element

Invisible Crypto[1]

Can Matrix be both secure and easy to use?

Andy Balaam, Element Crypto Team

[1] "Crypto" = "Encryption"

element

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

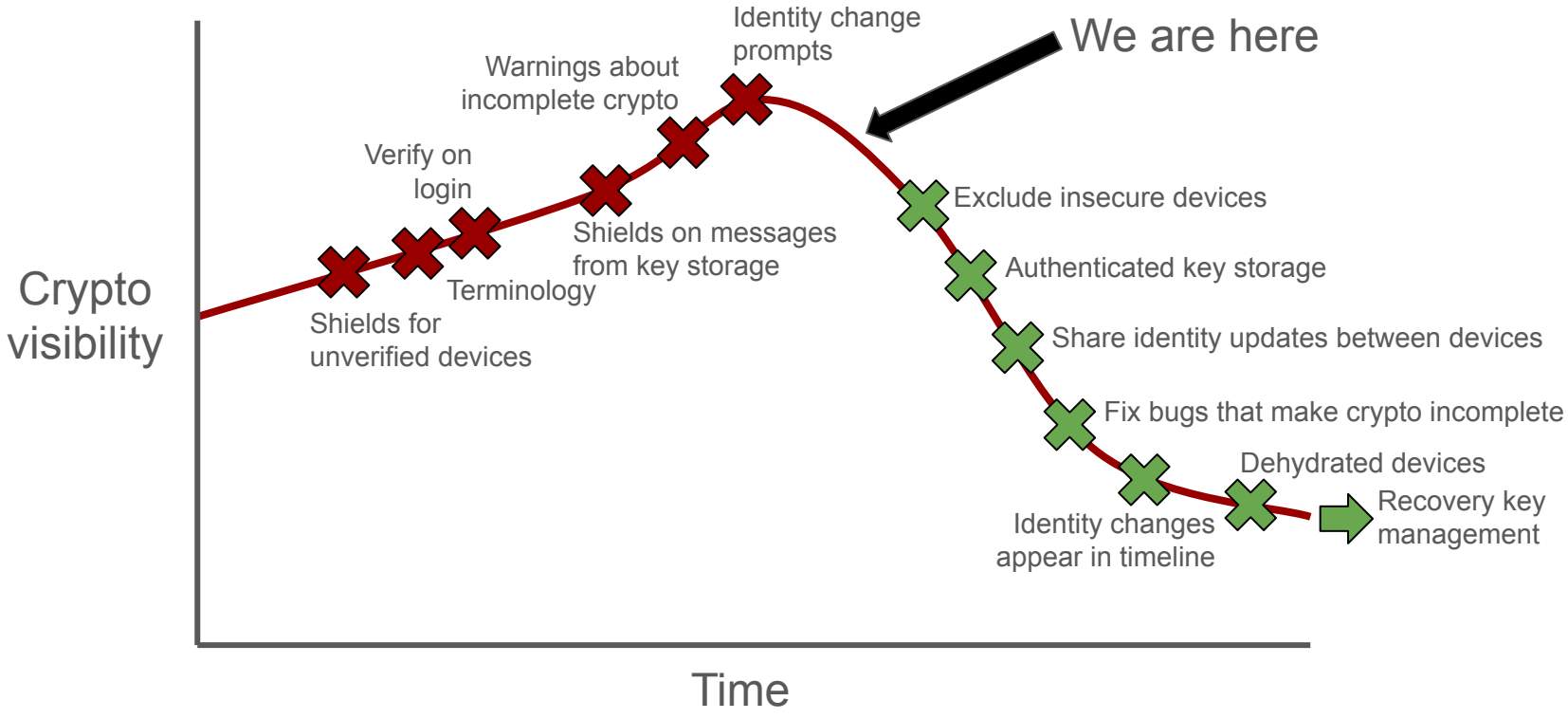
Invisible Crypto

element

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

Getting over the hump

element



The vision: secure and easy to use

element

- 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

element

