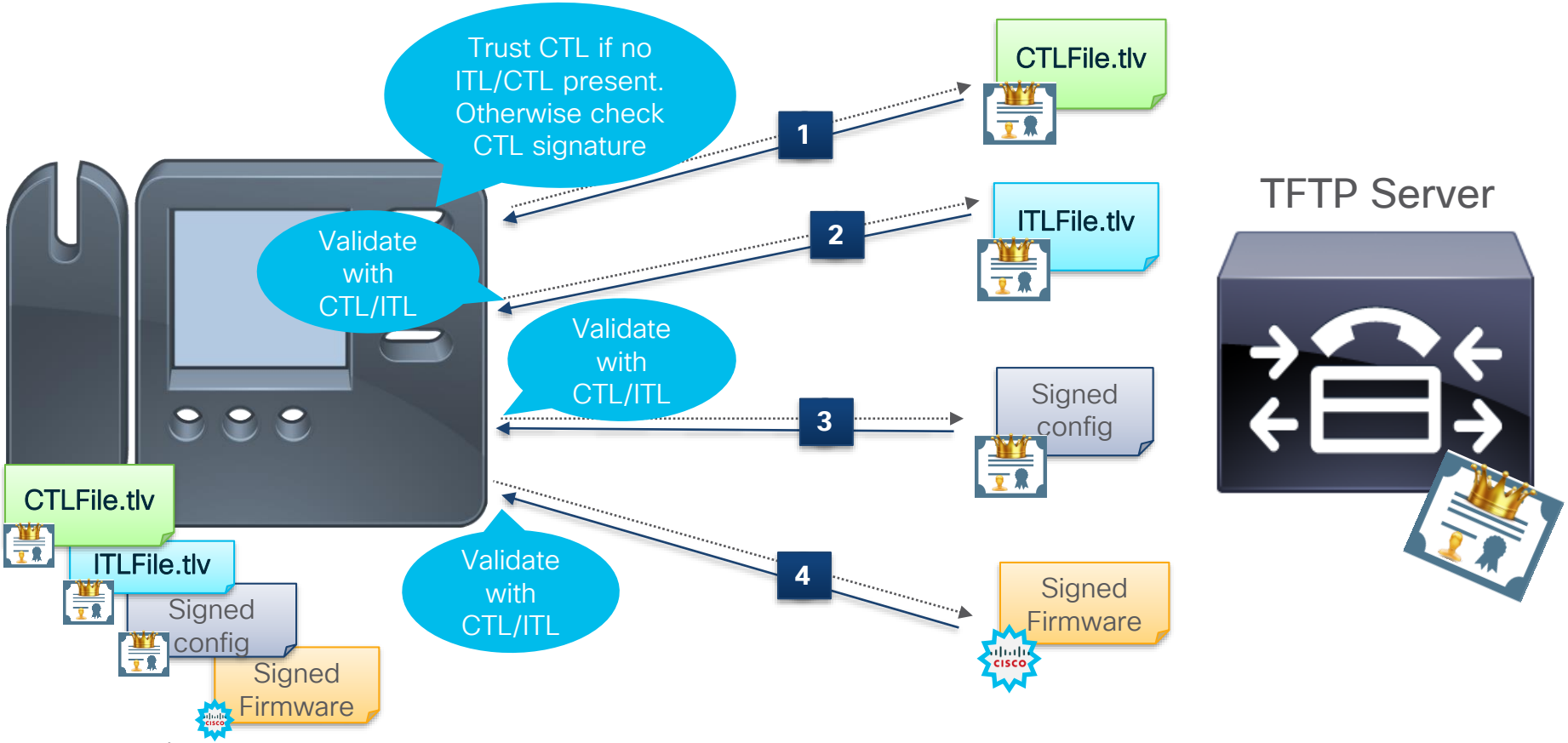


Phone Trust List and Verification



Note: CTL needs to be updated manually if any of its certificate changes.

UCM in mixed mode



Contents of CTL and Trust Anchor

Certificate	CTLFile.tlv
CallManager	☑ from all nodes
CAPF	☑ pub only, if activated
ITLRECOVERY	☑ UCM 10.5Su2+
Signing Certificate (Token Based method)	☑ USB Token Certificates
Signing Certificate (Tokenless method)	☑ Pub. CallManager certificate Or ☑ ITLRECOVERY

Legacy

Before 12.0

As of 12.0

Securing Endpoints

- Non-Secure

  No media & signaling encryption

- Encrypted (LSC or MIC)

  Mixed mode required, LSC required on Jabber

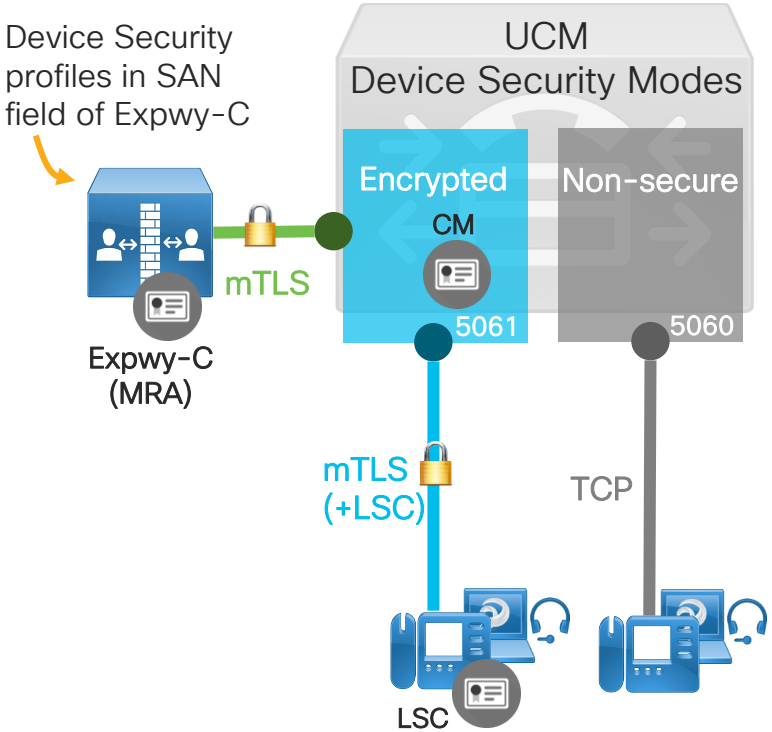
  MIC can be used on endpoints

  Inconvenient – multiple device installation

Phone Security Profile Information

Product Type:	Cisco Unified Client Services Framework
Device Protocol:	SIP
Name*	Cisco Unified Client Services Framework - Standard SIP Secure Pro
Description	Cisco Unified Client Services Framework - Standard SIP Secure Pro
Device Security Mode	Encrypted
Transport Type*	TLS

☐ TFTP Encrypted Config



Phone Security Modes

- **Authenticated mode** – provides integrity and authentication for TLS connection. Be aware, that neither the signaling nor the media is encrypted.
- **Encrypted mode** – on the endpoint provides integrity, authentication, and encryption of signaling. Media is also encrypted using SRTP if other communicating party support it as well.

