CISCO
Collaboration

The bridge to possible

Securing Webex Meetings with Zero Trust Security

Tony Mulchrone
Senior Technical Marketing Engineer
Cisco Collaboration Technology Group

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

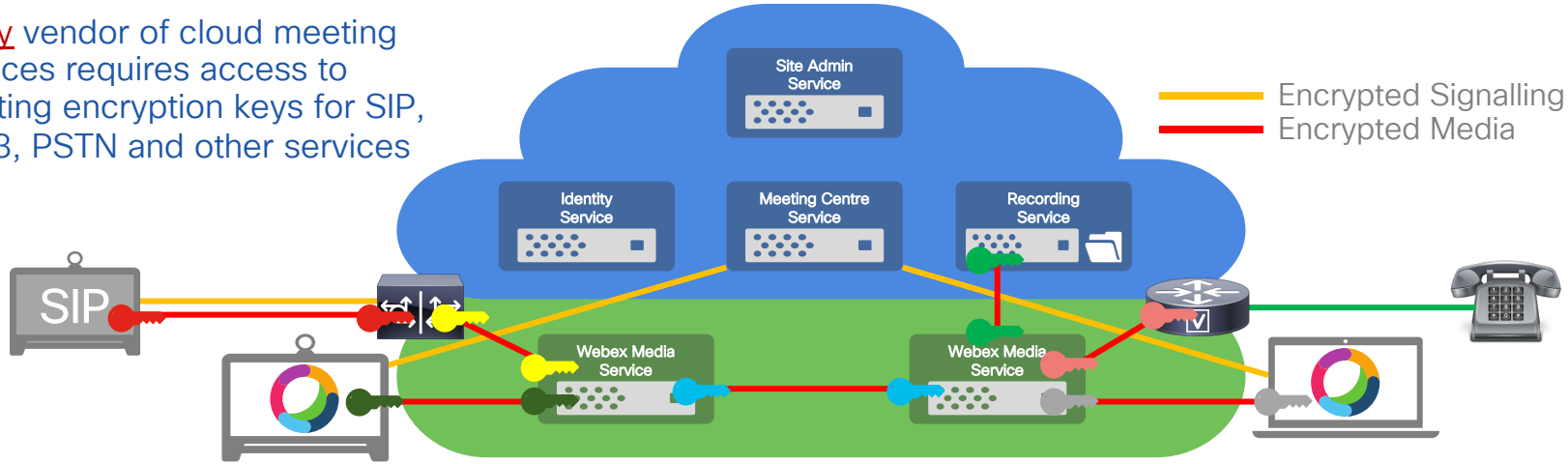
- Standard Encrypted Meetings
- E2E Encrypted Meetings

