element

Joining the conversation

Balancing privacy with usability for encrypted messages

Richard van der Hoff, Element Crypto team

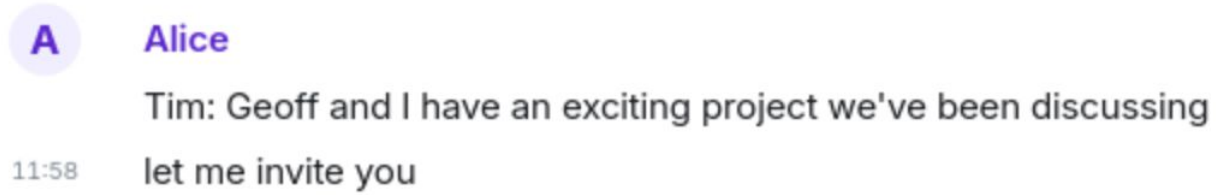
Sharing room keys for past messages

element

- **What this is, and why we are doing it**
- How not to solve it
- How we are solving it
- What's taking so long
- What's next

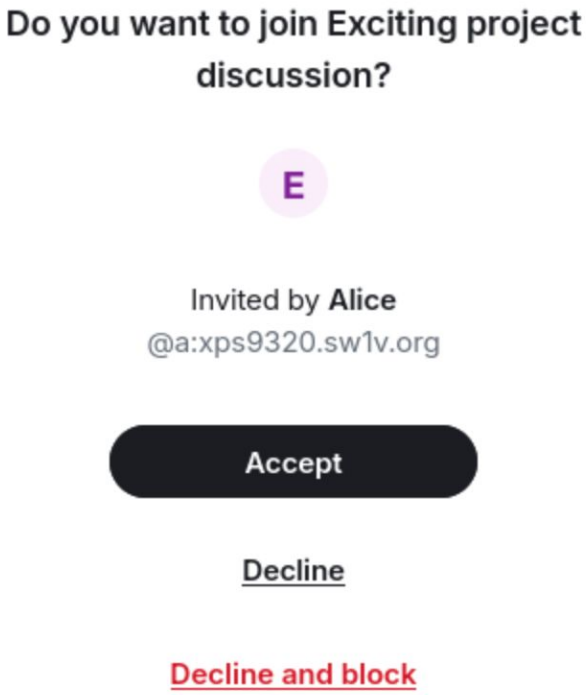
The situation today

element

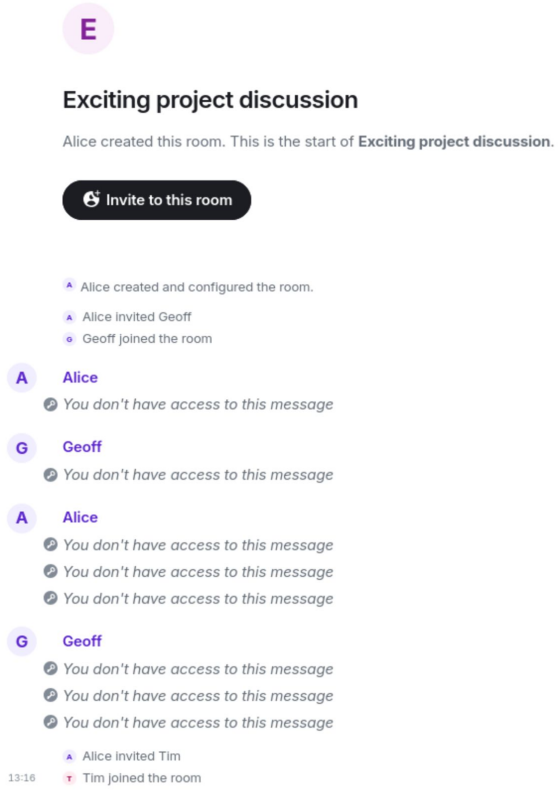


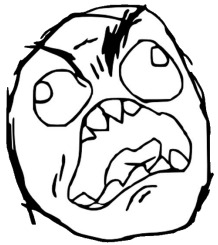
The situation today

element



The situation today





Sharing room keys for past messages

element

- What this is, and why we are doing it
- **How not to solve it**
- How we are solving it
- What's taking so long
- What's next

How not to solve it

element

- MSC3061
- Shared key store
- Request the keys after join

How not to solve it

element

- MSC3061
  - This used to work!