Challenges – Jabber & Mixed mode

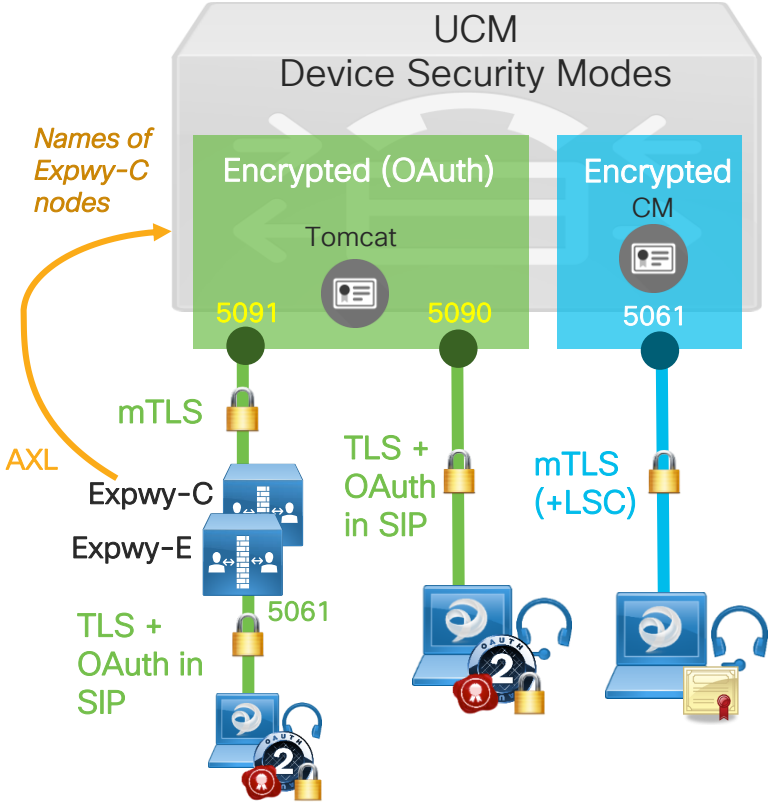
- LSC installation/update required (no support for MIC)
  - CAPF operation needed
  - LSC required anytime Jabber installed on new device
  - Difficulties when Jabber switches between on-premises and off-premises (CAPF not supported over MRA)
- Monitoring LSC expiration
- Challenges with LSC on multiple laptops

Solution: SIP OAuth

Securing Jabber with SIP OAuth (New)

- **SIP OAuth** enables media/signaling encryption without an endpoint certificate (LSC)
- Jabber client is authenticated through OAuth token instead of LSC
- No CAPF requirement (no problem over MRA)
- Works with/without mixed-mode
- Introduced in UCM 12.5(1), Jabber 12.5 and Expressway X12.5

Note: In future releases, plan to add SIP OAuth support on the 7800/8800 series phones.

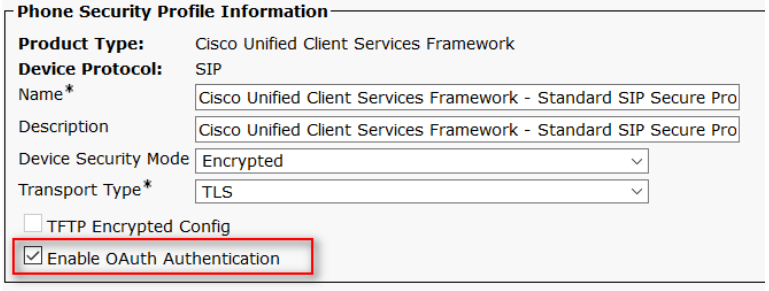


SIP OAuth configuration

- Configure Refresh Logins in Enterprise Parameters (OAuth with Refresh Login Flow)
- Enable SIP OAuth Mode (pub admin cli)*

```
admin:utils sipOAuth-mode enable
SIP OAuth mode enabled.
Please restart the Cisco CallManager service on all nodes in the cluster where it is running.
admin:
```

- Enable OAuth support in Phone Security profile

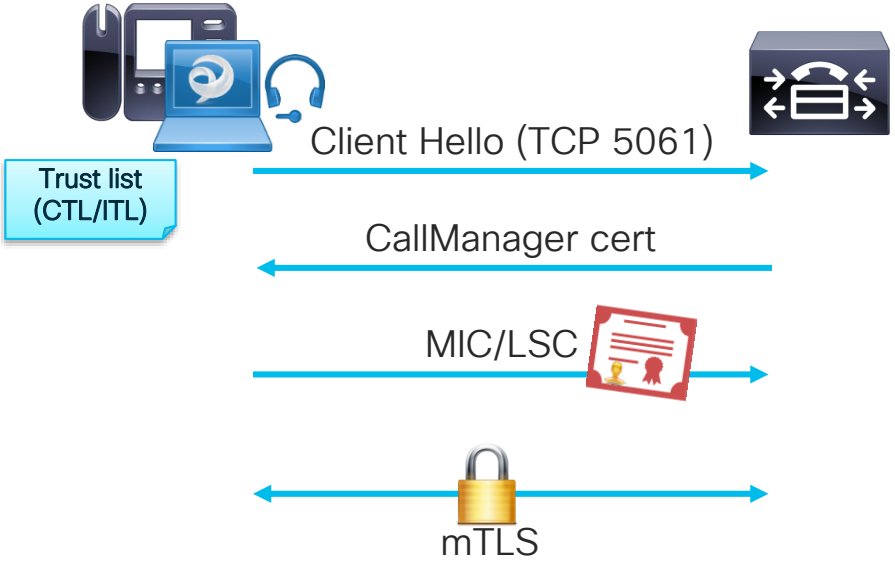


* Ensure that UCM is registered to a Smart or Virtual account with “Allow export-controlled functionality”

