

# Invisible Crypto<sup>1</sup>

Can Matrix be both secure and easy to use?

Andy Balaam, Element Crypto Team

<sup>1</sup>"Crypto" = "Encryption"

**This vital work is being done by Element**

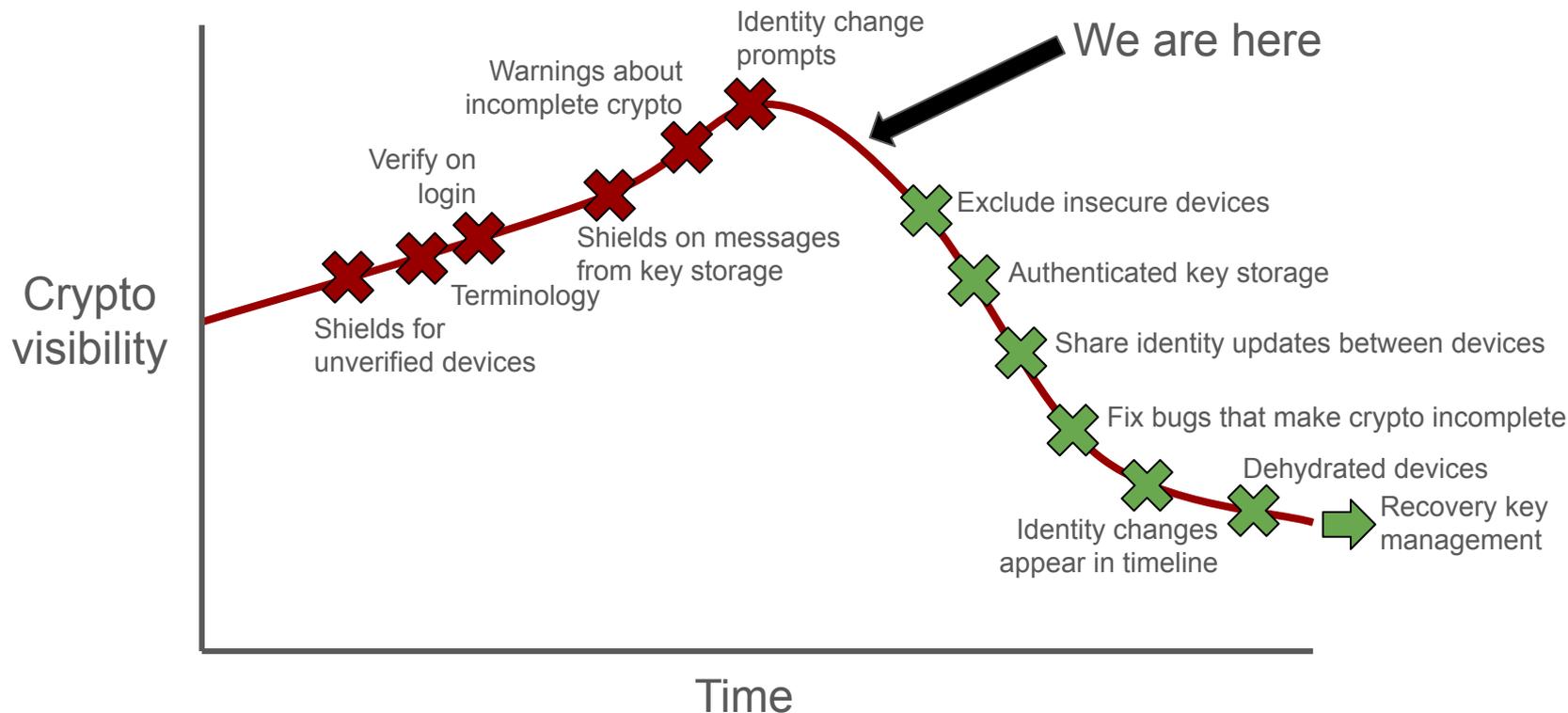
**It is 100% Free/Open Source Software**

