



TURN IT UP

CISCO *Live!*

#CiscoLive



The bridge to possible

Securing Webex Meetings with Zero Trust Security

Standards based End to End Encryption and Identity Verification

Tony Mulchrone
Senior Technical Marketing Engineer
Cisco Collaboration Technology Group
BRKCOL-2710



#CiscoLive





Agenda

- What is End to End Encryption ?
- Encrypting Webex Meetings Today
- Zero Trust Security for Webex Meetings :
 - New - End to End Encryption
 - New - End to End Identity Verification
- Summary and Roadmap

End to End Encryption



What is End to End Encryption ?

https://en.wikipedia.org/wiki/End-to-end_encryption

“End-to-end encryption (E2EE) is a system of communication where only the communicating users can read the messages. In principle, it prevents

There are many definitions of End to End Encryption....
But in simple layman's terms....

End to End Encryption is where your service provider does not have your encryption key and cannot decrypt your content

End-to-end encryption: The encryption of information at its origin and decryption at its intended destination without any intermediate decryption.

Encryption for Webex Meetings today

- Standard Encrypted Meetings
- E2E Encrypted Meetings

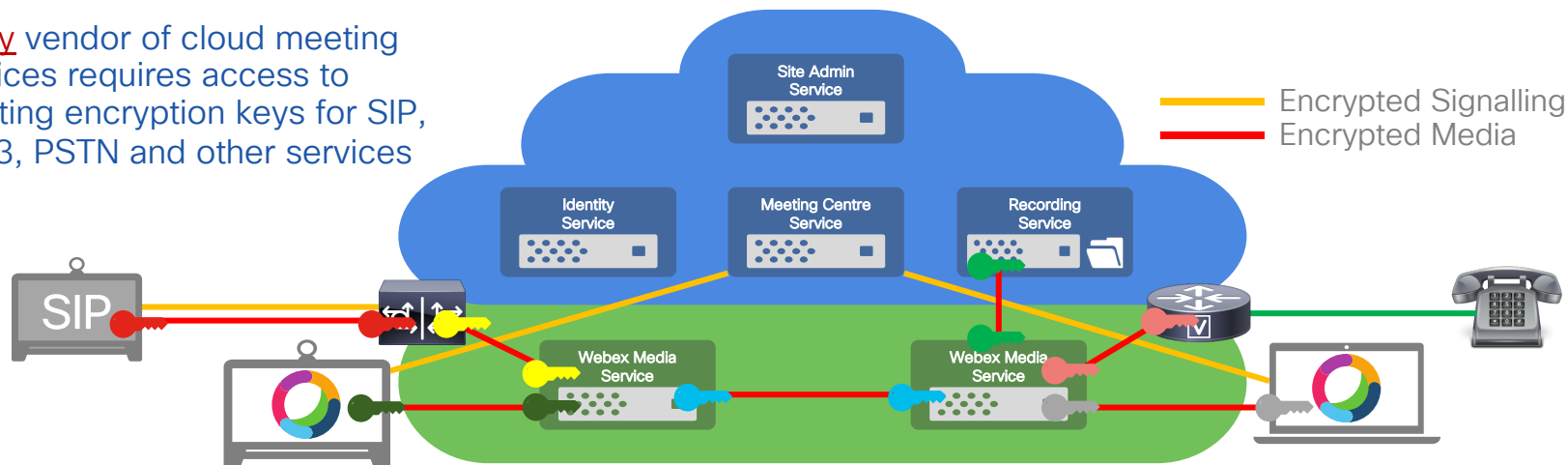


Encryption for standard Webex Meetings

With standard Webex Meetings, all signalling and media in the Webex cloud is encrypted
Webex apps and devices use encrypted signalling and encrypted media
SIP devices can encrypt signalling and media, PSTN audio is encrypted by the Webex cloud

With standard Webex Meetings, the cloud needs to access to encryption keys to decrypt SRTP media from SIP devices, PSTN gateways and for other services such as recording

Every vendor of cloud meeting services requires access to meeting encryption keys for SIP, H323, PSTN and other services

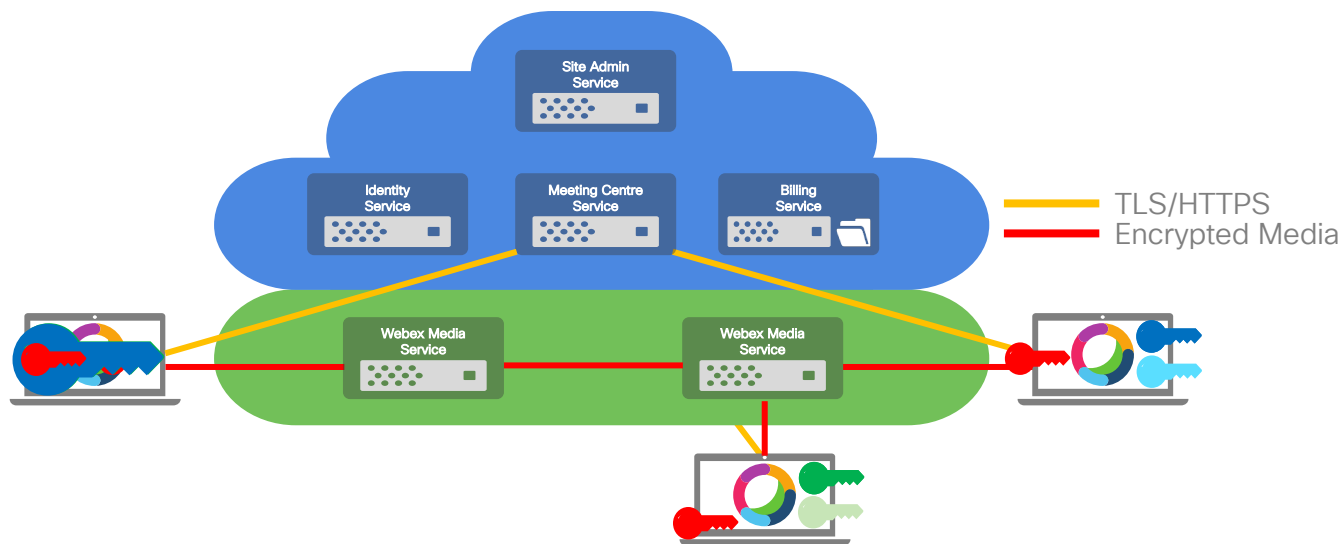


Confidential End-to-End Encrypted Webex Meetings

With E2E encrypted Meetings, the Webex cloud does not have access your meeting encryption key

The meeting encryption key is generated by the meeting host's Webex app

The meeting host encrypts the meeting key with participant's public and securely returns it over TLS



Cisco introduced E2E Encryption for Webex Meetings in 2008

<https://help.webex.com/en-us/WBX44739/What-Does-End-to-End-Encryption-Do>

Zero Trust Security for Webex Meetings

New

End to End Encryption &
End to End Identity



Zero-Trust Security : Strengthening and extending E2E Encryption for Webex Meetings