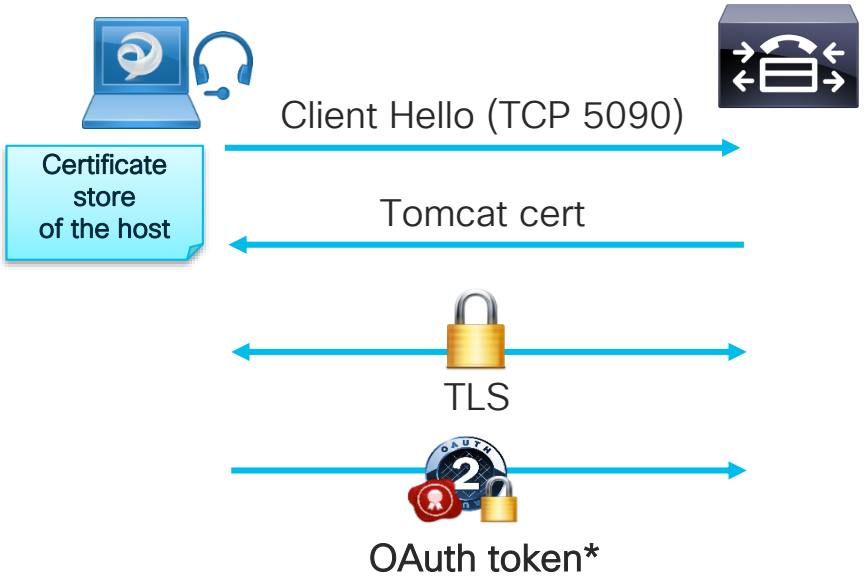
For more details click here

High Level View of Secure Signaling

Endpoint in Encrypted mode with MIC/LSC



Jabber in Encrypted mode + **SIP OAuth**



*OAuth token sent inside of SIP REGISTER message

What's Secure RTP?

- As per RFC 3711: SRTP is a profile of the Real-time Transport Protocol (RTP), which can provide confidentiality, message authentication, and replay protection to the RTP traffic
- It uses **AES** (Advanced Encryption Standard) as the default cipher for stream encryption
- **HMAC** (Hash-based Message Authentication Code) is used to authenticate the message and protect its integrity

a=crypto:<tag> <crypto-suite> <key-params> [<session-params>]

SDP for RTP

```
m=audio 8256 RTP/AVP 0
c=IN IP4 14.50.248.31
a=rtpmap:0 PCMU/8000
```

SDP for SRTP

```
m=audio 8264 RTP/SAVP 0
c=IN IP4 14.50.248.31
a=rtpmap:0 PCMU/8000
a=crypto:1 AES_CM_128_HMAC_SHA1_32 inline:
L5+zq2AXJxLk+058lu/XRQWJZiK0c0D0
```

Click here for more details

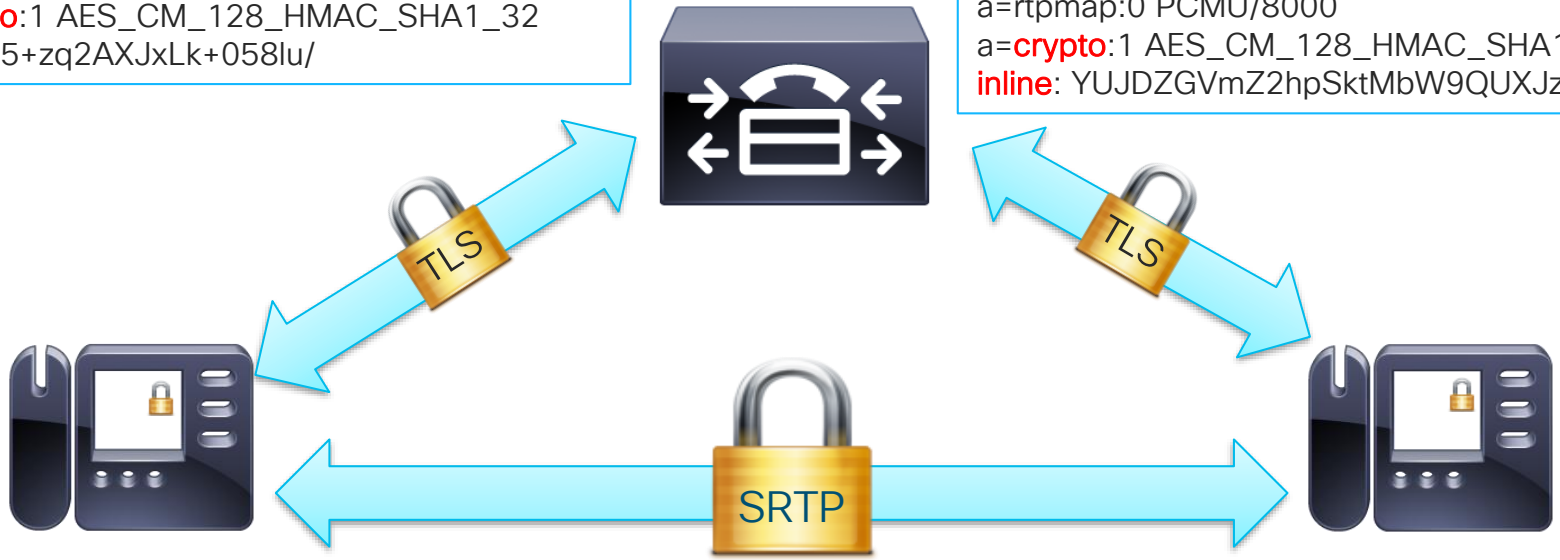
End-to-End Phone Encryption

Crypto keys exchange

```
INVITE sip:2000@10.1.1.1;user=phone SIP/2.0
<output omitted>
m=audio 8264 RTP/SAVP 0
c=IN IP4 10.1.1.2
a=rtpmap:0 PCMU/8000
a=crypto:1 AES_CM_128_HMAC_SHA1_32
inline: L5+zq2AXJxLk+058lu/
```

