Monsters of the DiD

Jon Crowcroft

16/4/26

Politics: Identity friction

“We live in two worlds... the world into which we were born, and the otherworld that was born within us. Both may be a blessing or a curse. We choose.” – Druid saying.

NO2ID
Stop the Database State

Philosophy: Identity & Self

"*The whole of this doctrine leads us to a conclusion, which is of great importance in the present affair, viz. that all the nice and subtile questions concerning personal identity can never possibly be decided, and are to be regarded rather as grammatical than as philosophical difficulties. Identity depends on the relations of ideas; and these relations produce identity, by means of that easy transition they occasion. But as the relations, and the easiness of the transition may diminish by insensible degrees, we have no just standard, by which we can decide any dispute concerning the time, when they acquire or lose a title to the name of identity.* " David Hume

Ideation: What makes you you? What is identity = or ==

Analog

- Heraclitus – objective context
- You can't step in the same river twice
- The Ship of Theseus or Trigger's Broom
- Locke – cognitive context, Memories (solipsistic)
- ***You*** are who ***they*** say you are (socially constructed)
- E.g. you are always your parents child (etc) (at least til you take over care/attorney!)

A2D

- Mind/Body (Sajnani)
  - How does being digital change anything?
  - Mind/Body/Bits/Body/Mind journey
  - How do we get from real to virtual, digitally?
- What about Bad People with Bad Software
- Personation, Mission Impossible…

Society: Big Ids of the World

e.g.

मेरा आधार
मेरी पहचान

National ID
ብሔራዊ መታወቂያ

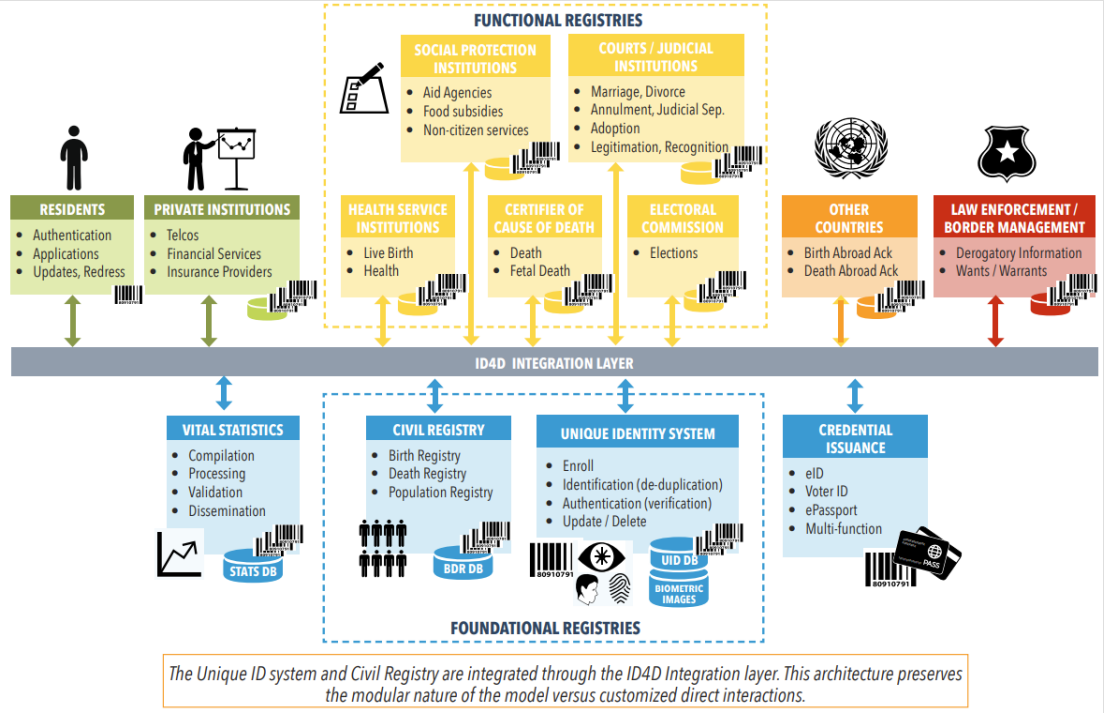
Why Digital? Some use cases

	Uniqueness Matters	Uniqueness is Less Critical
Functional ID Systems	**Foundational ID systems** (e.g. national ID, civil registry)	**Loyalty programs / memberships**
	Voter registration & elections	**Transportation cards / event passes**
	Social protection/welfare programs	**E-commerce or social media accounts**
	Subsidy distribution (e.g. food, fuel, cash transfers)	**Education records (basic)**
	Immigration/border control	**Digital login/auth systems** (e.g. OAuth, SSO)
	Pension/employment tracking	**Short-term or anonymous surveys/census**
	Criminal justice systems	
	Refugee registration / humanitarian aid	
	National health insurance schemes	

"Uniqueness of identity is essential when a system confers rights, benefits, or responsibilities to individuals — where one person must not claim entitlements meant for another.

