How Zoom is Building End-to-End Encryption

Merry Ember Mou
Zoom Video Communications
Swiss Cyber Storm
Oct 12 2021

Presenter

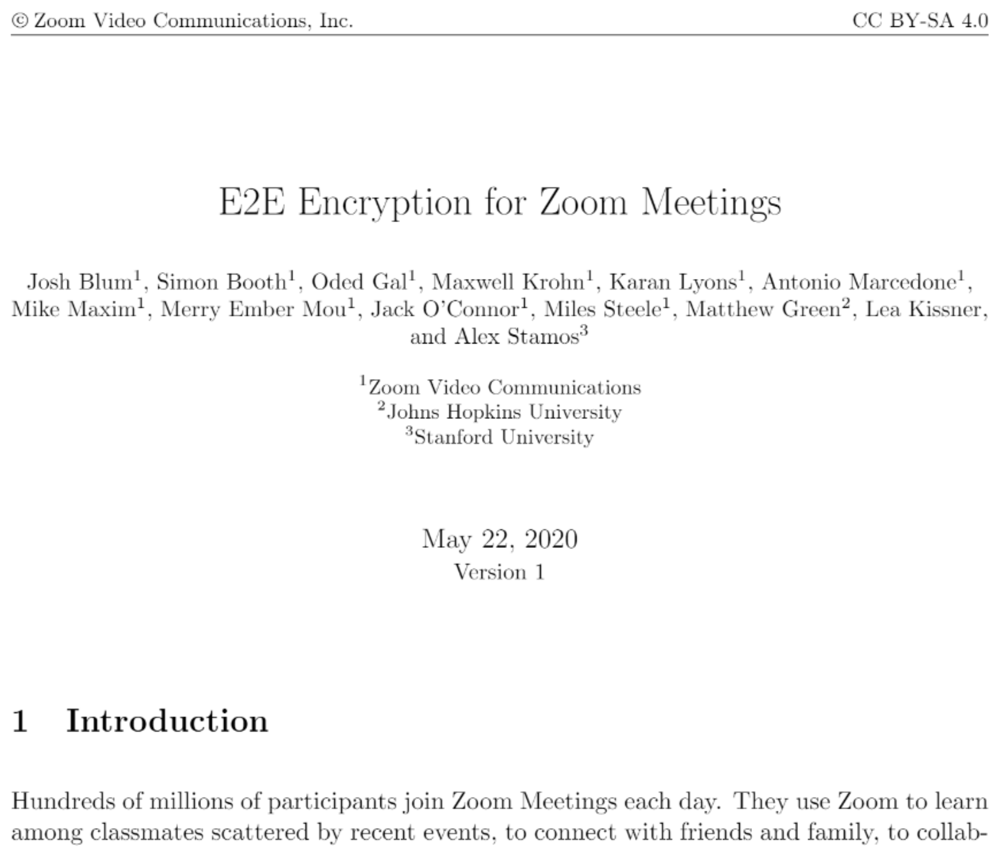
Merry Ember Mou

Security Software Engineer

Zoom Video Communications

Agenda

- Integrating E2EE into Zoom
- Building user identity



E2E Encryption for Zoom Meetings

Josh Blum[1], Simon Booth[1], Oded Gal[1], Maxwell Krohn[1], Karan Lyons[1], Antonio Marcedone[1], Mike Maxim[1], Merry Ember Mou[1], Jack O'Connor[1], Miles Steele[1], Matthew Green[2], Lea Kissner, and Alex Stamos[3]

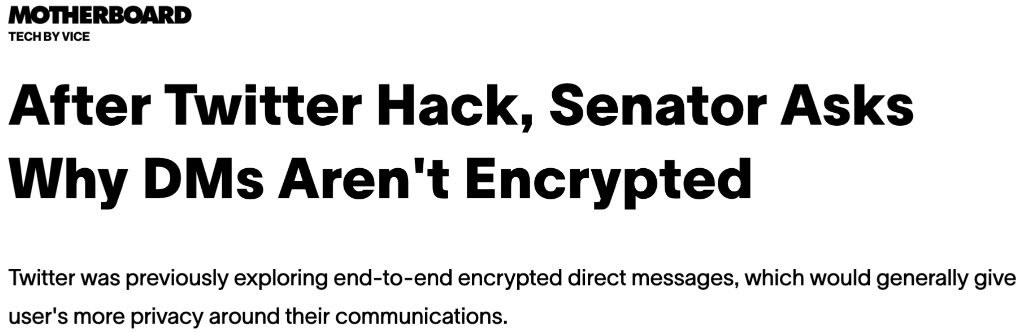
[1]Zoom Video Communications
[2]Johns Hopkins University
[3]Stanford University

May 22, 2020
Version 1

1 Introduction

Hundreds of millions of participants join Zoom Meetings each day. They use Zoom to learn among classmates scattered by recent events, to connect with friends and family, to collab-

https://github.com/zoom/zoom-e2e-whitepaper



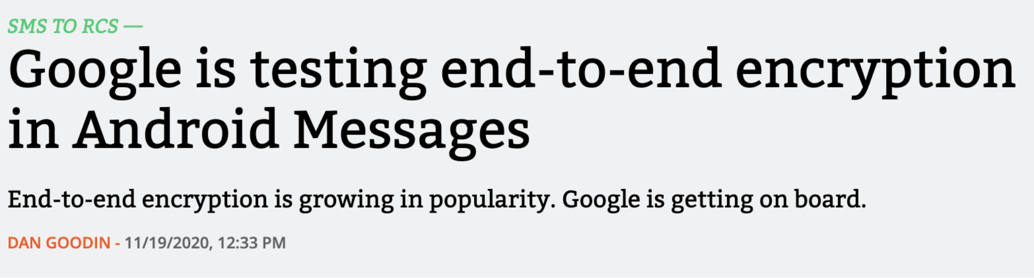
MOTHERBOARD
TECH BY VICE

After Twitter Hack, Senator Asks Why DMs Aren't Encrypted

Twitter was previously exploring end-to-end encrypted direct messages, which would generally give user's more privacy around their communications.

By Joseph Cox

July 16, 2020, 9:22am

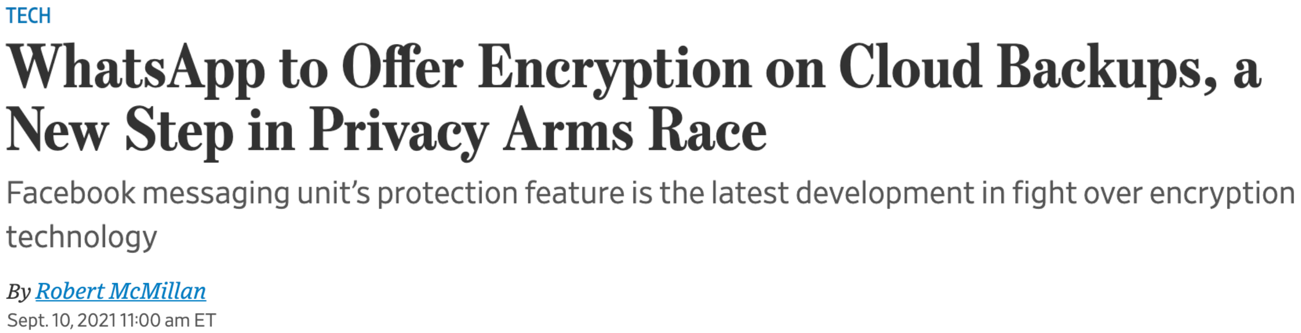


SMS TO RCS —

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



TECH

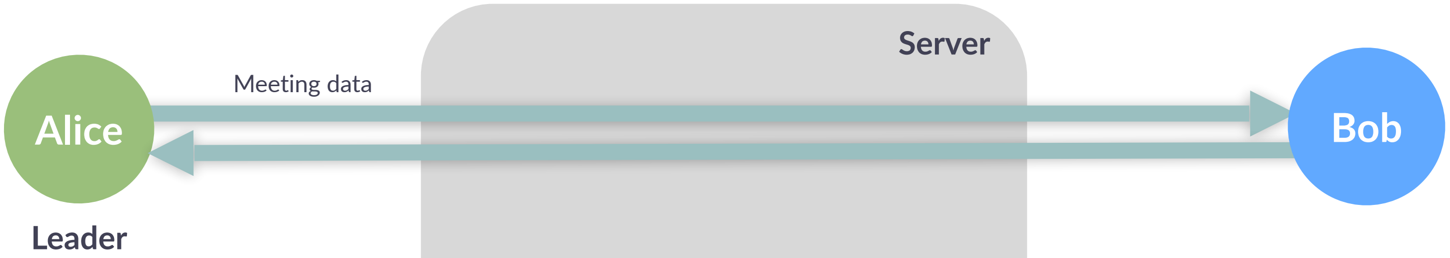
WhatsApp to Offer Encryption on Cloud Backups, a New Step in Privacy Arms Race

Facebook messaging unit's protection feature is the latest development in fight over encryption technology

