Building E2EE and User Identity



Merry Ember Mou
Zoom Video Communications
Enigma 2021

zoom © 2021 Zoom Video Communications, Inc.

The New York Times

Former Twitter Employees Charged With Spying for Saudi Arabia

The Justice Department's charges raised questions about the security of technology companies.

CADE METZ BUSINESS 04.05.2016 11:00 AM

Forget Apple vs. the FBI: WhatsApp Just Switched on Encryption for a Billion People

This morning, WhatsApp made the scope of the Apple-FBI encryption battle look kinda small.

SMS TO RCS —

Google is testing end-to-end encryption in Android Messages

End-to-end encryption is growing in popularity. Google is getting on board.

DAN GOODIN - 11/19/2020, 12:33 PM

zoom © 2021 Zoom Video Communications, Inc.

Agenda

- Integrating E2EE into Zoom
- Building user identity in subsequent phases



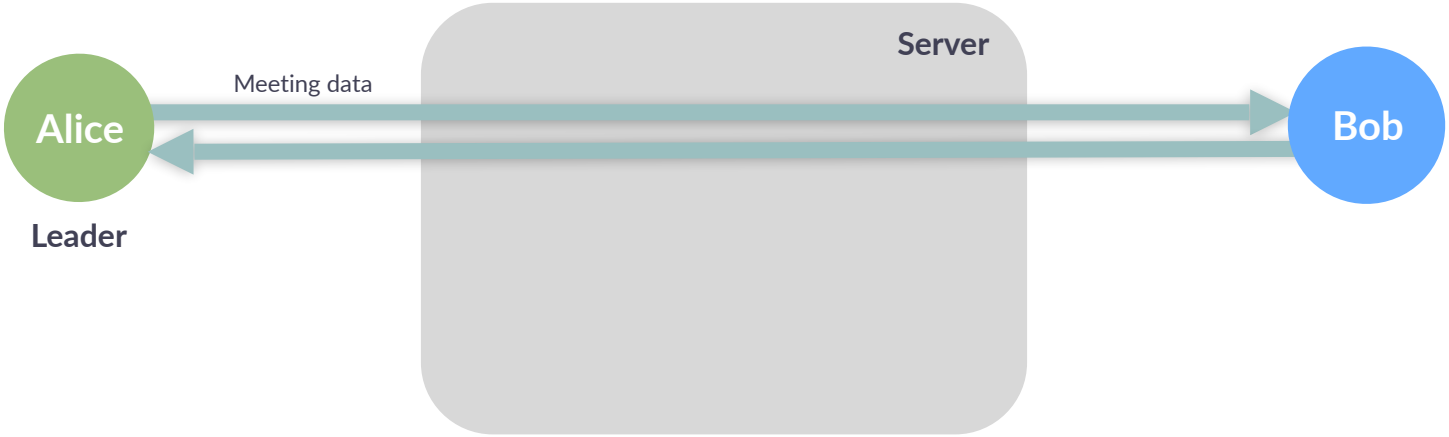
© 2021 Zoom Video Communications, Inc.

Moving Key Generation to the Client



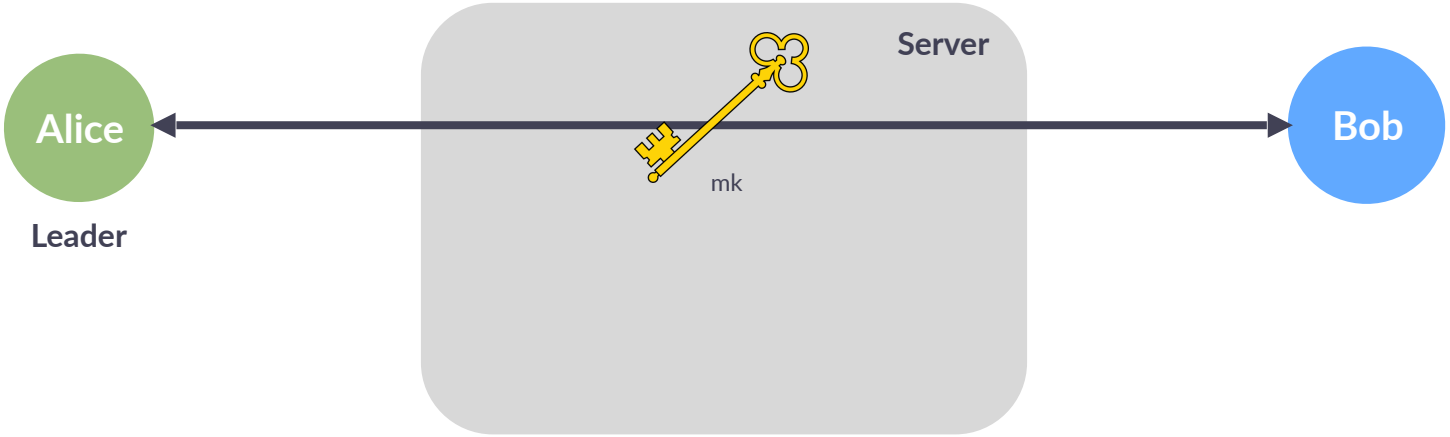
© 2021 Zoom Video Communications, Inc.

Zoom Meetings



© 2021 Zoom Video Communications, Inc.

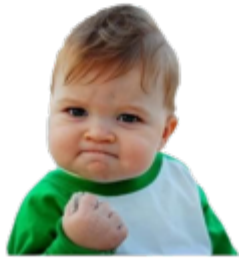
Server-Managed Meeting Key



© 2021 Zoom Video Communications, Inc.

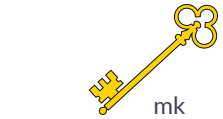
E2EE Implementation Goals

- Minimize changes to existing code
- Reduce introducing complexity
- Maintain meeting quality and performance



zoom © 2021 Zoom Video Communications, Inc.

