element

Why do I have two passwords?

How to talk about encryption in Matrix

Andy Balaam, Element Crypto Team

This work is funded by Element

and is donated to the Matrix community

This work is not complete!

You can help: see MSC4161

What words should we use?

- **Why standardise the words we use?**
- The words
- Some metaphors that might help

Why standardise the words we use?

- People switching clients will understand better
- People using different clients will understand each other
- **We will improve our own understanding**
  - ...meaning fewer bugs!

Let's try to build a shared vocabulary for Matrix crypto.

What words should we use?

- Why standardise the words we use?
- **The words**
- Some metaphors that might help

Devices/Sessions 📱

- A **device/session** is a "sign-in"
- When you sign in we create a device/session
- When you sign out the device/session disappears
    - **Note: signing out is significant!**

Devices/Sessions

- After logging in you need to **verify** your device to make it secure.
  - Proposed update: **link**
- Unverified devices are **insecure**
  - Proposed update:
    - your devices can be **unlinked**
    - other people's devices can be **unconfirmed** (but soon we won't care)

Devices/Sessions

- Avoid "cross-signing"
- Avoid "device keys"

Verified users ✓

- When you **verify** a user they become **verified**
  - This is quite rare at the moment
  - You do it by comparing emoji in person
- Verifying a user means no-one is listening in
- This is totally different from verifying devices!
  - Even though it looks the same :-(
- If you verify a user it means ***you care about identity changes*** *(because now someone could be listening in!)*

Identity

- Your **identity** is proof of who you are
  - Who needs that proof? Not the server: other people
  - Proposed update: **digital ID**
- And it gives you access to *key storage*, which gives you access to *message history*

Tech note: we say "identity" for the collection of keys: the master signing key, user signing key, device signing key, key storage key and others.

Message key

- A **message key** is used to decrypt a message
- If we have a message but we don't have the key, we are unable to decrypt and say something like:
    - "you don't have access to this message" or
    - "waiting for this message"

Message history

- **Message history** is old messages, especially when stored on the server
- If messages are encrypted, to access history, we must store the keys on the server too, using *key storage*

Key storage

- If you enable **key storage**, your *message keys* are stored (encrypted) on the server
- This gives you access to encrypted *message history*
- Avoid "key backup". Backups normally mean copying messages into a different system

Recovery

element

- **Recovery** allows you to save your *identity* to the server
- It is protected by a **recovery key** or **recovery passphrase**
  - Your recovery key is very important! If someone steals it they can impersonate you and read your *message history*.

- Avoid "secret storage"
- Avoid "4S"

Summary 1: words to use

- Devices/sessions can be verified, making them secure
- Verified users mean no-one is listening in
- Identity is proof of who you are and unlocks key storage
- Message keys unlock messages
- Key storage allows you to unlock message history
- Recovery stores your identity and can be unlocked with a recovery key

What words should we use?

- Why standardise the words we use?
- The words
- **Some metaphors that might help**

Why is Matrix crypto so confusing?

- Because end-to-end encryption is unfamiliar:
  - In most modern systems we give absolute trust to the server
  - In Matrix, the server is just a connection to the network
  - **Our trust is reserved for people**

But, Andy:

Why do I have two passwords?

Why do I have two passwords?

- It's about who you are talking to.
- Your **password** is for proving who you are to the **server**
- Your identity is for proving who you are to **people**

- Think of your identity as being like an ID card
- Your **recovery key** is for getting your ID card back if you lose it
  - (and with your ID card, you can get message history too)

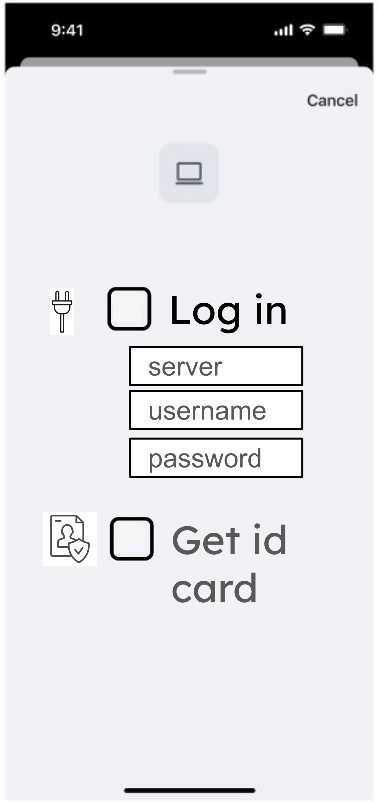
Welcome to the land of Andy's Wild Ideas

Identity is like an ID card

So logging in has two steps:

- Connect to the network
- Get a copy of your ID card

Identity is like an ID card



□ Log in

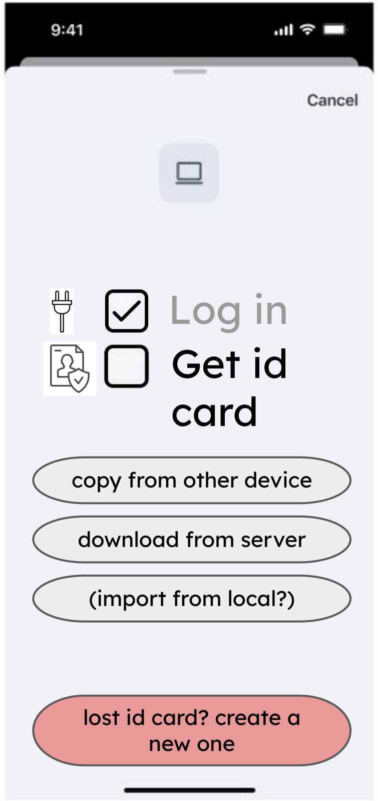
server

username

password

□ Get id card

Identity is like an ID card



9:41

Cancel

☑ Log in

□ Get id card

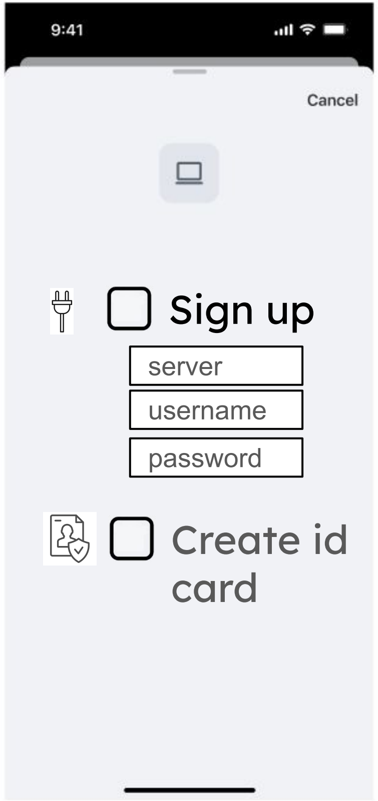
copy from other device

download from server

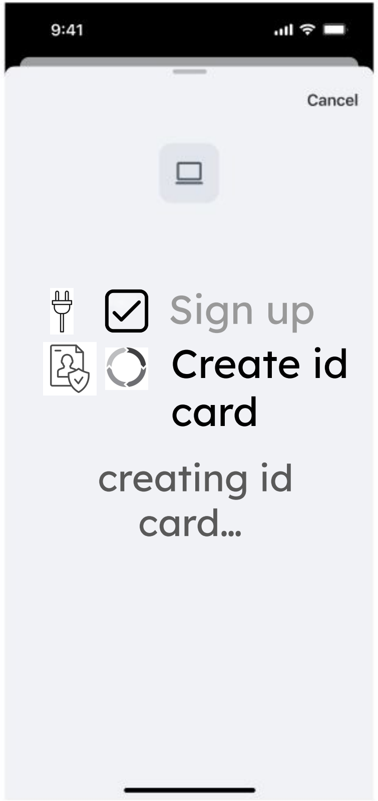
(import from local?)

lost id card? create a new one

Identity is like an ID card



Identity is like an ID card

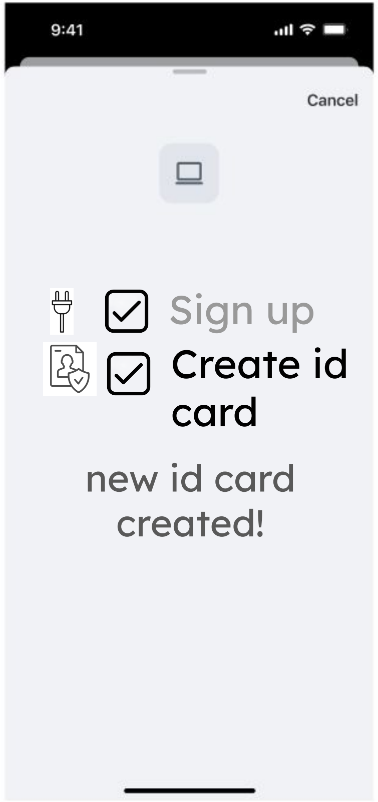


☑ Sign up

○ Create id card

creating id card...

Identity is like an ID card



☑ Sign up

☑ Create id card

new id card created!

Now we can talk about the ID card

"verify device"

becomes

"get my ID card"

- From device 🪪 ⬅️ 📱 or
- From server 🪪 ⬇️🔐 or
- Maybe one day: from local backup?

Now we can talk about the ID card

"set up recovery"

becomes

"save my ID card to server"🪪 ⬆ 🔒

Now we can talk about the ID card

"reset crypto identity"

becomes

"lost ID card? create a new one"

Now we can talk about the ID card

"recreate/reset recovery"

becomes

"forgot recovery key? re-save your ID card"

What is an ID card?

- It proves who you are to **humans** (not the server)
- It allows you to encrypt messages to other people
- It allows you to decrypt messages from other people
    - including old messages, if you have key storage on

What is an ID card?

- It can be **copied** to/from other devices
- It can be **saved** into a "safe deposit box" on the server
  - To get it back you need the recovery key
- Losing it is a big deal
- Someone stealing it is even worse

No really, what is an ID card?

Tech note:

- The ID card is all the identity information that can be stored in 4S:
  - master, self-signing and user-signing keys
  - key backup key
  - dehydrated device key
  - … possibly others in future
- The ID card does not contain the message keys
- The "safe deposit box" is Recovery

What is recovery?

- It's like a safe deposit box
- The bank can't open your box - they hand it to you and you use your key to open it

Image by -JvL-

What is a recovery key?

- It is a key that the server does not have
- It unlocks the safe deposit box on the server that stores your ID card
- If someone gets your recovery key, they can steal your ID card

Summary 2: suggesting metaphors

- Identity = ID Card
- Recovery = Safe deposit box
- Recovery key = Key for safe deposit box

The ID Card proves who we are to people, and can be copied to all our devices.

Questions?

element

MSC4161: Crypto Terminology

https://github.com/matrix-org/matrix-spec-proposals/pull/4161

@andybalaam:matrix.org

#andybalaam:matrix.org