**Much of it is directly donated to the Matrix Foundation**

# Invisible Crypto

- **The vision: secure and easy to use**
- Making everything worse
- Making everything better
- Important announcement

# Getting over the hump



# The vision: secure and easy to use

- Your information should be safe and private
- You should not need deep knowledge of encryption
- You should be secure by default
- It should be clear what is happening
- We should nudge you towards more secure practice

*a peaceful, hassle-free experience of encrypted messaging*

# The vision: secure and easy to use

"Matrix cannot be secure unless it is easy to use"

# Invisible Crypto

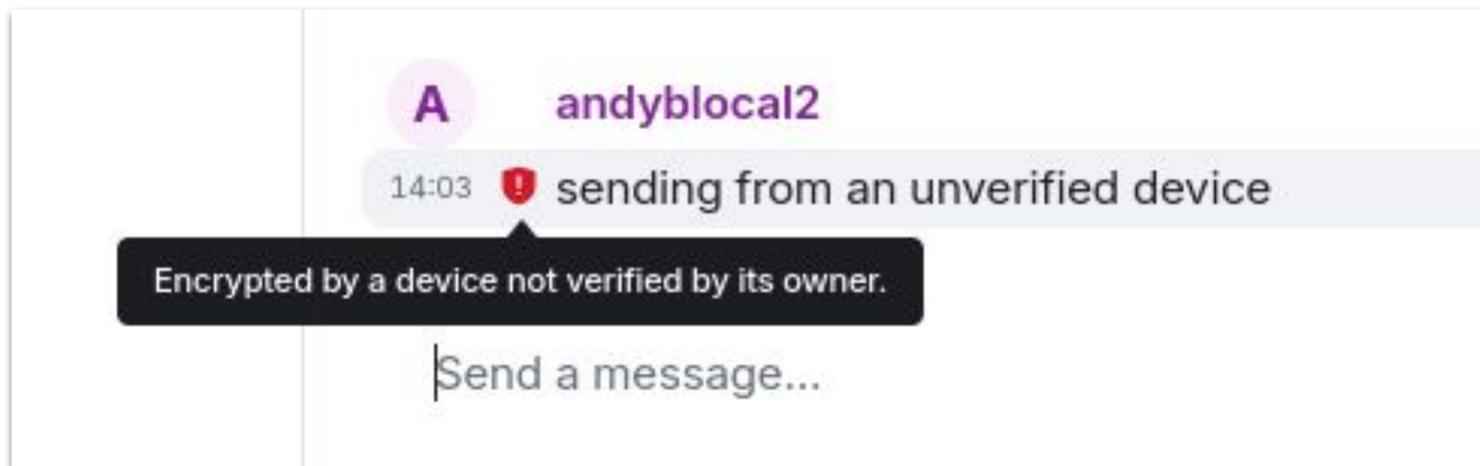
- The vision: secure and easy to use
- **Making everything worse**
- Making everything better
- Important announcement

# Making everything worse

- Encryption is temporarily becoming *more* visible
  - Warnings on messages from insecure devices
  - Encouraging device verification
  - Building a shared language to talk about encryption
  - Warnings if your device has incomplete setup
  - Warnings about the sender of a message if unsure
  - Warnings on messages decrypted via key storage
  - Pop-ups about user identity changes