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

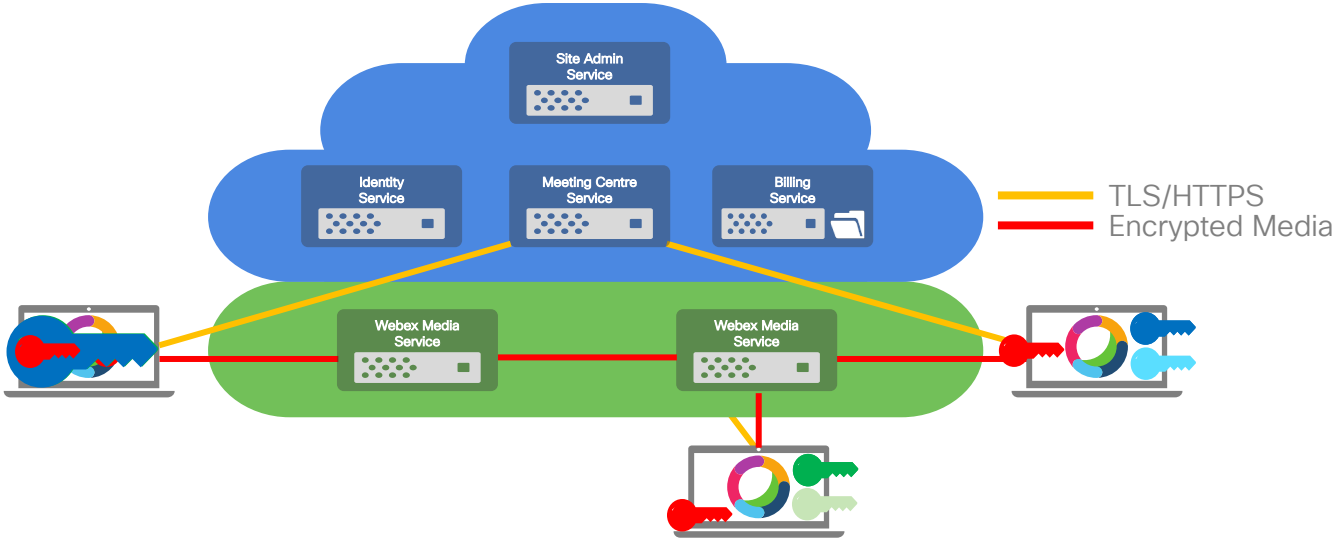


Confidential End-to-End Encrypted Webex Meetings

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

Zero Trust Security for Webex Meetings

New
End to End Encryption & End to End Identity

Early Field Trials today
Roll out starts Q2 CY2021

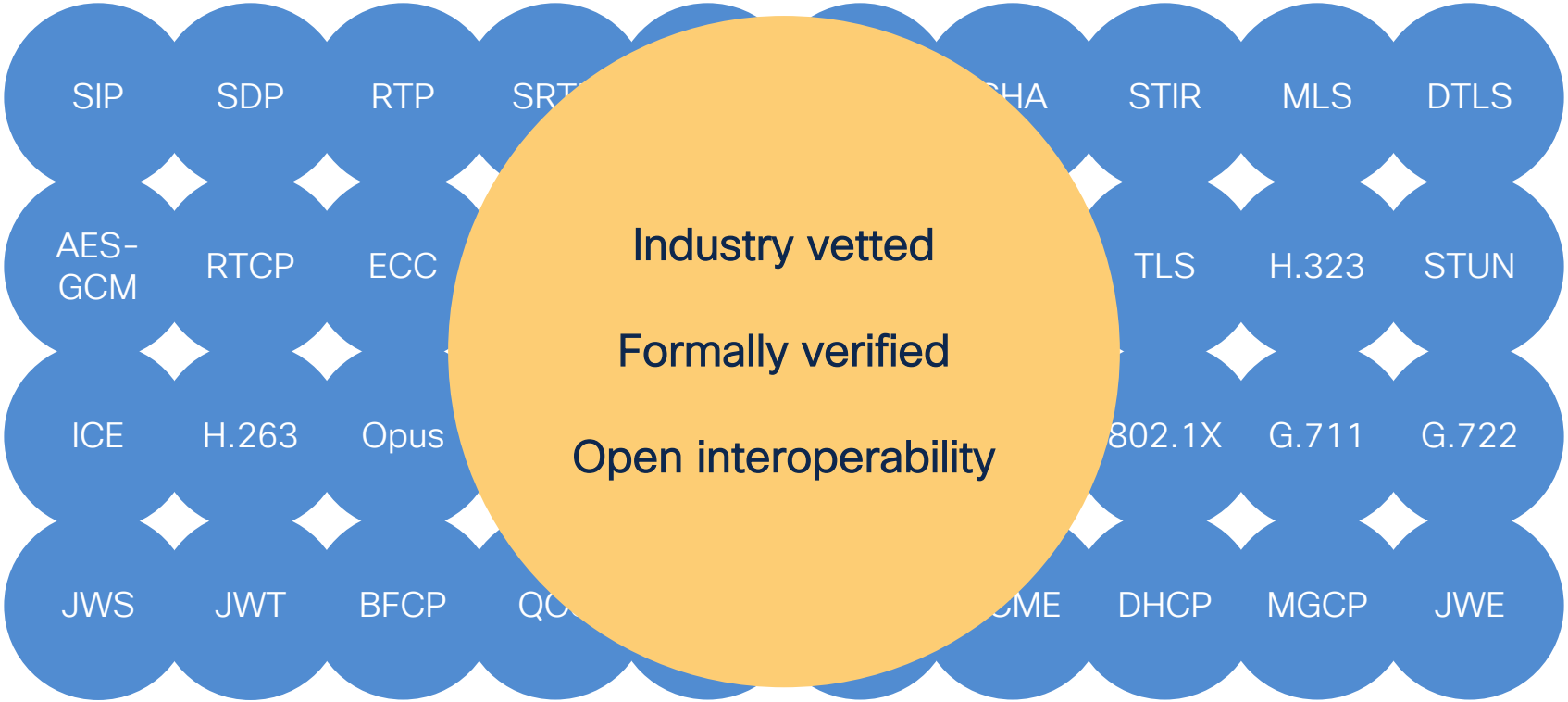
Zero-Trust Security : Strengthening and extending E2E Encryption for Webex Meetings

Standards

Identity

Devices

Cisco's engagement in standards-based innovation



New Standards for E2E Encrypted Webex Meetings

	Today	Zero Trust Security adds....
Identity	SSO (SAML, OpenID)	Automated Certificate Management Environment (ACME) — Open Source !
Key Exchange	SDES / DTLS	Messaging Layer Security (MLS) — Open Source !
Media Encryption	SRTP — 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

New
End to End Encryption

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
Break Out Rooms	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.

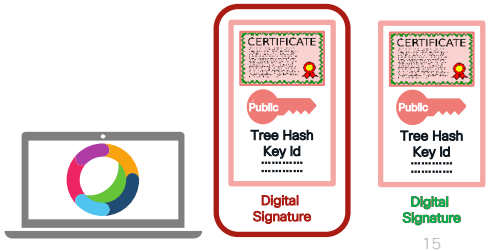
Identity Certificates are used by MLS (in MLS key packages) to identify meeting participants and as part of the MLS E2E encryption key generation process
https://tools.ietf.org/html/draft-ietf-mls-architecture-05
https://tools.ietf.org/html/draft-ietf-mls-protocol-11

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

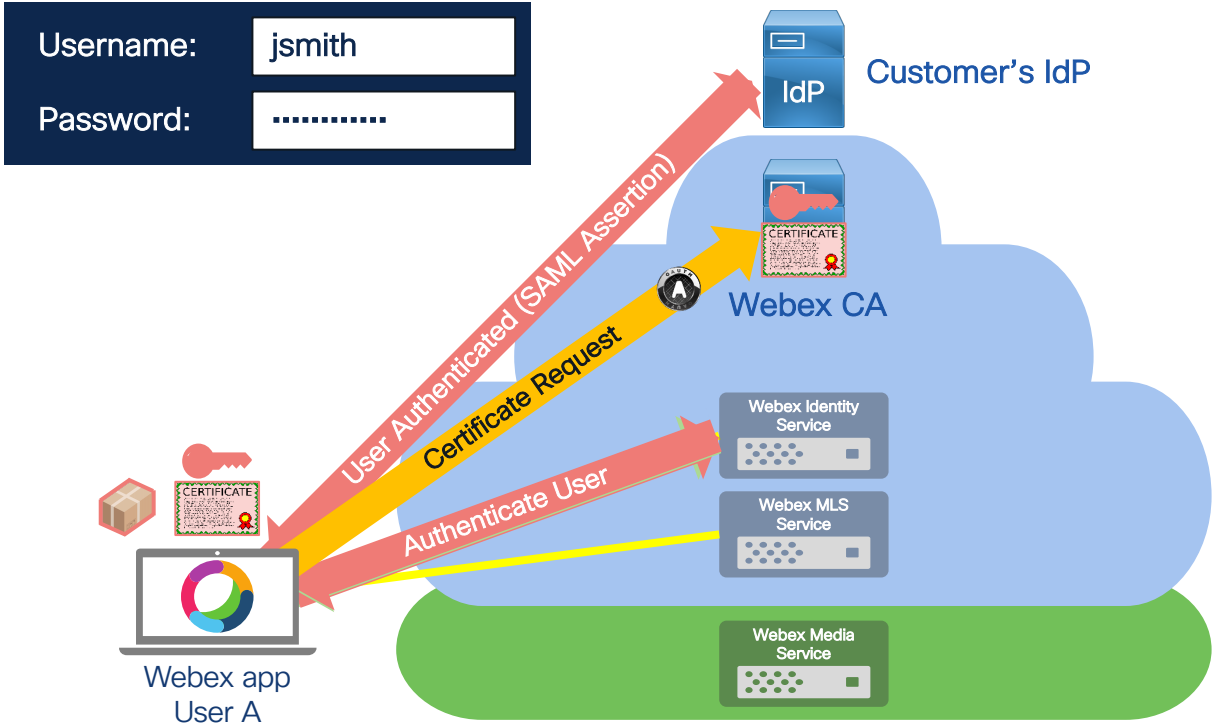
Each MLS key package contains :