E2EE Design



Alice

Leader

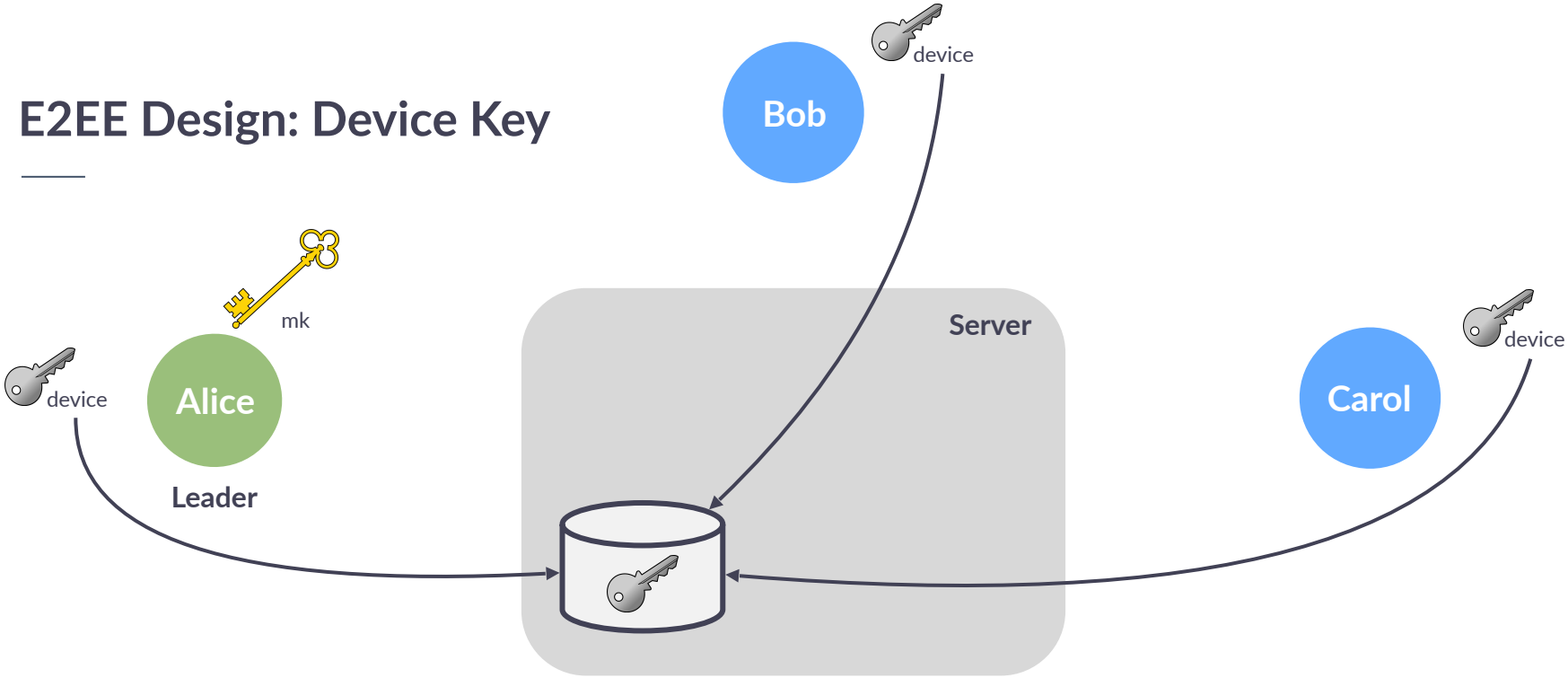
Bob

Server

Carol

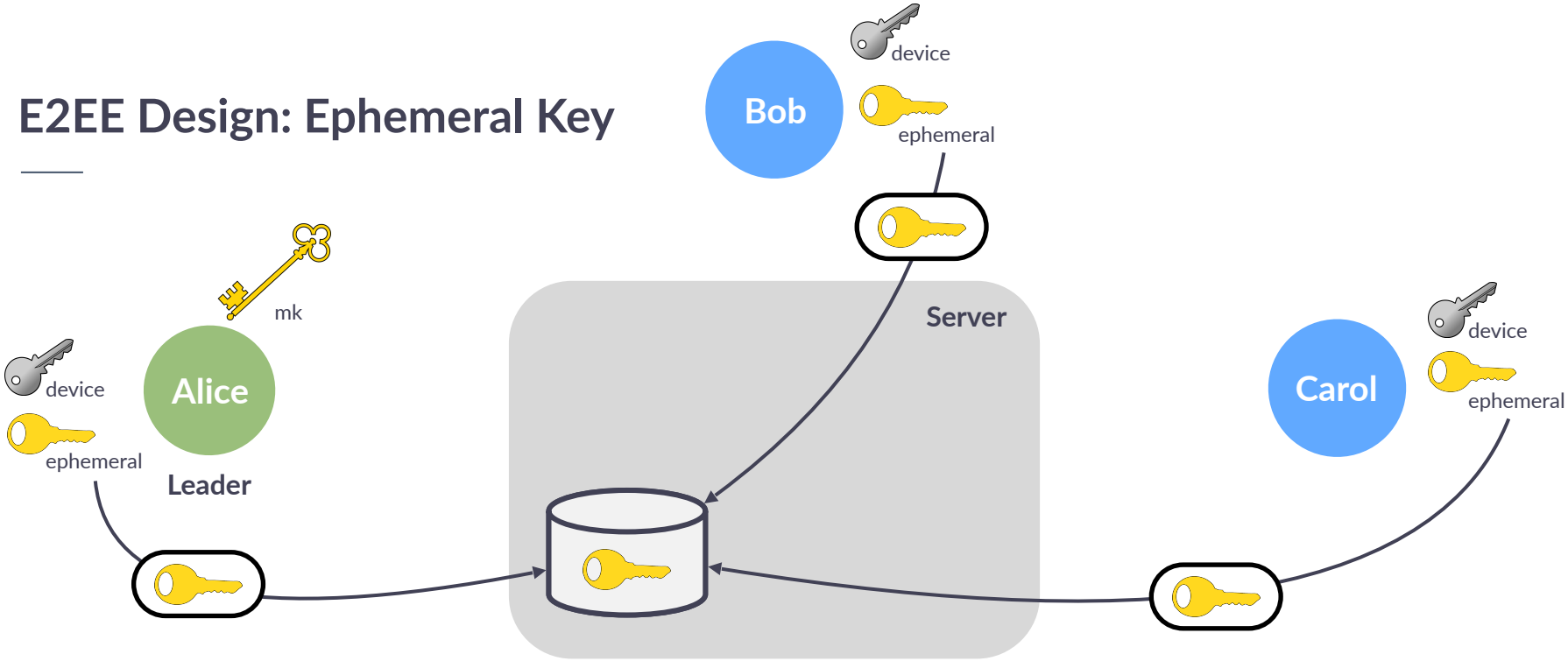
© 2021 Zoom Video Communications, Inc.