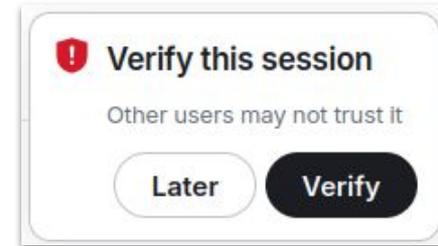
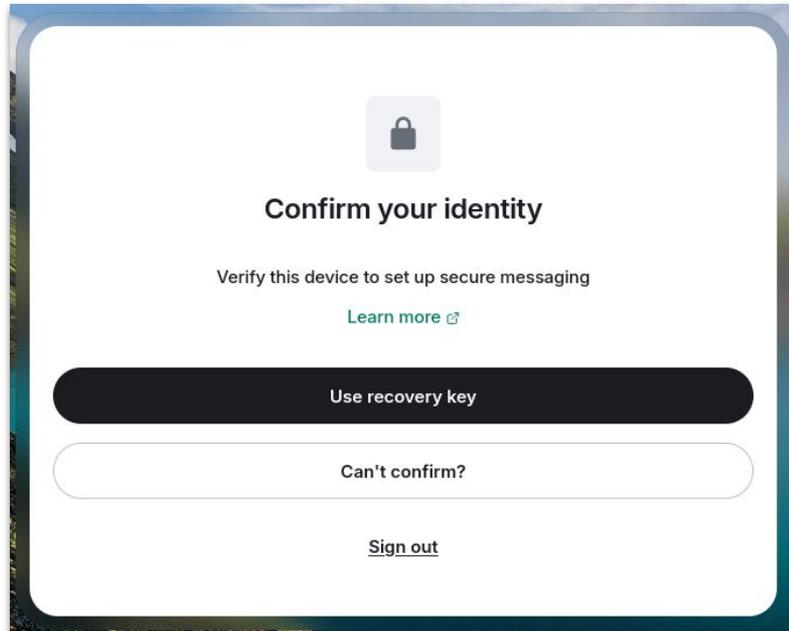
# Making everything worse

- Encryption is temporarily becoming *more* visible
  - Warnings on messages from insecure devices



# Making everything worse

- Encryption is temporarily becoming *more* visible
  - Encouraging device verification



# Making everything ~~worse~~ more visible

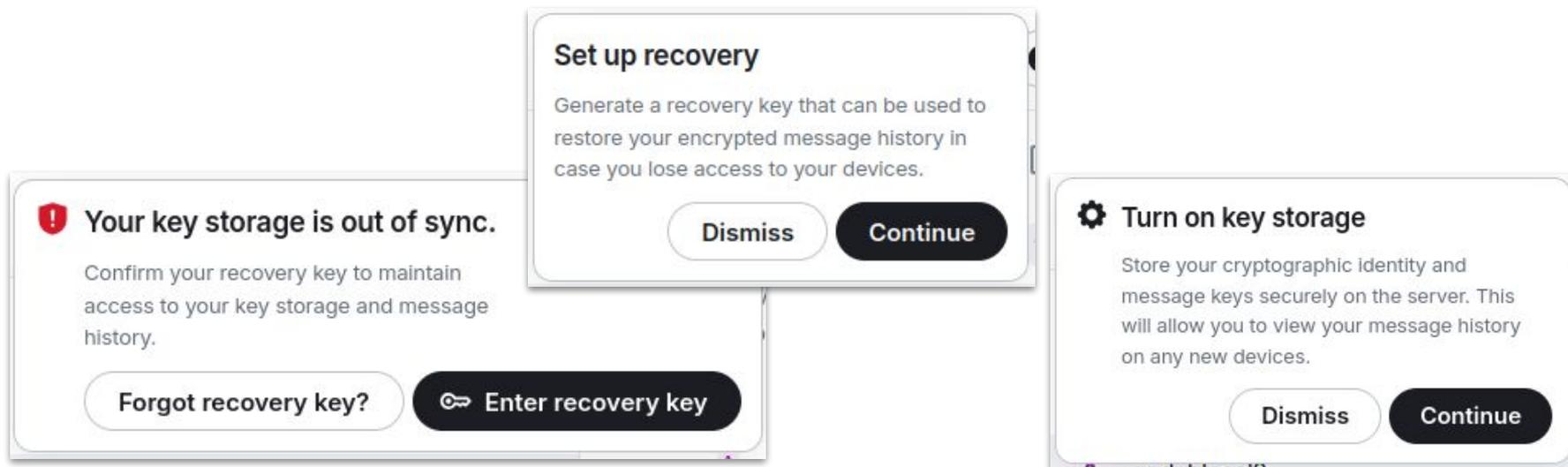


- Encryption is temporarily becoming *more* visible
  - Building a shared language to talk about encryption