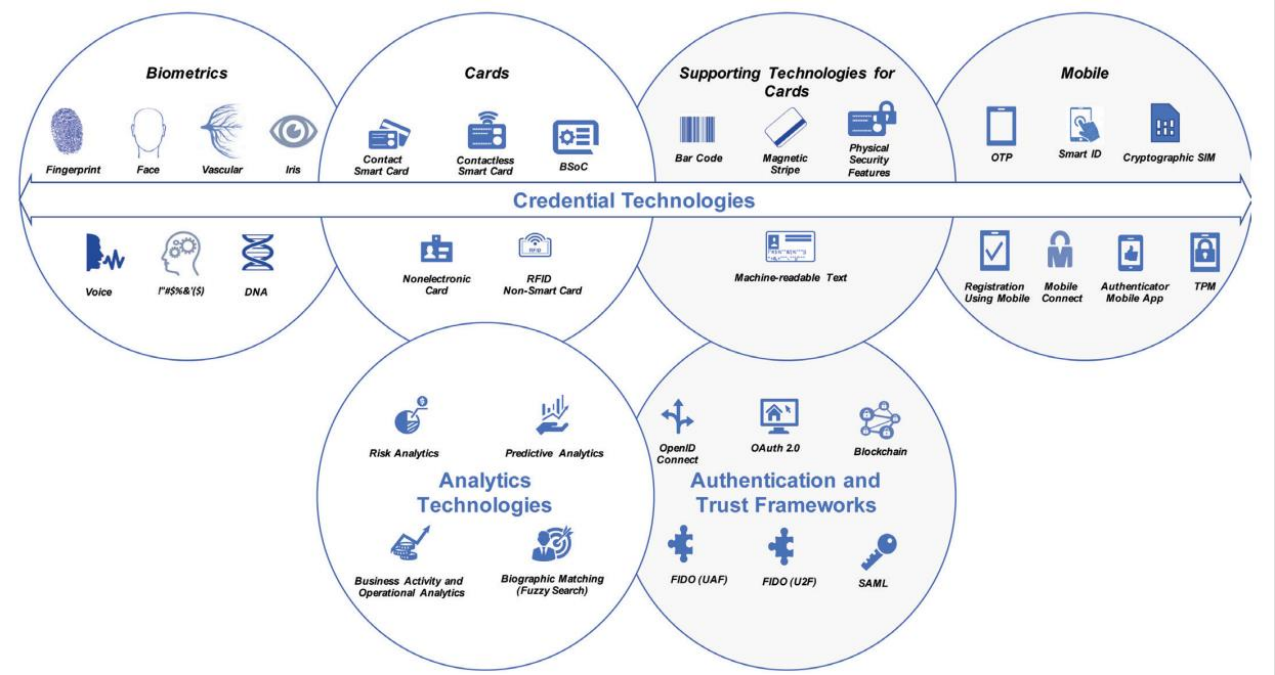
In contrast, when systems support preferences, pseudonymity, or general usage tracking without legal or social consequences, strict uniqueness becomes less critical"

Functional vs Foundational



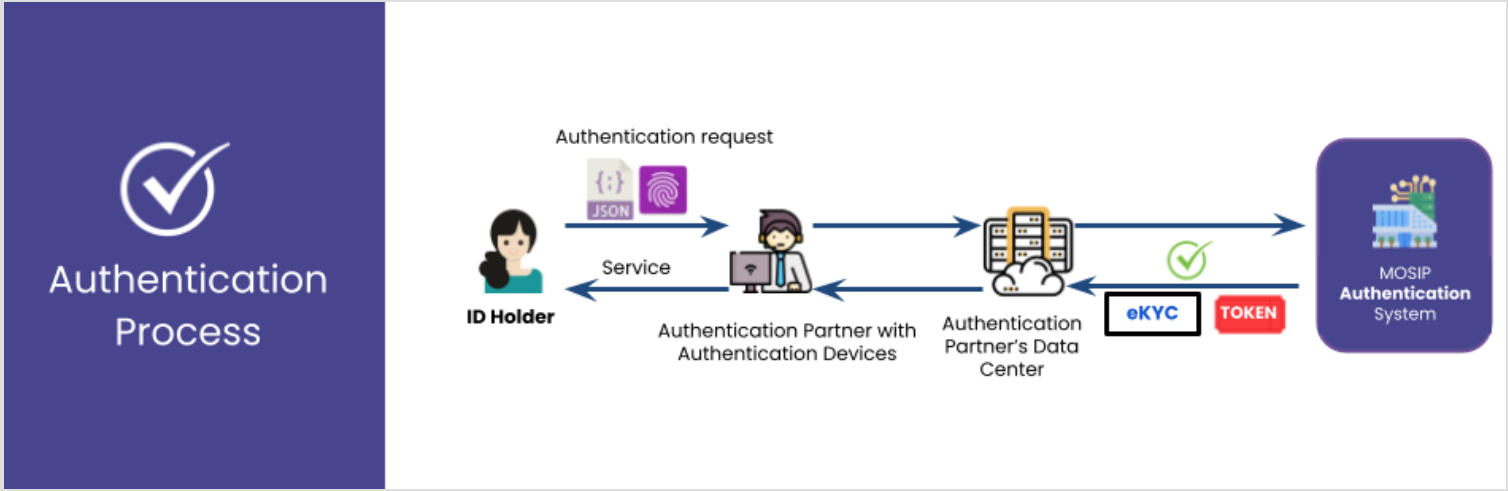
https://www.biometricupdate.com/wp-content/uploads/2015/09/ID4D-report-World-Bank-Accenture.pdf

Technology Landscape



https://documents1.worldbank.org/curated/en/199411519691370495/Technology-Landscape-for-Digital-Identification.pdf

Workflow: Identity Verification



https://docs.mosip.io/1.2.0/id-lifecycle-management/identity-verification/id-authentication