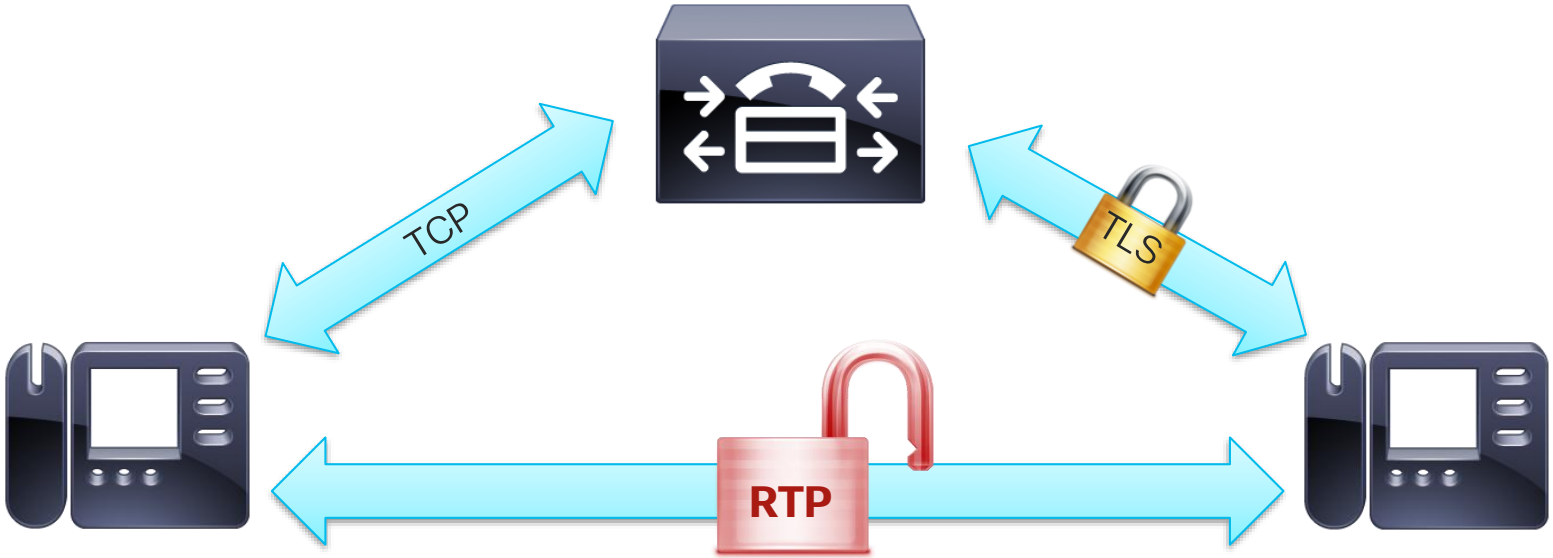
```
SIP/2.0 200 OK
<output omitted>

m=audio 3820 RTP/SAVP 0
c=IN IP4 10.1.1.3
a=rtpmap:0 PCMU/8000
a=crypto:1 AES_CM_128_HMAC_SHA1_32
inline: YUJDZGVmZ2hpSktMbW9QUXJzV
```



Secure to Non-Secure Interworking

- UCM will automatically fallback to RTP when one of the endpoints does not have Encrypted mode configured due to the fact that confidentiality of audio stream cannot be guaranteed since the SRTP crypto keys might be exposed



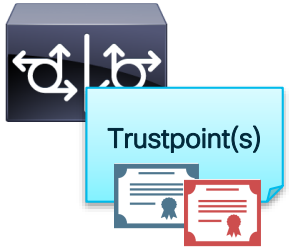
Securing CUBE

Trustpoints and Identity certificates

- A **trustpoint** is an abstract container to hold a certificate in IOS. A single trustpoint is capable of storing two active certificates at any given time.

- Certificate management

  - Define the trustpoint — *crypto pki* ***trustpoint*** *<trustpoint_name>*
  - Generate CSR — *crypto pki* ***enroll*** *<trustpoint_name>*
  - Import CA root certificate — *crypto pki* ***authenticate*** *<trustpoint_name>*
  - Import Identity certificate — *crypto pki* ***import*** *<trustpoint_name>* ***certificate***



Protecting Media and Signaling

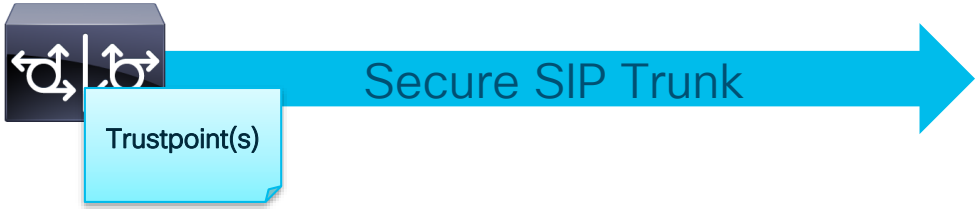
Enabling Signaling Encryption

- Associate the trust point to SIP trunk

```
sip-ua
  crypto signaling remote-addr 10.1.1.100 255.255.255.255 trustpoint <name>
  crypto signaling remote-addr 10.1.2.0 255.255.255.0 trustpoint <name>
  crypto signaling default trustpoint default trustpoint <name>
```

- Enable TLS at dial-peer or global level

```
session transport tcp tls
```



Protecting Media and Signaling

Enabling Media Encryption

- Define SRTP Crypto Suites (optional)

```
voice class srtp-crypto 1
 crypto 1 AEAD_AES_256_GCM
 crypto 2 AEAD_AES_128_GCM
 crypto 3 AES_CM_128_HMAC_SHA1_80
 crypto 4 AES_CM_128_HMAC_SHA1_32
```

1. Configure specific SRTP cipher suite support whereas default preference is as follow:
   - AEAD_AES_128_GCM*
   - AEAD_AES_256_GCM*
   - AES_CM_128_HMAC_SHA1_80
   - AES_CM_128_HMAC_SHA1_32

*Support for NGE cipher suite from IOS XE16.5.1

- Enable SRTP on Dial-peer (globally or under tenant)

```
dial-peer voice 1 voip
 srtp
 voice-class sip srtp-crypto 1
 srtp pass-thru
```