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

Invisible Crypto

element

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

Making everything worse

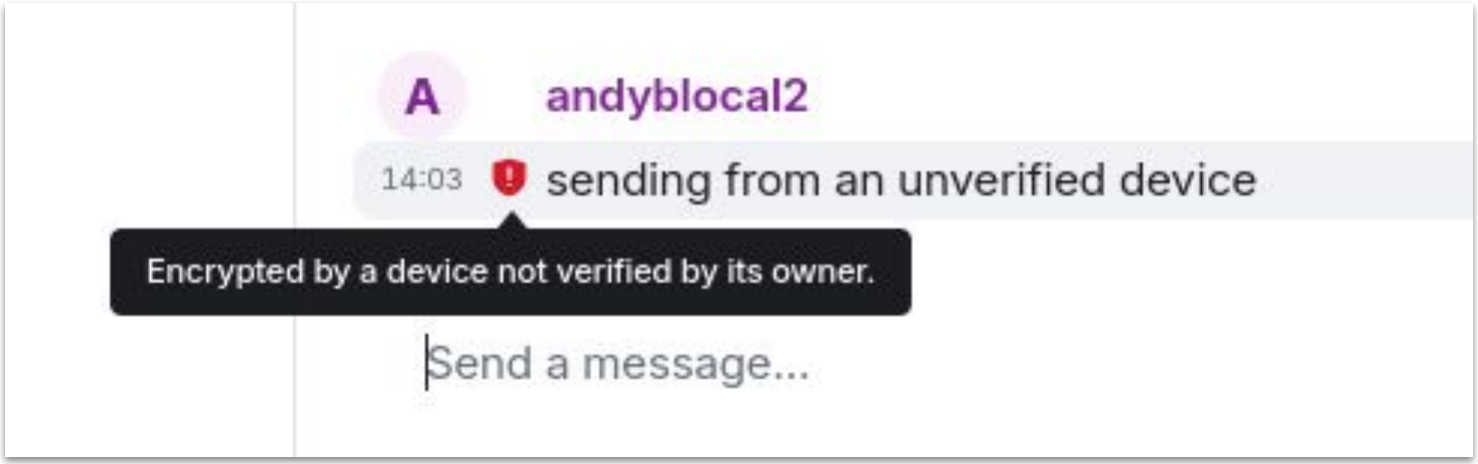
element

- 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

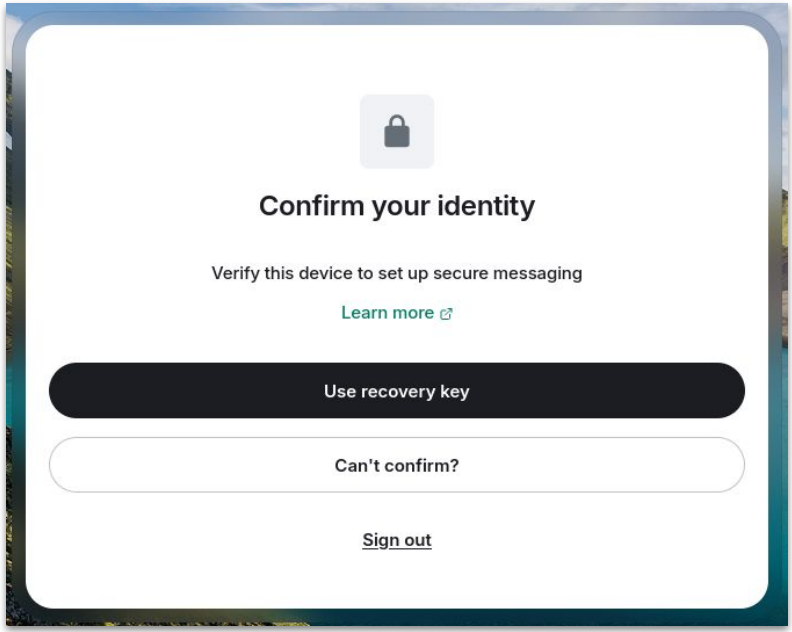
element

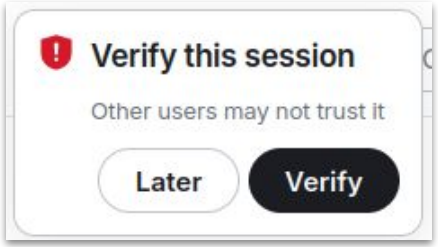
- Encryption is temporarily becoming *more* visible
  - Warnings on messages from insecure devices