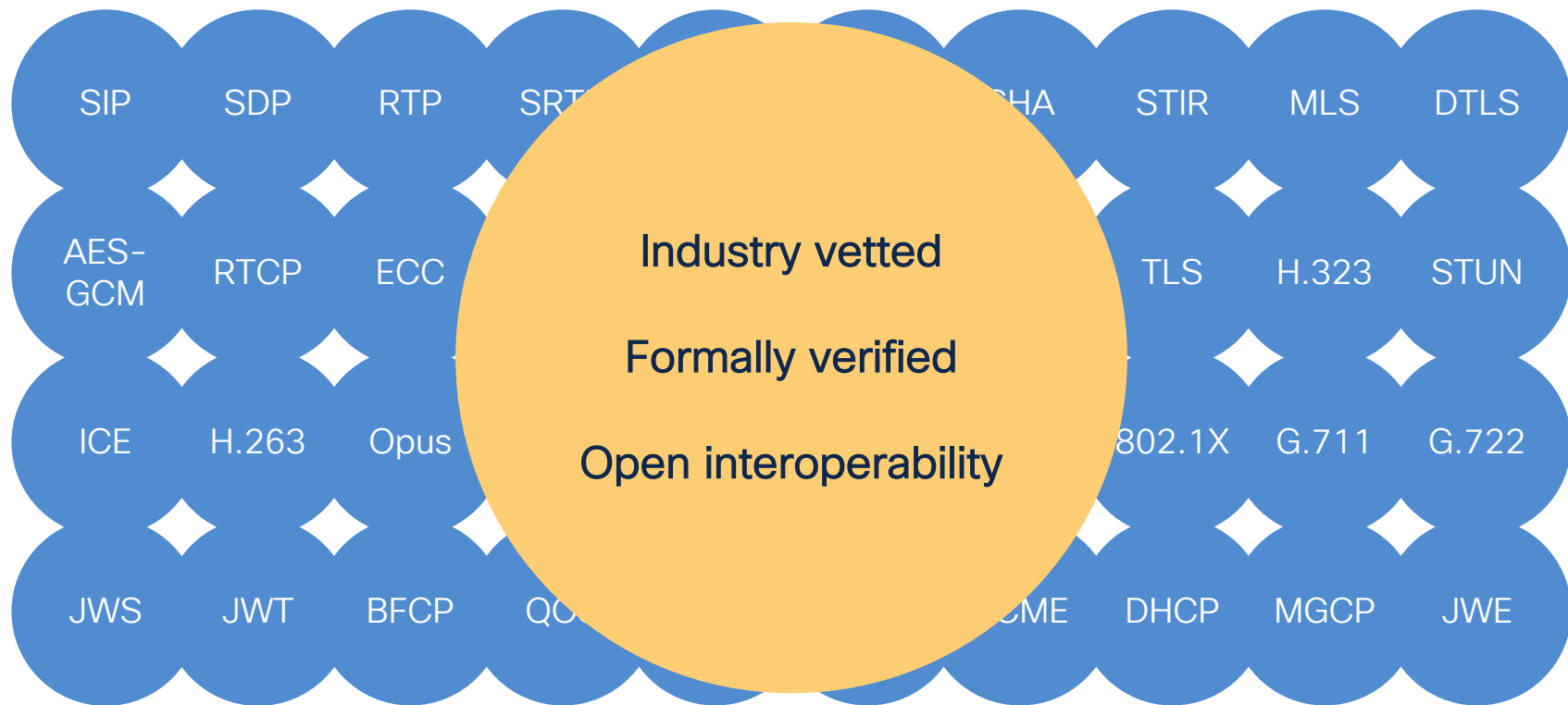


Standards

Identity

Devices

Cisco's engagement in standards-based innovation



New Standards for E2E Encrypted Webex Meetings

Today

Identity

SSO
(SAML, OpenID)

Key Exchange

SDS / DTLS

Media Encryption

SRTP

Open
Source
!

Zero Trust Security adds....

Automated Certificate
Management Environment
(ACME)

Open
Source
!

Messaging Layer Security
(MLS)

Open
Source
!

Secure Frames
(SFrame)

Open
Source
!

New Standards for E2E Encrypted Webex Meetings

Messaging Layer Security (MLS)

Developed as a security layer for E2E encrypting group messaging.

Repurposed for Webex Meetings E2E encryption.

Certificates are used by MLS to identify meeting participants and as part of the MLS E2E encryption key generation process

<https://tools.ietf.org/html/draft-ietf-mls-architecture-05>
<https://tools.ietf.org/html/draft-ietf-mls-protocol-11>

Secure Frames (SFrame)

Secure Media Frames provides an extra layer of authenticated encryption for media.

The media frame is encrypted before being placed into individual SRTP payloads

SFrame uses MLS to provide the encryption keys that each meeting participant needs

<https://tools.ietf.org/html/draft-omara-sframe>
<https://tools.ietf.org/html/draft-barnes-sframe-mls-00>

Automated Certificate Management Environment (ACME)

The ACME protocol is used to generate user and device identity certificates. ACME automatically handles Certificate Signing Requests sent to Certificate Authorities

Device Cert. name validation via public DNS server name check

Username validation via SAML assertion from a federated IdP

<https://tools.ietf.org/html/rfc8555>
<https://tools.ietf.org/html/draft-biggs-acme-sso-00>

Zero Trust Security for Webex Meetings :

Phase One

New End to End Encryption

Early Field Trials today
Roll out starts Q2 CY2021



Webex Meetings E2E Encryption Implementations Feature Comparison

	Webex E2E Encryption (Today)	Webex E2E Encryption with Zero Trust Security
Based on standards track protocols	No	Yes
Encryption key traverses the cloud ?	Yes (Encrypted and sent over TLS)	No – Only meta data sent over TLS
Personal Meeting Rooms	No	Yes
Join Before Host	No	Yes
Lobby	No	Yes
Webex Web app	No	Planned
Video Device support	No (SRTP: Requires Webex key access)	Yes – Webex cloud registered devices
SIP devices	No (SRTP: Requires Webex key access)	No (SRTP: Requires Webex key access)
PSTN	No (SRTP: Requires Webex key access)	No (SRTP: Requires Webex key access)
Network Based Recording	No (SRTP: Requires Webex key access)	No (SRTP: Requires Webex key access)
Transcripts, Speech Recognition	No (SRTP: Requires Webex key access)	No (SRTP: Requires Webex key access)
Live streaming	No (SRTP: Requires Webex key access)	No (SRTP: Requires Webex key access)

End to End Encryption from all meetings service providers share a common limitation in that SRTP based apps and devices cannot be supported – As this gives your provider access to the meeting encryption key

Rolling Out Zero Trust Security based E2E Encrypted Meetings

Requires no administrator or end user changes :

- 1) Cloud registered Webex Room devices will be upgraded to support E2E Encryption
- 2) The Webex app will be upgraded to support both forms of E2E encryption
- 3) Cluster by cluster enablement of Zero Trust E2E Encryption in the Webex cloud
- 4) When the cloud migration is completed, old E2E Encryption will be removed from the Webex app

MLS requires that all apps and devices have identity certificates

In this first phase, with End to End Encryption only, for zero touch roll-out :

The Webex CA will generate and distribute identity certificates to Webex apps and Webex Room devices

MLS for E2E Encrypted Webex Meetings

Messaging Layer Security (MLS)

Developed as a security layer for E2E encrypting group messaging.

Repurposed for Webex Meetings E2E encryption.