- 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

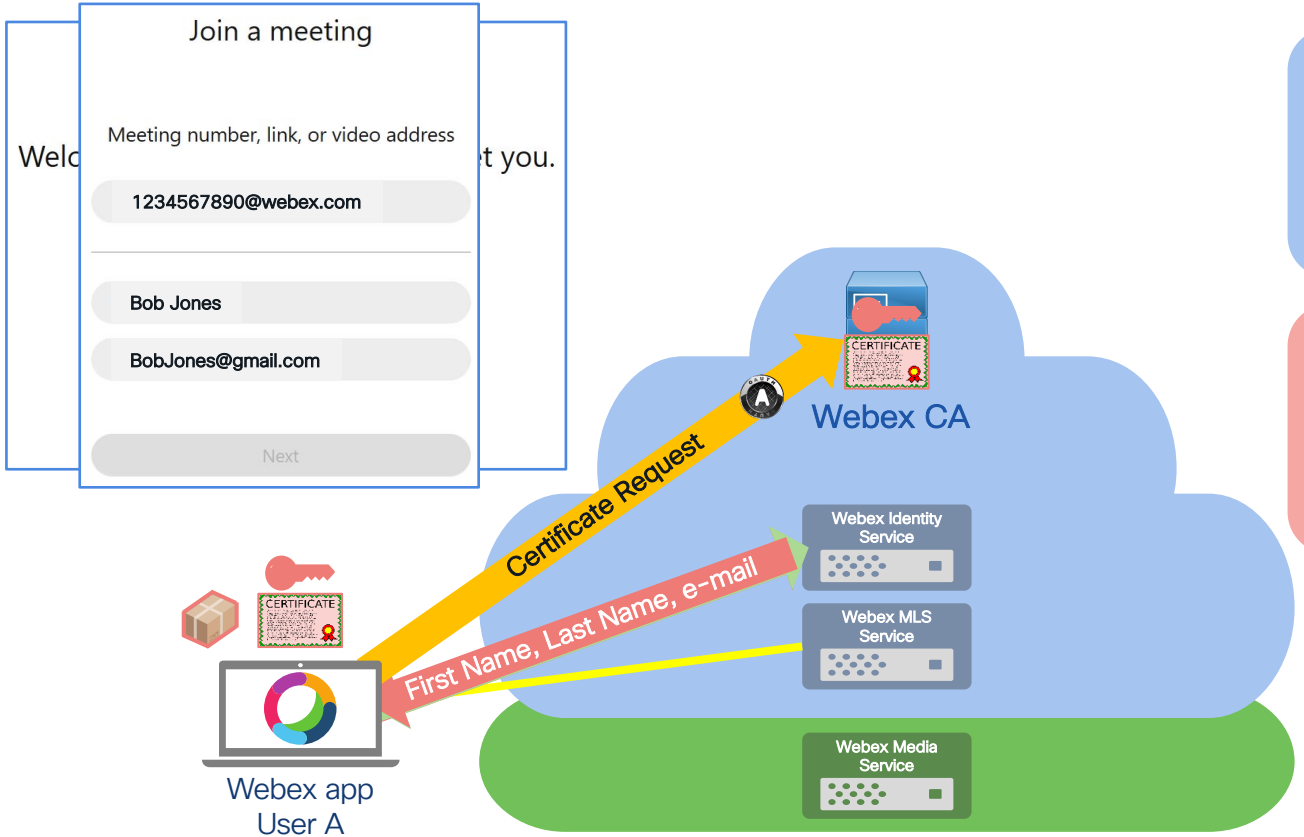
Each meeting participant signs their key package with their private key, so that other meeting participants can verify its authenticity



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



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



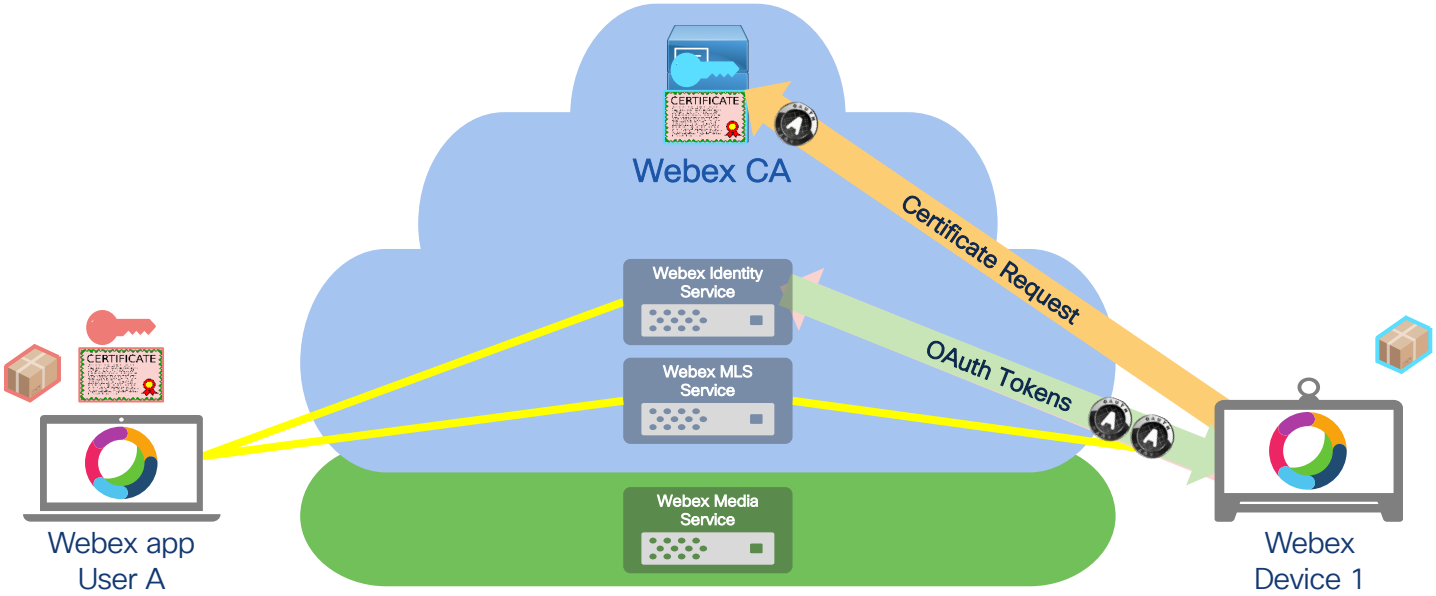
Users who have Not Signed In are assigned a temporary UUID and OAuth access token