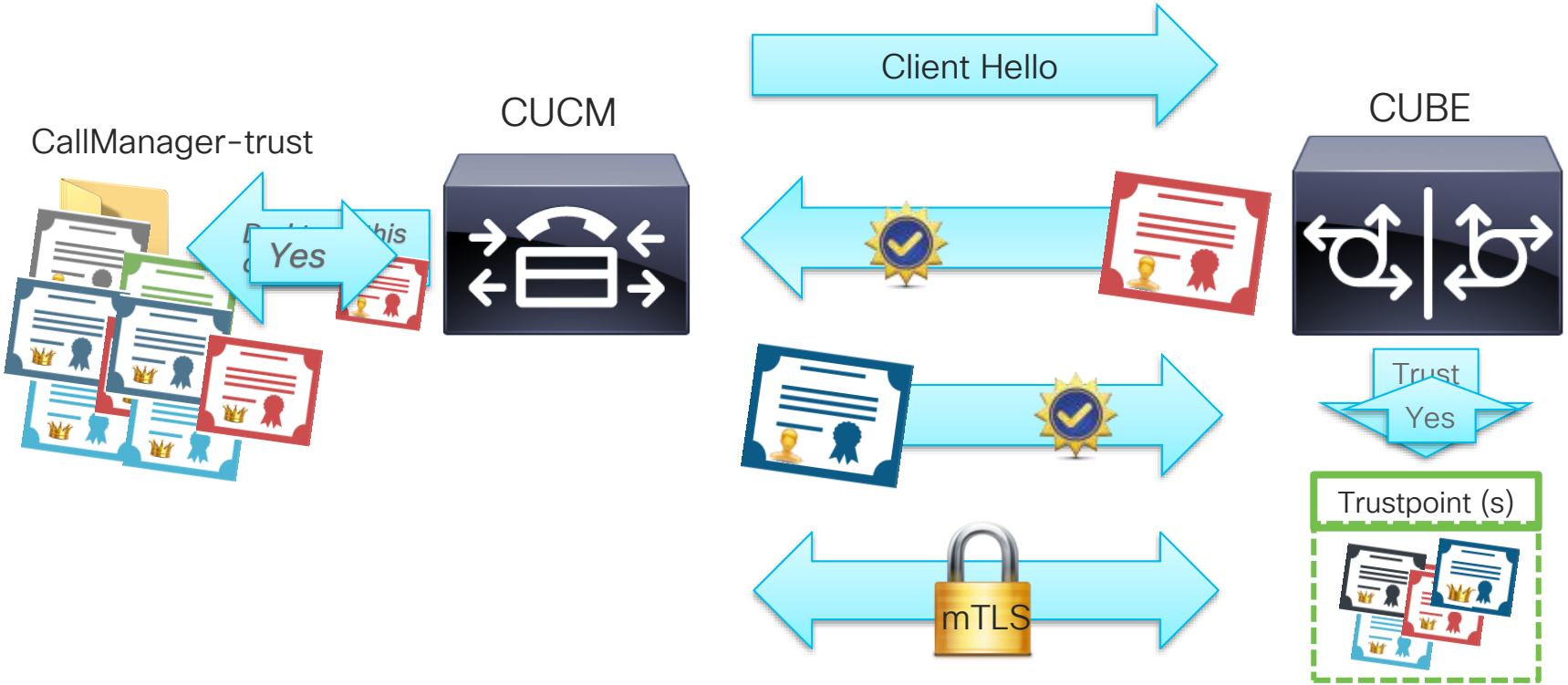
2. Enables SRTP

3. Applies Crypto Suite Selection

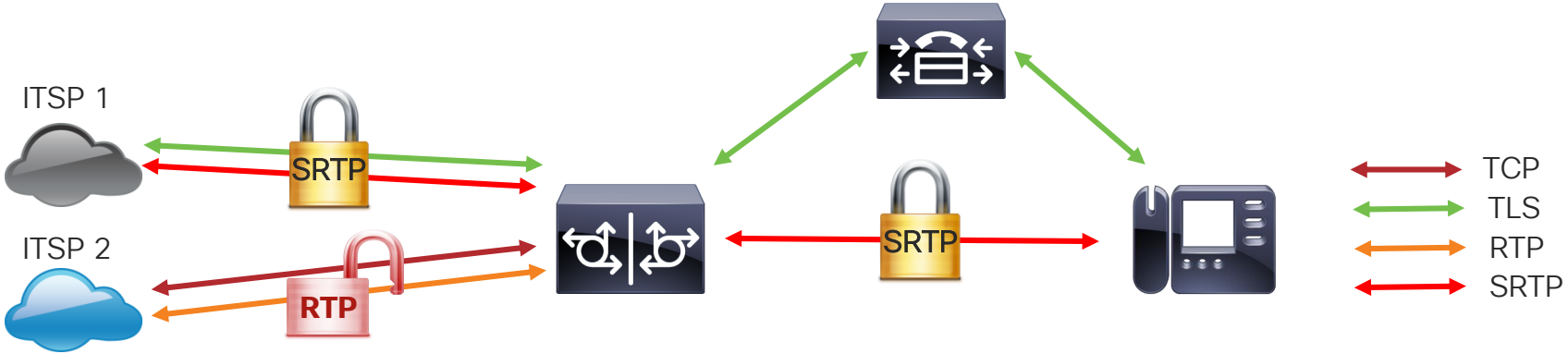
4. (Optional) Allows to pass unsupported crypto suites.

Click here for more details

High Level View of a Secure Connection



High Level View of Secure Media



- CUBE **session capacity** is impacted SRTP with SIP TLS (refer to Collaboration CVD On-Premises)
- **SRTP-SRTP support** - Secure calls between two enterprises using same and different cipher suites support
- **SRTP-SRTP pass-through -** feature allows pass-through of encrypted media for unsupported crypto suites from one call-leg to the other
- **SRTP-RTP interworking support** - Secure network to non-secure network calls support (DSP required on ISR G2, No DSP required for Cisco ISR G3, ASR 1000/ISR 1000, CSR 1000V)