Identity Certificates are used by MLS (in MLS key packages) to identify meeting participants and as part of the MLS E2E encryption key generation process

<https://tools.ietf.org/html/draft-ietf-mls-architecture-05>
<https://tools.ietf.org/html/draft-ietf-mls-protocol-11>

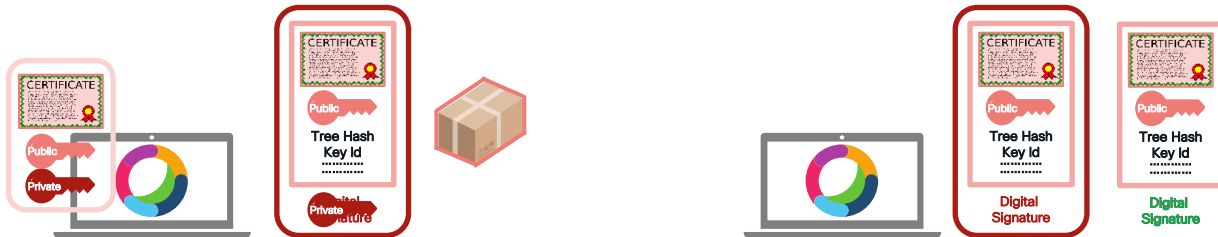


MLS uses “key packages” to identify users and to generate new meeting encryption keys as participants join and leave the meeting

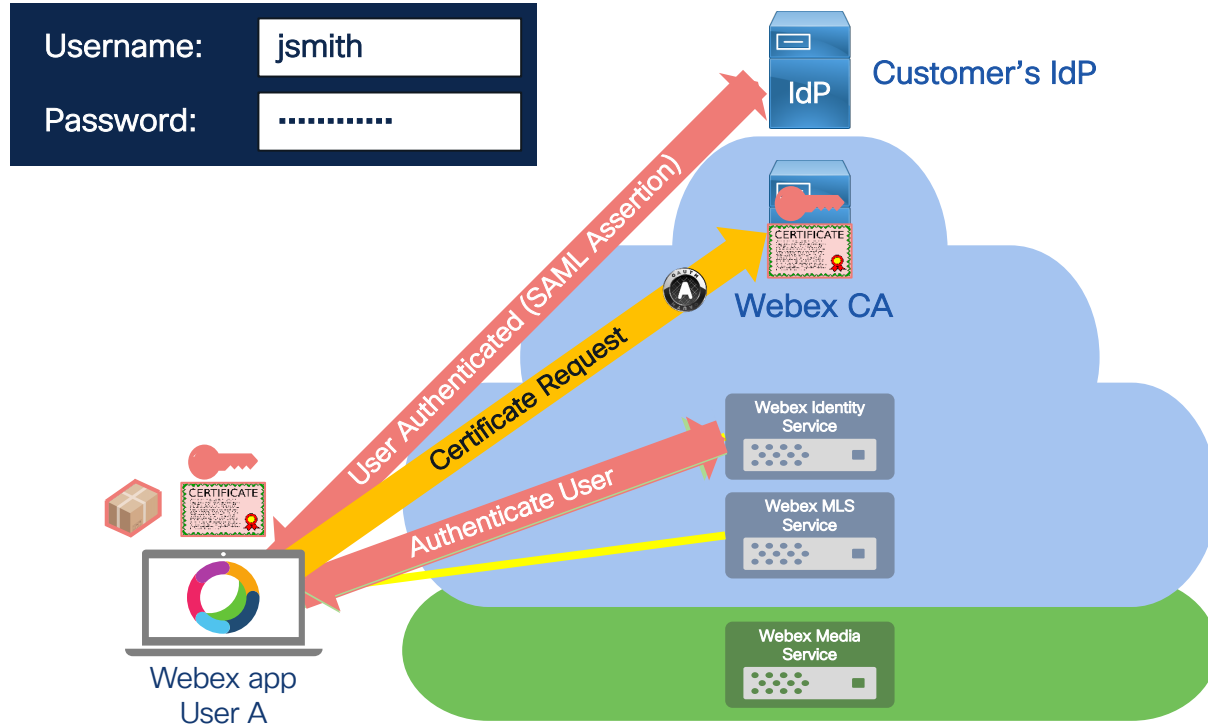
Each MLS key package contains :

- The meeting participant’s Identity Certificate
- A tree hash value that represents the cryptographic group state and credentials of the group members (meeting participants)
- An identifier for the current version of the meeting encryption key

Each meeting participant signs their key package with their private key, so that other meeting participants can verify its authenticity



SSO Users - Signing In with their Enterprise IdP : Webex CA Identity certificates



Users who have Not Signed In : Webex CA Identity Certificates :