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

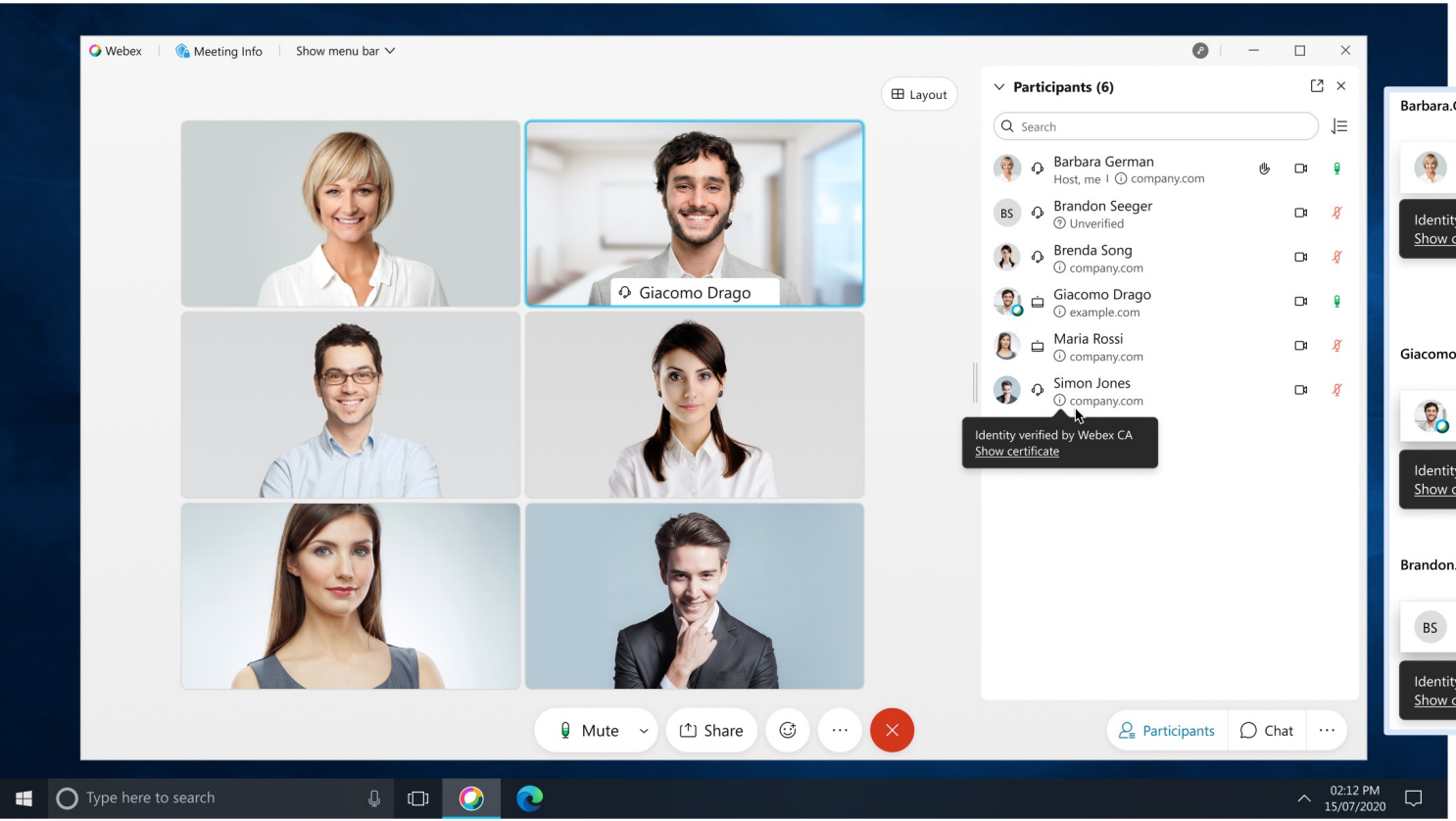
New
End to End Encryption
User Experience

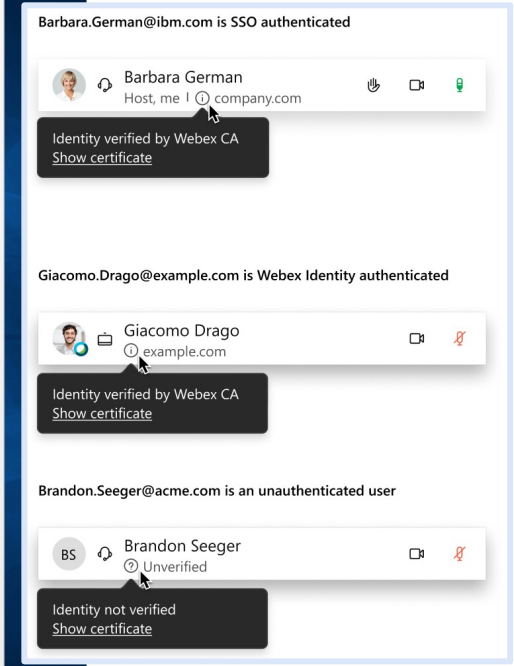
Zero Trust Security for Webex Meetings
New Meeting Security icons : Encrypted/ E2E Encrypted

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

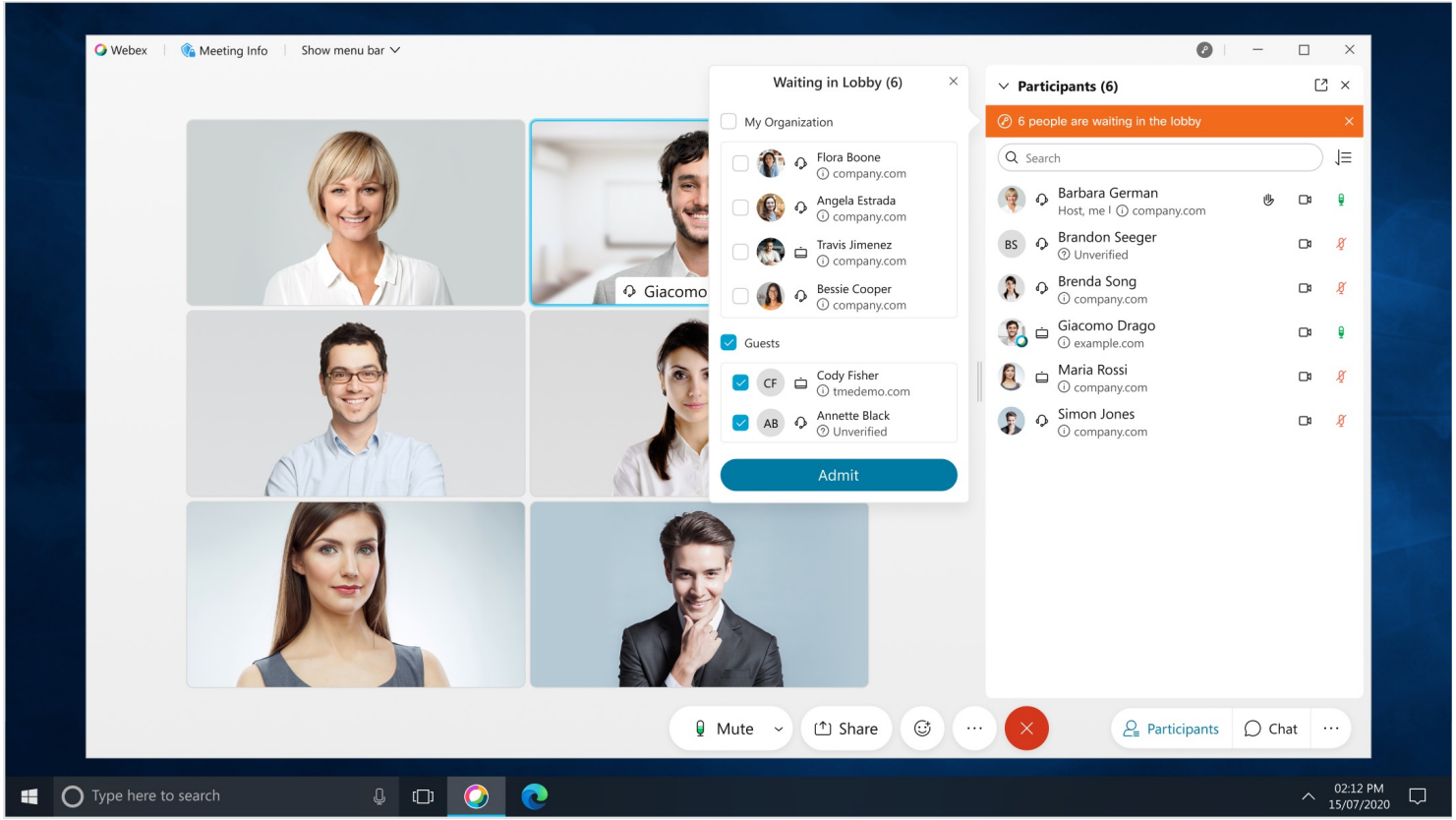
End to End Encrypted Meeting :
Webex app, Cloud registered Webex Room devices only
No SIP devices or PSTN users
No Network Services