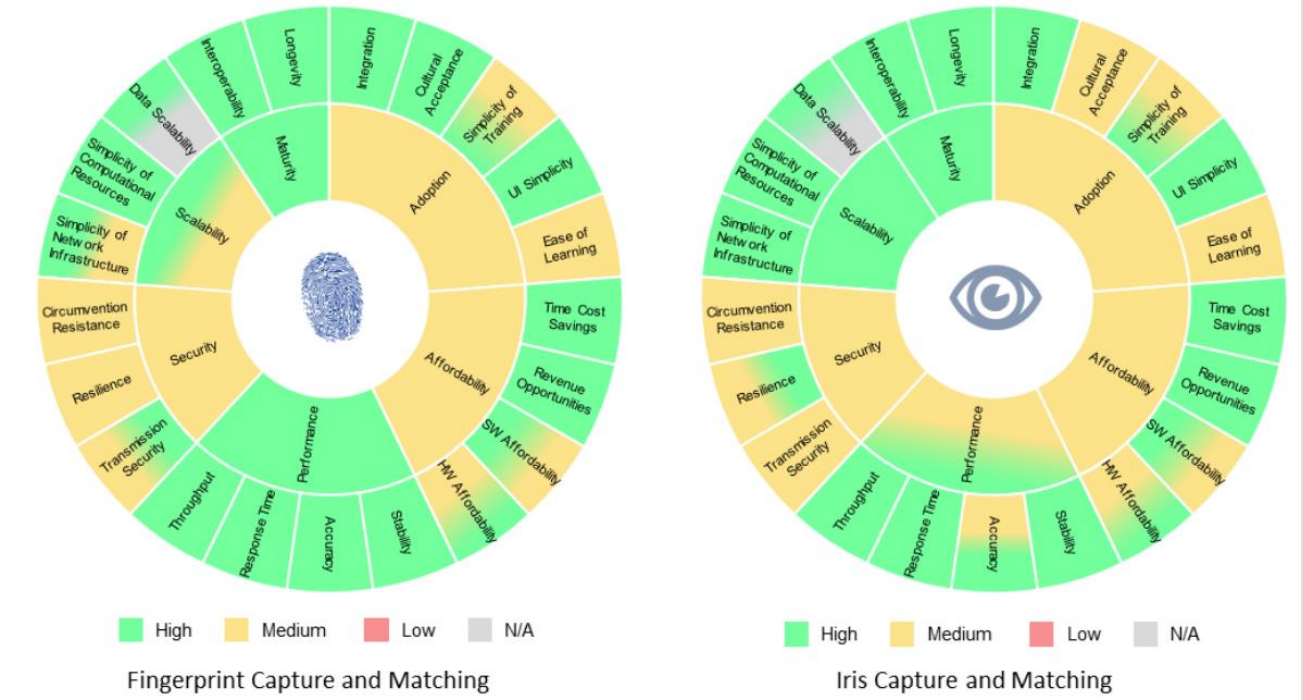
Data minimisation

Mechanism	Description
Cryptographic Tokens	Unique, signed tokens (e.g. QR, NFC) issued per user or claim, validated on use
Verifiable Credentials (VCs)	Issued by trusted parties; users prove eligibility or uniqueness cryptographically
Zero-Knowledge Proofs (ZKPs)	Users prove they haven't claimed before, without revealing identity
Fuzzy Demographic Deduplication	Matching individuals based on partial or noisy personal data (name, DOB, etc.)

Pros and Cons

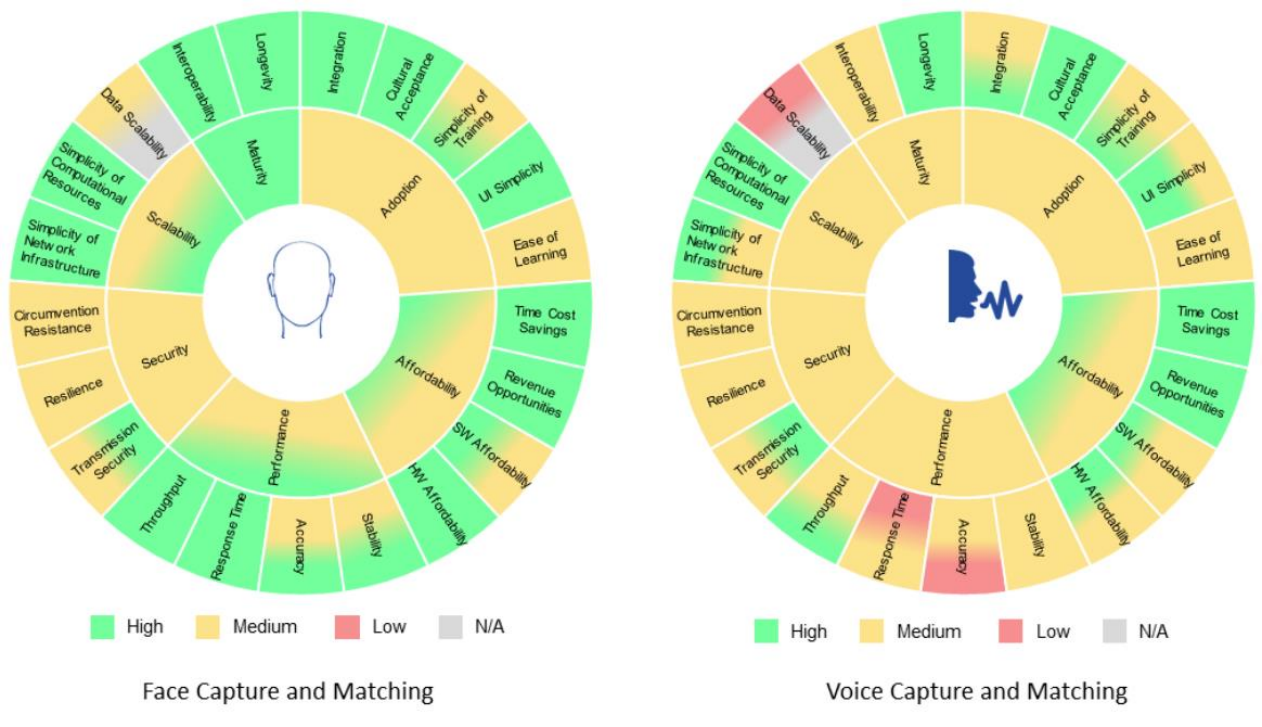
Mechanism	Pros	Cons
Cryptographic Tokens	- Easy to deploy offline- Low-cost- Strong one-time use control	- Requires secure issuance and tracking- Token loss = benefit loss
Verifiable Credentials	- Privacy-preserving- Reusable & portable- Enables selective disclosure	- Requires digital wallets & trusted issuers- Not trivial to deploy at scale
Zero-Knowledge Proofs	- Maximum privacy- Strong uniqueness without identity disclosure	- Technically complex- Harder to implement in low-tech environments
Fuzzy Demographic Matching	- No biometric or advanced tech needed- Scalable for existing databases	- Prone to errors (false matches or misses)- Lower trust in low-data-quality contexts