The screenshot shows a GitHub pull request interface. At the top, there are navigation links: '15 Pull requests (545)', 'Actions', 'Projects (2)', and 'Settings'. The main title of the pull request is 'MSC4161: Crypto terminology for non-technical users #4161'. Below the title, it says 'Open andybalaam wants to merge 56 commits into main from andybalaam/crypto-terminology'. There are also links for 'Conversation (176)', 'Commits (56)', 'Checks (1)', and 'Files changed (1)'. A comment from 'andybalaam' is visible, dated 'Jun 27, 2024', with an 'edited' status. The comment text reads: 'Rendered Conflict of Interest declaration: I am employed by Element. This MSC was written as part of my work on the Element Cryptography team.' Below the comment, there are reaction counts: a smiley face with 20 reactions, a thumbs up with 6 reactions, a heart with 9 reactions, and a rocket with 1 reaction.

# Making everything worse

- Encryption is temporarily becoming *more* visible
  - Warnings if your device has incomplete setup



The image shows three overlapping mobile app warning dialog boxes. The top box is titled 'Set up recovery' and contains the text 'Generate a recovery key that can be used to restore your encrypted message history in case you lose access to your devices.' with 'Dismiss' and 'Continue' buttons. The bottom-left box is titled 'Your key storage is out of sync.' and contains the text 'Confirm your recovery key to maintain access to your key storage and message history.' with a 'Forgot recovery key?' link and an 'Enter recovery key' button. The bottom-right box is titled 'Turn on key storage' and contains the text 'Store your cryptographic identity and message keys securely on the server. This will allow you to view your message history on any new devices.' with 'Dismiss' and 'Continue' buttons.

**Set up recovery**

Generate a recovery key that can be used to restore your encrypted message history in case you lose access to your devices.

**Your key storage is out of sync.**

Confirm your recovery key to maintain access to your key storage and message history.

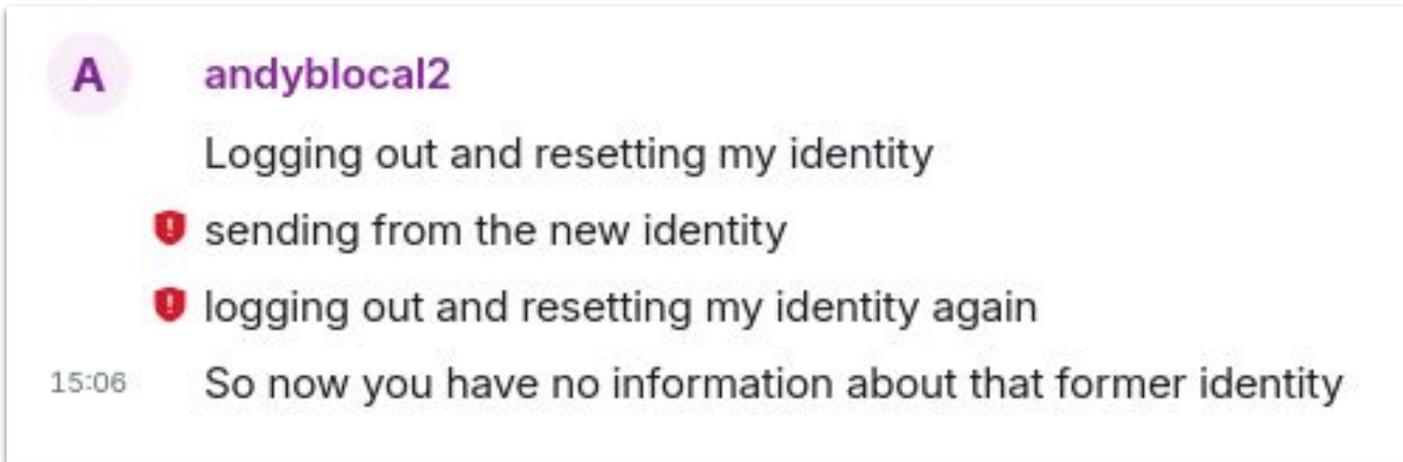
Forgot recovery key? Enter recovery key

**Turn on key storage**

Store your cryptographic identity and message keys securely on the server. This will allow you to view your message history on any new devices.