E2EE Design: Device Key



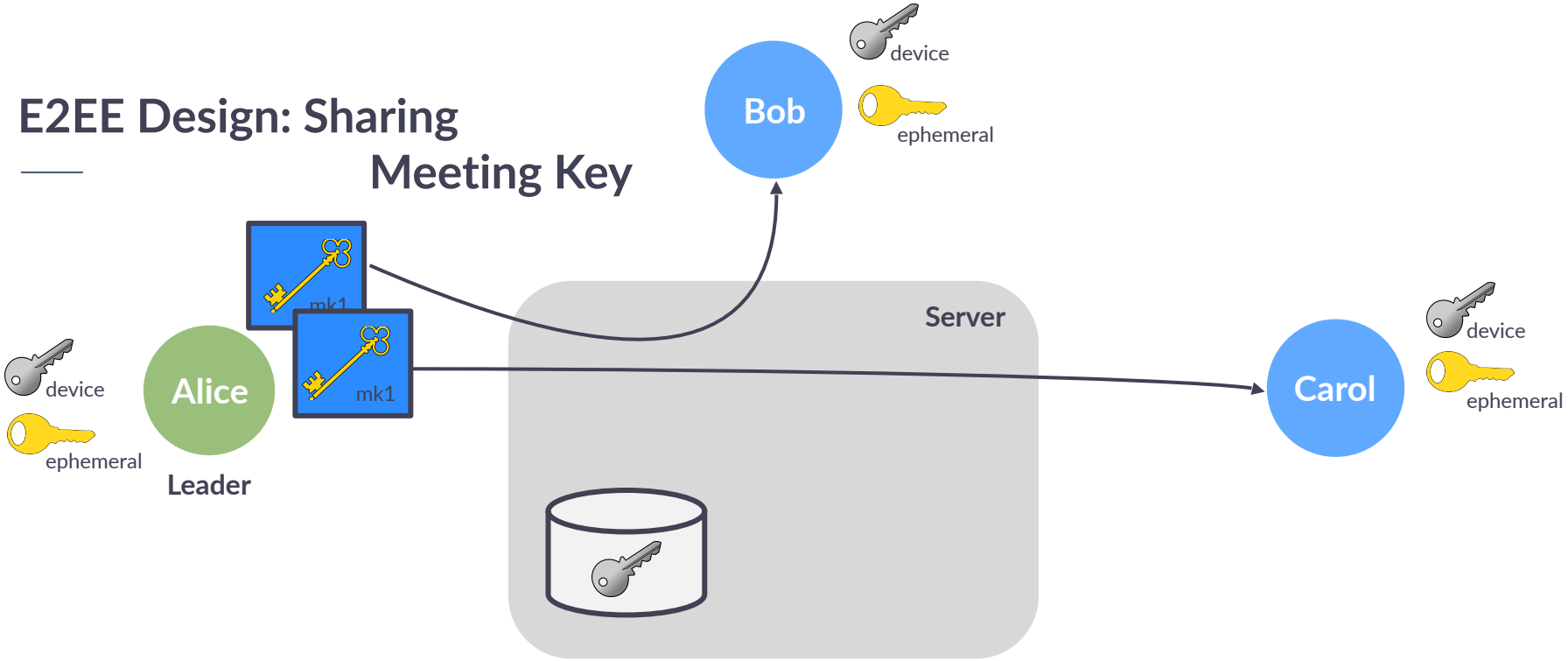
zoom © 2021 Zoom Video Communications, Inc.

E2EE Design: Ephemeral Key



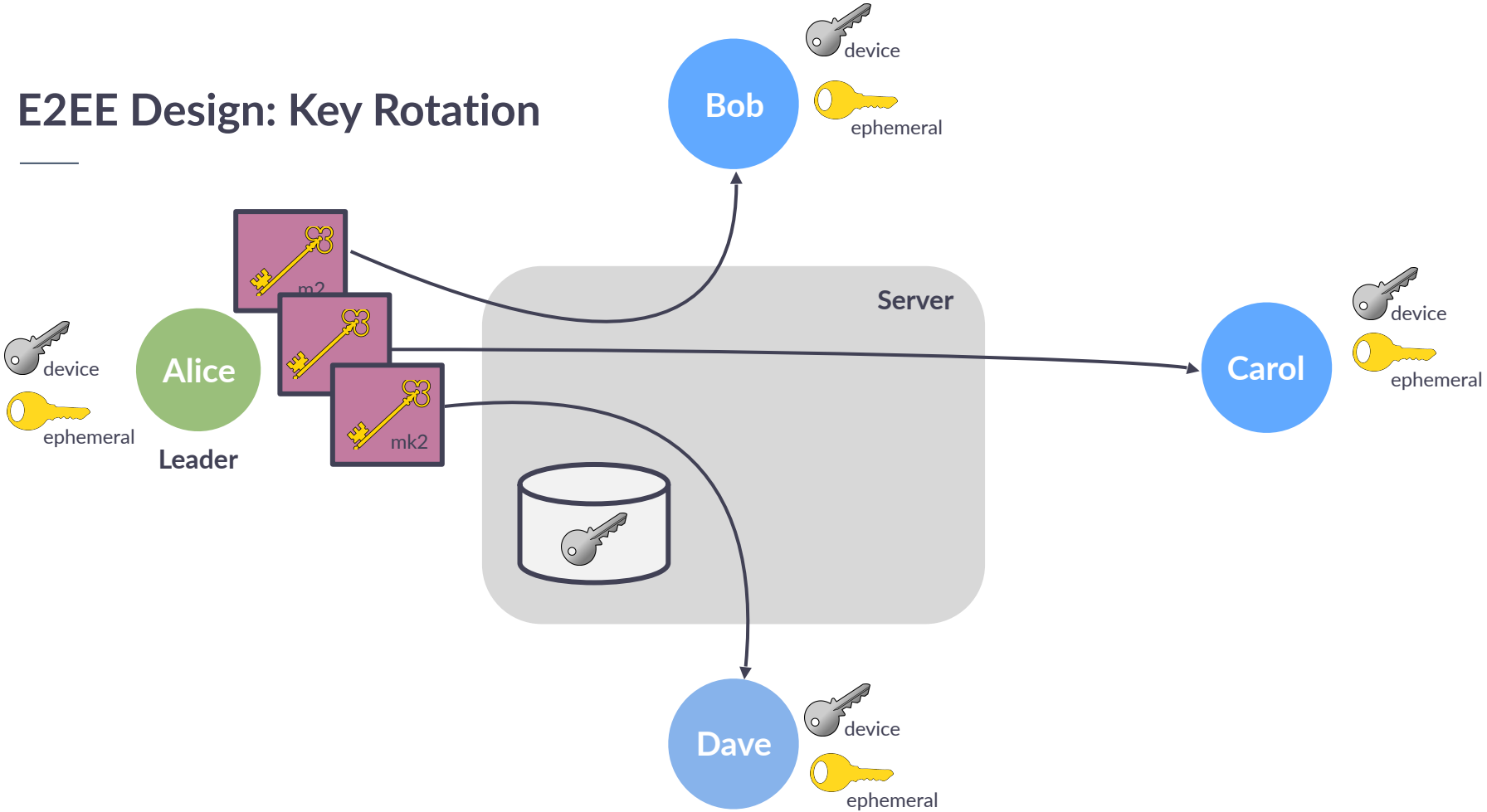
zoom © 2021 Zoom Video Communications, Inc.