Wetware: Fingerprint & Iris



https://documents1.worldbank.org/curated/en/199411519691370495/Technology-Landscape-for-Digital-Identification.pdf

Wetware: Face & Voice



https://documents1.worldbank.org/curated/en/199411519691370495/Technology-Landscape-for-Digital-Identification.pdf

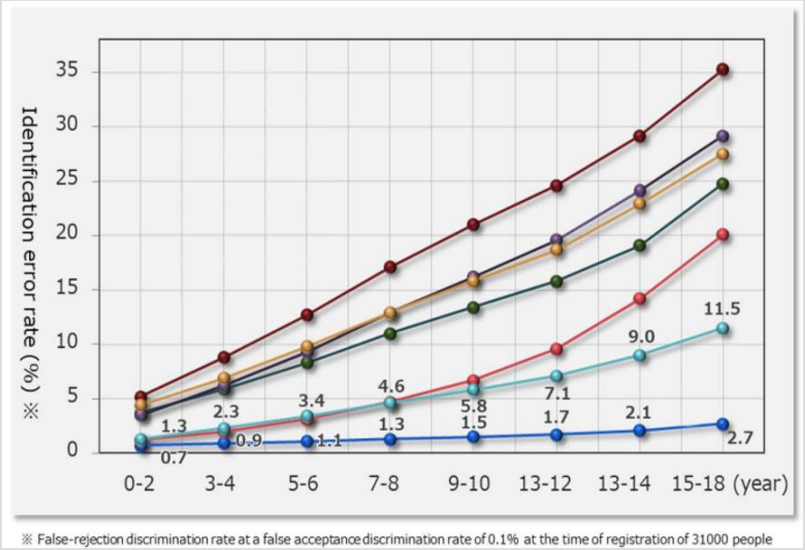
Liveware: Demographic Bias & Age

Demographic Bias

Race /Ethnicity	Sample Images	Verification Accuracy (%)
East Asian		93.72
Black		94.67
South Asian		93.98
Caucasian		96.18

Face Verification performance by ArcFace [1] on each race/ethnicity cohort in RFW dataset [2]

Algorithmm Accuracies over Aging Photos



※ False-rejection discrimination rate at a false acceptance discrimination rate of 0.1% at the time of registration of 31000 people

https://biometrics.cse.msu.edu/Presentations/Biometric_Summer_School_2021_Final.pdf
https://biometrics.cse.msu.edu/Presentations/MBZUAI_Sept_1_2020.pdf

Identity friction – say no…or?

- UX – I am not a number, papers please, alien nation

versus

- **Re-Decentralised** Viz Estonia…self-sovereign…

Malware: bad state actor versus individual inclusion

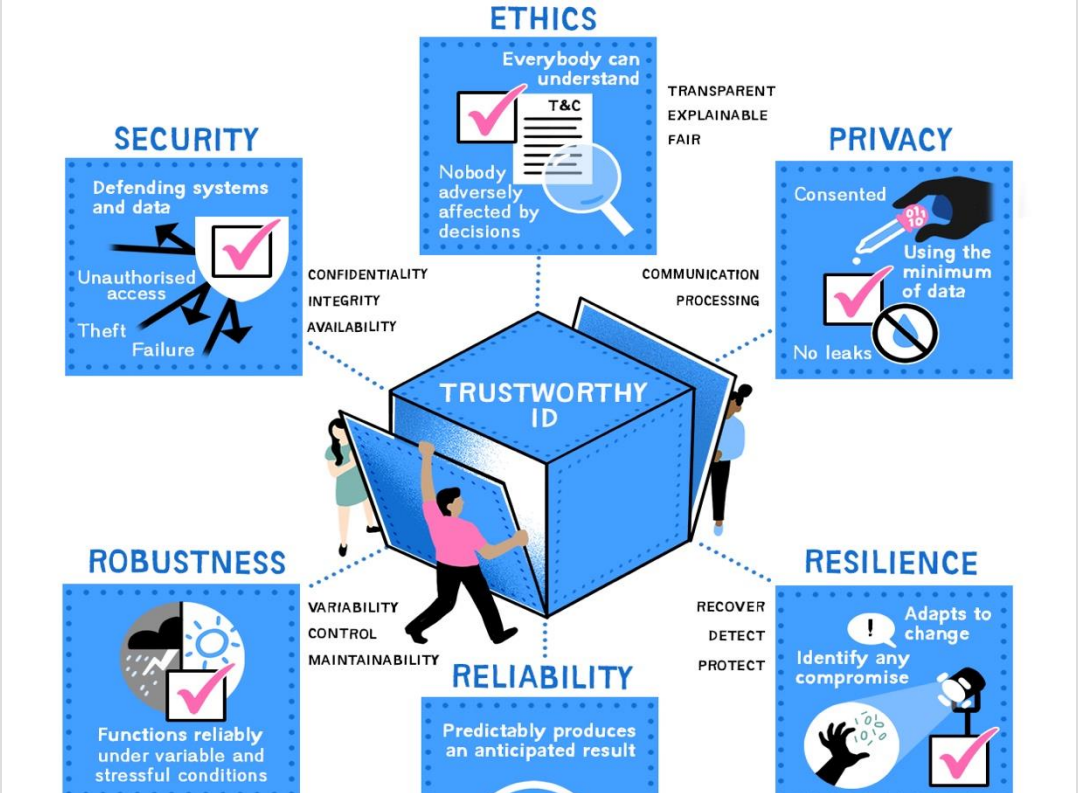
- Manyfold
  - Privacy
  - Security
  - Fairness
  - Explainability
  - Robustness