Join a meeting

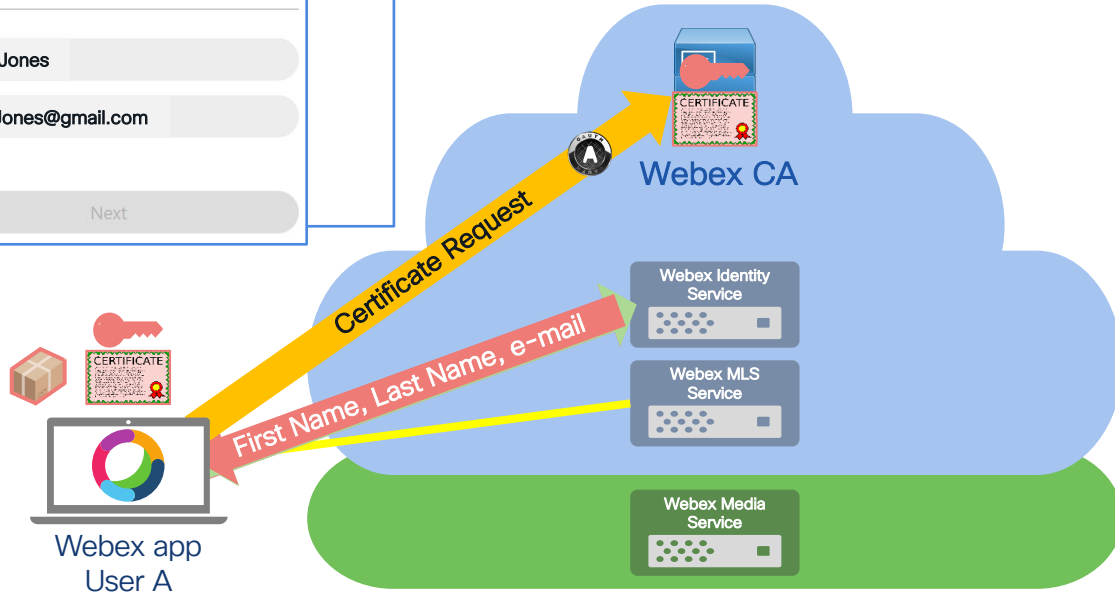
Meeting number, link, or video address

1234567890@webex.com

Bob Jones

Bob.Jones@gmail.com

Next

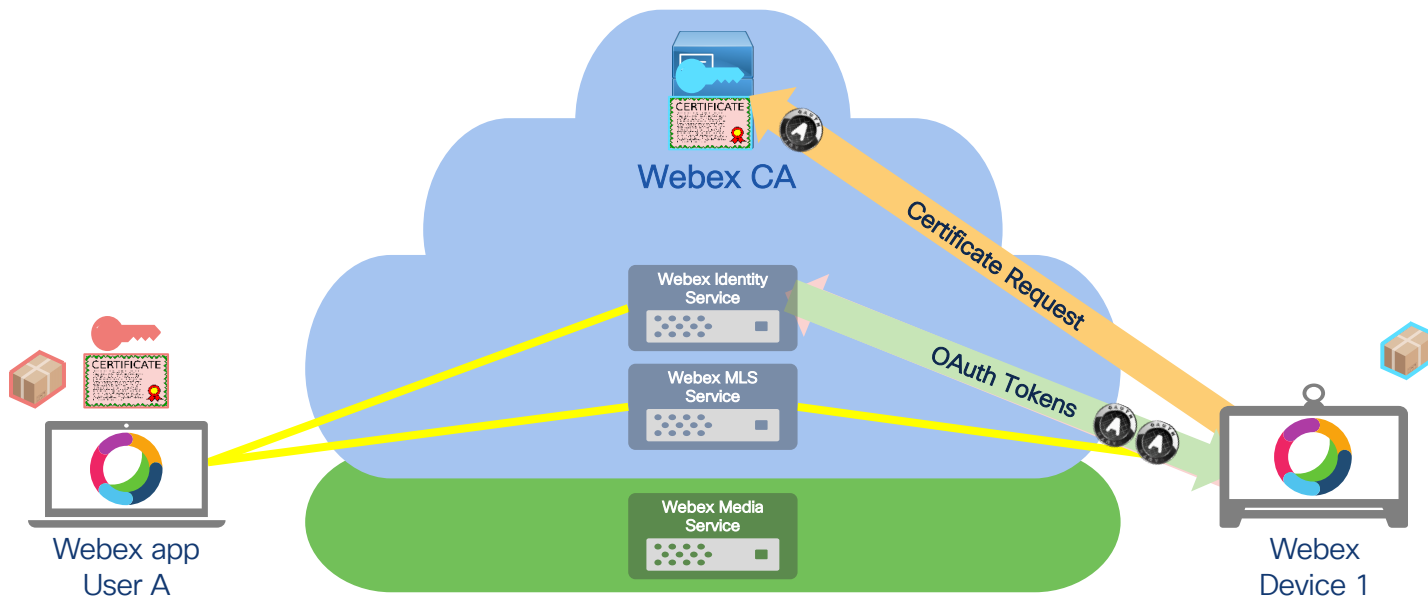


Users who have Not Signed In are assigned a temporary UUID and OAuth access token

Users who have Not Signed In are listed as **Unverified** in the Meeting Lobby and Roster List

Meeting Host has Admit/Eject controls

Webex cloud registered Devices (Machine account authentication with Webex Identity service) Webex CA Identity certificates



Zero Trust Security for
Webex Meetings

End to End Encryption
New User Experience

CISCO *Live!*



Zero Trust Security for Webex Meetings

New Meeting Security icons : Encrypted/ E2E Encrypted



Encrypted Meeting :

Webex app, Webex Room devices, SIP devices, PSTN
Network based : Recording, Transcription, Speech
Recognition, Closed Captions, Webex Assistant etc



End to End Encrypted Meeting :

Webex app, Cloud registered Webex Room devices only
No SIP devices or PSTN users
No Network Services

Zero Trust Security for Webex Meetings

E2E Encrypted Meeting Roster List – New User Details

The screenshot displays a Webex meeting interface. On the left, a 3x2 grid shows six participants: Barbara German (Host), Giacomo Drago, Brandon Seeger, Brenda Song, Maria Rossi, and Simon Jones. On the right, a 'Participants (6)' list shows the same individuals with their email addresses and authentication status. Three callouts provide detailed authentication information:

- Barbara.German@ibm.com is SSO authenticated**
Barbara German
Host, me | company.com
Identity verified by Webex CA
[Show certificate](#)
- Giacomo.Drago@example.com is Webex Identity authenticated**
Giacomo Drago
example.com
Identity verified by Webex CA
[Show certificate](#)
- Brandon.Seeger@acme.com is an unauthenticated user**
Brandon Seeger
Unverified
Identity not verified
[Show certificate](#)

The bottom of the interface shows a Windows taskbar with the search bar, system icons, and the time 02:12 PM on 15/07/2020.

Zero Trust Security Webex Meetings

E2E Encrypted Meeting Lobby – New User Details

The screenshot displays the Webex Meeting Lobby interface. At the top, there's a navigation bar with 'Webex', 'Meeting Info', and 'Show menu bar'. The main area shows a grid of six video thumbnails of participants. A 'Waiting in Lobby (6)' panel is overlaid on the right side of the grid, listing participants from 'My Organization' and 'Guests'. The 'Participants' panel on the far right shows a list of six participants with their names, roles, and status icons. The bottom of the interface features a control bar with 'Mute', 'Share', and other icons. The Windows taskbar is visible at the very bottom.

Waiting in Lobby (6)

- ☐ My Organization
 - ☐ Flora Boone (company.com)
 - ☐ Angela Estrada (company.com)
 - ☐ Travis Jimenez (company.com)
 - ☐ Bessie Cooper (company.com)
- ☒ Guests
 - ☒ CF Cody Fisher (tmedemo.com)
 - ☒ AB Annette Black (Unverified)

Participants (6)

6 people are waiting in the lobby

- Barbara German (Host, me! company.com)
- Brandon Seeger (Unverified)
- Brenda Song (company.com)
- Giacomo Drago (example.com)
- Maria Rossi (company.com)
- Simon Jones (company.com)

Meeting Controls: Mute, Share, Video, Audio, Chat, Participants

Zero Trust Security for Webex Meetings

E2E Encrypted Meeting Security Information

The screenshot displays a Webex meeting window with a sidebar on the left containing security details. The main area shows a grid of four participants. The bottom of the window features a control bar with icons for Mute, Stop video, Share, and other functions. The Windows taskbar is visible at the very bottom.

Webex Meeting Info

Intelligence, Security & Analytics - Monthly Product Briefing

Host: Barbara German

Copy meeting link Invite and remind

General Security

You are securely and confidentially connected to this meeting with strong end-to-end encryption.

Security code ⓘ Copy

KKH 7CV MGV QTC 37J

Server connection
TLS with ECDH and AES-256-GCM

Media connection
AES-256-GCM

End-to-end encrypted connections
Audio: Yes
Video: Yes
Desktop and application sharing: Yes