# Making everything worse

- Encryption is temporarily becoming *more* visible
  - Warnings about the sender of a message if unsure



A

**andyblocal2**

Logging out and resetting my identity

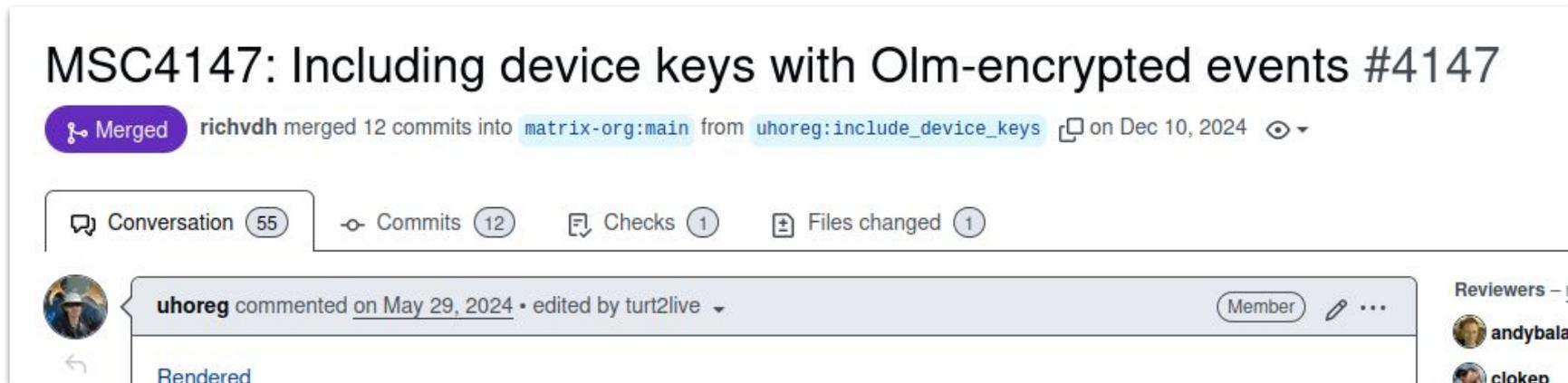
! sending from the new identity

! logging out and resetting my identity again

15:06 So now you have no information about that former identity

# Making everything ~~worse~~ just work

- Encryption is temporarily becoming *more* visible
  - Warnings about the sender of a message if unsure
    - Although we actually made this better by including device keys with message keys



MSC4147: Including device keys with Olm-encrypted events #4147

Merged richvdh merged 12 commits into `matrix-org:main` from `uhoreg:include_device_keys` on Dec 10, 2024

Conversation (55) Commits (12) Checks (1) Files changed (1)

uhoreg commented on May 29, 2024 • edited by turt2live

Member

Reviewers

- andybalala
- cloken

Rendered

# Making everything worse

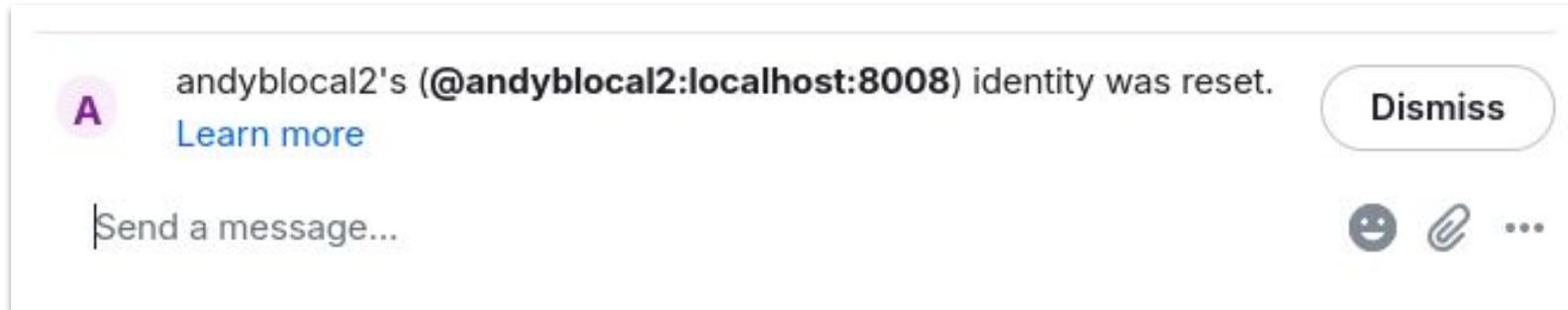
- Encryption is temporarily becoming *more* visible
  - Warnings on messages decrypted via key storage

