Decentralised Wallets are coming hurrah!

Abstract: We've been working in the Global South on Trustworthy Digital Infrastructure (starting with Digital Identity) with Gates Foundation funding for 5+ years. Way back near the start, I suggested that decentralised id would be the way to go to gain the populations' trust in many countries. Initial reactions were at best sceptical - we build a prototype service (trustchain) and mobile
(feature phone) client (SIMple Id) that presented tokenized verifiable credentials, and people were impressed but dismissive - may, clearly has government agencies breathing down their necks to make sure population surveillance would be enhanced...of
course, populations got that and responded with "well, hey, then we won't use your pesky intrusive service"
.
So now the reaction is very different, and many nations we visit are working actively on distributed wallet based systems (similar to proposed European approach).

All that remains centralised is foundation id (typically things issued by governments anyhow
like birth certificates and passports and maybe driving licenses etc).
The other side of this is a nice idea on how to make the infrastructure for partly state-bases services sustainable in terms of software support - by allowing wallets to proliferate, be diverse with varying roots of trust, and interoperate via federation, there is now a commercial model for such services and a means for government to collect fees for commercial use of the government root of trust, if necessary

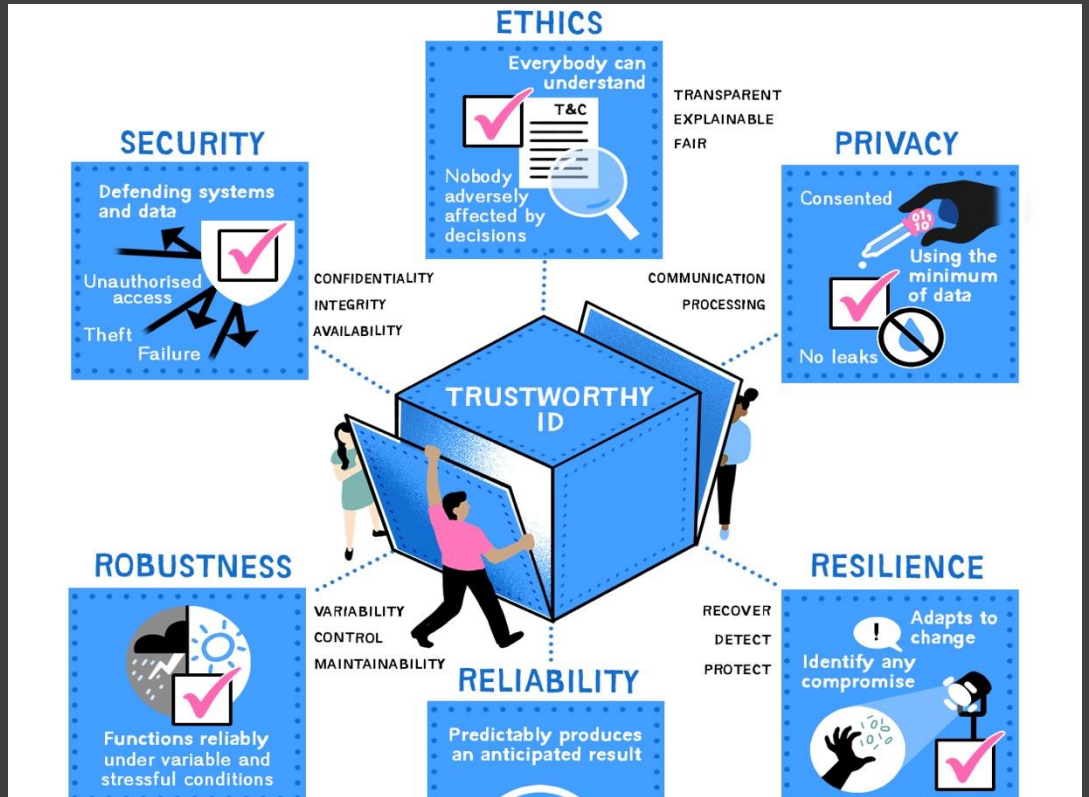
Challenges

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

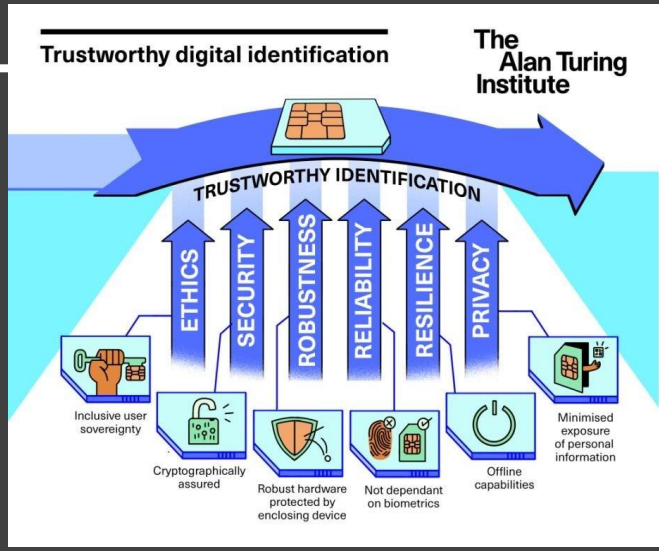


The Framework

Six facets
Measurable features & attributes
Creative Commons licence



A comprehensive framework for establishing the different assurance levels of an identity system in terms of its system components, information system flows, physical and logical processes, and information systems.



Accompanying assessment tool is ready for use.

Comprises of 381 metrics across 65+ mechanisms amalgamated of standardisation documents, best practices, guidelines and codes, e.g. ISO27000x / NIST CFS/ NIST SP80xx family / ETSI 319411 / GDPR / ISO 29146 29115 / MAGERIT/ MITR

Reviewed by members of World Bank, ID4Africa and Aadhaar teams.

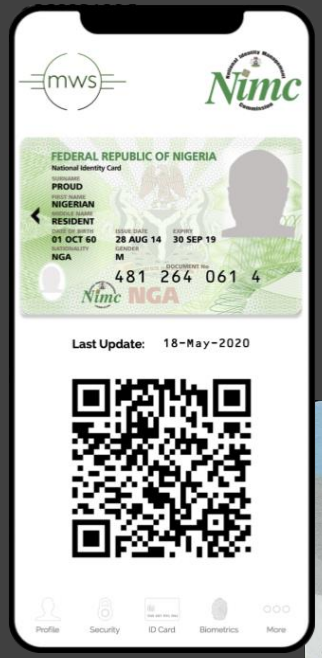
In-country testing and release to community expected over late 2024.