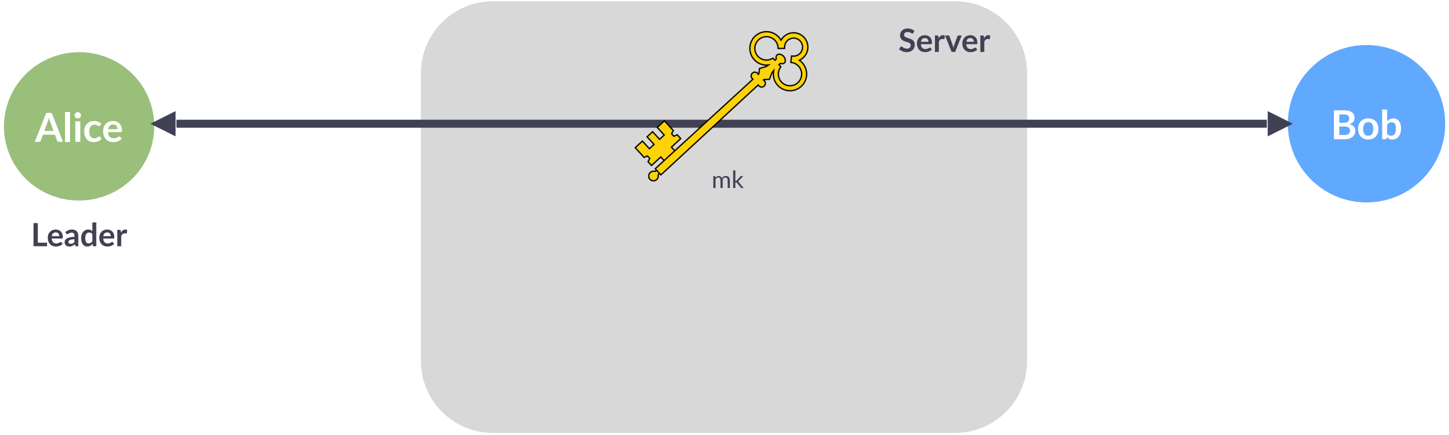
By Robert McMillan

Sept. 10, 2021 11:00 am ET

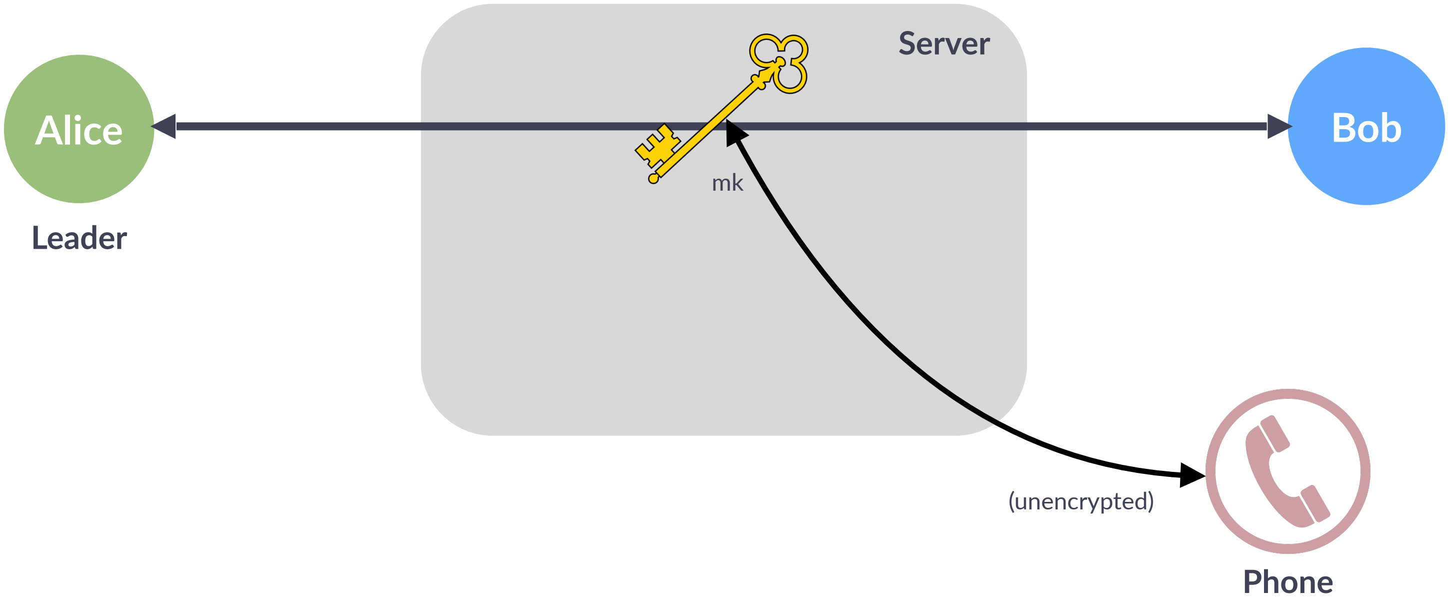
Zoom Meetings



Server-Managed Meeting Key



Server-Managed Meeting Key



Moving Key Generation to the Client

Building E2EE

Add new security affordances to notice unexpected participants

Building E2EE

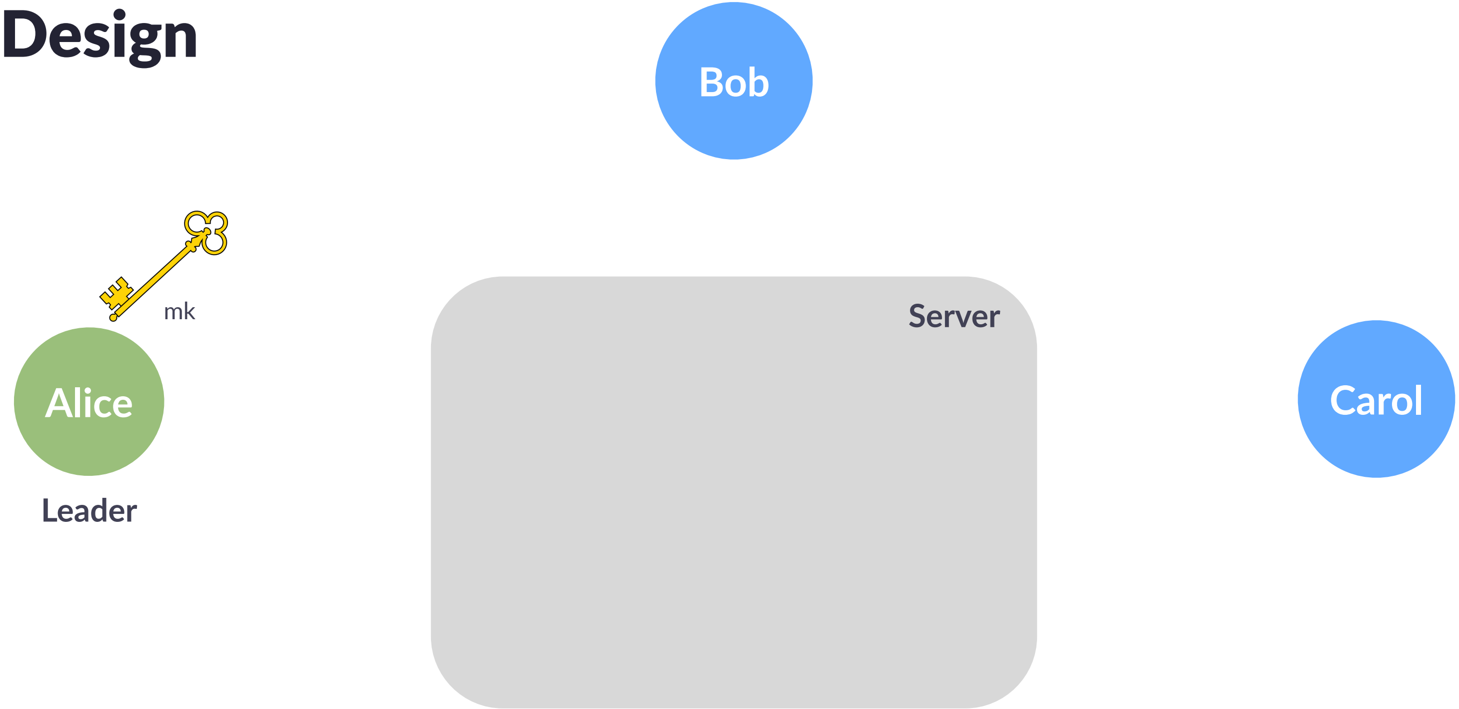
Add new security affordances to notice unexpected participants

Minimize scope and implementation complexity

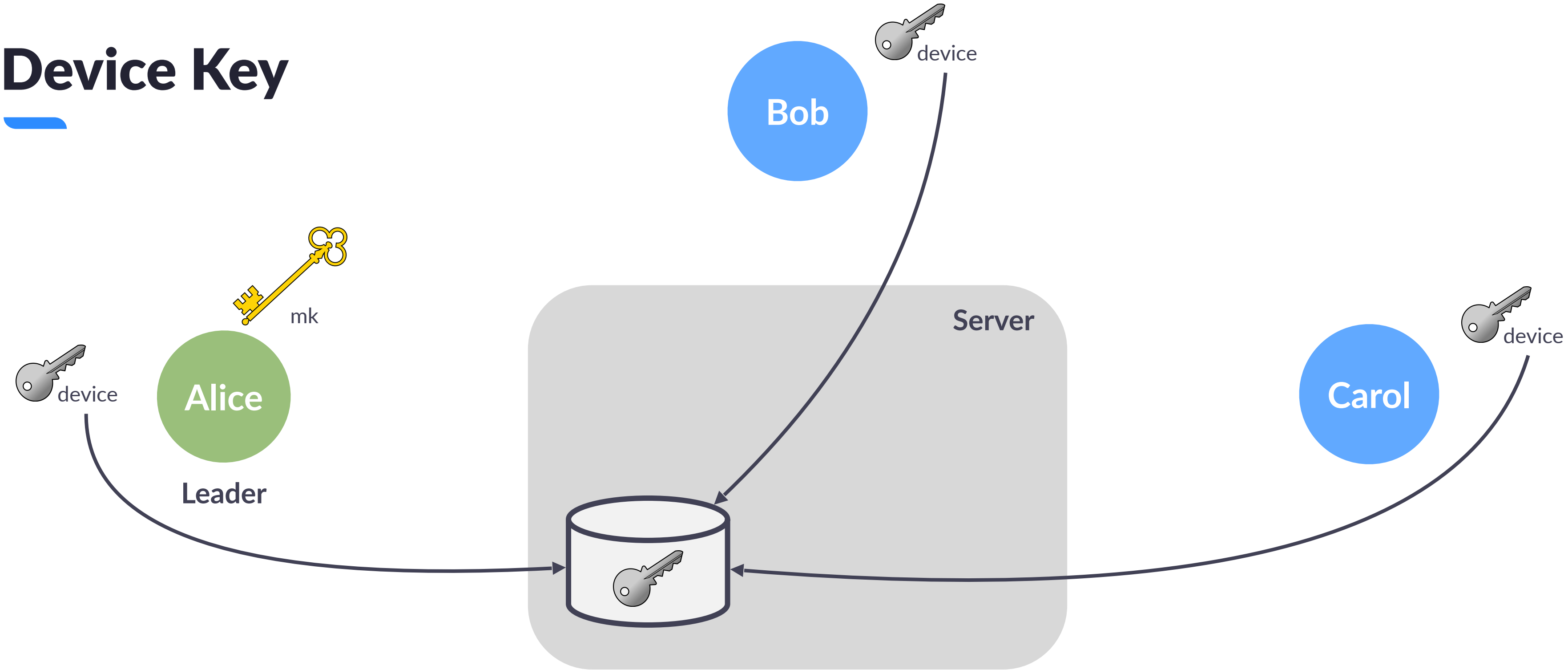
Building E2EE

- Add new security affordances to notice unexpected participants
- Minimize scope and implementation complexity
- Maintain meeting quality and performance