How not to solve it

element

- MSC3061
  - This used to work!
  - But:
    - Poor performance
    - Terrible security

How not to solve it

element

- Per-room shared key store
  - Just give new members access to an encrypted store
  - Might even replace per-user key backup?

How not to solve it

element

- Per-room shared key store
  - Just give new members access to an encrypted store
  - Might even replace per-user key backup?
  - But:
    - Who is responsible for populating the store?
    - What about federation?
    - What happens when someone leaves the room?

How not to solve it

- Request the keys after join
  - “Tim is requesting keys to the room”

How not to solve it

element

- Request the keys after join
  - “Tim is requesting keys to the room”
  - But:
    - Manual: automating the response is unsafe
    - Do we broadcast a request, or target it?
    - Vulnerable to social engineering attacks
  - We might need this anyway

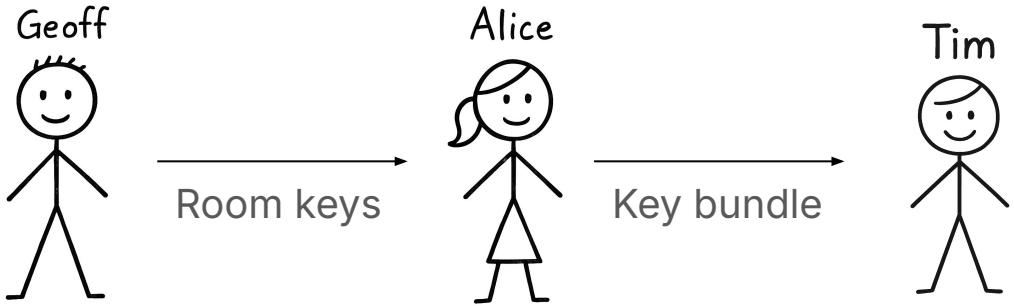
Sharing room keys for past messages

element

- What this is, and why we are doing it
- How not to solve it
- **How we are solving it**
- What's taking so long
- What's next

How we are solving it

- MSC4268
- MSC3061, except:
  - Only verified devices
  - Pack the keys in a single blob, and upload as encrypted attachment



How we are solving it

element

Demo time!

Sharing room keys for past messages

element

- What this is, and why we are doing it
- How not to solve it
- How we are solving it
- **What's taking so long**
- What's next

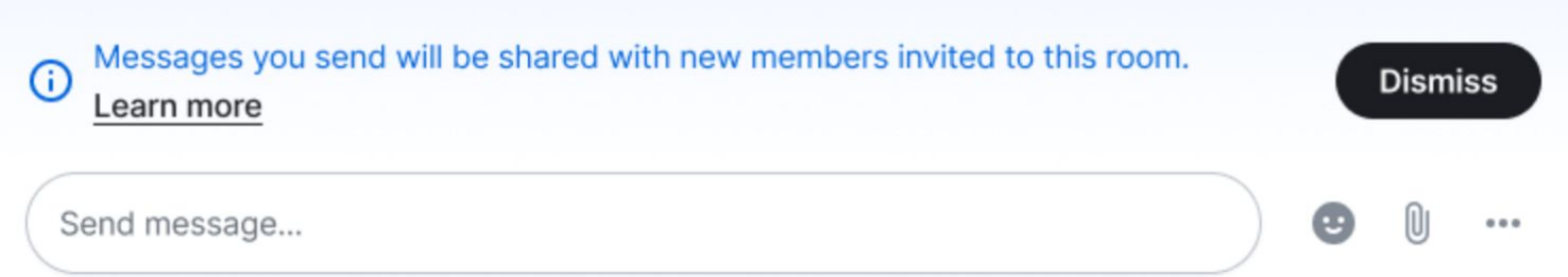
What’s taking so long

element

- Managing sender expectations
  - Different users have very different expectations

What’s taking so long

- Managing sender expectations
  - Different users have very different expectations