Making everything worse

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

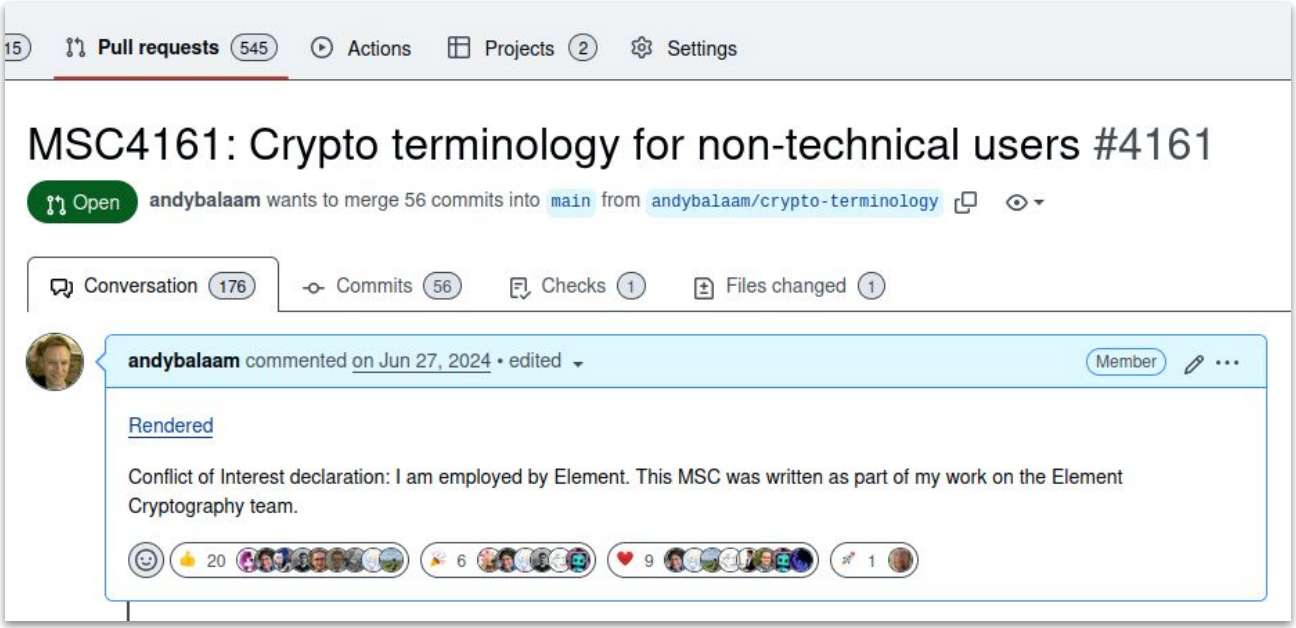




Making everything ~~worse~~ more visible

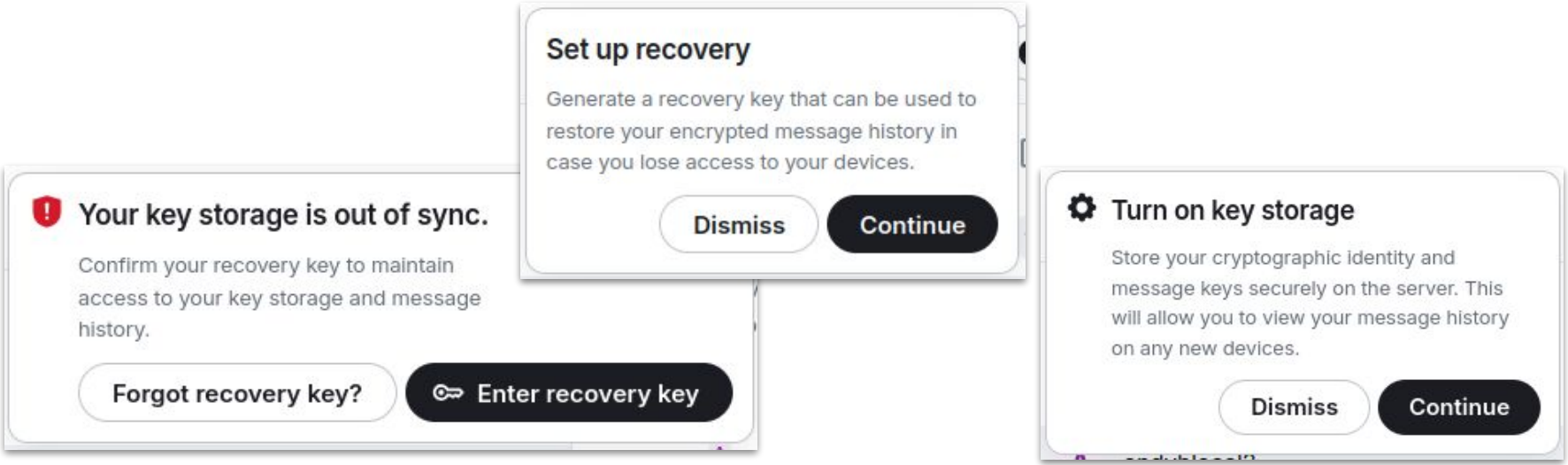
element

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



Making everything worse