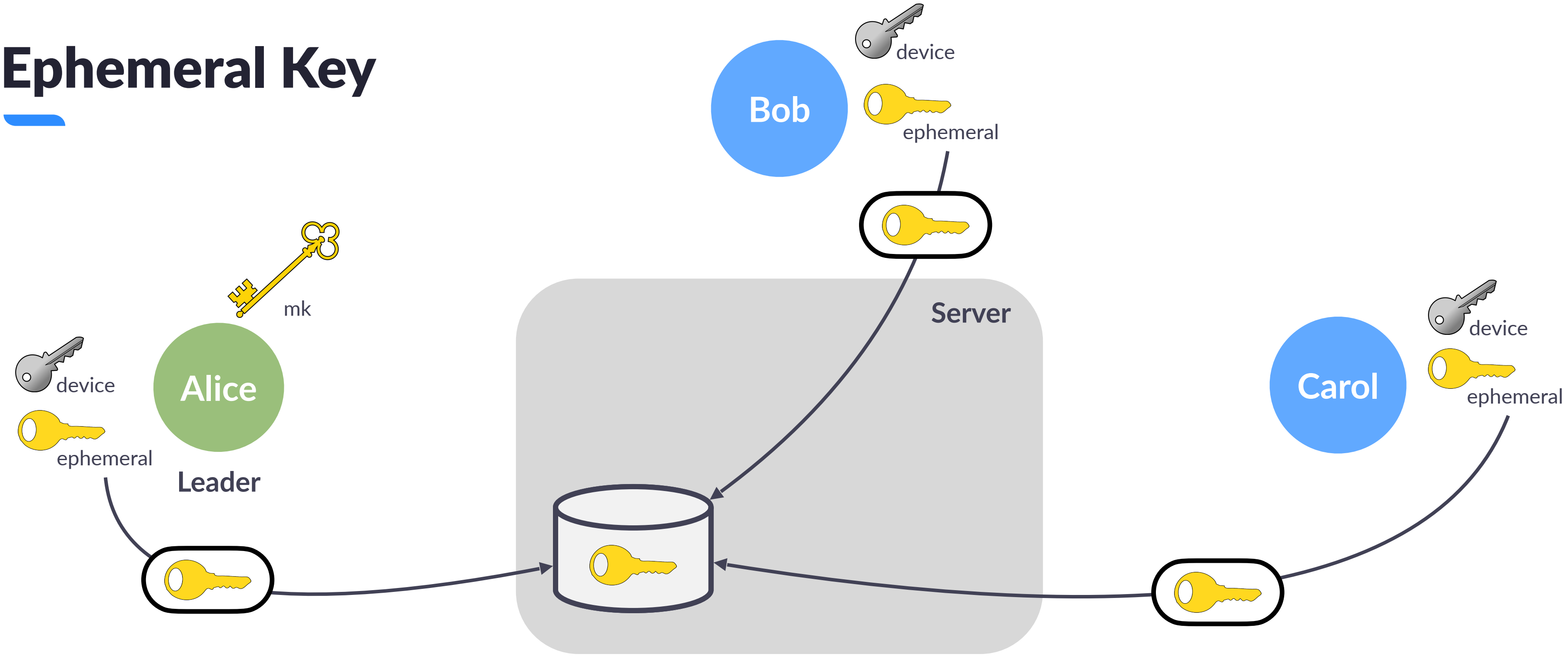
E2EE Design



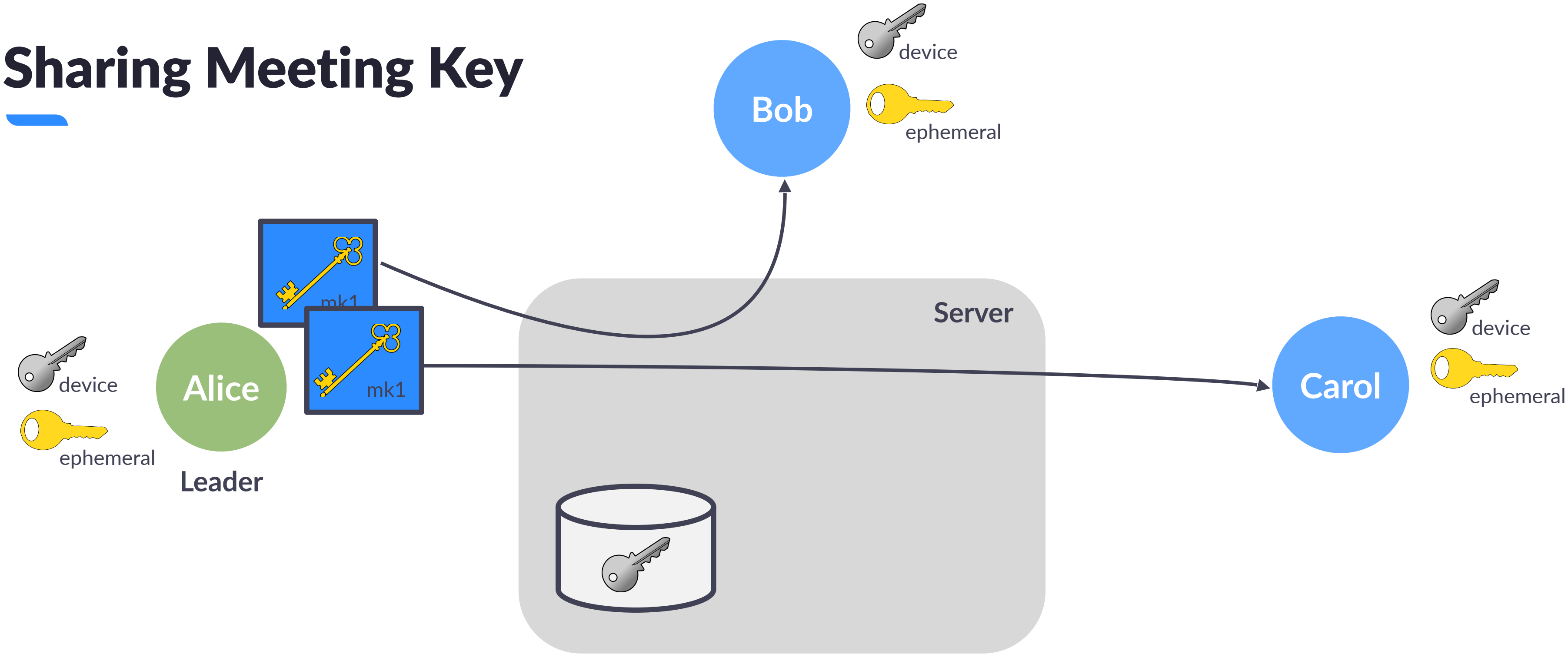
Device Key



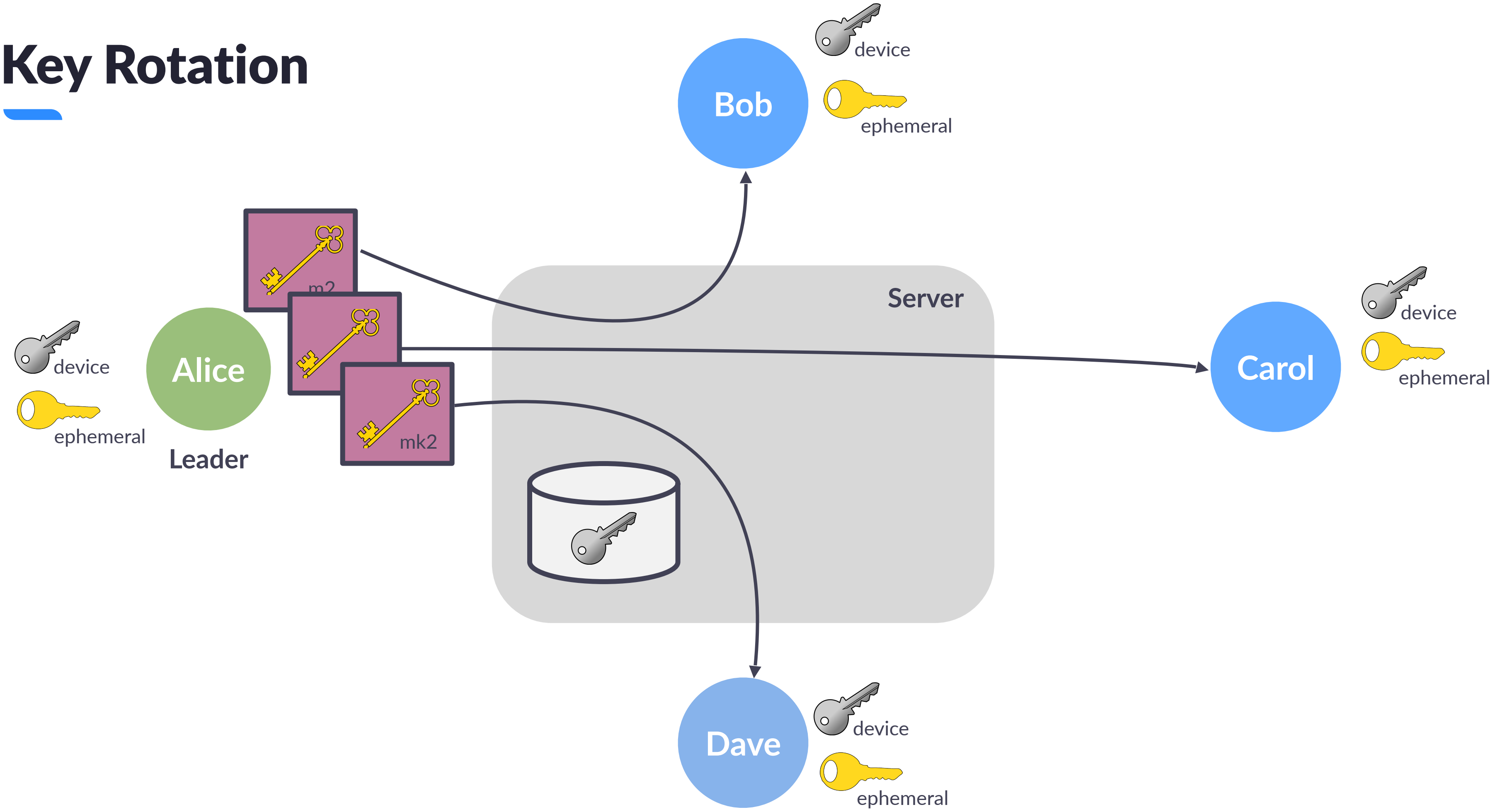
Ephemeral Key



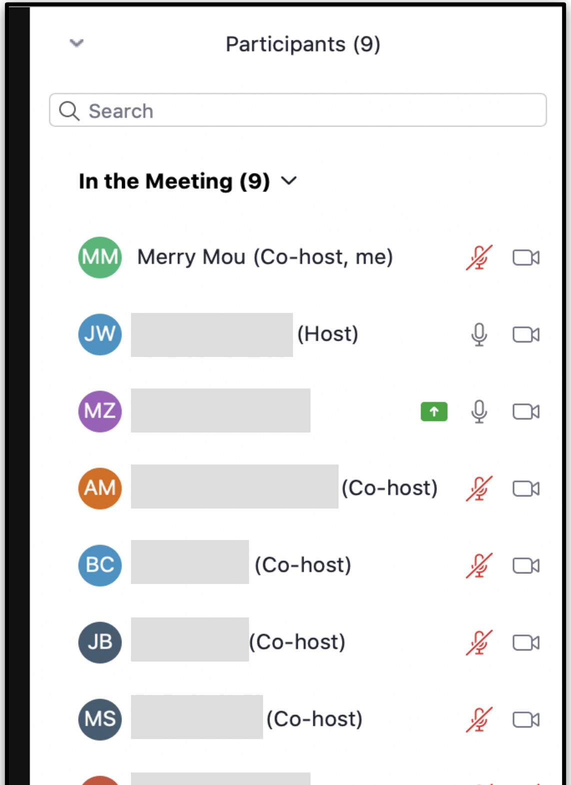
Sharing Meeting Key



Key Rotation



Participant List



Participants (9)

Search

In the Meeting (9)

MM Merry Mou (Co-host, me)

JW [redacted] (Host)

MZ [redacted]

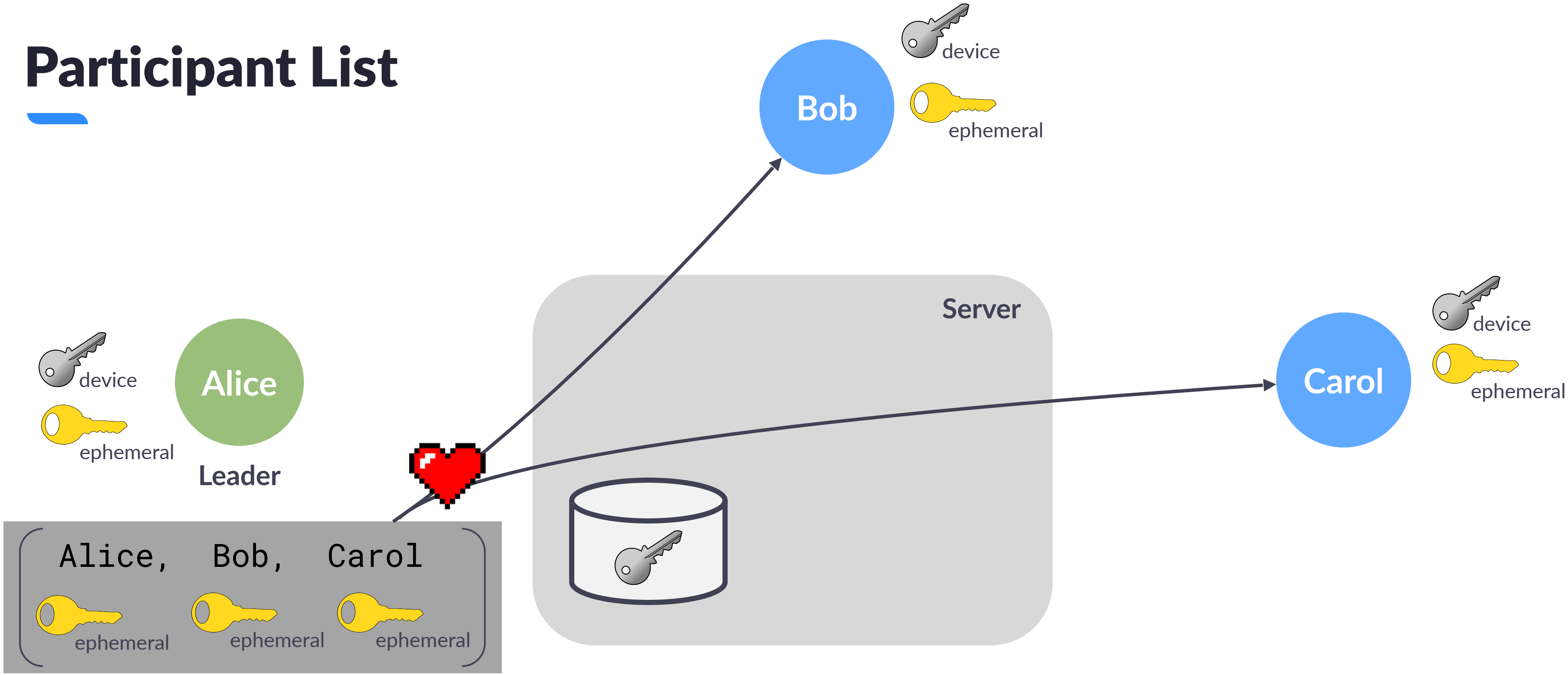
AM [redacted] (Co-host)

BC [redacted] (Co-host)

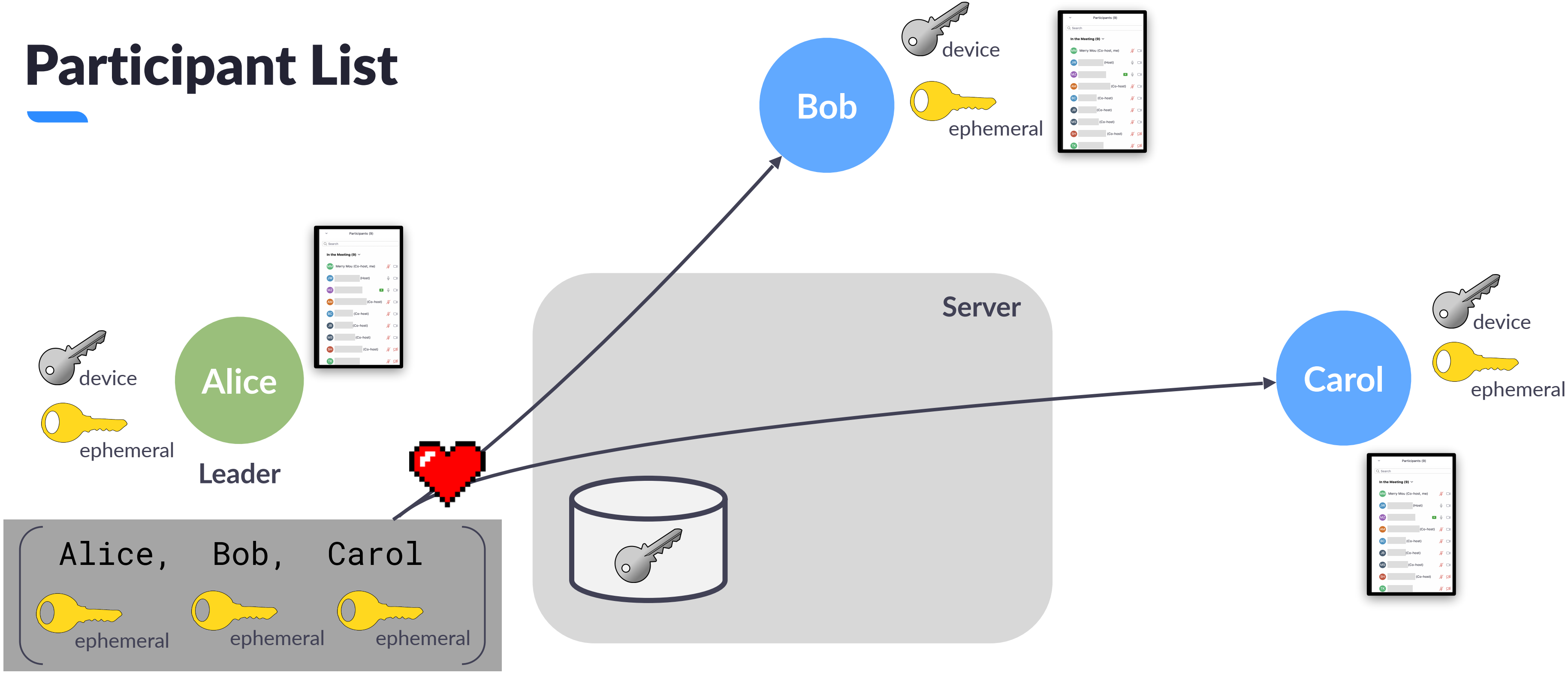
JB [redacted] (Co-host)