  - Bad Actors
    - State Surveillance
    - Id theft
    - Fake id

Trust: Owning and regaining

Two Practical Things we did about it

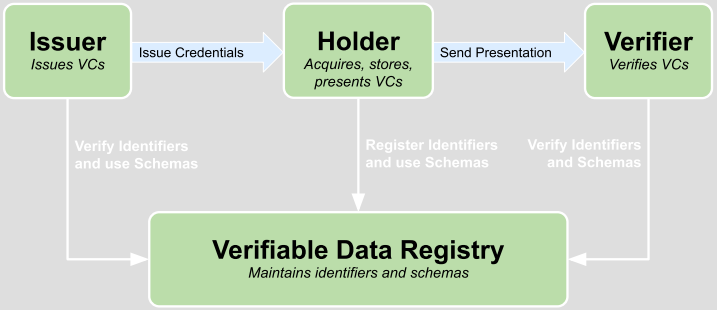
TrustChain & SIMple ID.

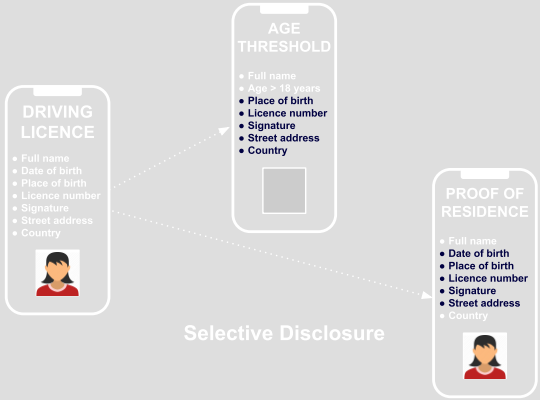


1. **Trustchain:** Trustworthy ***Decentralised*** Public Key Infrastructure