E2EE Design: Sharing Meeting Key



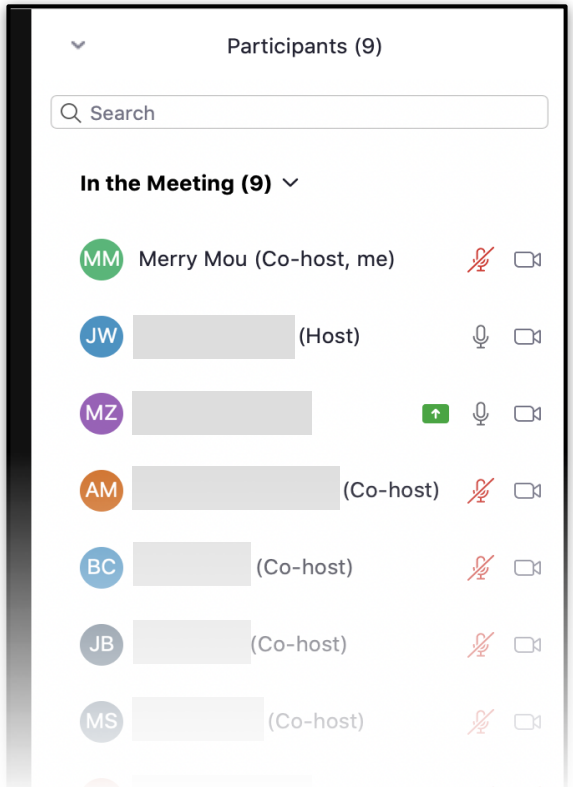
zoom © 2021 Zoom Video Communications, Inc.

E2EE Design: Key Rotation



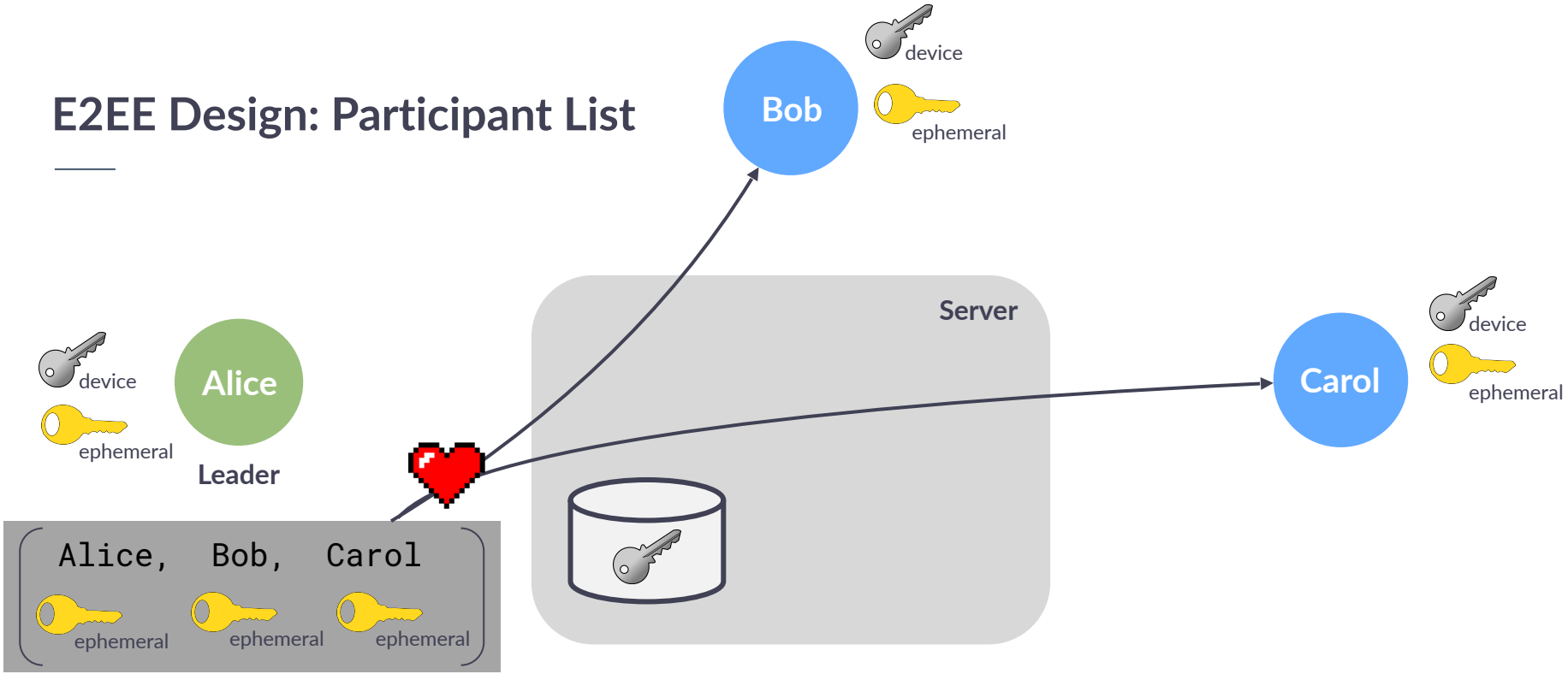
zoom © 2021 Zoom Video Communications, Inc.