SHN7-16-GREAT WALL

Mute Stop video Share Participants Chat

02:12 PM 15/07/2020

Zero Trust Security for Webex Meetings

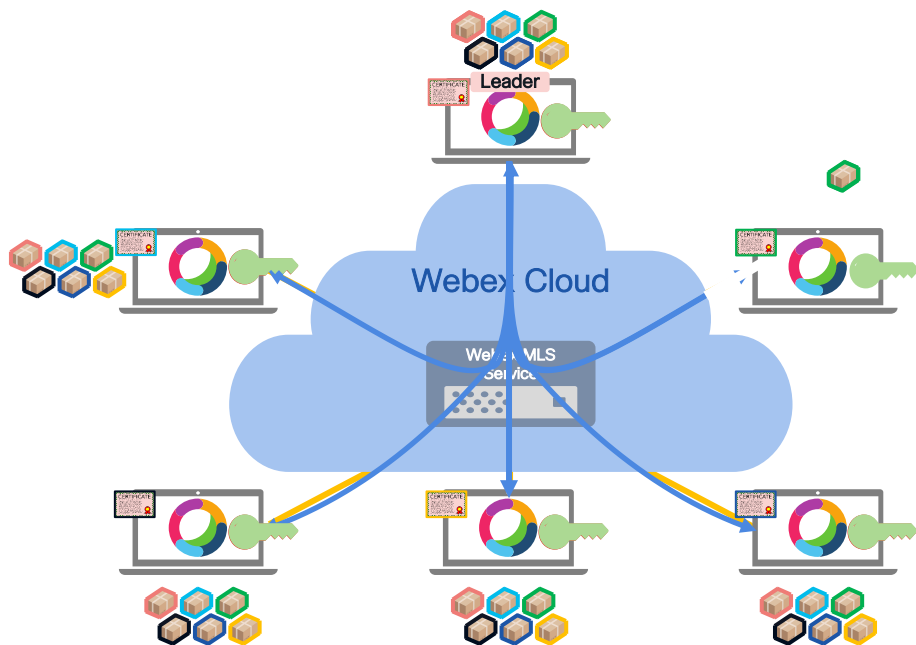
MLS and SFrame details



MLS Operation : Meeting Participant Join



MLS key package : contains the participant's certificate and other meta data used for identity verification and meeting encryption key generation.



New meeting participants send their key package to the meeting leader (In MLS, the leader does not need to be the Meeting Host)

The meeting leader shares the new participant's key package with the other participants.

The meeting leader shares the existing meeting participants' key packages with the new participant.

All meeting participants generate a new meeting encryption key
(MLS uses timers to reduce key churn when large numbers of participants join the meeting in a short time interval)

A new meeting encryption key is created when participants join or leave the meeting

SFrame for E2E Encrypted Webex Meetings

Secure Frames (SFrame)

Secure Media Frames provides an extra layer of authenticated encryption for media.

The whole media frame is encrypted before being placed into individual SRTP payloads

SFrame uses MLS to provide the encryption keys that each meeting participant needs

<https://tools.ietf.org/html/draft-omara-sframe>

<https://tools.ietf.org/html/draft-barnes-sframe-mls-00>

Double Encryption process

- 1) Unencrypted media frame
- 2) Packetize unencrypted media frame
- 3) Encrypt packets using SFrame E2E Meeting Encryption key
- 4) Encrypted SFrame packets -> Encrypted with SRTP keys
- 5) Media meta data moved to SRTP header extension (authenticated)

SFrame encryption cipher AES-256-GCM

Encrypted SFrame format :

SFrame header – Frame counter (used for encryption IV) – Key Id

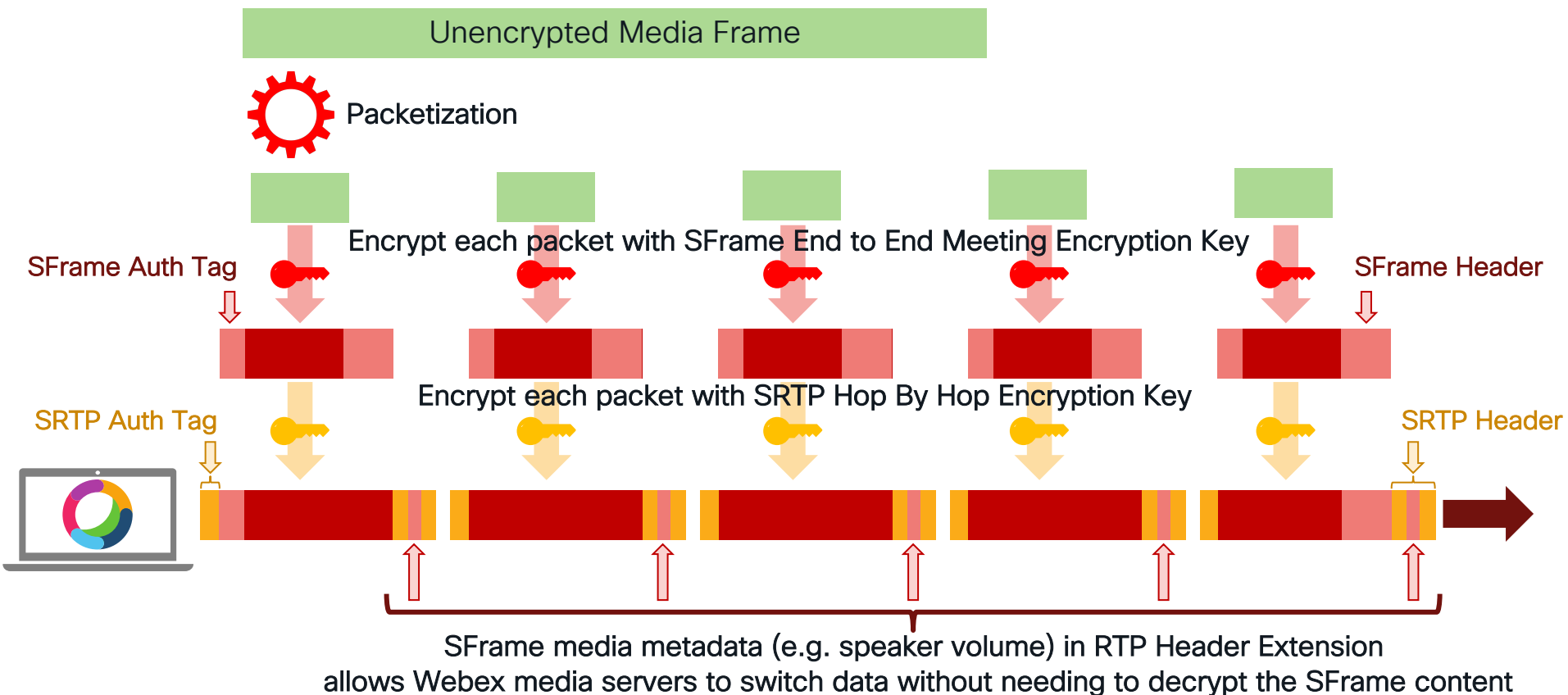
SFrame Encrypted Media

SFrame authentication tag

Authenticated SRTP header extension

Speaker volume indication (used by Webex media servers to switch media without decrypting SFrame content)

Secure Frames (SFrame)