MS [redacted] (Co-host)

Participant List



Participant List

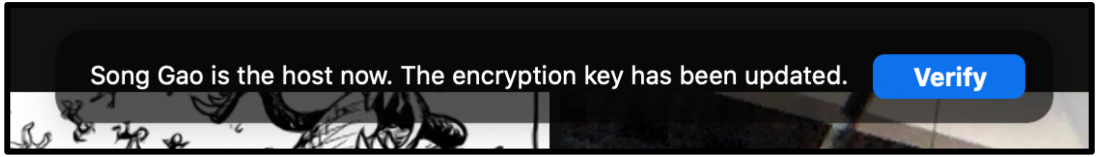


Participants (9)

Search

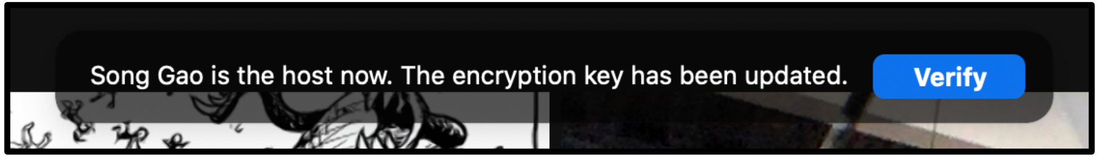
In the Meeting (9)

- MM Merry Mou (Co-host, me)
- JW [redacted] (Host)
- MZ [redacted]
- AM [redacted] (Co-host)
- BC [redacted] (Co-host)
- JB [redacted] (Co-host)
- MS [redacted] (Co-host)
- SH [redacted] (Co-host)
- TK [redacted]



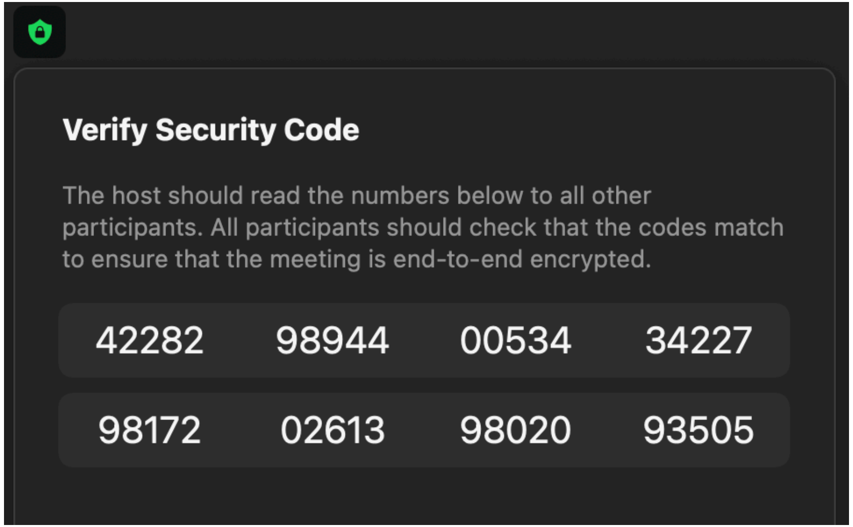
Song Gao is the host now. The encryption key has been updated.

Leader change notification



Song Gao is the host now. The encryption key has been updated.

Leader change notification



Verify Security Code

The host should read the numbers below to all other participants. All participants should check that the codes match to ensure that the meeting is end-to-end encrypted.

42282	98944	00534	34227
98172	02613	98020	93505

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

Delivering E2EE

Performance: Meeting Keys

Joining a meeting must be easy

Performance: Meeting Keys

Joining a meeting must be easy

Participants must get meeting keys

Performance: Meeting Keys

Joining a meeting must be easy

Participants must get meeting keys

Throttling rekeys

Performance: Participant List Heartbeats ❤

UI update frequency

zoom © 2021 Zoom Video Communications, Inc.

Performance: Participant List Heartbeats ❤️

UI update frequency

Network traffic

Performance: Participant List Heartbeats ❤

UI update frequency

Network traffic

Noticing notifications

Deploying E2EE

Client library interface

Deploying E2EE

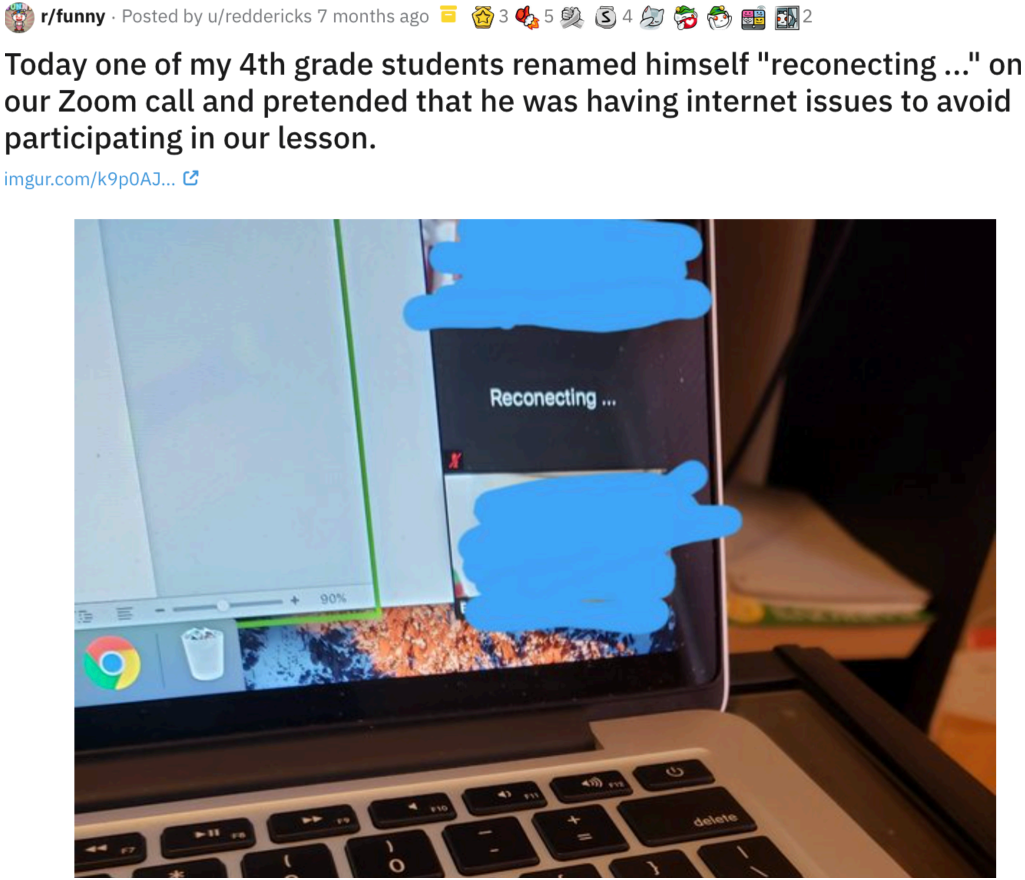
Client library interface

Stand-alone keyservers

Deploying E2EE

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

From Device Key to User Identity



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

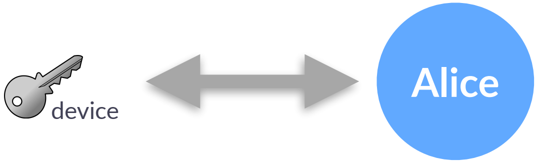
Today one of my 4th grade students renamed himself "reconecting ..." on our Zoom call and pretended that he was having internet issues to avoid participating in our lesson.

imgur.com/k9p0AJ...

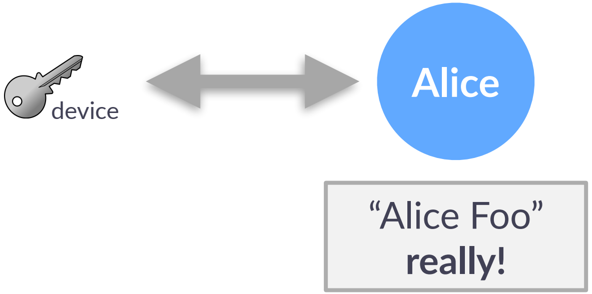
[redacted]

[redacted]

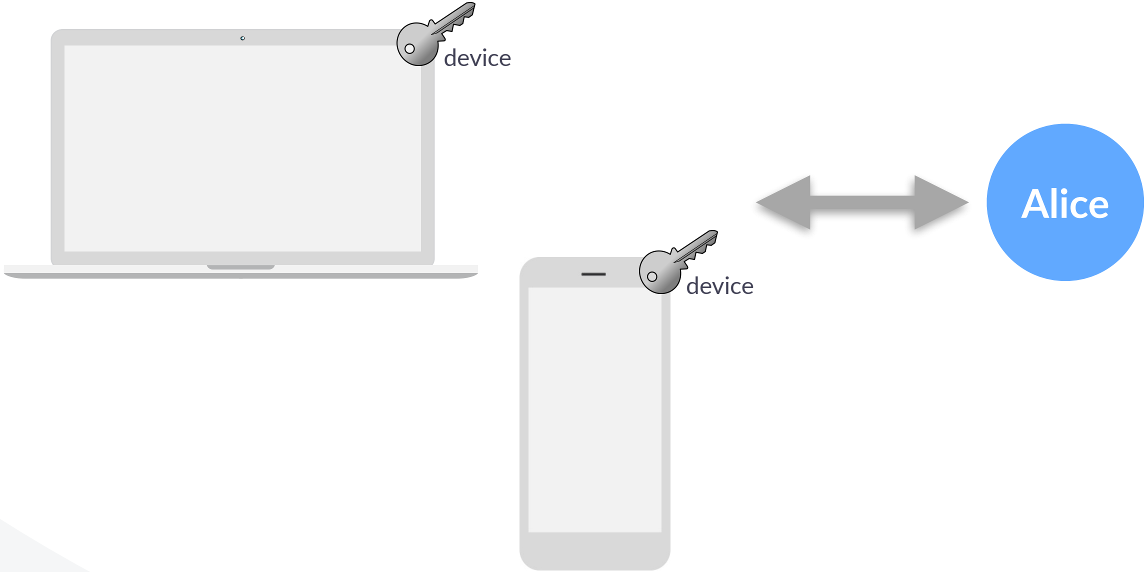
Building User Identity



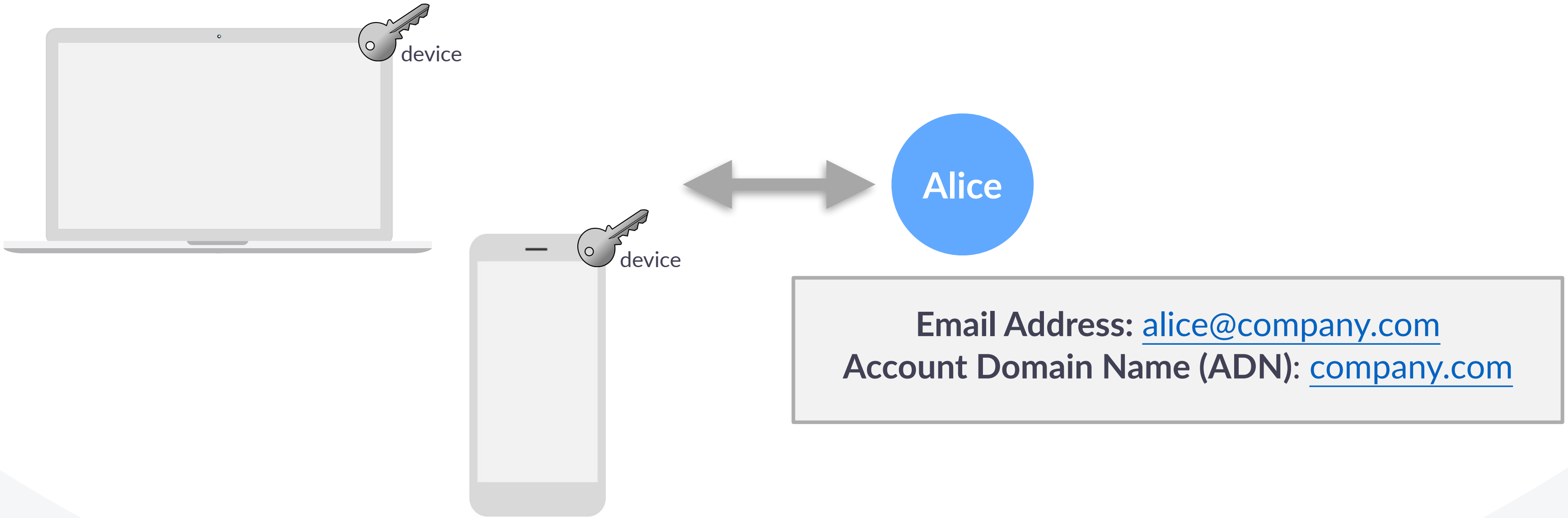
Building User Identity



A User is

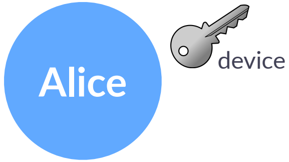


A User is



Email Address: alice@company.com
Account Domain Name (ADN): company.com

Verifying User Identity



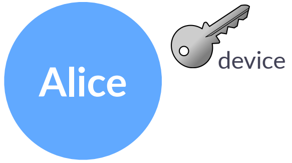
Email Address: alice@company.com
Account Domain Name (ADN): company.com