E2EE Design: Leader Participant List



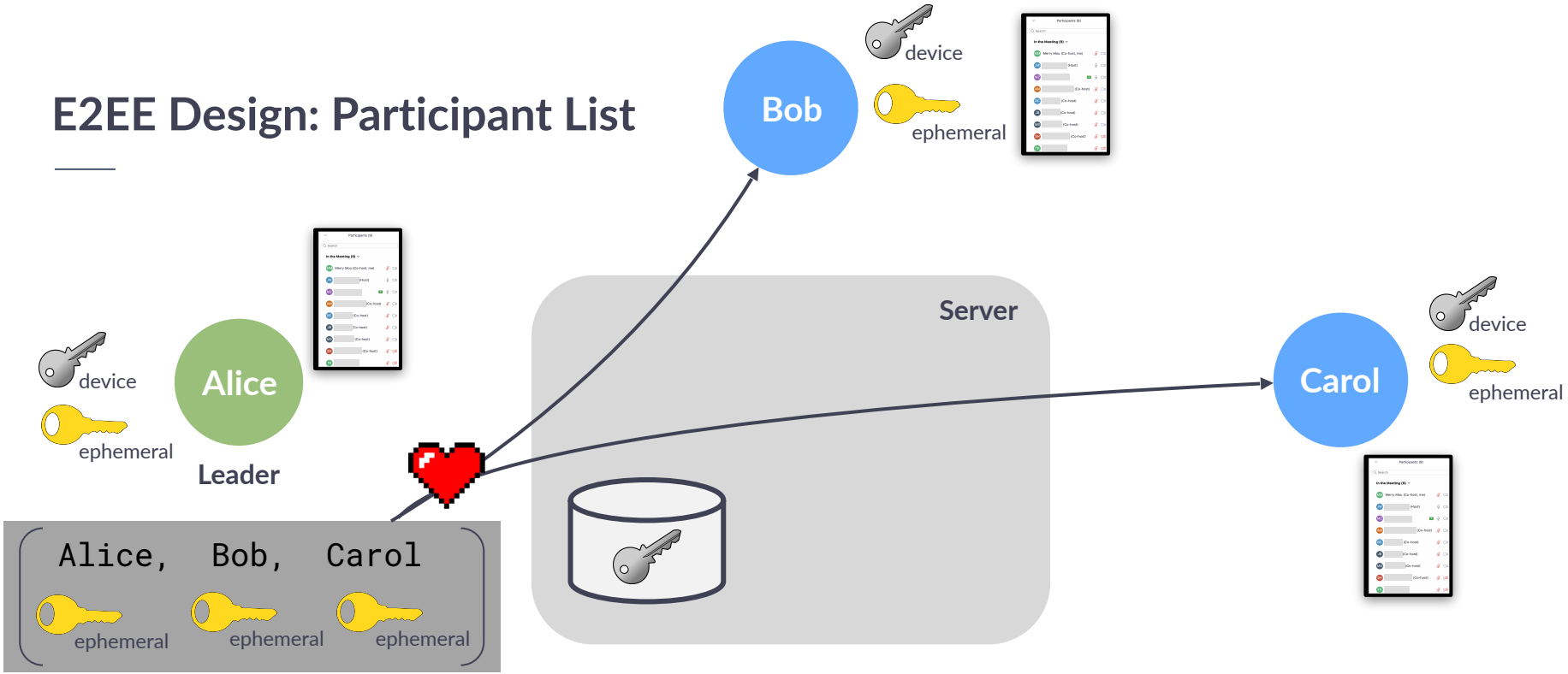
zoom © 2021 Zoom Video Communications, Inc.

E2EE Design: Participant List

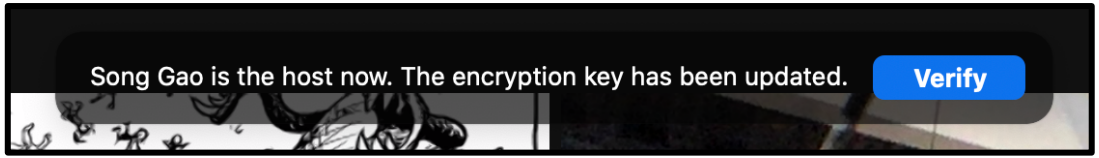


zoom © 2021 Zoom Video Communications, Inc.

E2EE Design: Participant List

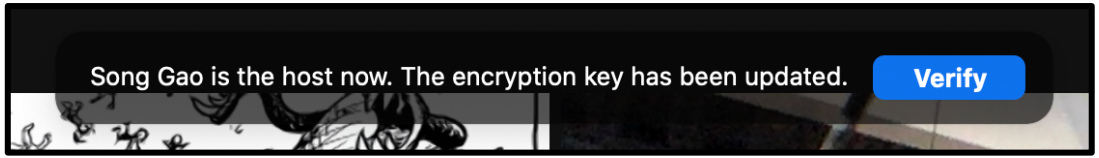


zoom © 2021 Zoom Video Communications, Inc.