Digital ID

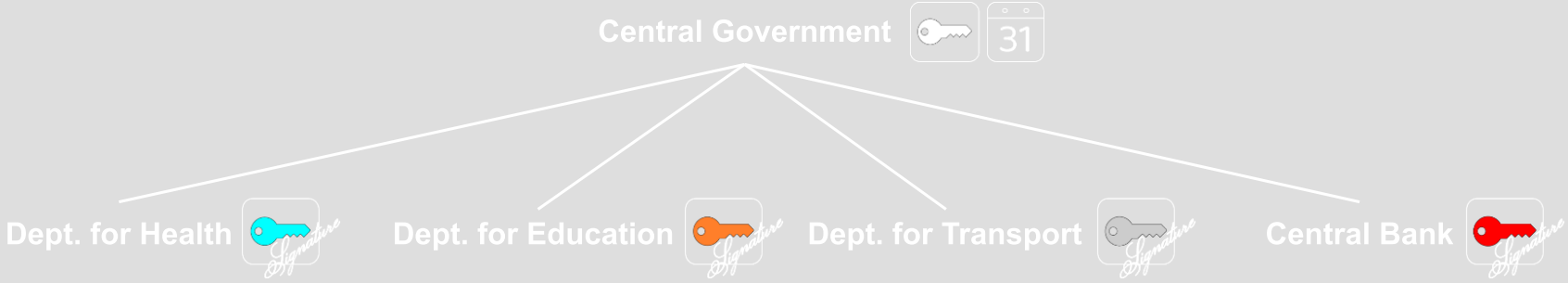
Credentials & Attributes

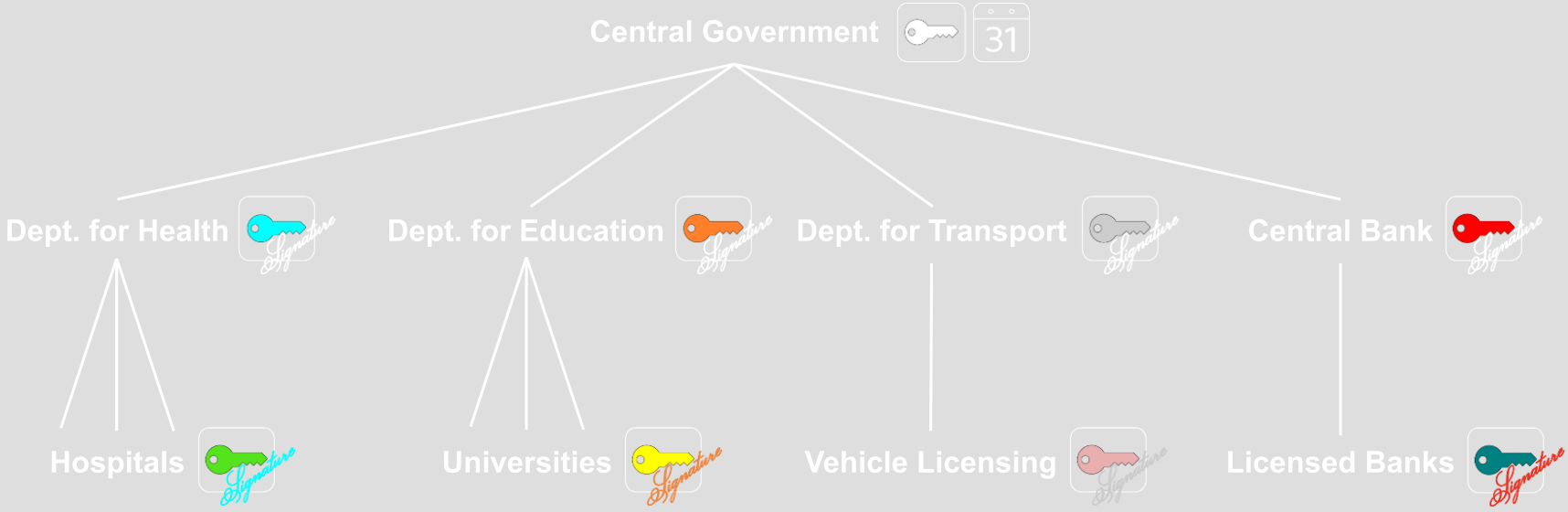


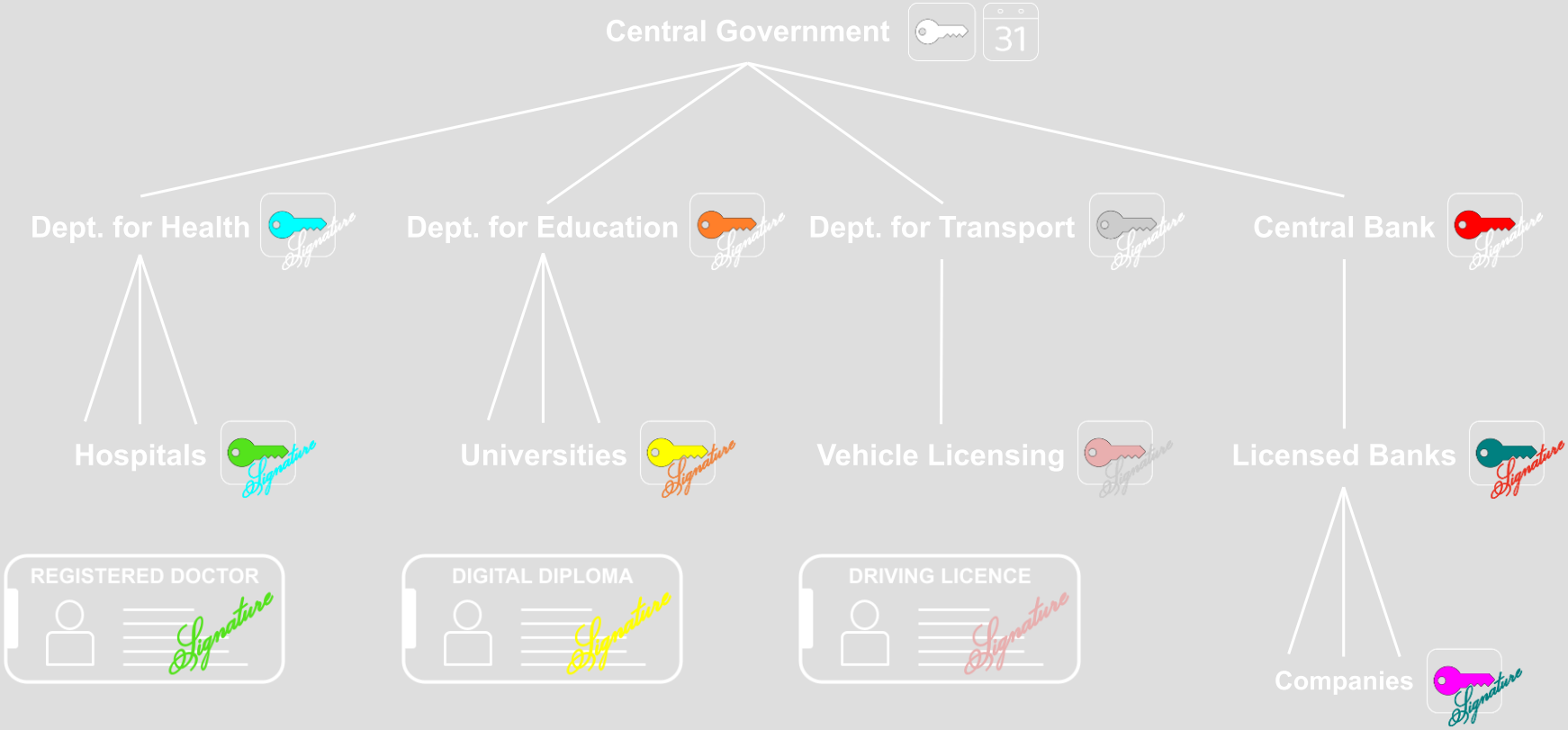


Decentralised Public Key Infrastructure

Trustchain employs decentralised networks and protocols to create a digital twin of existing hierarchical trust relationships.