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

Contact Sync: Clients remember others' device keys

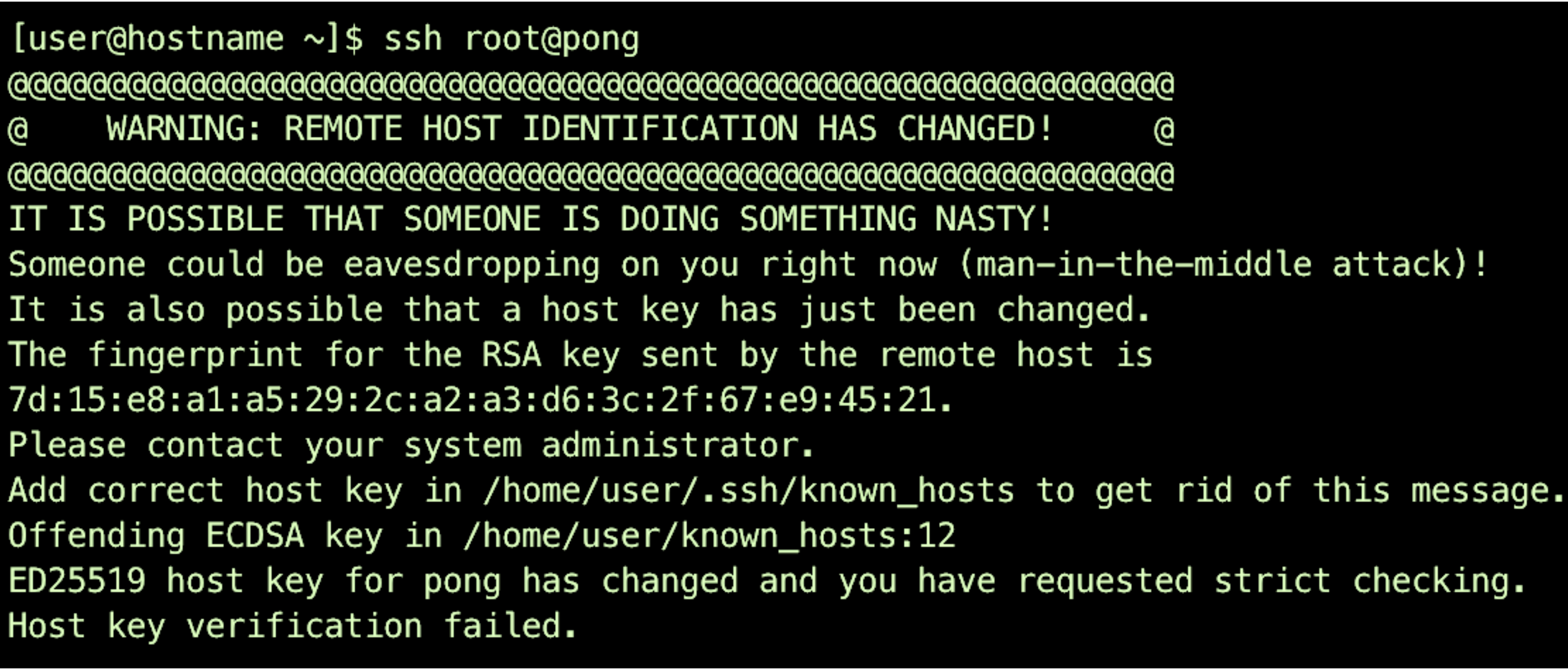
✓ Have **I seen** this user/device before?

Your device has never met Alice's device before!



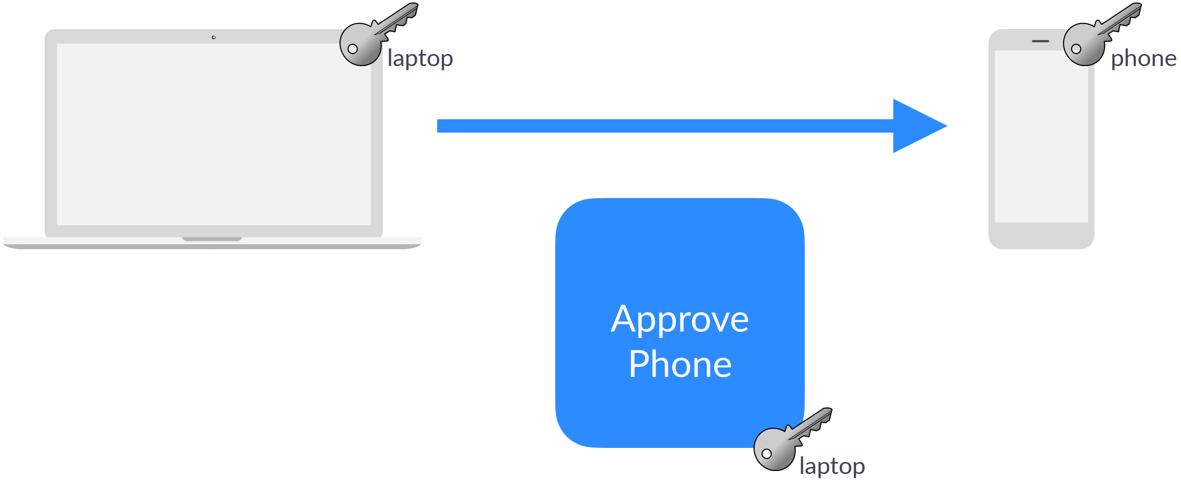
Email Address: alice@company.com
Account Domain Name (ADN): company.com

Contact Sync: Clients remember others’ device keys

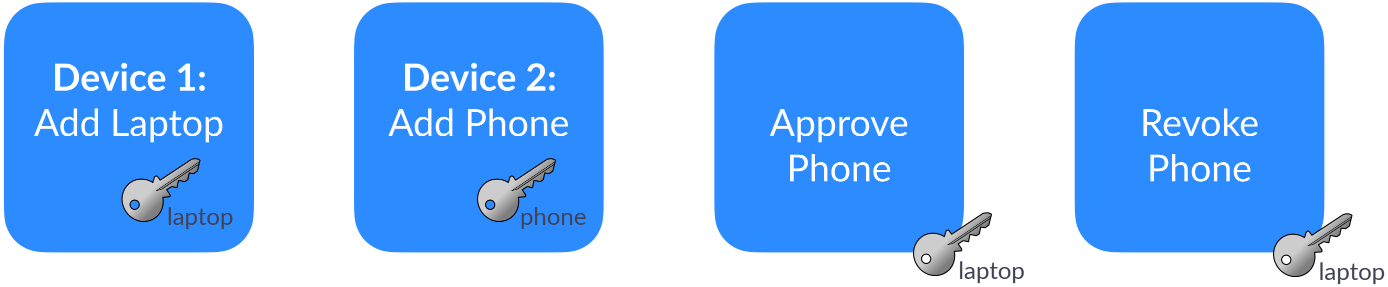


```
[user@hostname ~]$ ssh root@pong
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
7d:15:e8:a1:a5:29:2c:a2:a3:d6:3c:2f:67:e9:45:21.
Please contact your system administrator.
Add correct host key in /home/user/.ssh/known_hosts to get rid of this message.
Offending ECDSA key in /home/user/known_hosts:12
ED25519 host key for pong has changed and you have requested strict checking.
Host key verification failed.
```

Device Approvals



Device Approvals



Device 1:
Add Laptop

laptop

Device 2:
Add Phone

phone

Approve Phone

laptop

Revoke Phone

laptop

Contact Sync, Improved

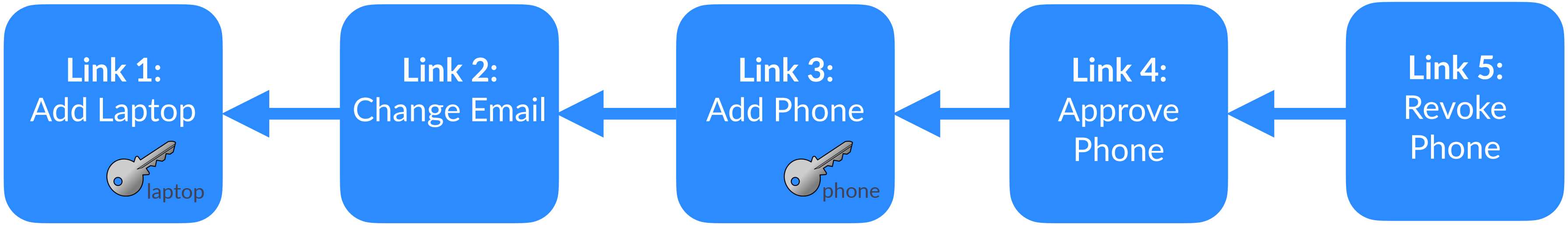
✓ Have **I seen** this user/device before?

You have never met **Alice** before!

Alice
device

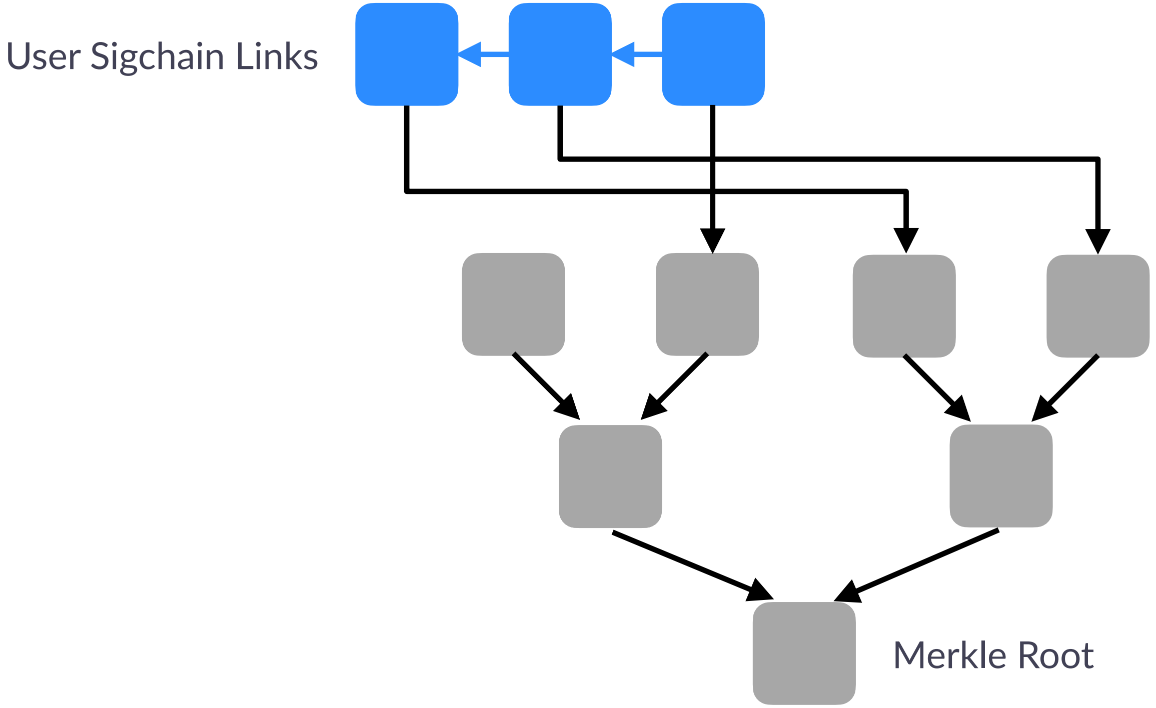
Email Address: alice@company.com
Account Domain Name (ADN): company.com

Auditable User Identity

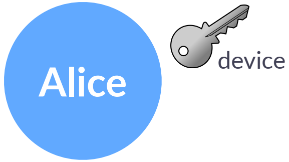


User **Sigchain**

Auditable User Identity



Verifying User Identity



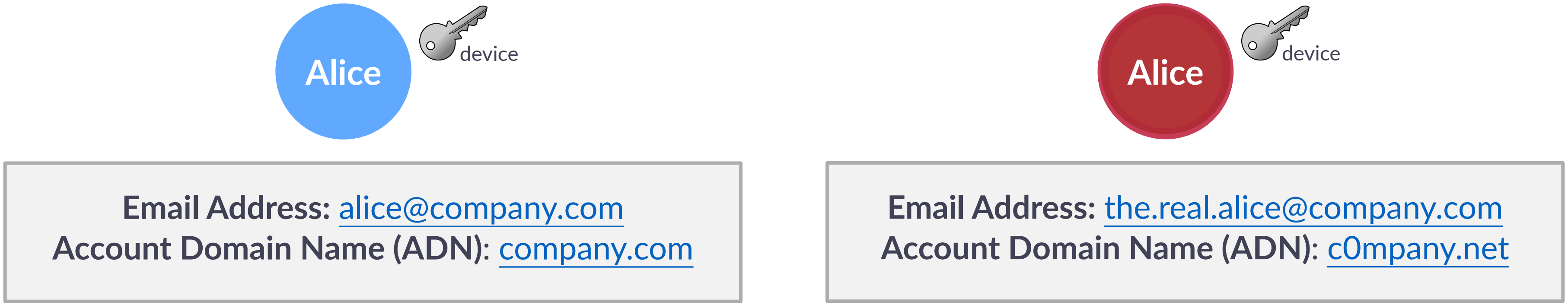
Email Address: alice@company.com
Account Domain Name (ADN): company.com

✓ Have **I seen** this user/device before?