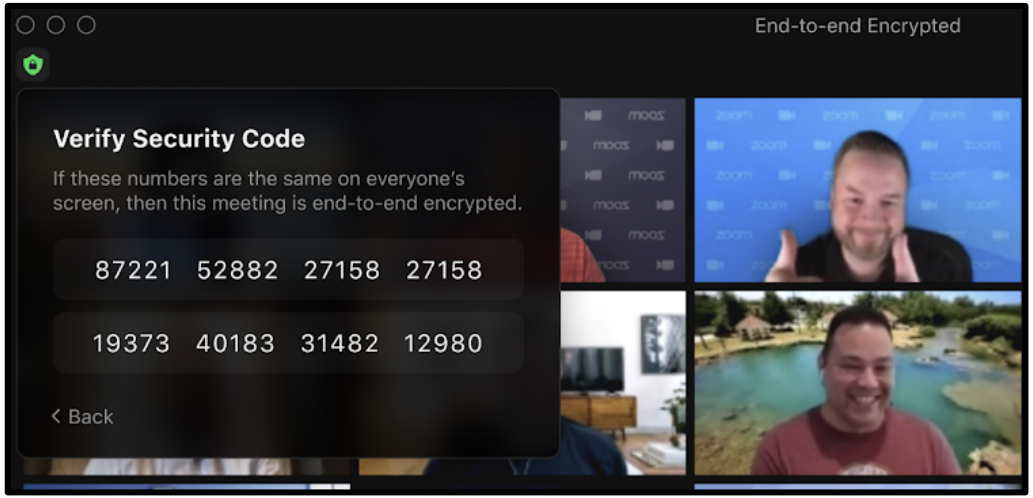


Leader change notification

© 2021 Zoom Video Communications, Inc.



Leader change notification



Meeting leader security code, to detect Meddlers-In-The-Middle (MITMs)

© 2021 Zoom Video Communications, Inc.

Delivering E2EE



© 2021 Zoom Video Communications, Inc.

Performance: Meeting Keys

- Joining a meeting must be easy



© 2021 Zoom Video Communications, Inc.

Performance: Meeting Keys

- Joining a meeting must be easy
- Participants must get meeting keys



© 2021 Zoom Video Communications, Inc.

Performance: Meeting Keys

- Joining a meeting must be easy
- Participants must get meeting keys
- Throttling rekeys



zoom © 2021 Zoom Video Communications, Inc.

Performance: Participant List Heartbeats

- UI update frequency



© 2021 Zoom Video Communications, Inc.

Performance: Participant List Heartbeats

- UI update frequency
- Network traffic



© 2021 Zoom Video Communications, Inc.

Performance: Participant List Heartbeats

- UI update frequency
- Network traffic
- Noticing notifications



© 2021 Zoom Video Communications, Inc.

Deploying E2EE

- Client library interface



© 2021 Zoom Video Communications, Inc.

Deploying E2EE

- Client library interface
- Stand-alone keyservers



© 2021 Zoom Video Communications, Inc.

Deploying E2EE

- Client library interface
- Stand-alone keyservers
- Backwards compatibility



zoom © 2021 Zoom Video Communications, Inc.

From Device Key to User Identity

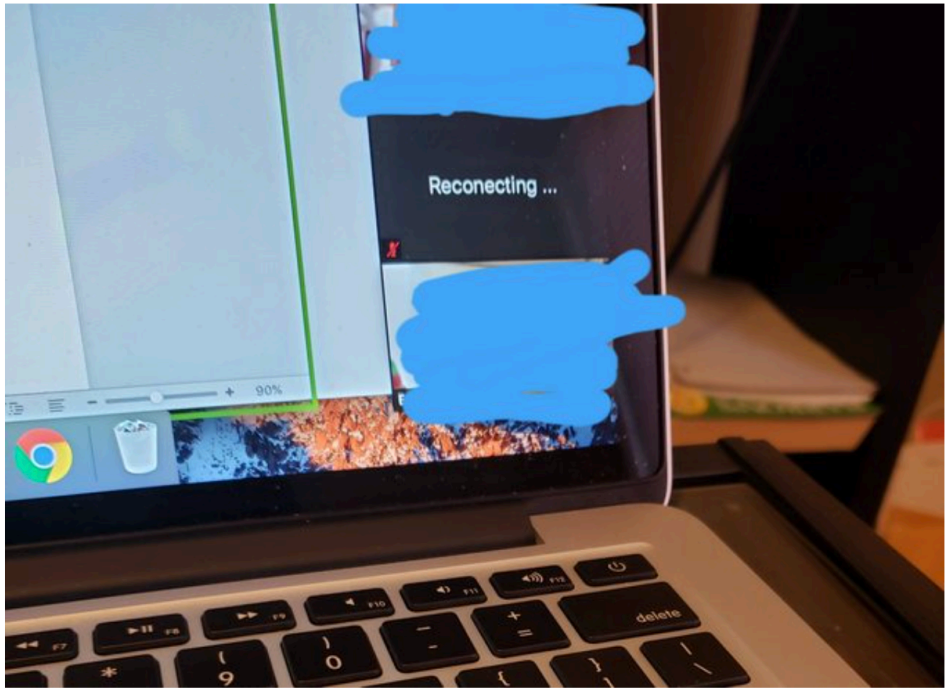


zoom © 2021 Zoom Video Communications, Inc.

r/funny · Posted by u/reddericks 7 months ago 3 5 4 2

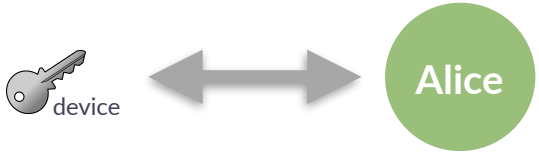
Today one of my 4th grade students renamed himself "reconecting ..." on our Zoom call and pretended that he was having internet issues to avoid participating in our lesson.

imgur.com/k9p0AJ...



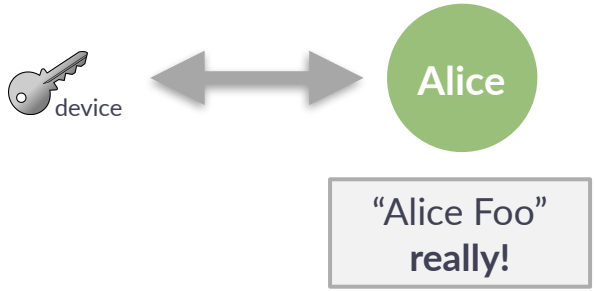
zoom © 2021 Zoom Video Communications, Inc.