Zero Trust Security for Webex Meetings
E2E Encrypted Meeting Roster List – New User Details





Zero Trust Security Webex Meetings
E2E Encrypted Meeting Lobby – New User Details



Zero Trust Security for Webex Meetings
E2E Encrypted Meeting Security Information

Webex | Meeting Info | Show menu bar

Layout

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

Type here to search

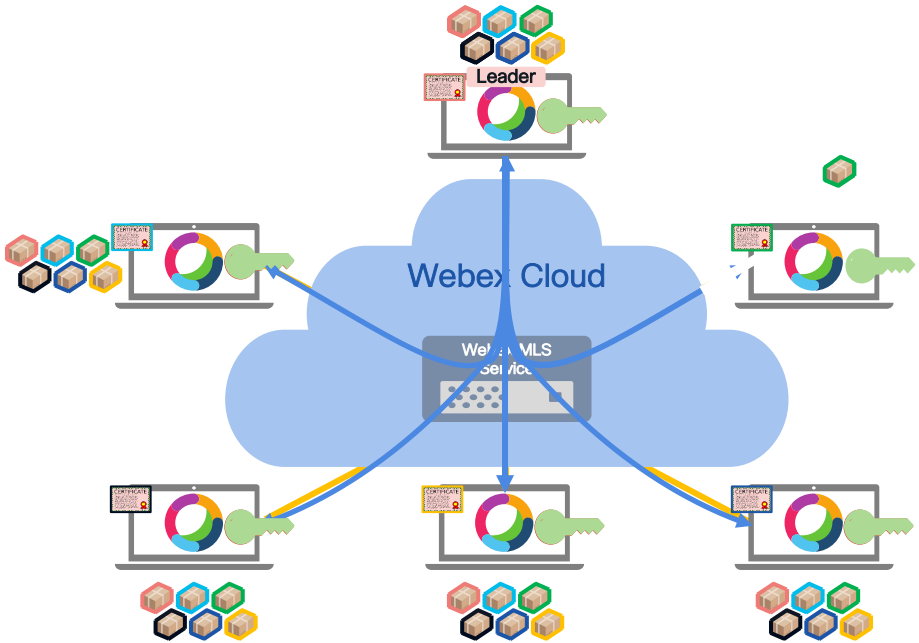
02:12 PM
15/07/2020

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

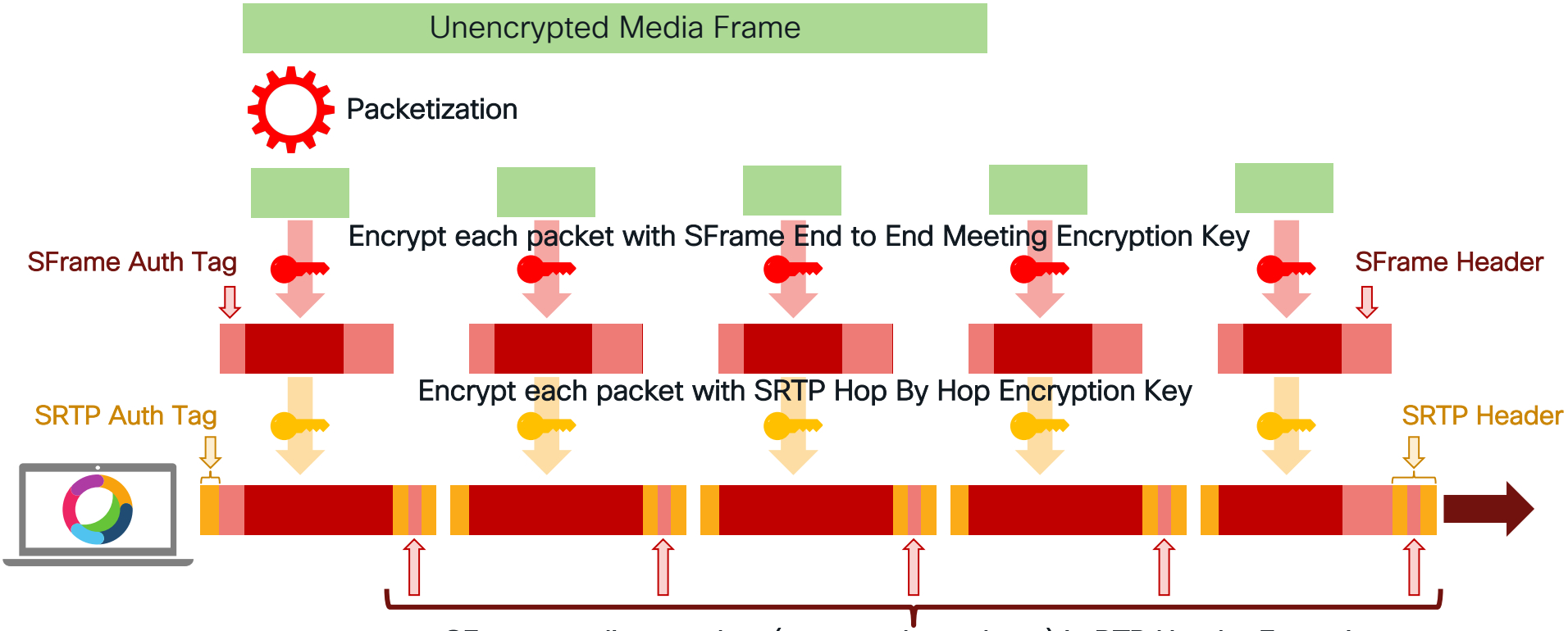
Encrypted SFrame format :

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)