15:14  Hello Mum I am in the Invisible Crypto talk!

The authenticity of this encrypted message can't be guaranteed on this device.

# Making everything worse

- Encryption is temporarily becoming *more* visible
  - Pop-ups about user identity changes



# Invisible Crypto

- The vision: secure and easy to use
- Making everything worse
- **Making everything better**
- Important announcement

# Making everything better

- Next up: making encryption *less* visible
  - Exclude insecure devices
  - Dehydrated devices
  - Recovery key management
  - Authenticated key storage
  - Sharing identity updates between devices
  - Fixing bugs making devices' crypto incomplete
  - Showing identity changes in the timeline

# Making everything better

- Next up: making encryption *less* visible
  - Exclude insecure devices
    - **No warnings: just ignore unverified devices!**

# Making everything better

- Next up: making encryption *less* visible
  - Dehydrated devices
    - **Receive messages while logged out!**
    - **Fewer unable-to-decrypt messages!**

# Making everything better

- Next up: making encryption *less* visible
  - Recovery key management
    - **No more lost recovery keys!**

# Making everything better

- Next up: making encryption *less* visible
  - Authenticated key storage
    - **No uncertainty about messages from backup!**

# Making everything better

- Next up: making encryption *less* visible
  - Sharing identity updates between devices
    - **Changing key storage key works across devices!**

# Making everything better

- Next up: making encryption *less* visible
  - Fixing bugs making devices' crypto incomplete
    - **It works without cryptic errors!**

# Making everything better

- Next up: making encryption *less* visible
  - Showing identity changes in the timeline
    - **Minor identity changes are less intrusive!**
    - **(If you care, it's still in your face)**

# Invisible Crypto

- The vision: secure and easy to use
- Making everything worse
- Making everything better
- **Important announcement**

**Important announcement**

**Exclude Insecure Devices  
is coming!**

# Exclude Insecure Devices is coming!

- MSC4153 has passed FCP, so
- In April 2026, Element will change its default:
  - Received messages from unverified devices will not be decrypted
  - Messages will not be sent to unverified devices
- **If your device is unverified, you will not be able to talk to someone who is using Element**
- On dev builds you can try it now with labs flag "Exclude Insecure Devices when sending/receiving messages"
- Very soon this option will appear in normal builds

# Exclude Insecure Devices is coming!

- Why?
  - To make users safer
  - To make encryption simpler
  
- Details: <https://github.com/matrix-org/matrix-spec-proposals/pull/4153>

# Exclude Insecure Devices is coming!

- To make users safer
  - Malicious server can't add devices to a chat
  - We know each device is trusted

# Exclude Insecure Devices is coming!

- To make encryption simpler
  - No more warnings about unverified devices!
  - We just ignore them

# Exclude Insecure Devices is coming!

- If your device is unverified, you will not be able to talk to someone who is using Element
  - or any other client complying with MSC4153

**Important announcement**

**Exclude Insecure Devices  
is coming!**

# Questions?

## Exclude Insecure Devices:

<https://github.com/matrix-org/matrix-spec-proposals/pull/4153>

<https://github.com/element-hq/element-meta/issues/2700>

@andybalaam:matrix.org

#andybalaam:matrix.org