Building User Identity



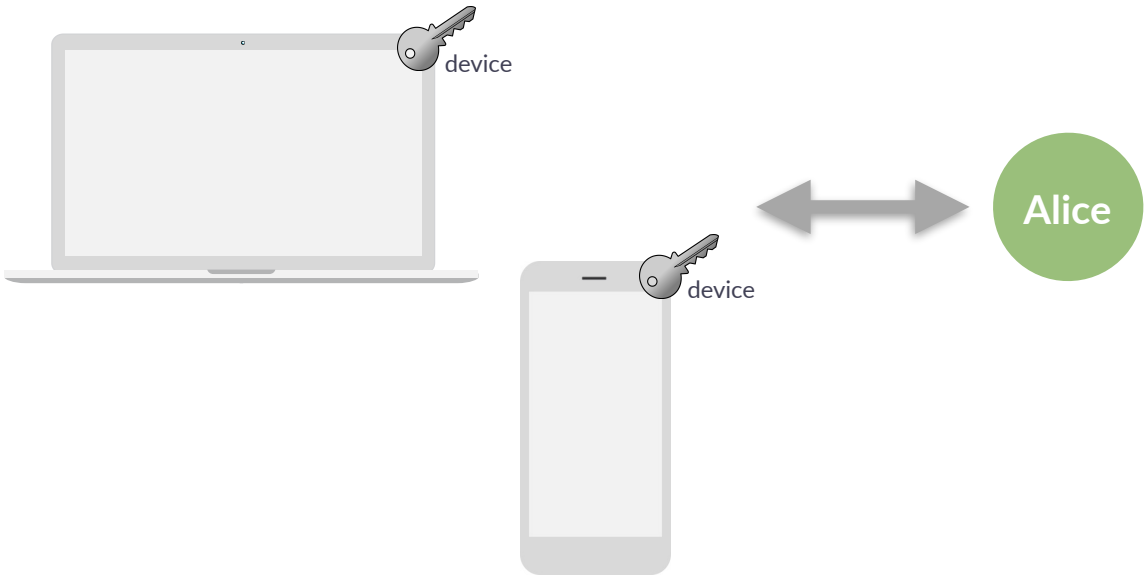
© 2021 Zoom Video Communications, Inc.

Building User Identity



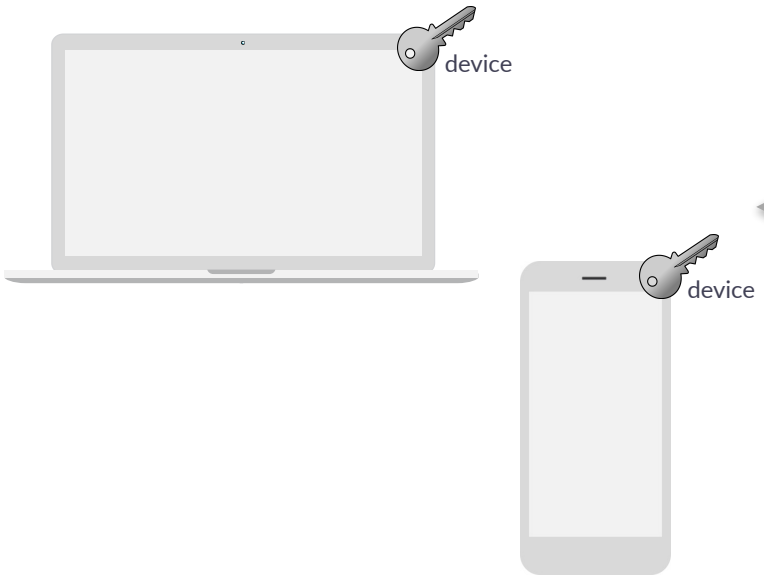
© 2021 Zoom Video Communications, Inc.

A User is



© 2021 Zoom Video Communications, Inc.

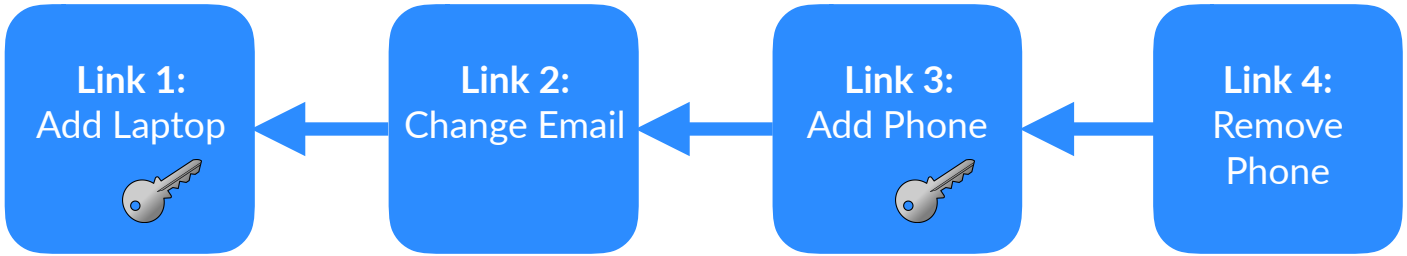
A User is



(**Display Name:** “Alice Foo”)
Email Address: alice@company.com
Account Domain Name (ADN): company.com

© 2021 Zoom Video Communications, Inc.