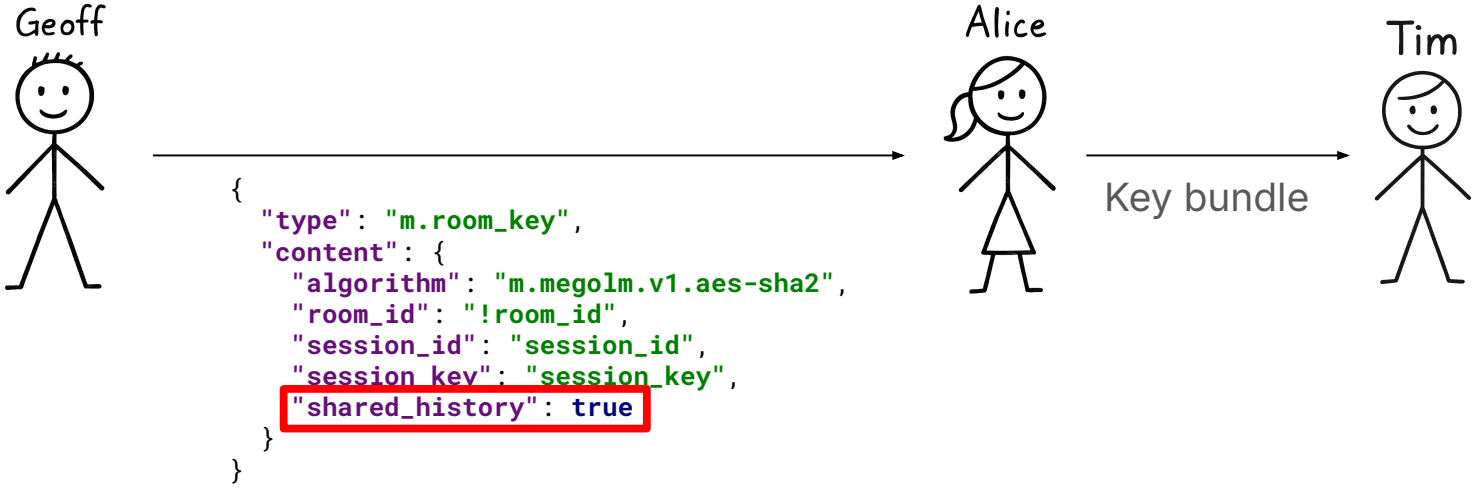
What’s taking so long

element

- Which keys are safe to share?
  - E2EE: We can’t trust the server

What's taking so long

- Which keys are safe to share?
  - E2EE: We can't trust the server
  - Depends on *the original sender's* view of the "history visibility"



- Requires support from everyone in the room

What’s taking so long

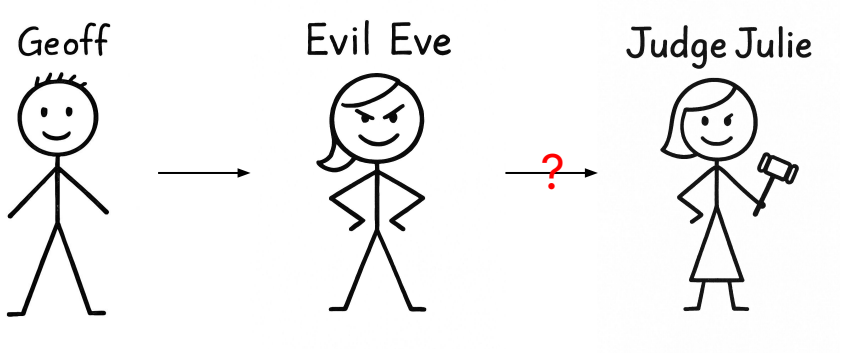
element

- Fixing the security hole
  - Only share keys with verified devices
  - [Exclude Insecure Devices is coming!]

What's taking so long

element

- Provenance of keys
  - Deniability: it is impossible for Evil Eve to prove to a third party that Geoff sent a message



  - So it is also impossible for Alice to prove to Tim that Geoff sent a message

What’s taking so long

element

Bob Bobbert

Here’s a text message

Alice shared this message

Erica Watts

Here’s a text message here’s a text message. Here’s a text message here’s a text message. Here’s a text message here’s a text message. Here’s a text message here’s a text message. Here’s a text message here’s a text message.

Alice shared this message

What’s taking so long

element

- … and more:
  - Avoid DoS attacks as recipient
  - Avoid sharing partial history
  - Merge incoming sessions
  - Resuming import on restart
  - Cleaning up used key bundles

Sharing room keys for past messages

element

- What this is, and why we are doing it
- How not to solve it
- How we are solving it
- What's taking so long
- **What's next**

What’s next

element

- Finish the implementation
  - https://github.com/element-hq/element-meta/issues/2829

What's next

element

- Restricted rooms
  - **Probably**: a request to other users to share history
  - May need to wait for cryptographically-constrained room membership

element

Questions