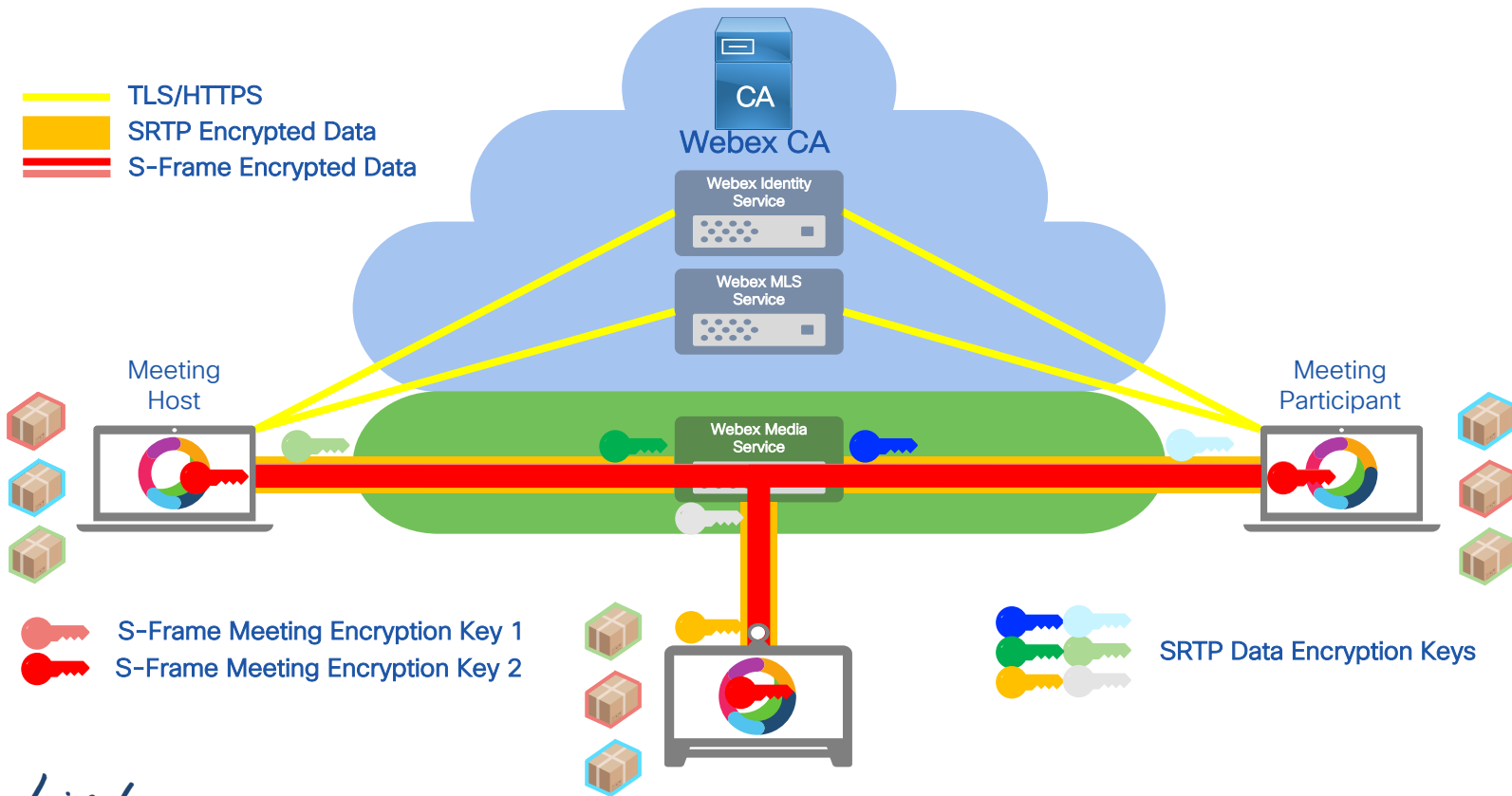
Zero Trust Security for Webex Meetings

Combined MLS and
SFrame operation



Zero Trust Security for Webex Meetings – E2E Encryption

MLS and SFrame operation



Zero Trust Security for Webex Meetings

New End to End Encryption
Meeting Security Codes



Zero Trust Security for Webex Meetings

E2E Encrypted Meetings – Meeting Security Code

The screenshot displays a Webex meeting window. On the left, a sidebar contains meeting information. The title is "Intelligence, Security & Analytics - Monthly Product Briefing" with host "Barbara German". Buttons for "Copy meeting link" and "Invite and remind" are present. The "Security" tab is selected, showing a confirmation: "You are securely and confidentially connected to this meeting with strong end-to-end encryption." Below this, the "Security code" is highlighted with a red box and includes a "Copy" link. The code is displayed as five individual tiles: KKH, 7CV, MG, V, QTC, and 37J. Further down, connection details are listed: "Server connection: TLS with ECDH and AES-256-GCM", "Media connection: AES-256-GCM", and "End-to-end encrypted connections: Audio: Yes, Video: Yes, Desktop and application sharing: Yes". The bottom of the sidebar shows a meeting ID: SHN7-16-GREAT WALL. The main area shows four video thumbnails of participants. At the bottom, a control bar includes buttons for "Mute", "Stop video", "Share", and icons for "Participants", "Chat", and a red "X" button. The Windows taskbar is visible at the very bottom with the search bar and system clock showing 02:12 PM on 15/07/2020.

Webex Meeting Info Show menu bar

Intelligence, Security & Analytics - Monthly Product Briefing

Host: Barbara German

Copy meeting link Invite and remind

General Security

You are securely and confidentially connected to this meeting with strong end-to-end encryption.

Security code ⓘ Copy

KKH 7CV MG V QTC 37J

Server connection
TLS with ECDH and AES-256-GCM

Media connection
AES-256-GCM

End-to-end encrypted connections
Audio: Yes
Video: Yes
Desktop and application sharing: Yes


SHN7-16-GREAT WALL

Mute Stop video Share Participants Chat

Type here to search 02:12 PM 15/07/2020

Meeting Security Codes – Protecting against MITM attacks

Intelligence, Security & Analytics -
Monthly Product Briefing

 Host: Barbara German

Copy meeting link

Invite and remind

General

Security

You are securely and confidentially connected to this meeting with strong end-to-end encryption.

Security code ⓘ

Copy

KKH

7CV

MGV

QTC

37J

Server connection

TLS with ECDH and AES-256-GCM

Media connection

AES-256-GCM

End-to-end encrypted connections

Audio: Yes

Video: Yes

Desktop and application sharing: Yes

Other (chat, file uploads, whiteboard, etc.): Yes

The meeting security code is displayed to all meeting participants. If they all have the same value, then they know they have not been intercepted and impersonated by an attacker (Meddler In The Middle (MITM) attack)

The Webex E2E Encrypted Meeting Security code is derived from all participants' MLS key packages

If participants have the same code, they know they agree on all aspects of the group, including the group's secrets and the current participant list.

This value changes every time the group key changes, which is at least on every join/leave.