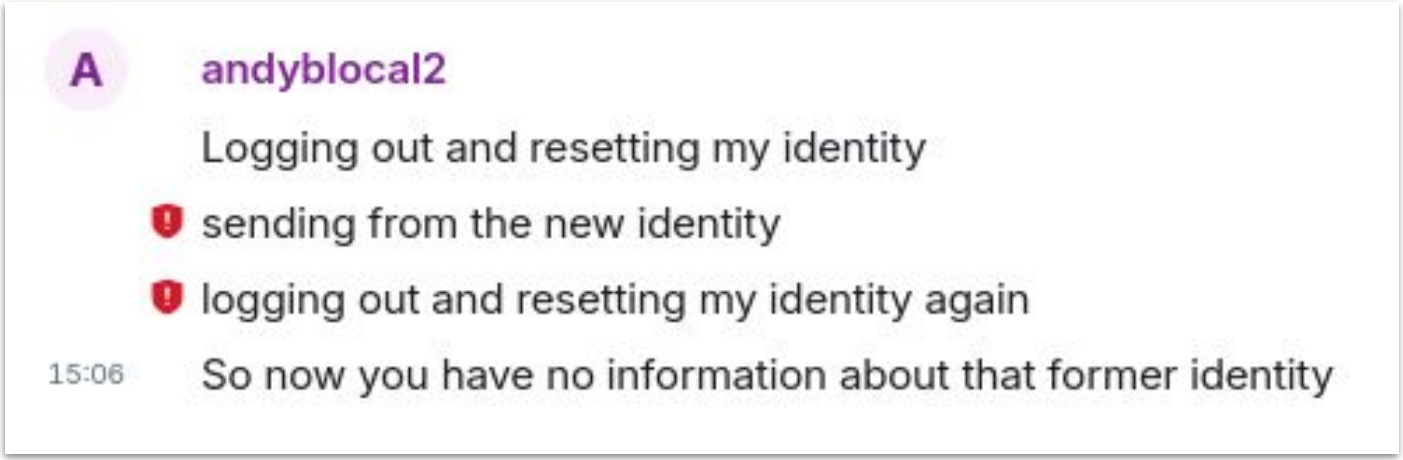
- Encryption is temporarily becoming *more* visible
  - Warnings if your device has incomplete setup



Making everything worse

element

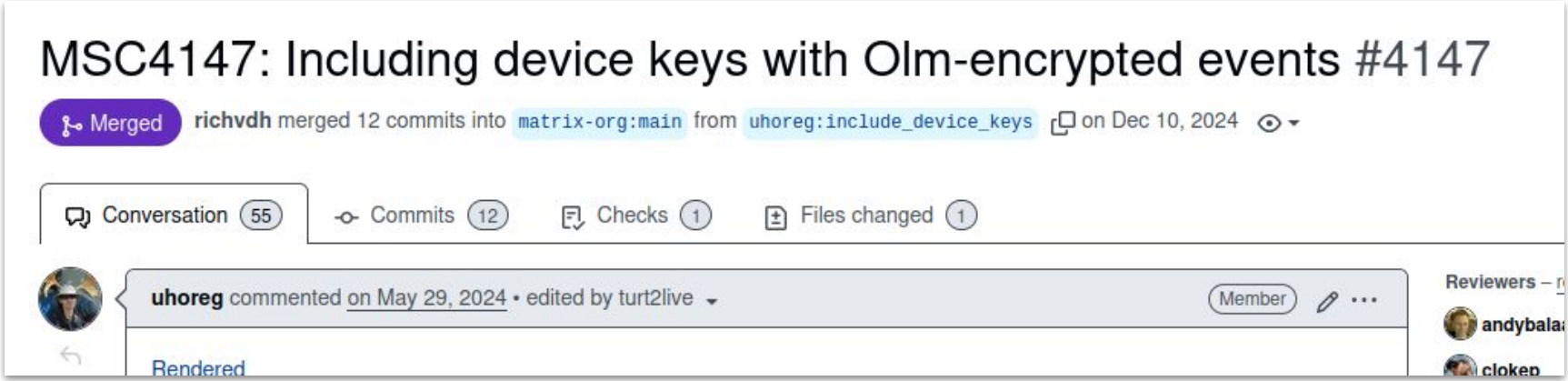
- Encryption is temporarily becoming *more* visible
  - Warnings about the sender of a message if unsure