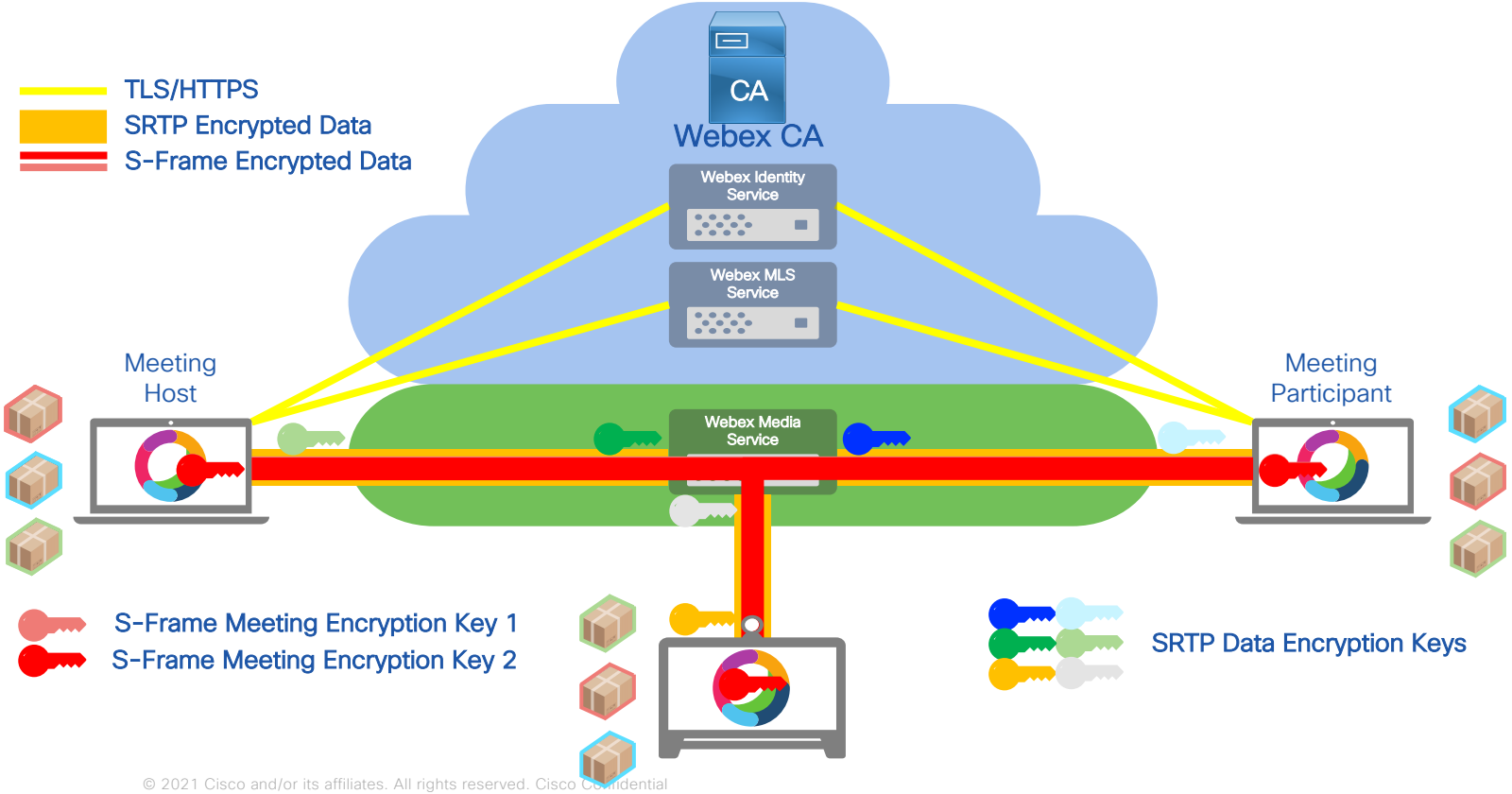


SFrame media metadata (e.g. speaker volume) in RTP Header Extension allows Webex media servers to switch data without needing to decrypt the SFrame content

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

Webex | Meeting Info | Show menu bar

Layout

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

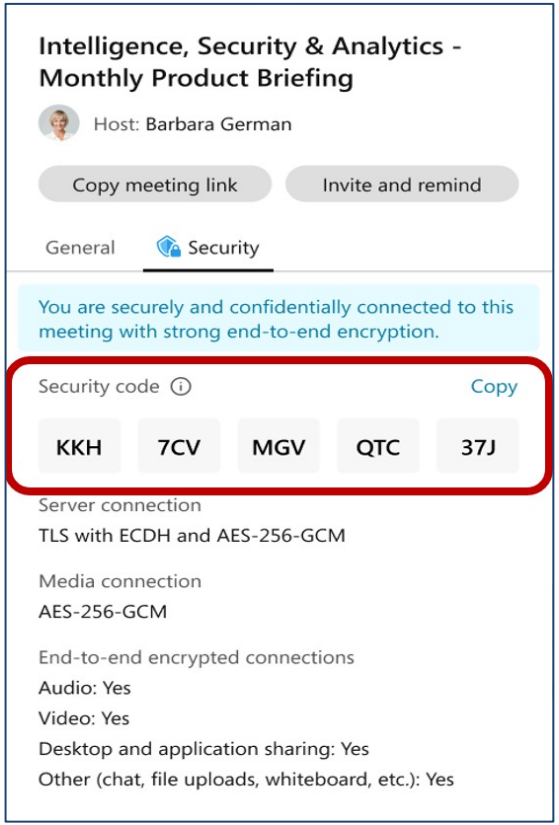
SHN7-16-GREAT WALL

Mute | Stop video | Share | Participants | Chat

Type here to search

02:12 PM
15/07/2020

Meeting Security Codes – Protecting against MITM attacks



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

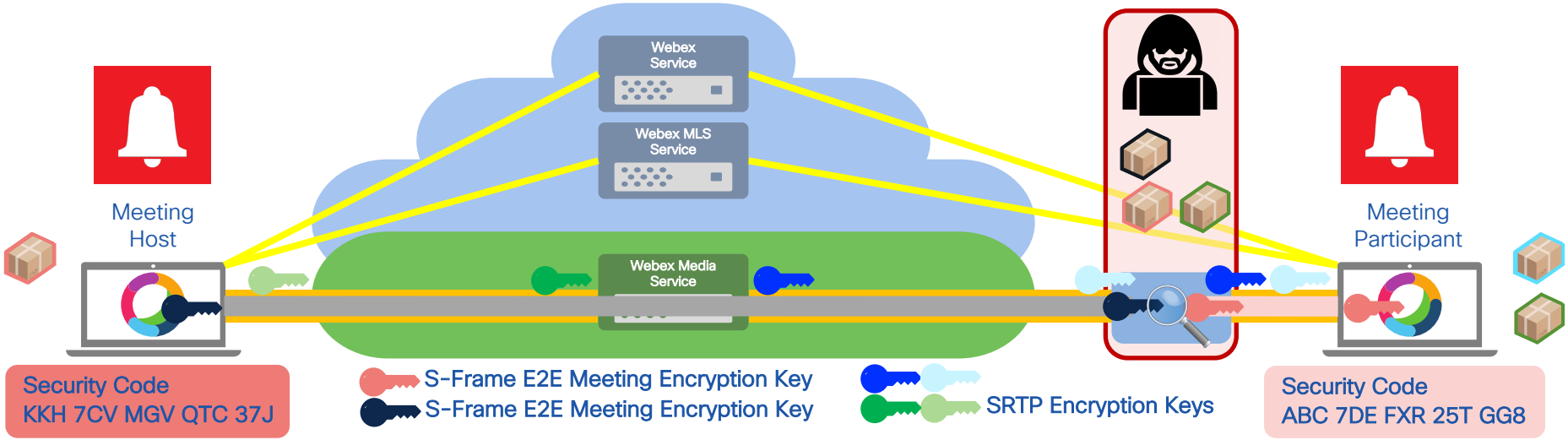
What a MITM attacker needs access to :