Meeting Security Codes – Protecting against MITM attacks

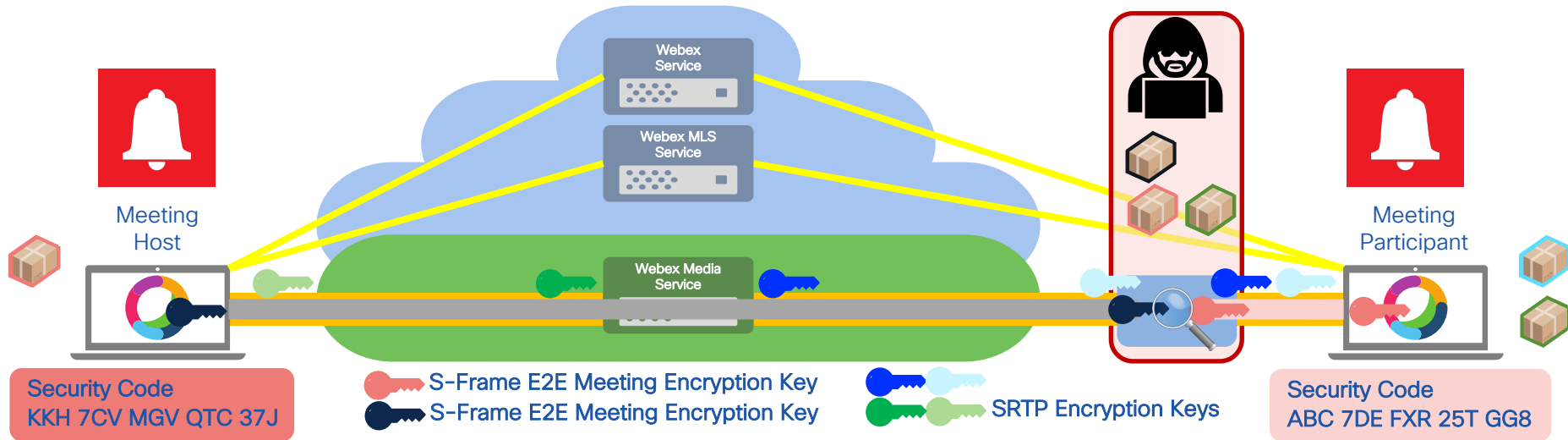
What a MITM attacker needs access to :

Your encrypted media – SRTP encryption keys, all MLS E2E Meeting Encryption keys

Your TLS connections to Webex, including the MLS service and all MLS key packages

To impersonate you – At a minimum, a MITM attacker needs to :

Intercept all MLS key packages and replace them with their own



The Security Codes generated by each Webex app using their MLS key packages should match

Zero Trust Security for Webex Meetings

New End to End Identity

Early Field Trials Q2 CY2021
Roll out starts Q3 CY2021

cisco *Live!*



ACME for E2E Identity with Webex Meetings

Automated Certificate Management Environment (ACME)

The ACME protocol is used to generate user and device identity certificates. ACME automatically handles Certificate Signing Requests sent to Certificate Authorities

Device certificate name validation via public domain name check

User CSR validation via SAML assertion from a federated IdP

<https://tools.ietf.org/html/rfc8555>
<https://tools.ietf.org/html/draft-biggs-acme-sso-00>

ACME is protocol that can be used by a Certificate Authority and a Certificate applicant to automate the process of identity verification and certificate issuance...

RFC 8555

Describes an automated validation procedure that allows domain-name based certificates (e.g. device1.cisco.com) to be obtained without user intervention.

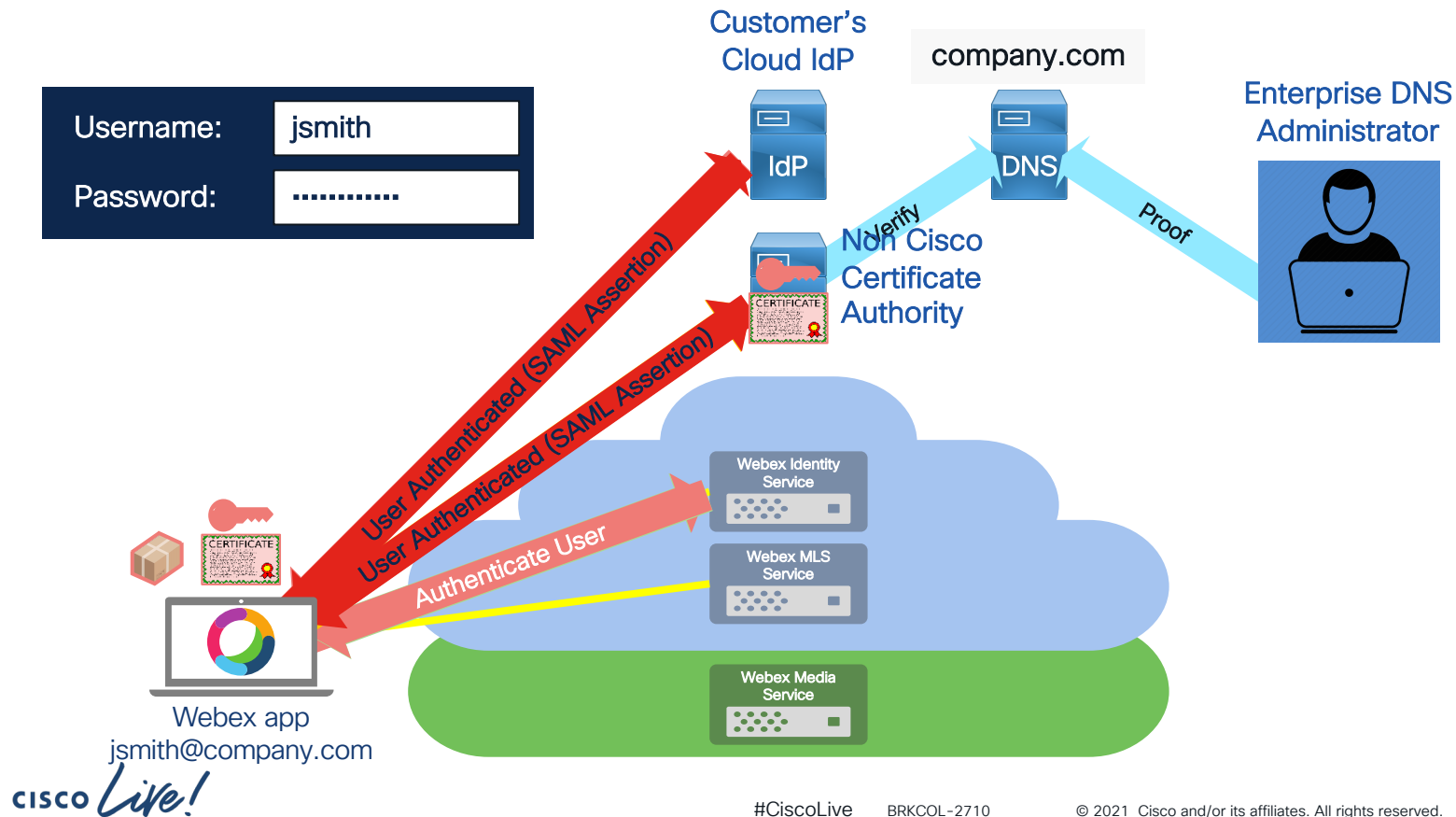
Draft-biggs-acme-sso

Extends the ACME protocol to enable the ACME service to validate a client's control of an email identifier (e.g. bob@cisco.com) using single sign-on (SSO) technologies