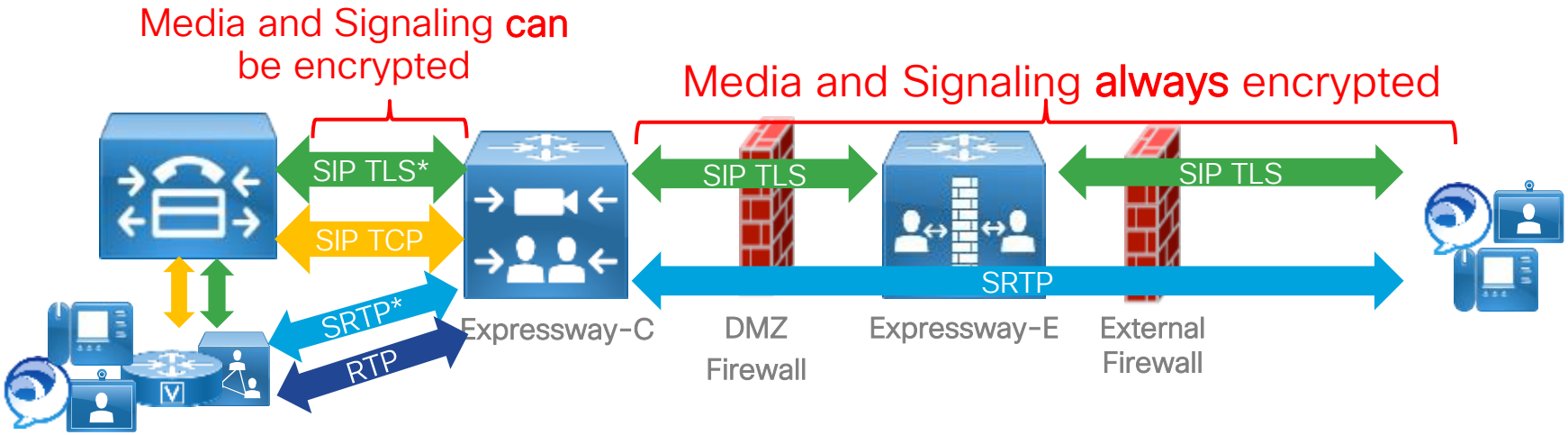
cisco Live!

Click here for more details

Expressway Mobile and Remote Access (MRA)

MRA Media and Signaling Encryption

- On the Internet and in the traversal zone: Media and Signaling are always encrypted.
- In the internal network, Media and Signaling encryption depends on the Unified CM configuration for the MRA endpoint.

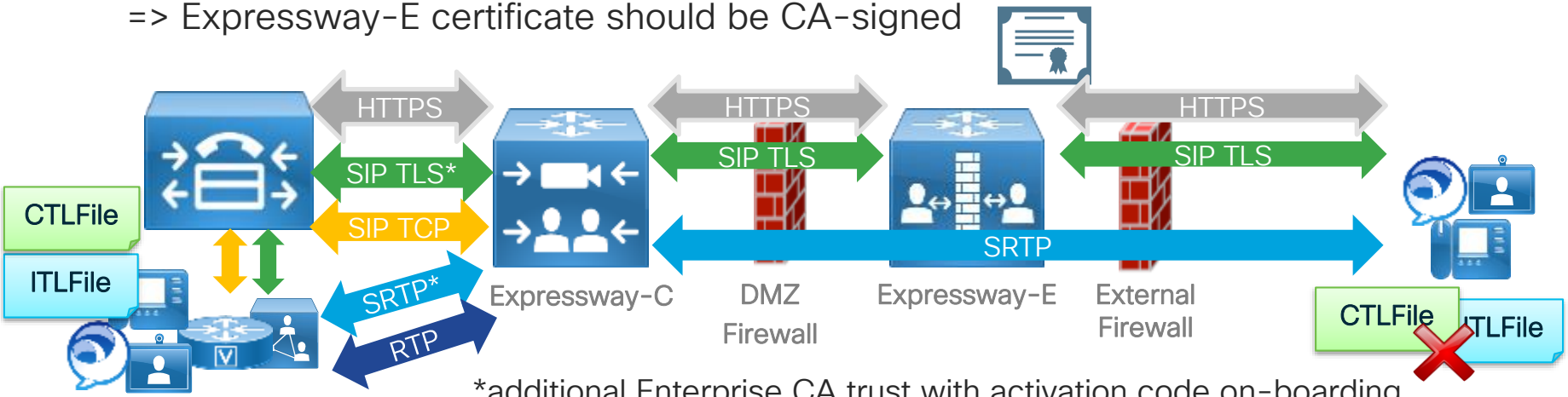


MRA Authentication

MRA Endpoint Authenticating Expressway-E

- MRA endpoints verify the Expressway-E Server Certificate.
  - **ITL/CTL not used**
  - Jabber Clients rely on the **underlying platform** trusted CA list
  - Hardware endpoints rely on a **trusted CA list included in firmware***