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

Auditable User Identity

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

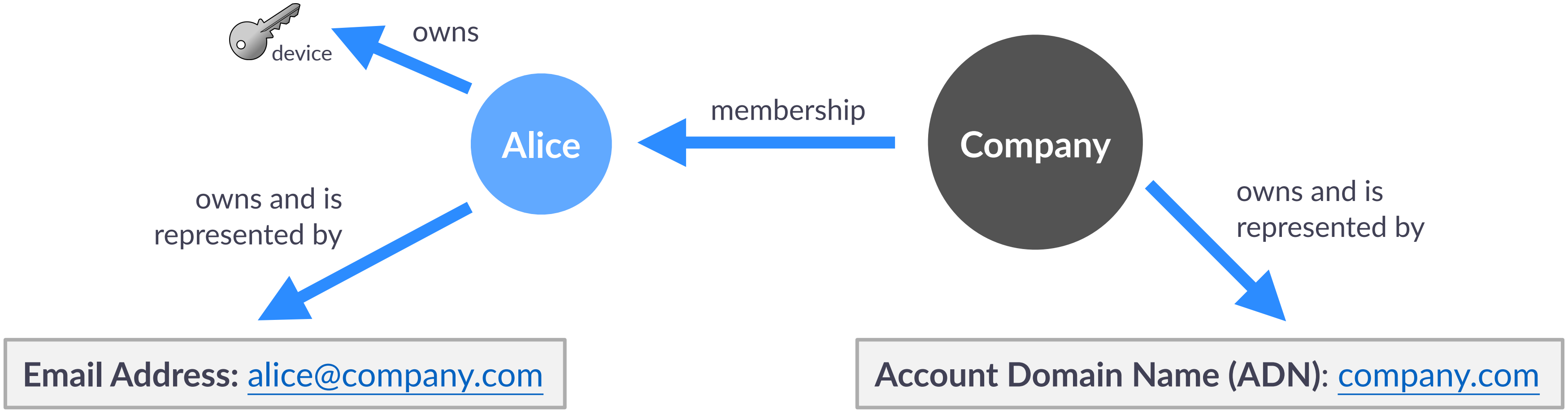


Email Address: alice@company.com
Account Domain Name (ADN): company.com

Email Address: the.real.alice@company.com
Account Domain Name (ADN): c0mpany.net

Auditable User Identity

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

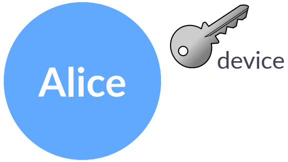


Email Address: alice@company.com

Account Domain Name (ADN): company.com

IDP-Backed User Identity

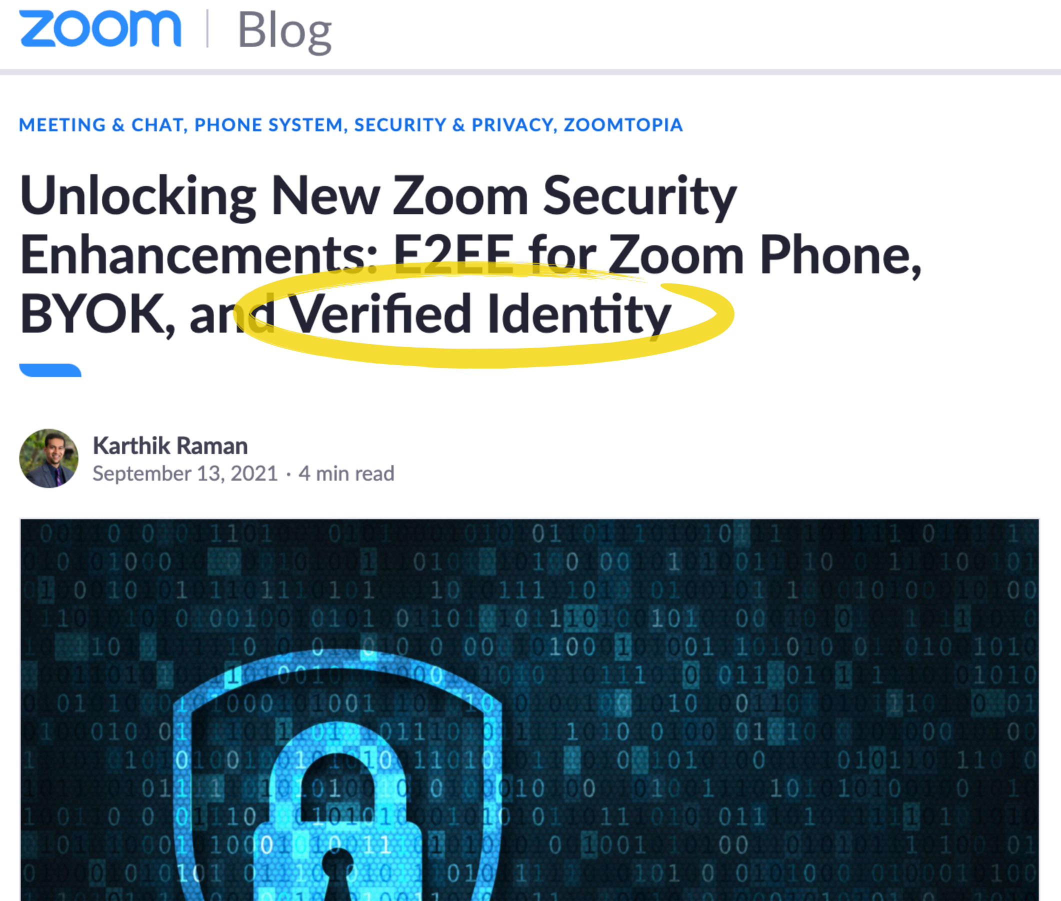
✓ Do I trust the **email** and **ADN** associated with this user?



Email Address: alice@company.com
Account Domain Name (ADN): company.com

backed by **Identity Provider (IDP) domain:**
company.idp.com

IDP-Backed User Identity



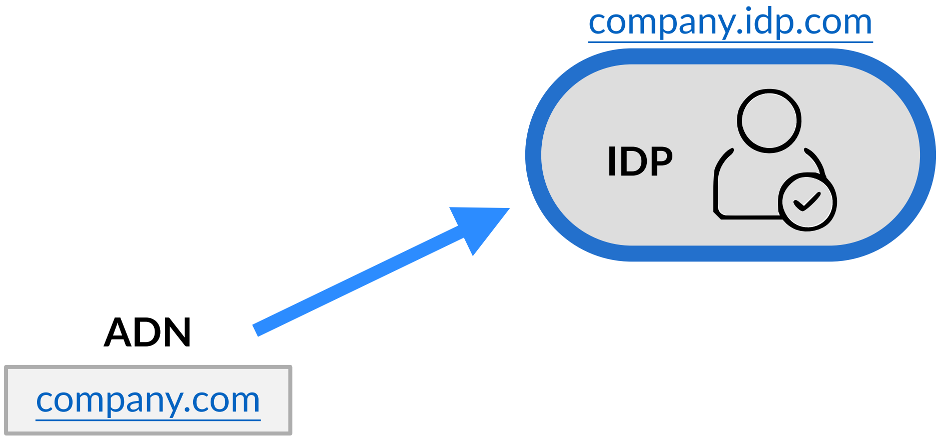
zoom | Blog

MEETING & CHAT, PHONE SYSTEM, SECURITY & PRIVACY, ZOOMTOPIA

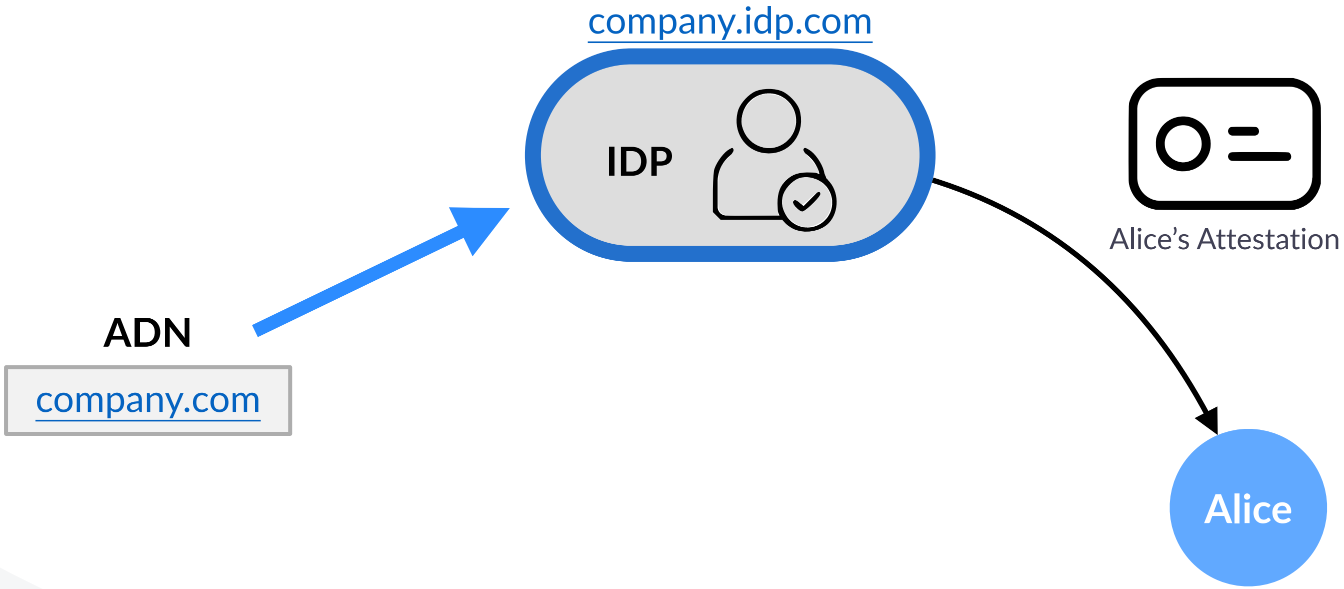
Unlocking New Zoom Security Enhancements: E2EE for Zoom Phone, BYOK, and Verified Identity