New – Webex End to End Identity Verification

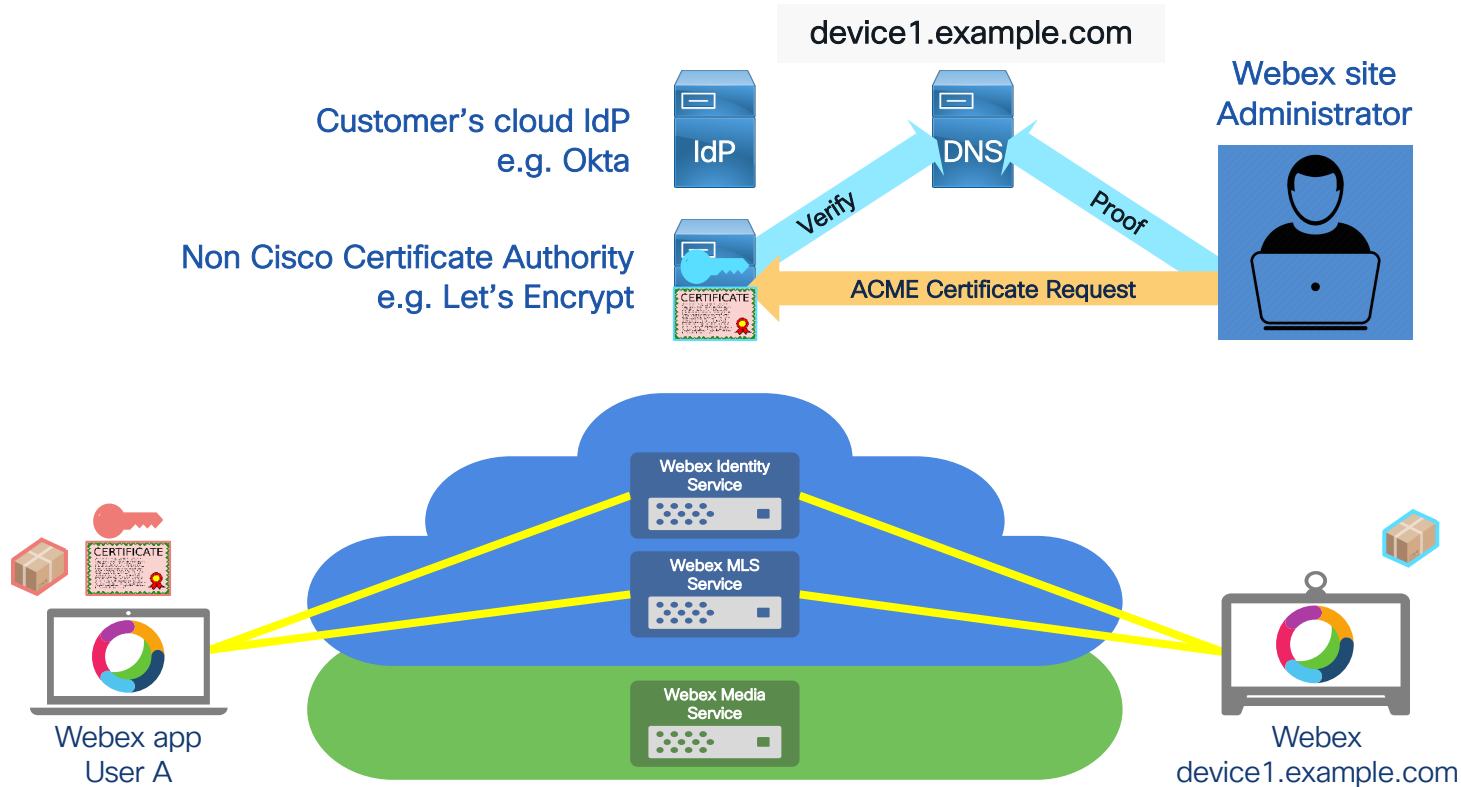
SSO Users authenticating with their Enterprise IdP

Using ACME to request a signed User Identity certificate from a non Cisco CA



New – Webex End to End Identity Verification

Webex device using ACME to request a signed Device Identity Certificate from a non Cisco CA



Zero Trust Security for Webex Meetings : Phase 2

Webex E2E Identity

Meeting Roster - New User Details

Webex Meeting Info Show menu bar

Layout

Participants (6)

- Barbara German (Host, me) company.com
- Brandon Seeger (Unverified)
- Brenda Song company.com
- Giacomo Drago (example.com)
- Maria Rossi company.com
- Simon Jones company.com

Identity verified by Let's Encrypt Show certificate

Barbara.German@ibm.com is SSO authenticated

Barbara German
Host, me | company.com

Identity verified by Let's Encrypt
[Show certificate](#)

Giacomo.Drago@example.com is Webex Identity authenticated

Giacomo Drago
example.com

Identity verified by Webex CA
[Show certificate](#)

Brandon.Seeger@acme.com is an unauthenticated user

Brandon Seeger
Unverified

Identity not verified
[Show certificate](#)

Zero Trust Security for Webex Meetings: Phase 2

Webex E2E Identity

Meeting Lobby – New User Details

The screenshot displays the Webex Meeting Lobby interface. At the top, there's a header with 'Webex', 'Meeting Info', and 'Show menu bar'. The main area shows a grid of six video thumbnails. A 'Waiting in Lobby (6)' overlay is present, listing participants under 'My Organization' and 'Guests'. The 'My Organization' list includes Flora Boone, Angela Estrada, Travis Jimenez, and Bessie Cooper. The 'Guests' list includes Cody Fisher, AB, and Annette Black. An 'Admit' button is at the bottom of the overlay. To the right, a 'Participants (6)' panel shows a search bar and a list of participants with their names, roles, and status (e.g., Host, Unverified). At the bottom of the lobby, there are controls for Mute, Share, and a red 'X' button. The Windows taskbar is visible at the very bottom, showing the search bar and system clock (02:12 PM, 15/07/2020).

Webex Meeting Info Show menu bar

Waiting in Lobby (6)

My Organization

- Flora Boone company.com
- Angela Estrada company.com
- Travis Jimenez company.com
- Bessie Cooper company.com

Guests

- Cody Fisher tmedemo.com
- AB
- Annette Black Unverified

Admit

Participants (6)

6 people are waiting in the lobby

Search

- Barbara German Host, me 1 company.com
- Brandon Seeger Unverified
- Brenda Song company.com
- Giacomo Drago example.com
- Maria Rossi company.com
- Simon Jones company.com

Mute Share ... X

Participants Chat ...

Type here to search

02:12 PM 15/07/2020

Summary and Roadmap



Zero Trust Security for Webex Meetings Summary and Roadmap

Phase 1

- Standards based Crypto
- New E2E Encryption
- Webex app + Devices
- Free to all customers

EFT Today
Roll-Out Q2 CY2021

Phase 2

- ACME based Cert Request
- E2E Verified Identity
- Webex app + Devices
- Customer IdP and CA

EFT Q2 CY2021
Roll-Out Q3 CY2021

Open
Ecosystem

Decentralized
Identity

Zero Trust
Security
Everywhere

Online Documents : Webex Meetings Security



Webex Meetings Security – Documentation

Zero Trust Security for Webex White Paper

<https://www.cisco.com/c/en/us/solutions/collateral/collaboration/white-paper-c11-744553.html>

Webex Meetings Security White Paper

<https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.html>

Webex app – Security White Paper

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/esp/Cisco-Webex-Apps-Security-White-Paper.pdf

Webex Rooms – Security White Paper

<https://www.cisco.com/c/dam/en/us/td/docs/telepresence/endpoint/webex/webex-rooms-security-white-paper.pdf>

Webex Meetings Privacy Data Sheet

<https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/collaboration/cisco-webex-meetings-privacy-data-sheet.pdf>

Network Requirements for Webex Services

<https://collaborationhelp.cisco.com/article/WBX000028782>

How End to End Encryption works

<https://help.webex.com/en-us/WBX44739/What-Does-End-to-End-Encryption-Do>



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLive





TURN IT UP

CISCO *Live!*

#CiscoLive