=> Expressway-E certificate should be CA-signed

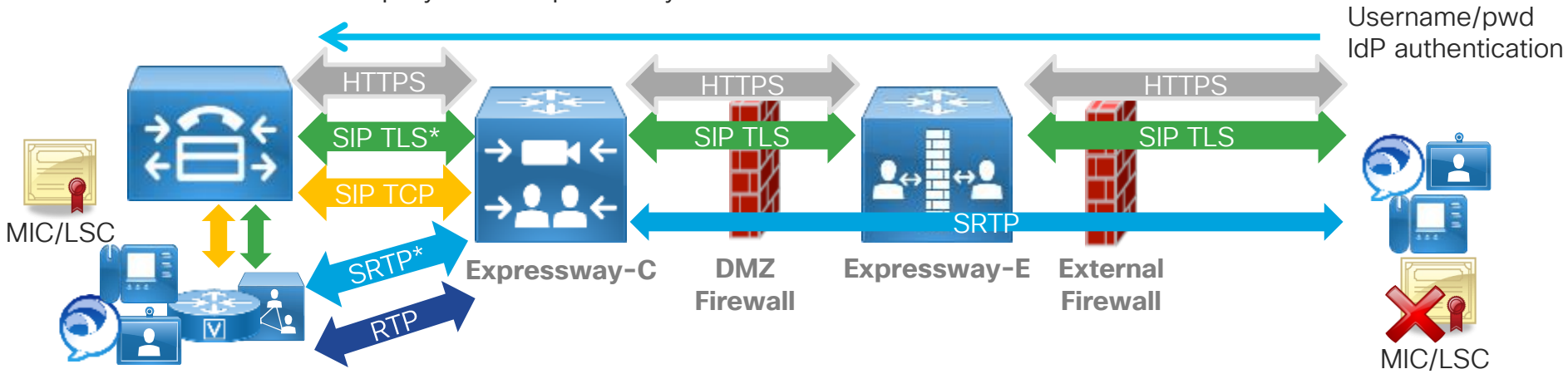


*additional Enterprise CA trust with activation code on-boarding

MRA Authentication

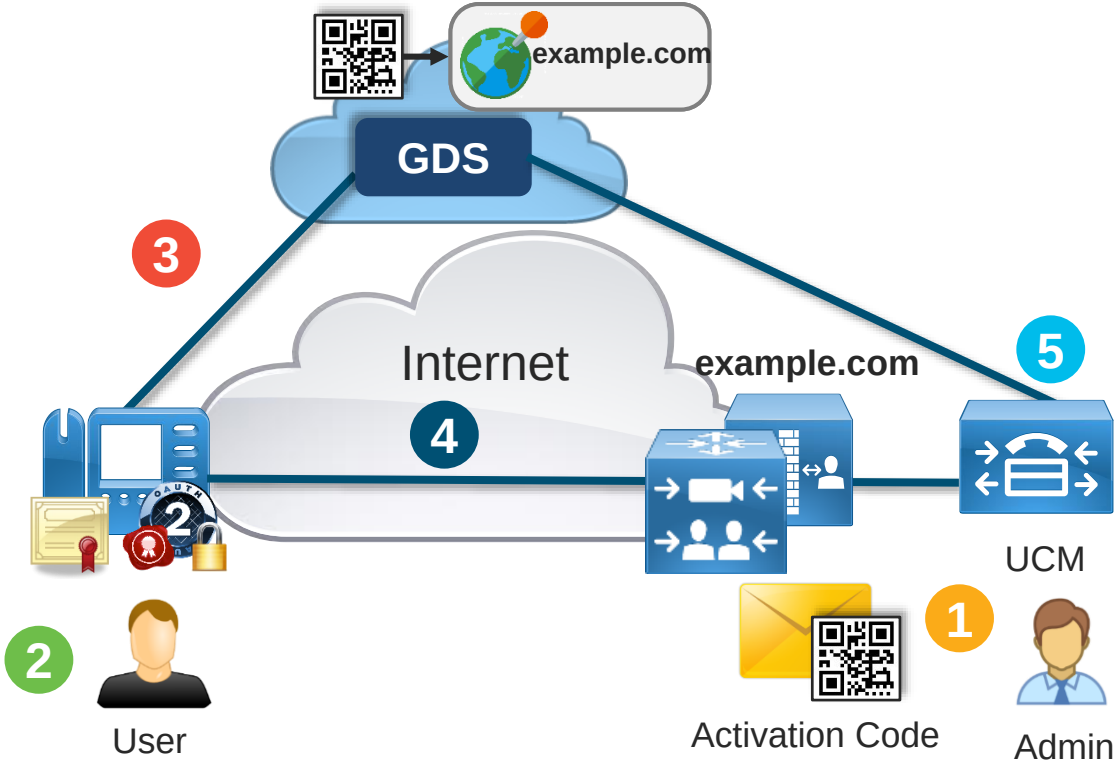
Authenticating the MRA Endpoint

- Expressway-E does not verify the MRA endpoint certificate (MIC/LSC). Instead:
  - Phones - End-user typically enters username/password for initial HTTPS connection (except with activation code onboarding
  - Jabber - End-user typically enters username/password or uses any other available IdP authentication method if SSO deployed on Expressway



Activation Code Device Onboarding over MRA

UCM 12.5(1)SU1



1. Administrator configures phone in UCM without having to specify MAC address and gets an activation code generated by GDS/UCM.
2. User (or installer) enters activation code in new MRA phone.
3. Phone gets MRA target (service domain) from GDS.
4. Phone connects to Expressway/UCM, authenticates using its MIC + activation code.
5. UCM updates device configuration in its database with phone MAC address. Phone then registers.

For more details, refer to BRKCOL-2794: A new Architecture for Easy Always-On UC Security

Conclusion

Key Takeaways

- Deploy **Multi-Layered** Security
- Manage **certificates** carefully and simplify (CA-signed certificate for Tomcat and CallManager, Multi-SAN)
- Enable **encryption for signaling and media** for endpoints:
  - For Jabber 12.5+/UCM 12.5+ use **OAuth (with refresh token)** / **SIP OAuth** (no need to install LSC)
  - For Phones, considering using UCM Mixed Mode (with LSC signed by CAPF or an online CA)
- Enable **encryption** on other links/products (IP Phone Services, LDAP, SIP Trunk, CUBE…)
- Use activation code onboarding

UC Security is a hassle…

- Additional configuration
- Complexity (ITL, CTL…)
- Potential interop issues
- Potential Loss of trust with phones
- Certificate Management (number of certificates, expiration)
- Defects

SUCCESS

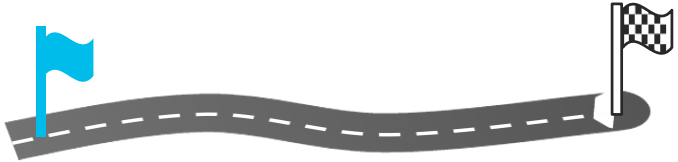
but we are trying to make it easier…

- SIP OAuth / No need to install LSC
- Endpoint certificates signing with Online CA
- ITLRecovery as a trust anchor
- Activation code onboarding
- Granular ciphersuite control

-------- Planned -------

- Centralized certificate management
- Certificate reduction
- Mismatched ITL Checksum report
- Certificate trust chain verification by phones

SUCCESS



Additional UC Security Sessions

- **BRKCOL-2794**: A new Architecture for Easy Always-On UC Security (Goodbye CAPF, Hello OAuth), Wednesday, 2:45 pm
- **BRKCOL-2000**: Media path optimization with ICE for MRA devices, Friday 11:30 am
- **BRKCOL-3224:** Implementing and Troubleshooting Secure Voice on Network Edge Devices, Tuesday, 11:00 am
- **BRKUCC-2801**: Enabling External Collaboration with Expressway, Tuesday 11:00 am

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

Continue your education

Demos in the Cisco campus

Walk-in labs

Meet the engineer 1:1 meetings

Related sessions

Thank you

CISCO

You make **possible**

Reference slides

Detecting CTL/ITL mismatches

1. Identify the signature of the current TL on each TFTP server
   - show itl
   - show ctl

2. Identity the signature of the current TL on the phones
   - Endpoint Webpage or Endpoint's screen or
   - DeviceTLInfo message in the UCM AlternateSyslog file