Karthik Raman
September 13, 2021 · 4 min read

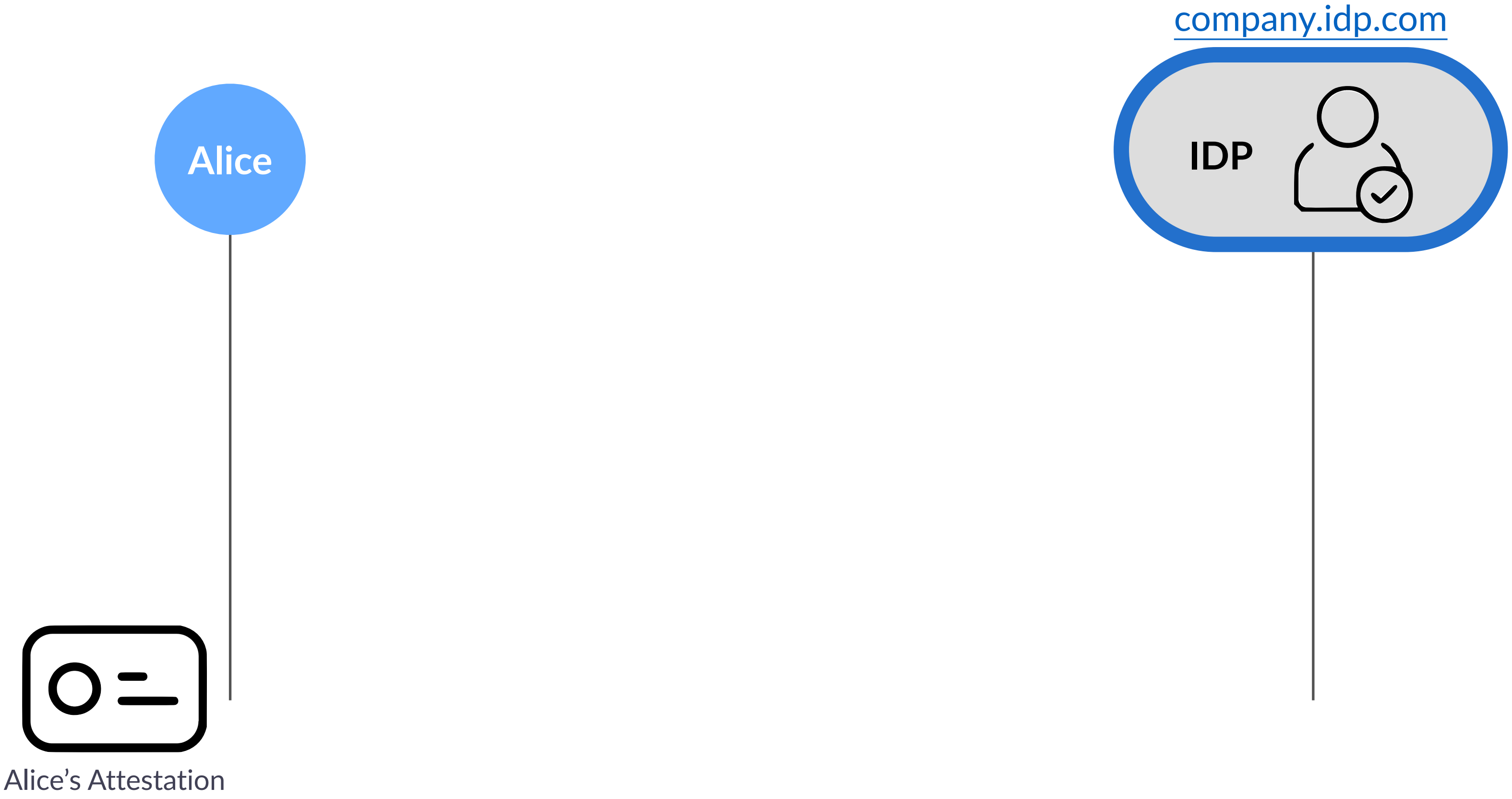
IDP-Backed User Identity



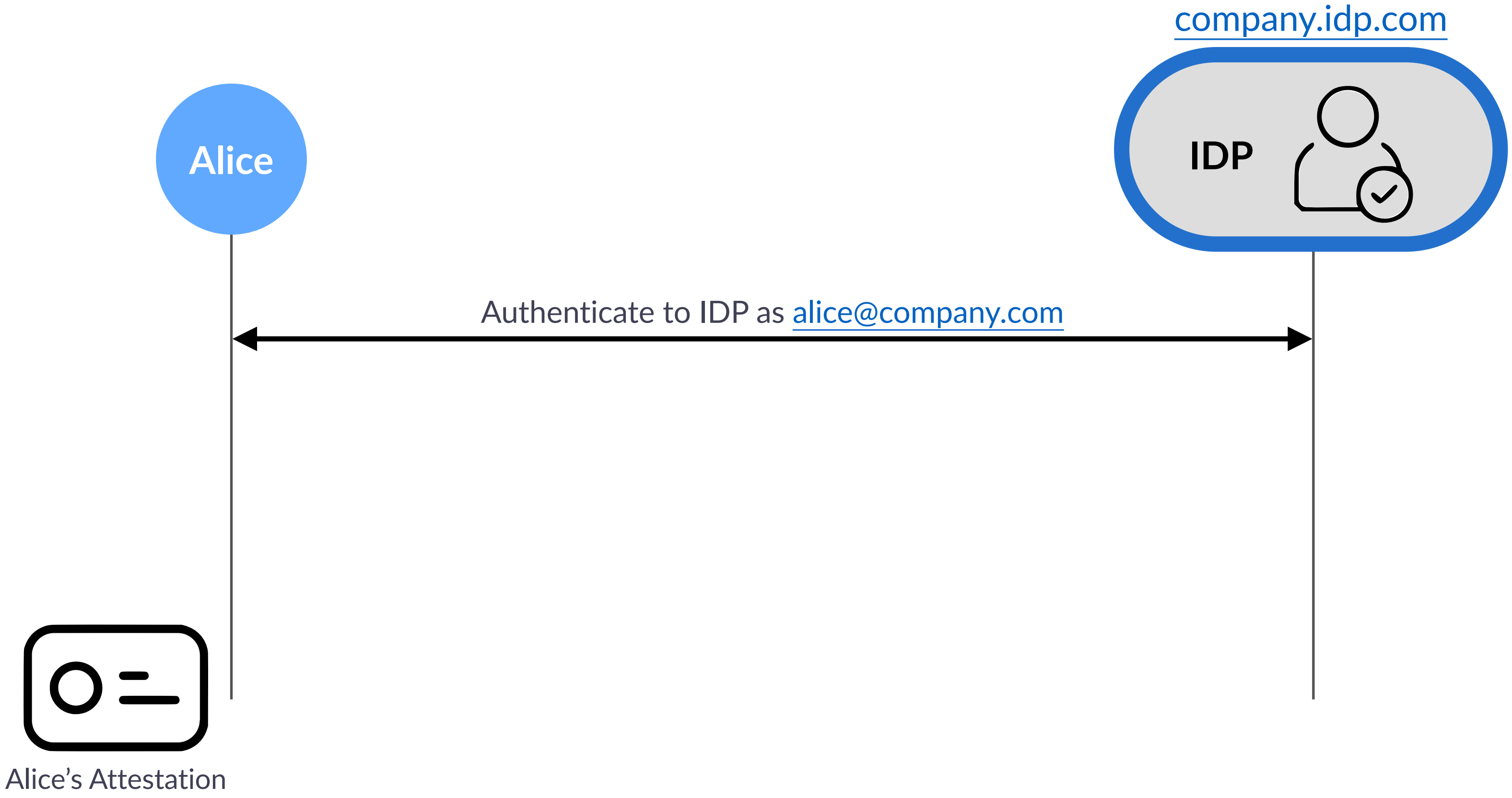
IDP-Backed User Identity



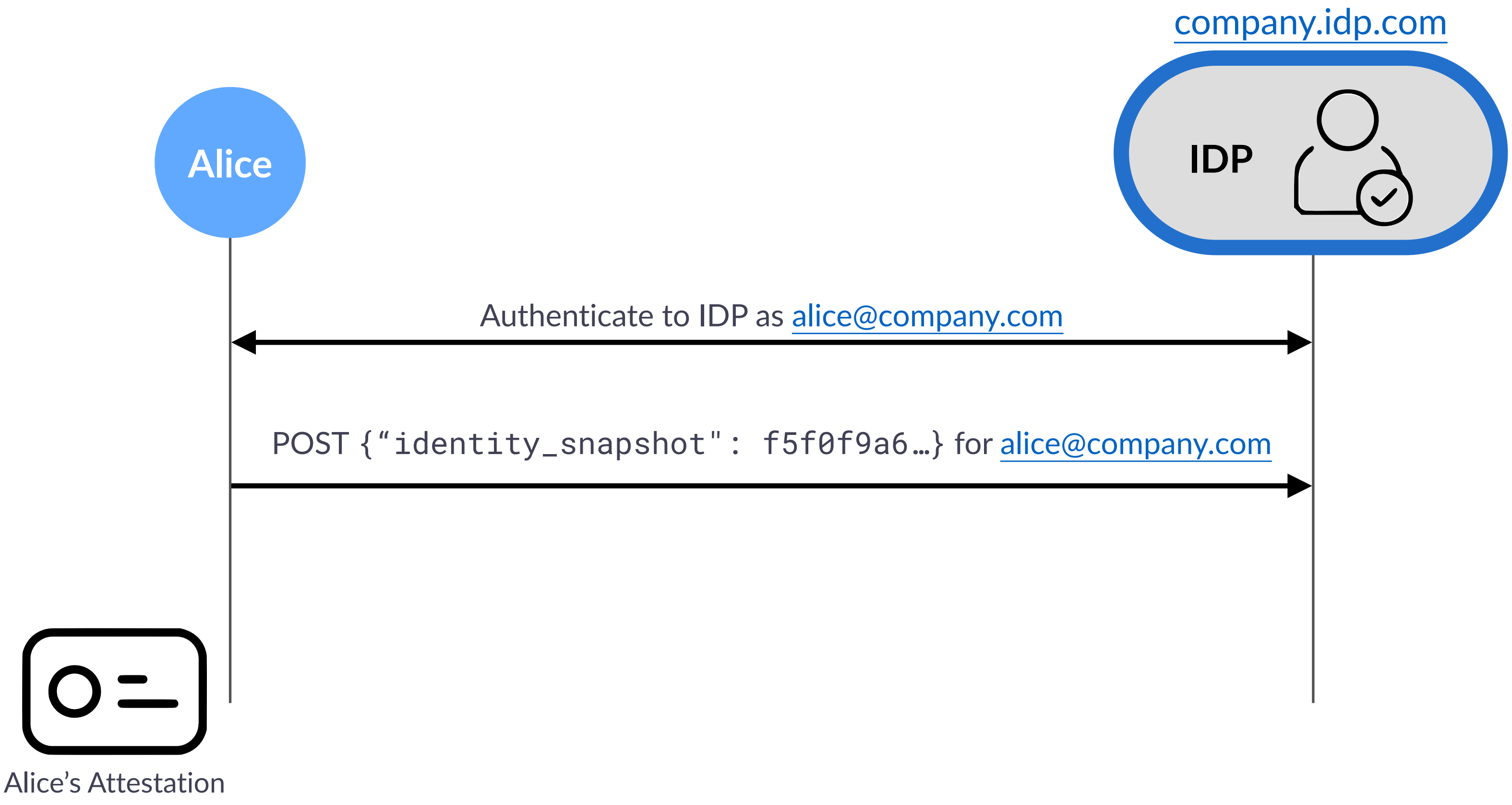
Obtaining IDP-Backed User Identity



Obtaining IDP-Backed User Identity



Obtaining IDP-Backed User Identity



company.idp.com

Alice

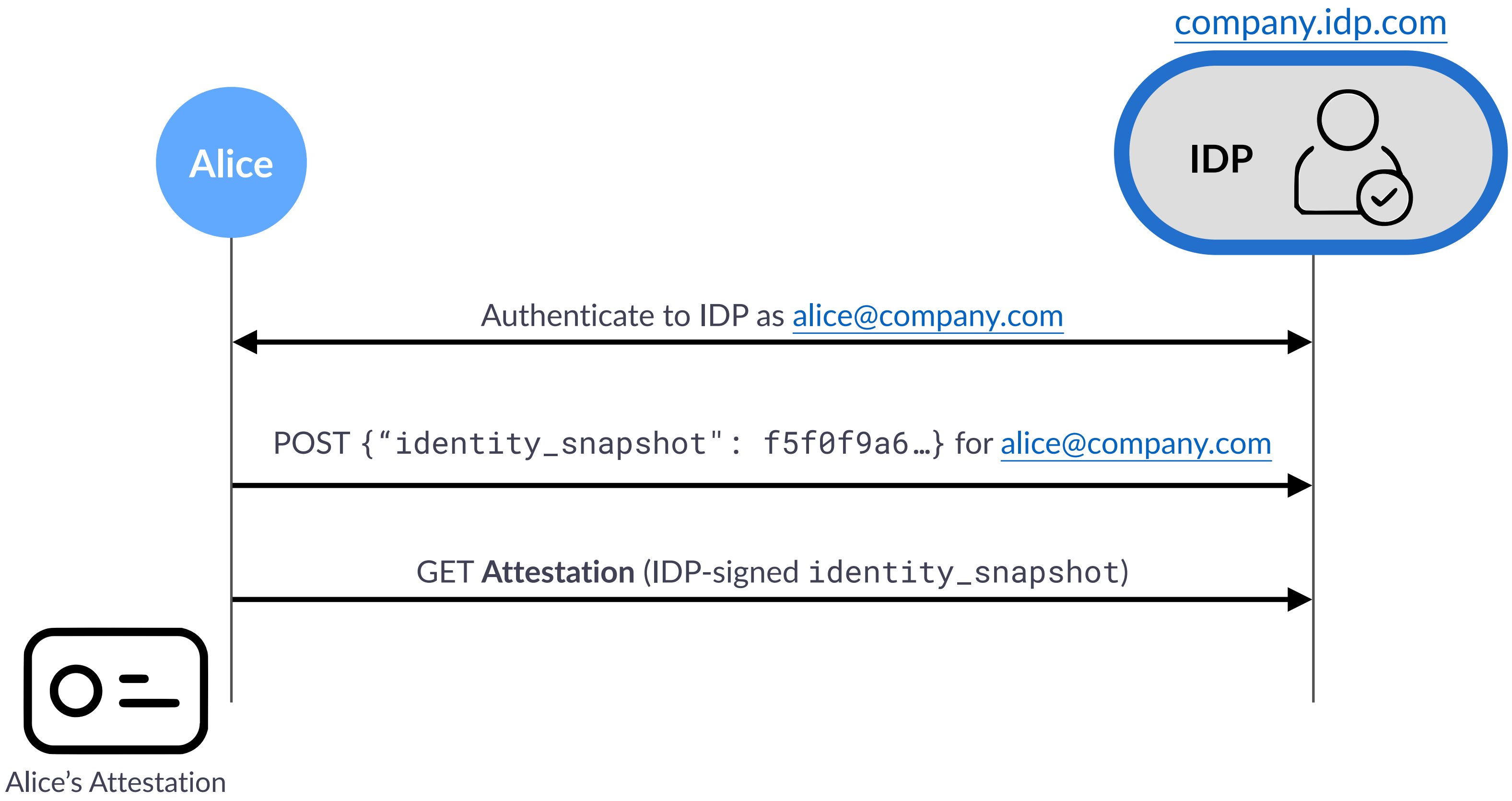
IDP

Authenticate to IDP as alice@company.com

POST {“identity_snapshot": f5f0f9a6…} for alice@company.com

Alice’s Attestation

Obtaining IDP-Backed User Identity



company.idp.com

Alice

IDP

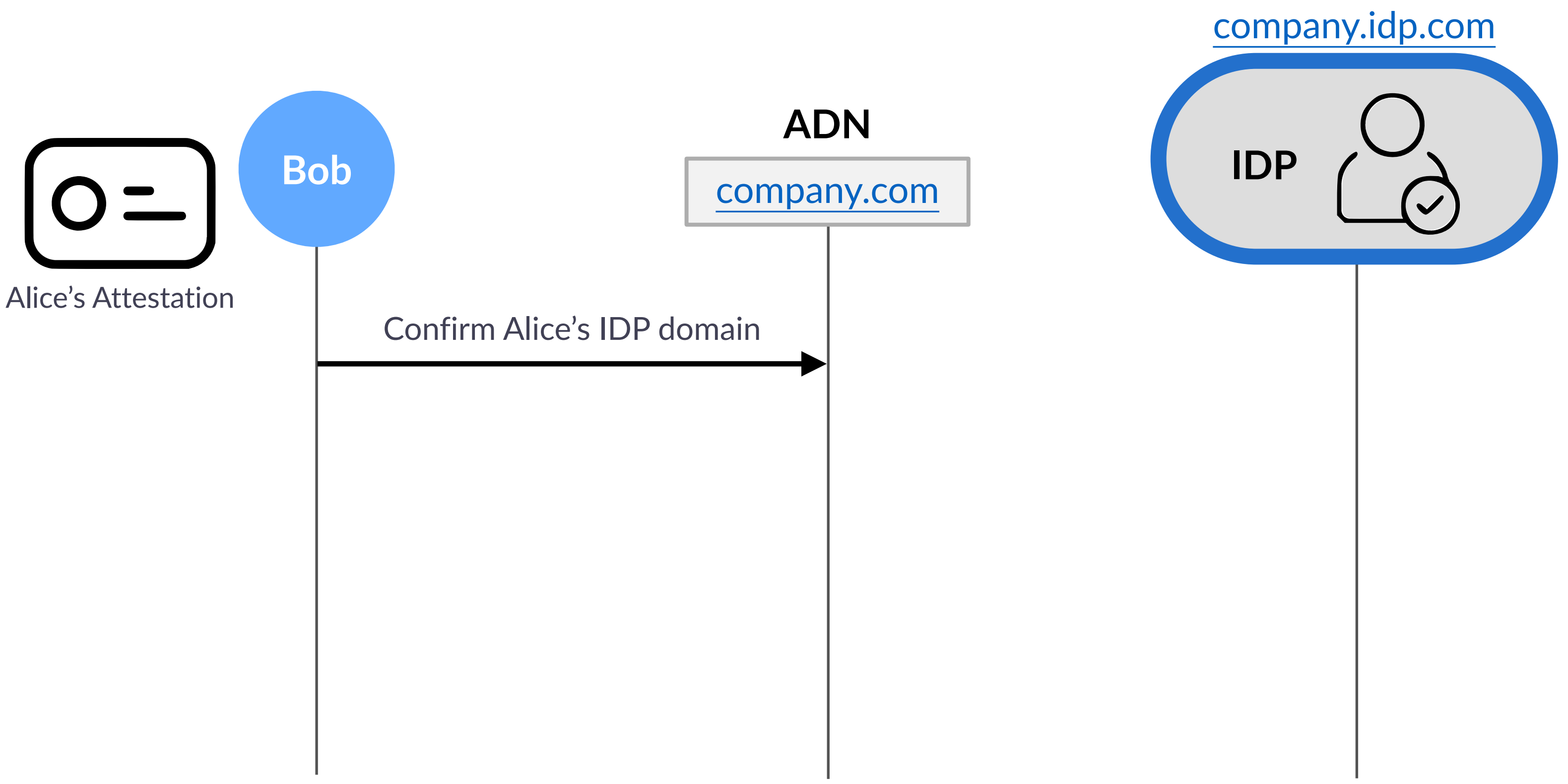
Authenticate to IDP as alice@company.com

POST {“identity_snapshot": f5f0f9a6…} for alice@company.com

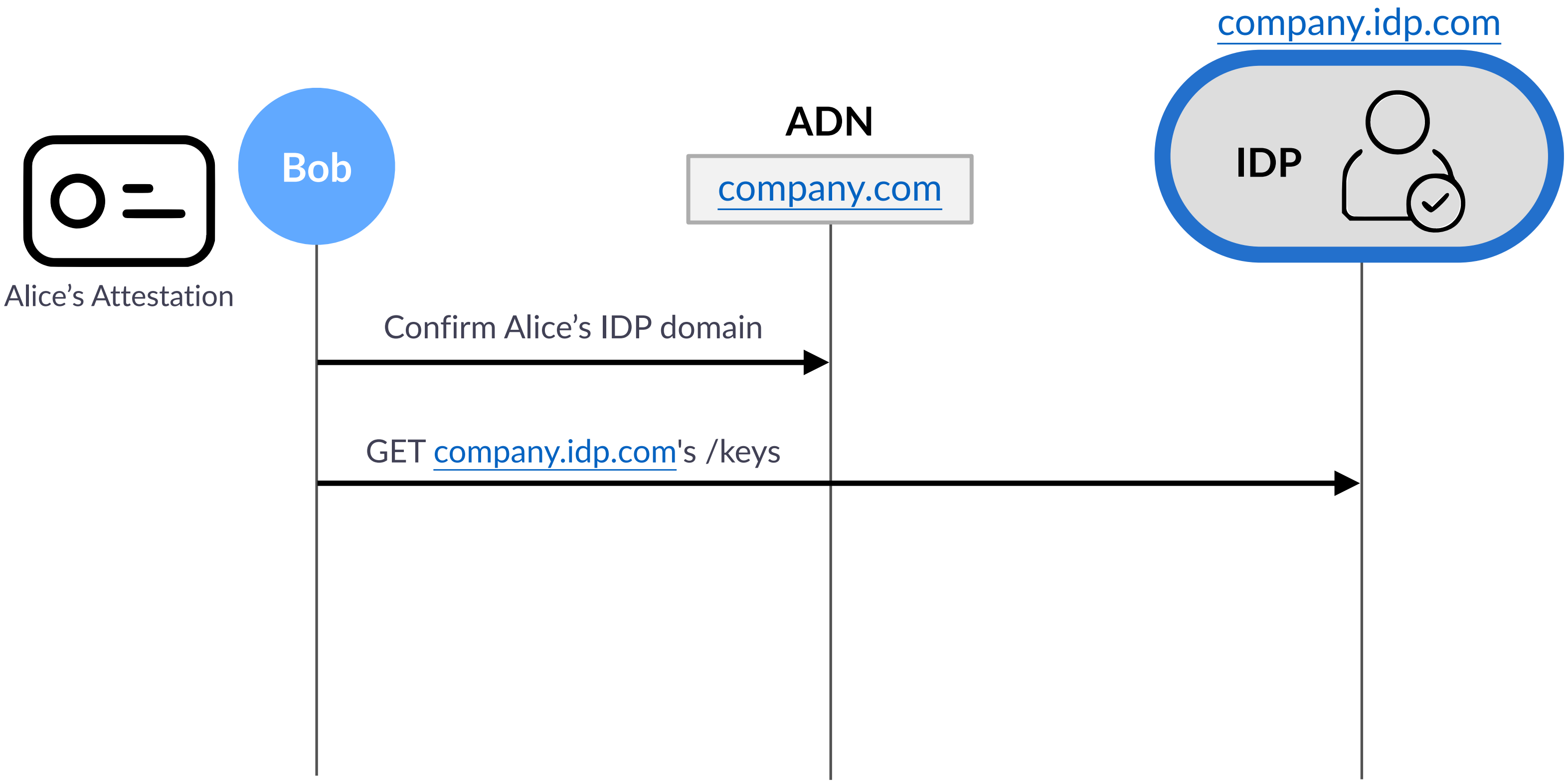
GET **Attestation** (IDP-signed identity_snapshot)

Alice’s Attestation

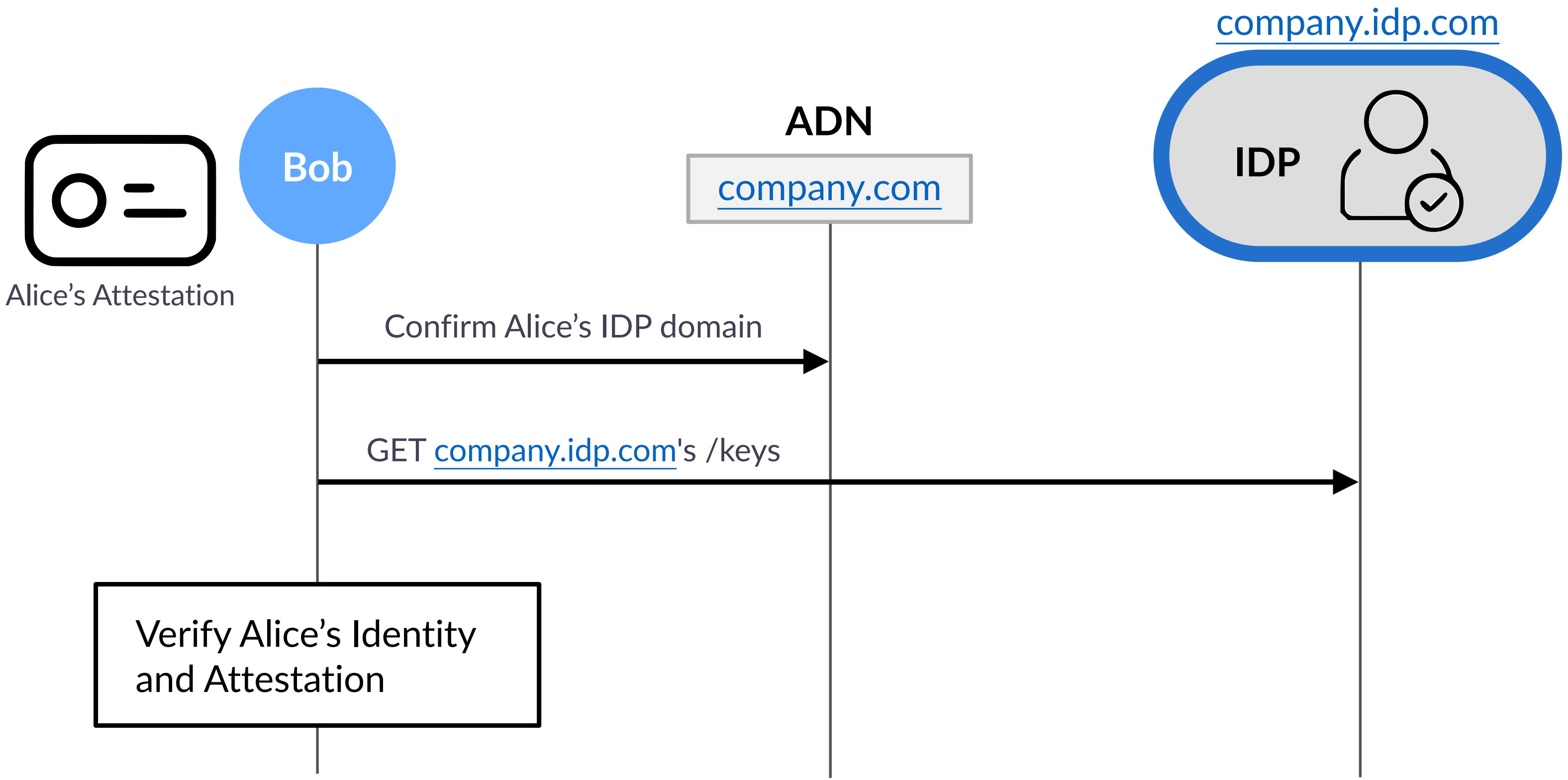
Verifying IDP-Backed User Identity



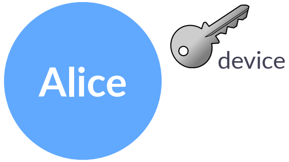
Verifying IDP-Backed User Identity



Verifying IDP-Backed User Identity


company.idp.com
Alice’s Attestation
Bob
ADN
company.com
IDP
Confirm Alice’s IDP domain
GET company.idp.com's /keys
Verify Alice’s Identity and Attestation

Verifying User Identity



Email Address: alice@company.com
Account Domain Name (ADN): company.com

✓ Have **I seen** this user/device before?

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

Multiple Security Mechanisms

Contact Sync and IDP complement each other

Third-party IDP attestations help prevent impersonations

Multi-device user identity is a powerful foundation

Conclusion

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

- Multi-device user identity
- Improved "TOFU"
- IDP-backed identity

Building E2EE in the real world

Existing architectural constraints

Building E2EE in the real world

Existing architectural constraints

Phased releases

Building E2EE in the real world

- Existing architectural constraints
- Phased releases
- End-user experience

zoom

Q

A

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