Auditable User Identity

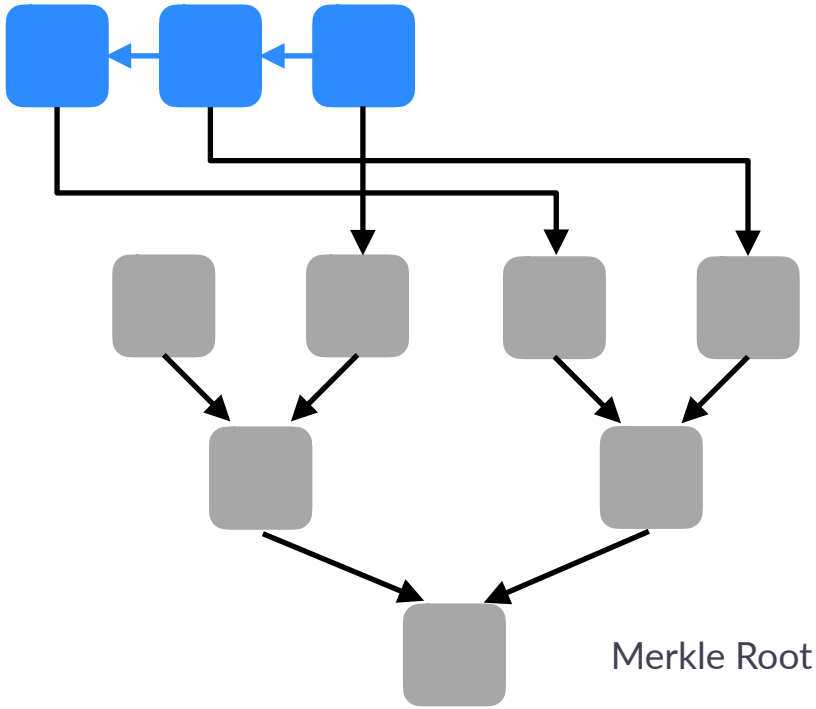


User Sigchain

zoom © 2021 Zoom Video Communications, Inc.

Auditable User Identity

User Sigchain Links



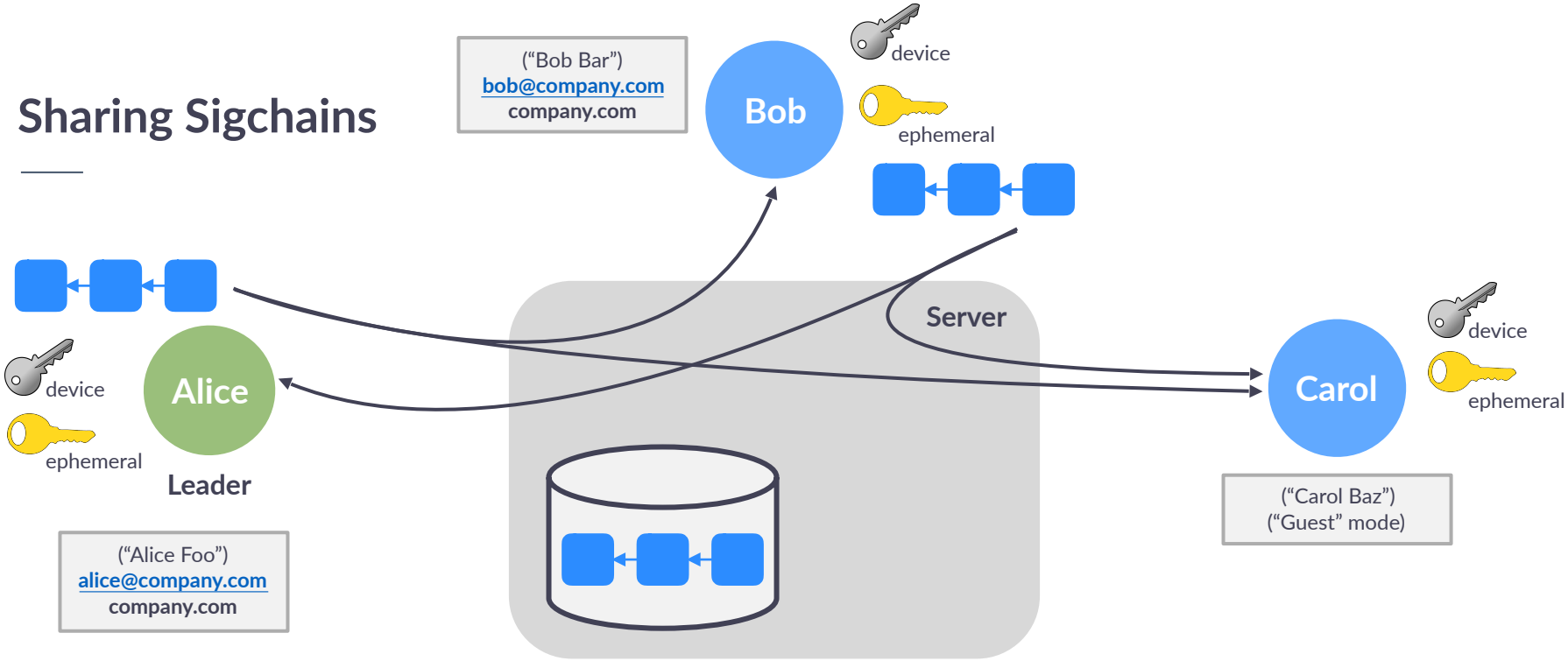
zoom © 2021 Zoom Video Communications, Inc.

User Identity In a Meeting



© 2021 Zoom Video Communications, Inc.

Sharing Sigchains



zoom © 2021 Zoom Video Communications, Inc.



Do I trust the **email** and **ADN** are associated with this user?

© 2021 Zoom Video Communications, Inc.

- Do I trust the **email** and **ADN** are associated with this user?
- Have **I seen** this user and/or this device before?

© 2021 Zoom Video Communications, Inc.

- Do I trust the **email** and **ADN** are associated with this user?
- Have **I seen** this user and/or this device before?
- Does this user have an **attestation** of their sigchain from **their IdP**? (if applicable)

© 2021 Zoom Video Communications, Inc.

Takeaways

- E2EE security depends on knowing who's at the "ends."

© 2021 Zoom Video Communications, Inc.

Takeaways

- E2EE security depends on knowing who's at the "ends."
- Building E2EE into an existing product requires balancing implementation complexity, performance, and UI/UX.

zoom © 2021 Zoom Video Communications, Inc.

Takeaways

- E2EE security depends on knowing who's at the "ends."
- Building E2EE into an existing product requires balancing implementation complexity, performance, and UI/UX.
- "Is it secure?" is not a yes/no question.

zoom © 2021 Zoom Video Communications, Inc.

Takeaways

- E2EE security depends on knowing who's at the "ends."
- Building E2EE into an existing product requires balancing implementation complexity, performance, and UI/UX.
- "Is it secure?" is not a yes/no question.

@zoom_us
@merry
merry.mou@zoom.us
github.com/zoom/zoom-e2e-whitepaper

zoom © 2021 Zoom Video Communications, Inc.