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

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…

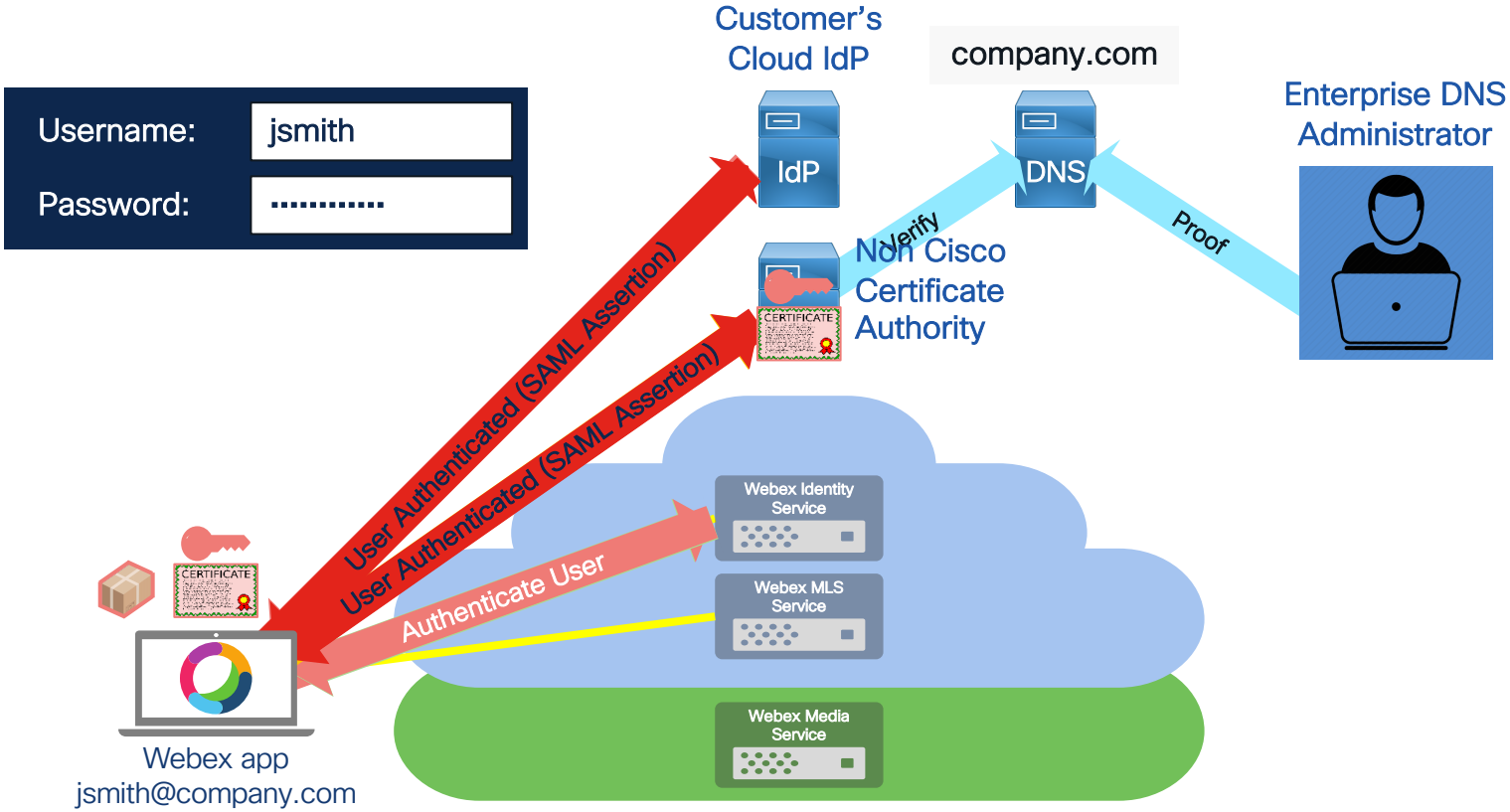
RFC 8555
Describes an automated validation procedure that allows domain-name based certificates (e.g. device1.cisco.com) to be obtained without user intervention.

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

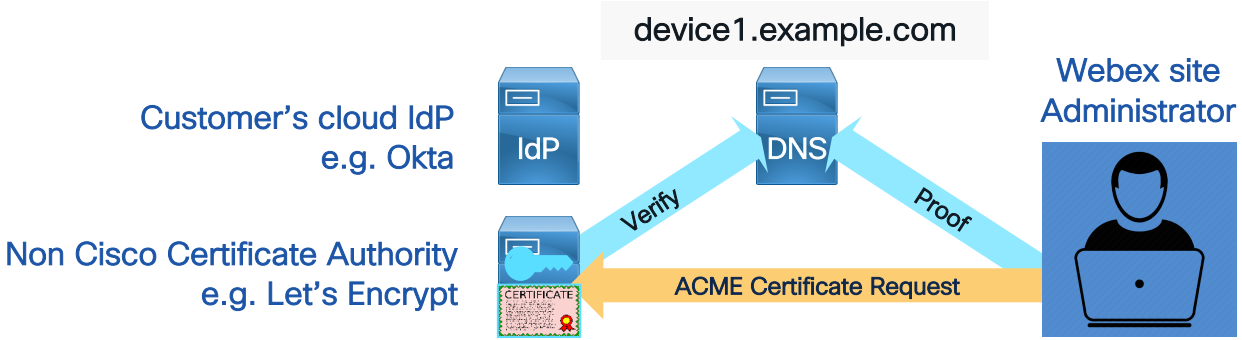
SSO Users authenticating with their Enterprise IdP