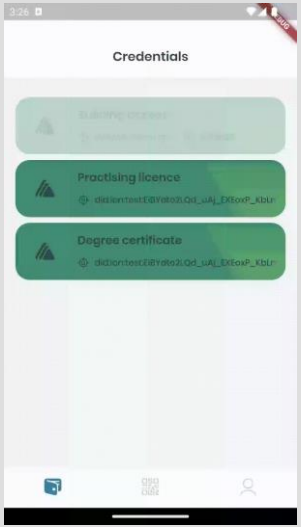

Central Government
31
Dept. for Health
Signature
Dept. for Education
Signature
Dept. for Transport
Signature
Central Bank
Signature

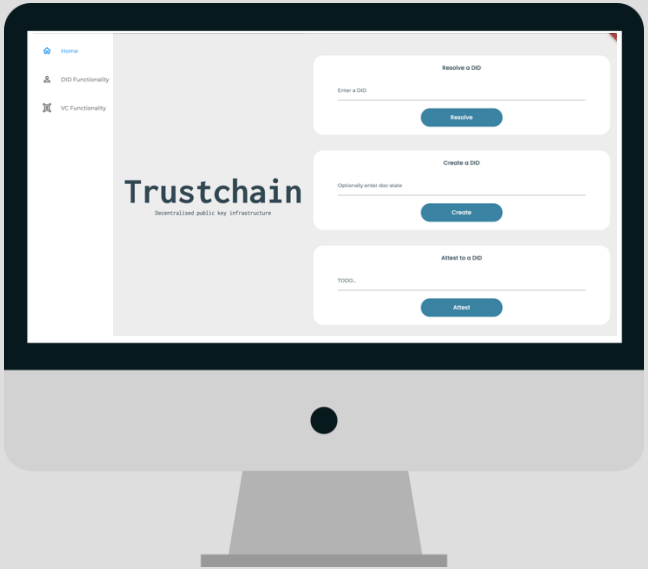

Central Government
31
Dept. for Health
Signature
Dept. for Education
Signature
Dept. for Transport
Signature
Central Bank
Signature
Hospitals
Signature
Universities
Signature
Vehicle Licensing
Signature
Licensed Banks
Signature


Central Government
Dept. for Health
Dept. for Education
Dept. for Transport
Central Bank
Hospitals
Universities
Vehicle Licensing
Licensed Banks
Companies
REGISTERED DOCTOR
DIGITAL DIPLOMA
DRIVING LICENCE
Signature

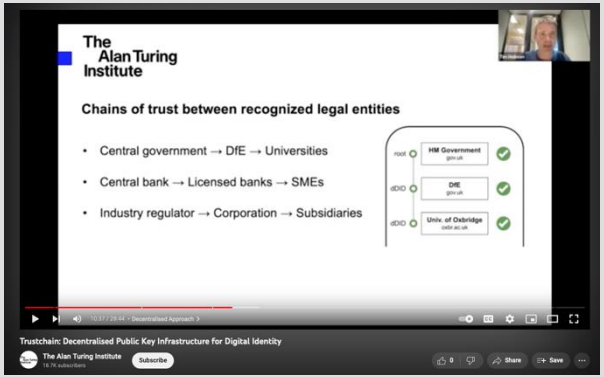
Trustchain resources

Open-source code: mobile and desktop apps





Demo video



Articles & technical notes

Trustchain – Trustworthy Decentralised Public Key Infrastructure for Digital Credentials

Tim Hobson[1], Lydia France[2], Sam Greenbury[3], Luke Hare[4], and Pamela Wochner[5]

The Alan Turing Institute, London, UK
thobson[1], lfrance[2], sgreenbury[3], lhare[4], pwochner[5]@turing.ac.uk

Abstract

The sharing of public key information is central to the digital credential security model, but the existing Web PKI with its opaque Certification Authorities and synthetic attestations serves a very different purpose. We propose a new approach to decentralised public key infrastructure, designed for digital identity, in which connections between legal entities that are represented digitally correspond to genuine, pre-existing relationships between recognisable institutions. In this scenario, users can judge for themselves the level of trust they are willing to place in a given chain of attestations. Our proposal includes a novel mechanism for establishing a root of trust in a decentralised setting via independently-verifiable timestamping. We also present a reference implementation built on open networks, protocols and standards. The system has minimal setup costs and is freely available for any community to adopt as a digital public good.

1 Introduction

Digital identity systems come in many guises, each design making a different set of trade-offs between diverse and collective disclosure*, a process by which a derivative Verifiable Presentation (VP) is used to disclose the minimum amount of information necessary to meet a given purpose.

The VC mechanism is predicated on the idea that verifiers

Trustchain: Possible Next Steps

- Replace verifiable time stamp source.
  Current use of bitcoin net isn't good for optics.

- Fabric Time Use.
  But would depend on permissioned Hyperledger, which in turn depends on verified id☹ oops…

- Scale consensus for ledger to deal with net outages.

- New work using DAGs and Mysteci platform promising…

2. SIMple ID

Can basic mobile phones display (signed) QR codes for digital credentials?

Fair Price Shops

- Resident visits FPS, presents Aadhaar UID, provides a fingerprint scan and specifies her order.
- The FPS submits Resident's authentication and authorisation data to UIDAI.
- FPS receives yes/no response.

