UX — Monsters of the Id

Jon Crowcroft

Identity friction

UX – not a number

Re-Decentralised

1. Partied out…UX i

- Proving some verified credential to access some service
- 4 way interaction – two tech, two human
  - Customer to customer's device
  - Customer device (e.g QR code) to service device
  - Service device to verification service (check cert/sig)
  - Biometric (face, or) to server

  - Human "in the loop" is a design error
    - Consequences (serious or trivial)> attention
    - What can go wrong (accidental or adversarial)?
    - Complexity v. Context
  - Consider human client<> human server as primary
    - And make device/design make that even simpler

So many parties…UX ii

- Similar (possibly broken) workflows for
  - Onboarding newbies
  - Remote onboarding newbies
  - Expiring (possibly archiving)
  - Revoking
  - De-revoking
  - Proxying

- Can we SIMplify all the above?
  - Can we use multiple interaction modes (incl face/gesture/voice)?
  - Can we use an LLM to analyse all the workflows and simplify?
  - E.g. remove redundant steps, or replace with simpler ones
  - Recombinant id

Order, order…UX iii

- E.g. from arriving at border control
  - Asked for photo, and fingerprint of right then left hand
  - But camera can tell where you are standing
  - So can do fingerprint in any order.
- Check on visa doc and passport yet visa has photo & passport no.
  - Redundancy – remove
  - And can read chip passport on any NFC phone,
    - so why optically scan?

- Too many steps => errors, delays, possible refusals…
  - Maybe use LLMs on the workflows to determine possible simplifications?

- Is it just Identity-theatre?

2. Federated Decentralised Id

- Federating centralised systems is a good id
  - Decentralised id is trickier
  - DIDs (W3C) are not inherently decentralised
- You need to disintermediate: i.e. remote government as intermediary
- Do this via a DLT and a wallet
  - We can design nice DLTs (ION/Trustchain – see elsewhere) ok
  - But can we design ok wallets?

EU initiative (and a Linux Foundation one too):- https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation

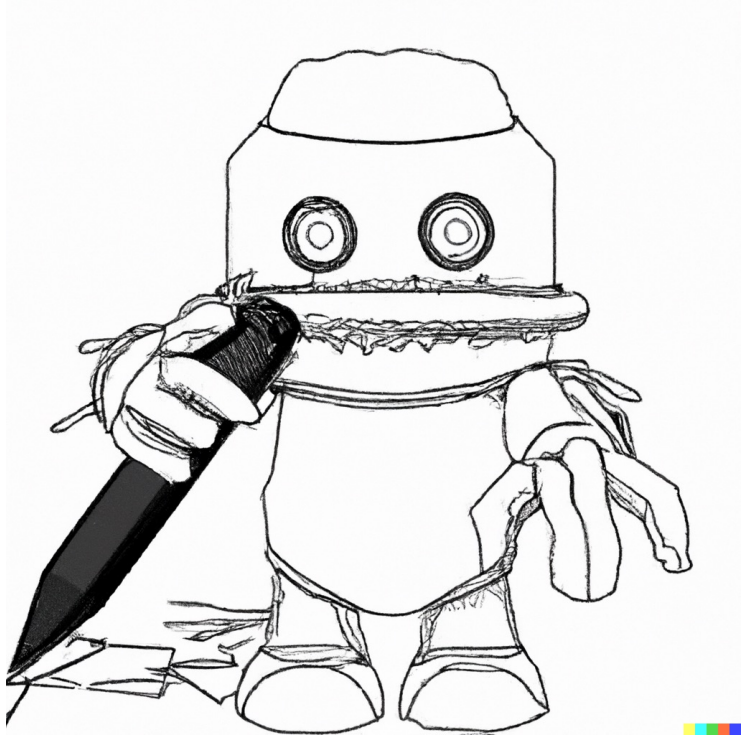
That’s not my wallet i

Everyone trusts a decentralised service…what could go wrong?
Wallet is replacement for central (government/bank) service
So is now the target for adversary.

- Sandbox/enclave
  - E.g. mobile banking apps (mostly ok)
  - Cryptocurrencies (mostly backdoored)
  - Which of these cultures will dominate for Id?
- Verified software
  - But also verified specification?
  - Who owns verification
  - Attestation (c.f. Intel SGX but not Arm)

Promise ii

- Who verifies verifiers experience?
- Who attests to attestation service?
- CA transparency (is a DLT)?



Alt iii

- Id for livestock
- Id for inanimate objects
- Fayda: value, benefit, profit!

Future work

- Use of Laconic Crypto to do “reverse” FHE
  - Use case – behavioural voice biometric check on server
  - Without service getting plain access to voice/speaker data
- Lightfield (behavioural) face recognition
  - to avoid replay attacks with flat images
  - See https://francois.pitie.net/3d/

Conclusions

calm

trust