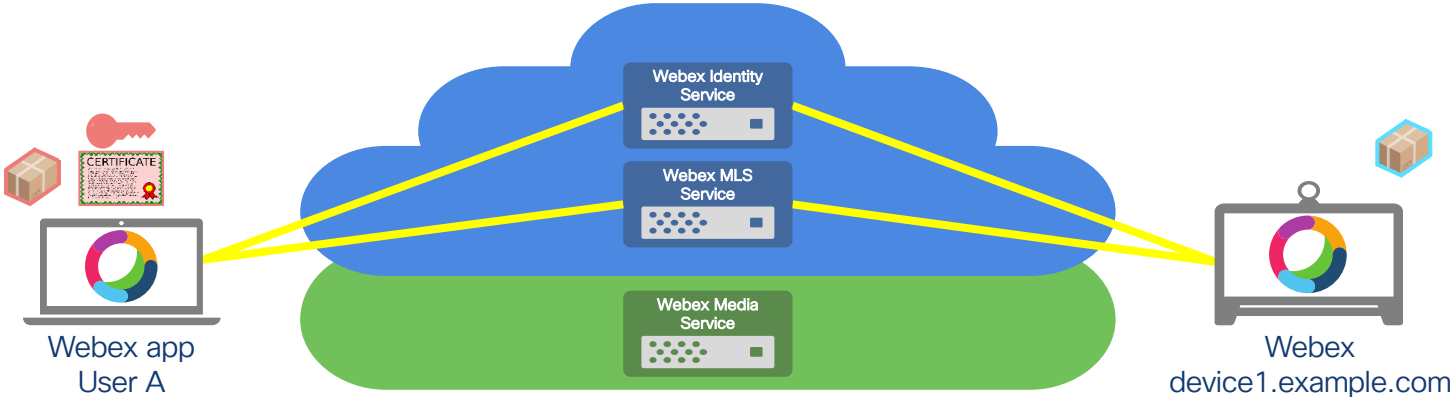
Using ACME to request a signed User Identity certificate from a non Cisco CA



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

Giacomo Drago

Participants (6)

Search

Barbara German
Host, me | company.com

BS 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

Mute | Share | Participants | Chat

Type here to search

02:12 PM
15/07/2020

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

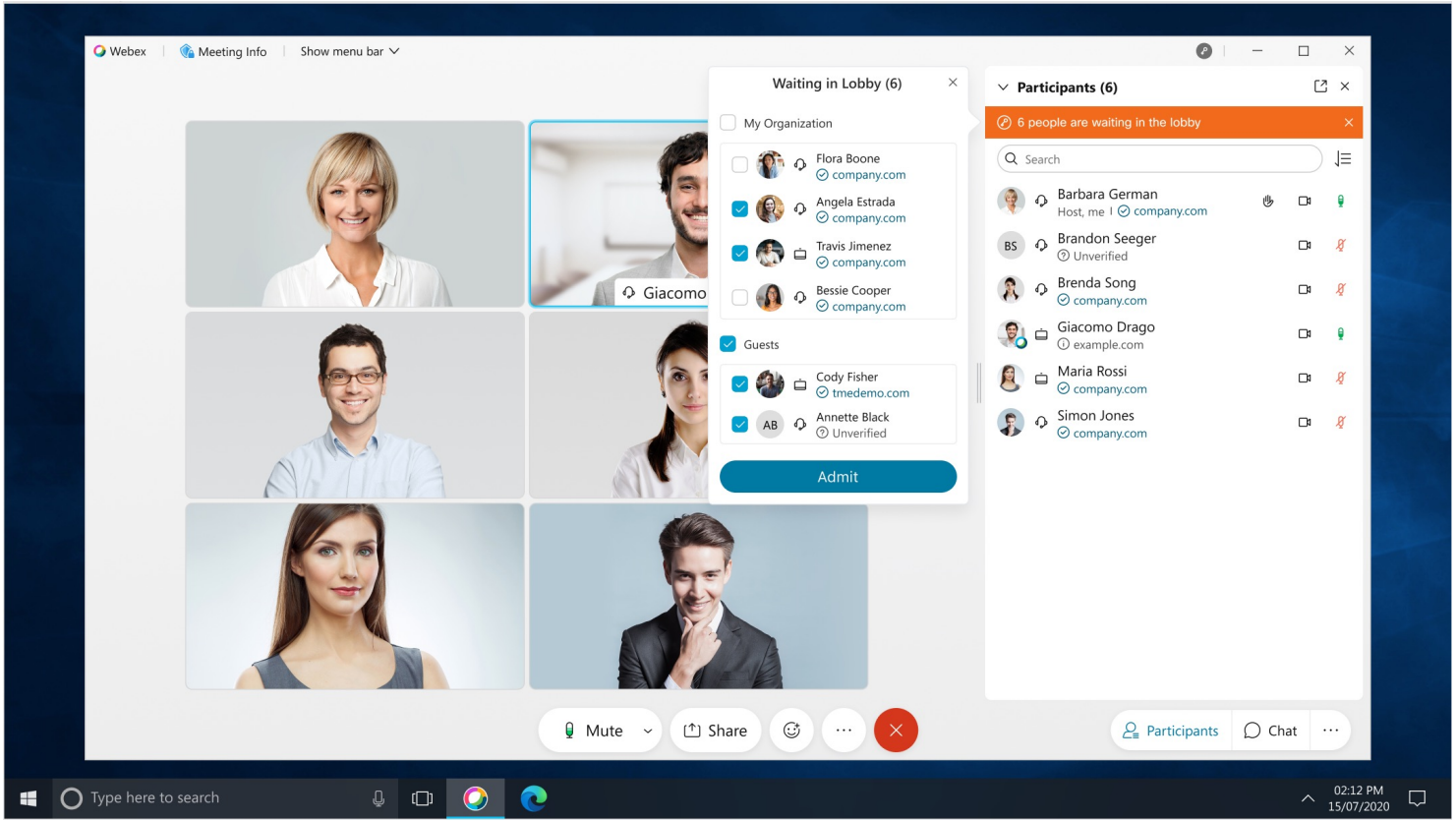
Identity verified by Webex CA
Show certificate

Brandon.Seeger@acme.com is an unauthenticated user

BS Brandon Seeger
Unverified

Identity not verified
Show certificate

Zero Trust Security for Webex Meetings: Phase 2
Webex E2E Identity
Meeting Lobby – New User Details



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 Q3 CY2021
Roll-Out Q4 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

Webex Security – Sales Connect Presentations

Webex Cloud security for Meetings, Messaging and Calling
https://salesconnect.cisco.com/open.html?c=37628ae0-2335-4569-a72c-37ac7eb83fbc

Webex Meetings – Cloud security and administrative security
https://salesconnect.cisco.com/open.html?c=0880b190-e268-4a1e-ab39-b18e48b2c6af

Webex Messaging – Cloud and hybrid security
https://salesconnect.cisco.com/open.html?c=fede7f0a-7902-4c80-b852-d990aaf7109f

Webex Messaging – Administrative security
https://salesconnect.cisco.com/open.html?c=88f805ce-9cca-42cd-bf3b-59eb7ca8e2fa

Webex – Enterprise Network Security
https://salesconnect.cisco.com/open.html?c=bdd9dc25-7947-4525-8620-08297fbd858f

Thank You

CISCO