The Alan Turing Institute

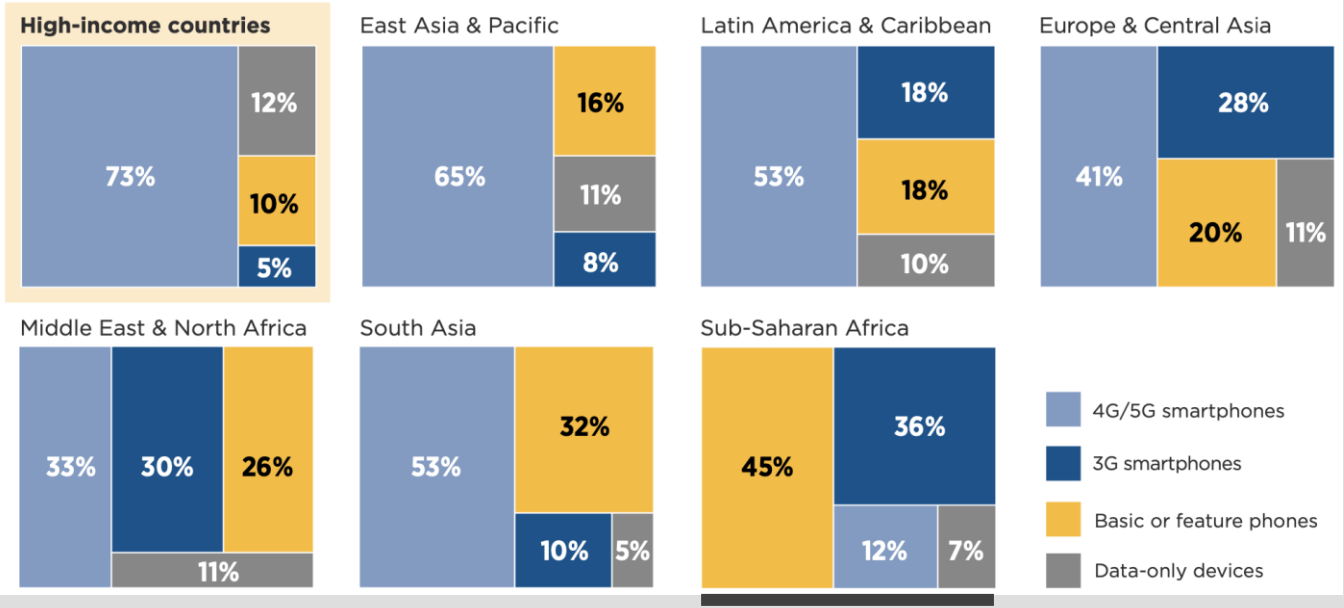
All these systems depend on…

and

or

The Alan Turing Institute

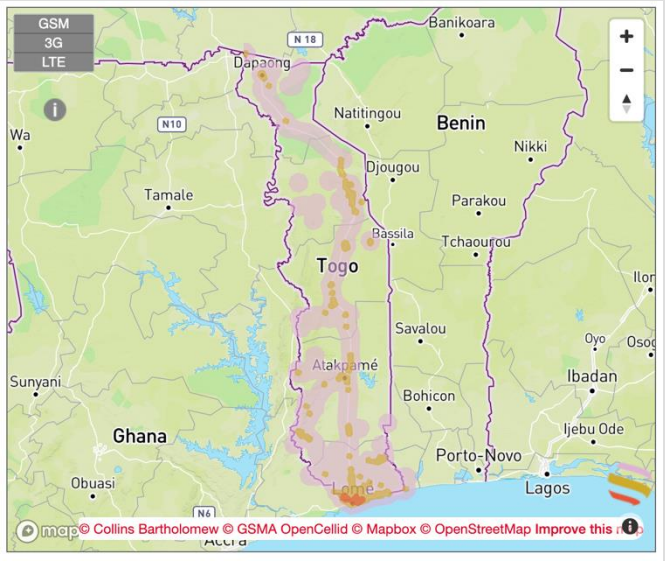
Mobile connections by device type for high-income countries and LMICs (by region), 2020

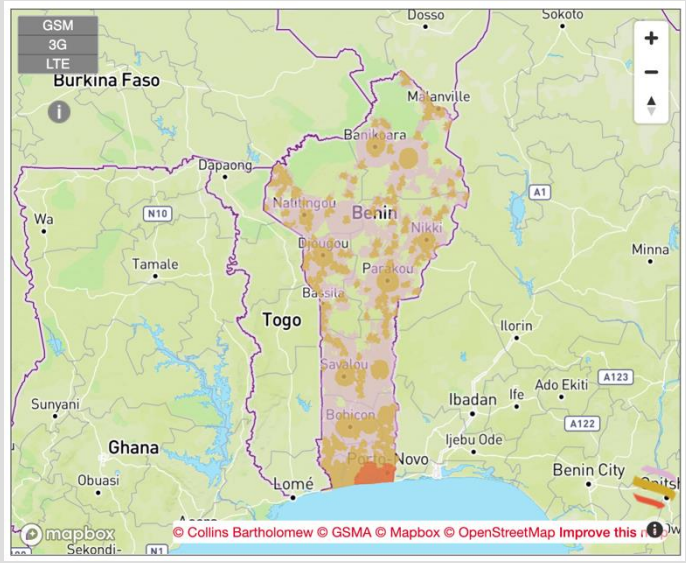


GSMA, 2021

The Alan Turing Institute

×





The Alan Turing Institute

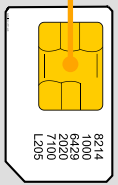
“When compared to other types of ID credentials, chip-based smart cards incur higher costs for design, printing and distribution”

– World Bank, 2018, Understanding the cost drivers of identification systems.

The Alan Turing Institute

Card Application Toolkit

a.k.a. the STK!



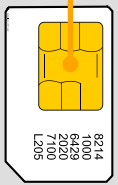
SET UP MENU
GET INKEY
GET INPUT
DISPLAY TEXT
PLAY TONE
SEND SHORT MESSAGE

https://www.cl.cam.ac.uk/~rja14/DigiTally/

The Alan Turing Institute

Card Application Toolkit

a.k.a. the STK!



SET UP MENU
GET INKEY
GET INPUT
DISPLAY TEXT
PLAY TONE
SEND SHORT MESSAGE

INCLUDE ICON

https://www.cl.cam.ac.uk/~rja14/DigiTally/

SIMple-ID – Standards

Standards

- Protocol/DiD W3C
- Redacted DID needs too
- QR > ITU

- Also, recall, M-Pesa

Impact/Adoption

- MOSIP adopt?
- Note A[illegible] interest
- Agno[illegible] phone too
- Virtual SIM version?

Software Defined Wetware
What if we could mod our biometrics?

- Link between bio- and digital no longer immutable (or unique)
- RNA/Bird Flu rewrite Iris
- Skin Display like Octopus Chromatophores