Making everything ~~worse~~ just work

element

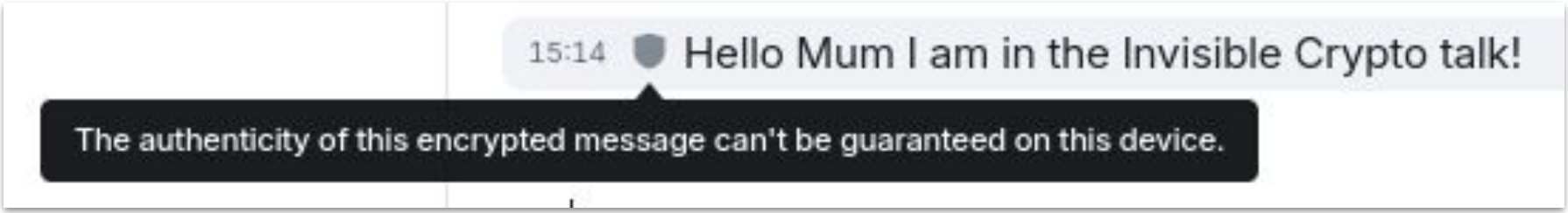
- Encryption is temporarily becoming *more* visible
  - Warnings about the sender of a message if unsure
    - Although we actually made this better by including device keys with message keys



Making everything worse

element

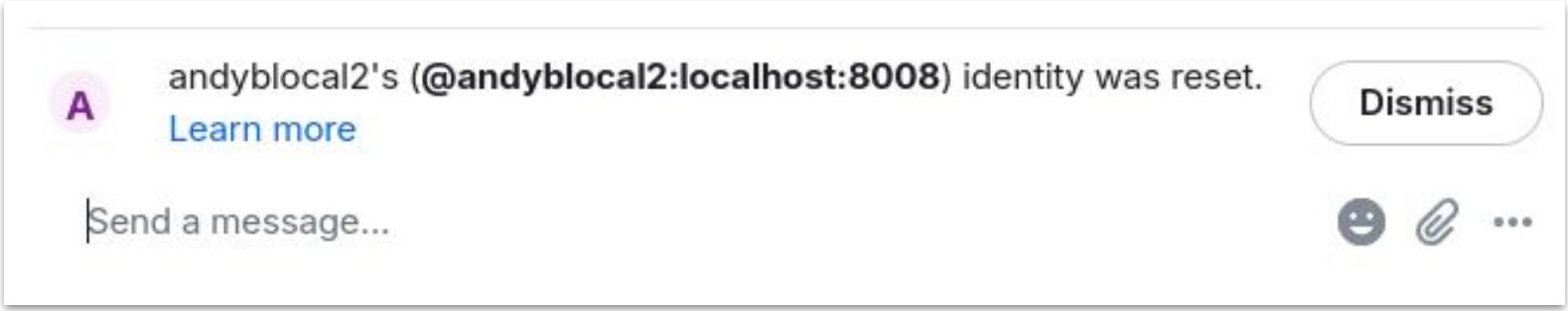
- Encryption is temporarily becoming *more* visible
  - Warnings on messages decrypted via key storage



Making everything worse

element

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



Invisible Crypto

element

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

Making everything better

element

- 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

element

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

Making everything better

element

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

Making everything better

element

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

Making everything better

element

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

Making everything better

element

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

Making everything better

element

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

Making everything better

element

- 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

element

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

element

Important announcement

Exclude Insecure Devices is coming!

Exclude Insecure Devices is coming!

element

- 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!

element

- 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!

element

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

Exclude Insecure Devices is coming!

element

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

Exclude Insecure Devices is coming!

element

- **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

element

Important announcement

Exclude Insecure Devices is coming!

Questions?

element

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