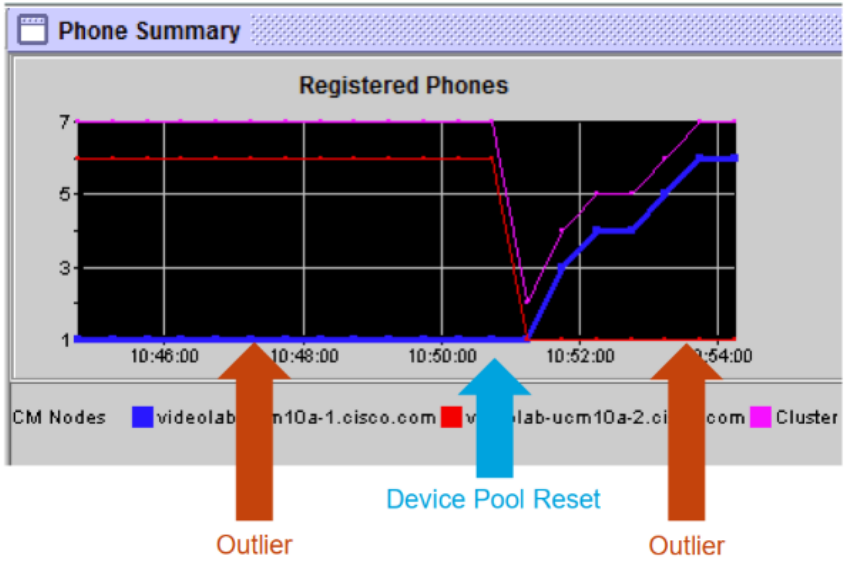
   file search activelog syslog/AlternateSyslog* DeviceTLInfo

   %UC_-3-**DeviceTLInfo**:%[DeviceName=SEPB000B4BA21BE][IPv4Address=192.186.1.55][CTL_Signature=05 A6 9A 0C 99 56 72 B3][ITL_Signature=ED AD 19 9F 16 E9 BF C4][ITL_TFTP_Server=ucmpub.cisco.lab][UNKNOWN_PARAMTYPE:StatusCode=1][AppID=Cisco CallManager][ClusterID=StandAloneCluster][NodeID=ucmpub]: Trust List Files are updated or installed

3. Compare

Detecting CTL/ITL mismatches at scale

- Change phone's settings and monitor
  1. Change a setting in the phone's xml configuration file, Example – CallManager group:
     - Old: Sub, Pub
     - New: Pub, Sub
  2. Reset Device pool for phones to pick up new configuration file
  3. Look for the endpoints that do not reflect the change
  4. Fix any outliers



- Mismatched ITL Checksum report
  - Coming in future releases
  - Provides a report of mismatched ITL files by utilizing the DeviceTLInfo messages

Identity Certificates used by Communications Manager

For your reference

CallManager
CallManager-EC

- Used for TLS connections to CallManager service (TCP port 5061 for SIP or 2443 for SCCP)
- Signs TFTP files: configuration files, localization files, etc

CAPF

- Use for TLS connections to CAPF service (TCP port 3804)
- Signer of the phones Locally Significant Certificates (LSC)

Tomcat
Tomcat-EC

- Used for HTTPS connections to Web services (TCP port 8443)
- Used to sign SSO SAML Requests (if required by IdP)

TVS

- For TLS connections to the TVS service (TCP port 2445)

Identity Certificates used by Communications Manager

For your reference

IPSec

- Used for IPSec connections and inter-cluster communication by DRS during backup operations

ITLRecovery

- Included in ITL file beginning with 10.0, CTL in 11.0
- Used by TFTP to sign TL files in certain scenarios

Certificate Trust Stores used with Client Connections

For your reference

CallManager-trust

- Used to Validate Certificates when CallManager is the Client side
- IE: Outbound SIP TLS Connections

CAPF-trust

- Used for CAPF Service to Validate Client side Certificate (mutual-authentication) when Authenticating Phones using MIC while installing their Locally Significant Certificates (LSC)

Tomcat-trust

- Used to Validate Certificates for all Web Applications' Client requests as well as LDAPS (DirSync + Ldap Authentication)
- IE: EMCC, CTI Manager LDAPS Authentication

TVS-trust

- Used for Intermediate and Root certificates that are issuers to CA-signed TVS certificates

Certificate Trust Stores used with Client Connections

For your reference

Userlicensing-trust	• Used by ELM and PLM
Phone-trust	• Allows TVS to authenticate certificates used by IP Phone Services
Phone-vpn-trust	• Holds server certificates for the Phone VPN feature
Phone-sast-trust	• Allows TVS to authenticate certificates used by TFTP to sign files
Phone-ctl-trust	• Used to include a certificate in a CTL file. • Only works for tokenless-CTL after version 11.5

Protecting Media and Signaling

Signaling – Cipher suite support

- TLS Cipher suite selection

sip-ua
crypto signaling default trustpoint cube <cipher selection>

Cipher selection	
<enter> (default)	All TLS_RSA_WITH_RC4_128_MD5 + all bellow
ecdsa-cipher	ECDSA-only *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 and *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384.
strict-cipher	RSA-Only TLS_RSA_WITH_AES_128_CBC_SHA, *TLS_DHE_RSA_WITH_AES_128_CBC_SHA1, *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, and *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

*Support from Cisco IOS 15.6(1)T onwards

Verign_Class_3_Secure_Server_CA - G3 Expiring

tomcat-trust	VeriSign_Class_3_Secure_Server_CA_-_G3	signed CA-signed	RSA	VeriSign_Class_3_Secure_Server_CA_-_G3	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5	02/07/2020	This certificate is used by UCM to communicate with Cisco if Call-Home feature is enabled.

- Verisign Certificate expiring on Feb 7th 2020.
- Available on the OS Certificate Management page.
- Action: Just delete this certificate, it was used only for Smart Call Home.
- Note: Smart Call Home does not use a Verisign certificate anymore. QuoVadis instead (CA certificate expires in 2031). This has been the case for some time now.
- https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_5_1SU1/adminGd/cucm_b_administration-guide-1251SU1/cucm_b_test-adminguide_chapter_010101.html

IOS Self-Signed Certificate Expiration on Jan. 1, 2020

- https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/215118-ios-self-signed-certificate-expiration-o.html

Cipher Management Control

SSH Ciphers

SSH Key Exchange

SSH MAC

Cipher Management

Save

SSH Ciphers	Type	SSH Ciphers
	Cipher String	aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com
	Actual Ciphers	aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com
SSH Key Exchange	Type	SSH KEX Algorithms
	Algorithm String	ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1,diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1
	Actual Algorithms	diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,diffie-hellman-group-exchange-sha1,diffie-hellman-group-exchange-sha256,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521
SSH MAC	Type	SSH MAC Algorithms
	Algorithm String	hmac-sha2-512,hmac-sha2-256,hmac-sha1
	Actual Algorithms	hmac-sha2-512,hmac-sha2-256,hmac-sha1

CISCO

You make **possible**