The Alan Turing Institute



Trustchain:
Trustworthy Decentralised Public Key Infrastructure

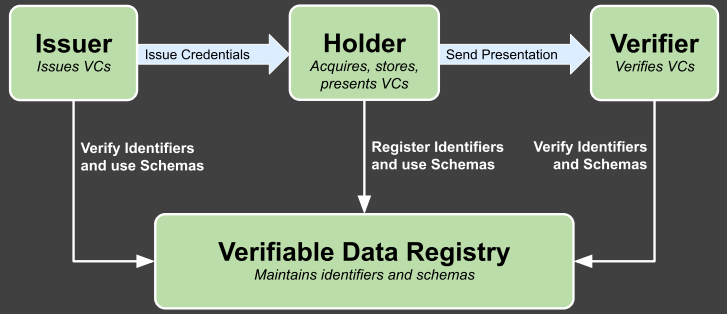
Digital ID

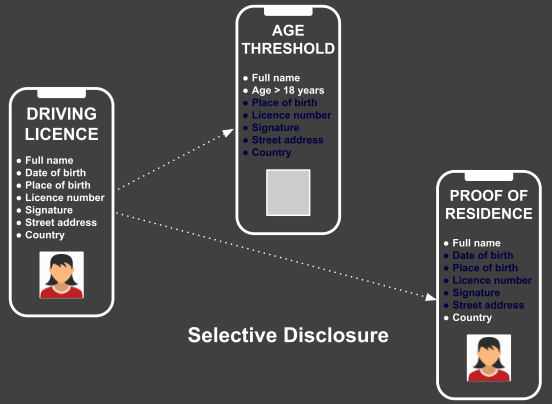






Credentials & Attributes



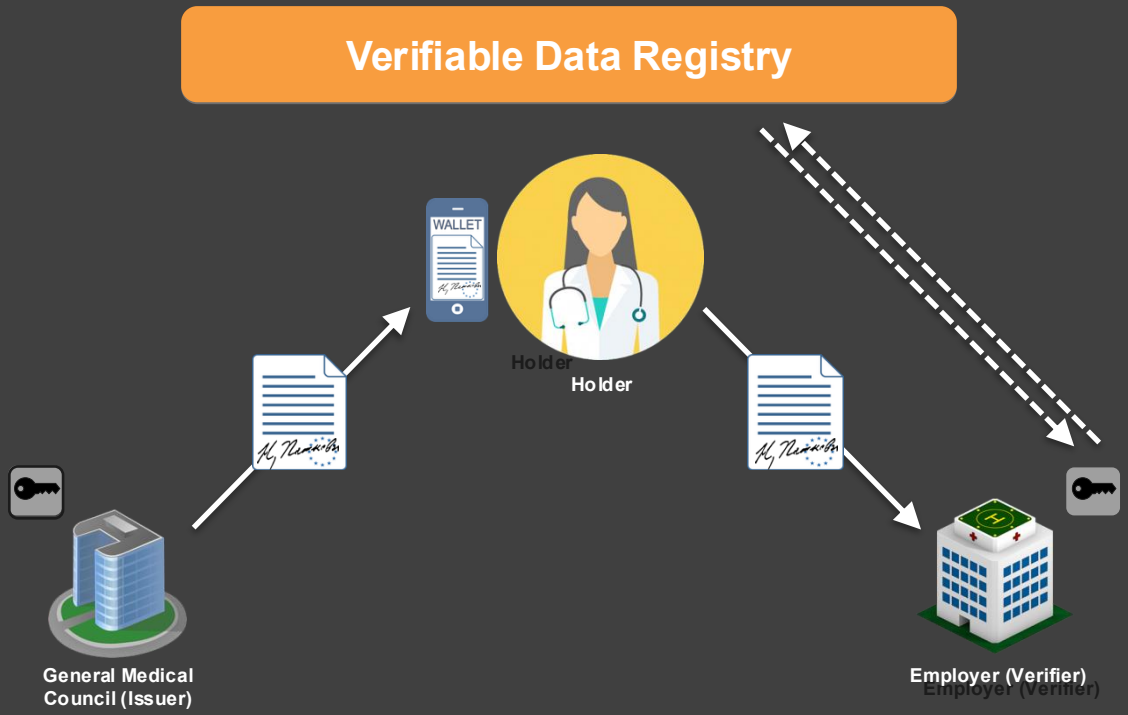




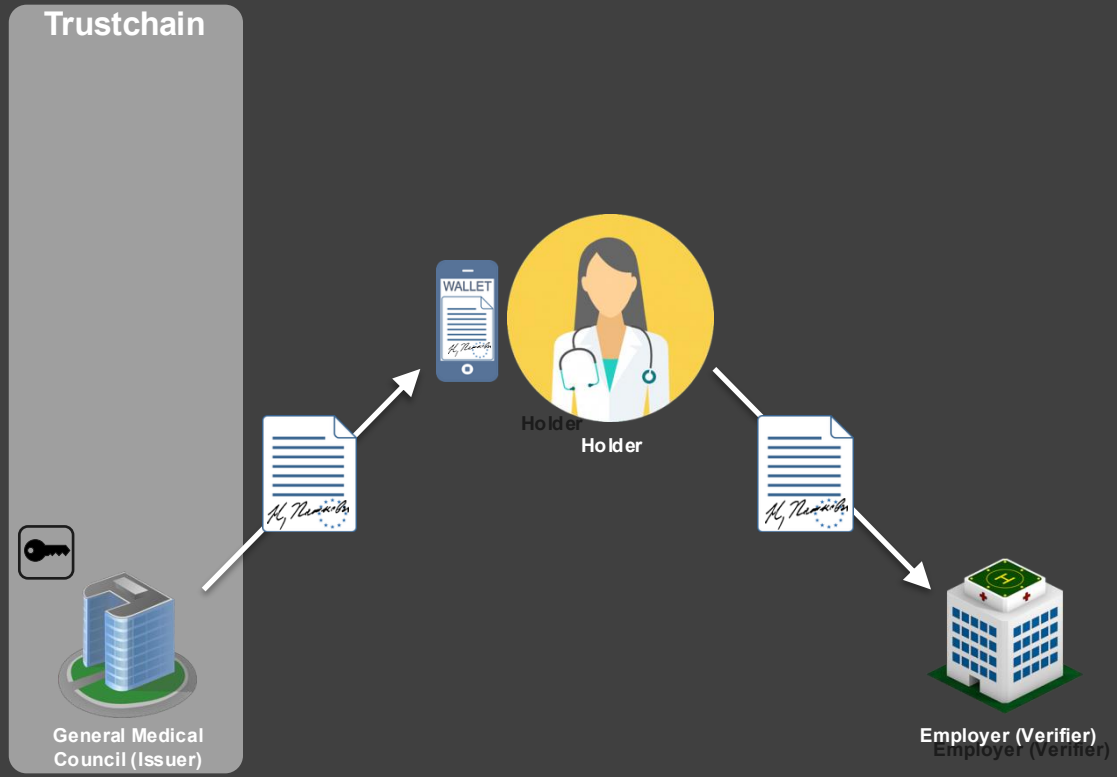
The trust framework aims to make it easier and more secure for people to use services that enable them to prove who they are or information about themselves. It is a **set of rules** for organisations to follow if they want to provide secure and trustworthy digital identity and/or attribute solutions . […]

This document does **not** […] **provide a technical architecture** for digital identity and attribute.”

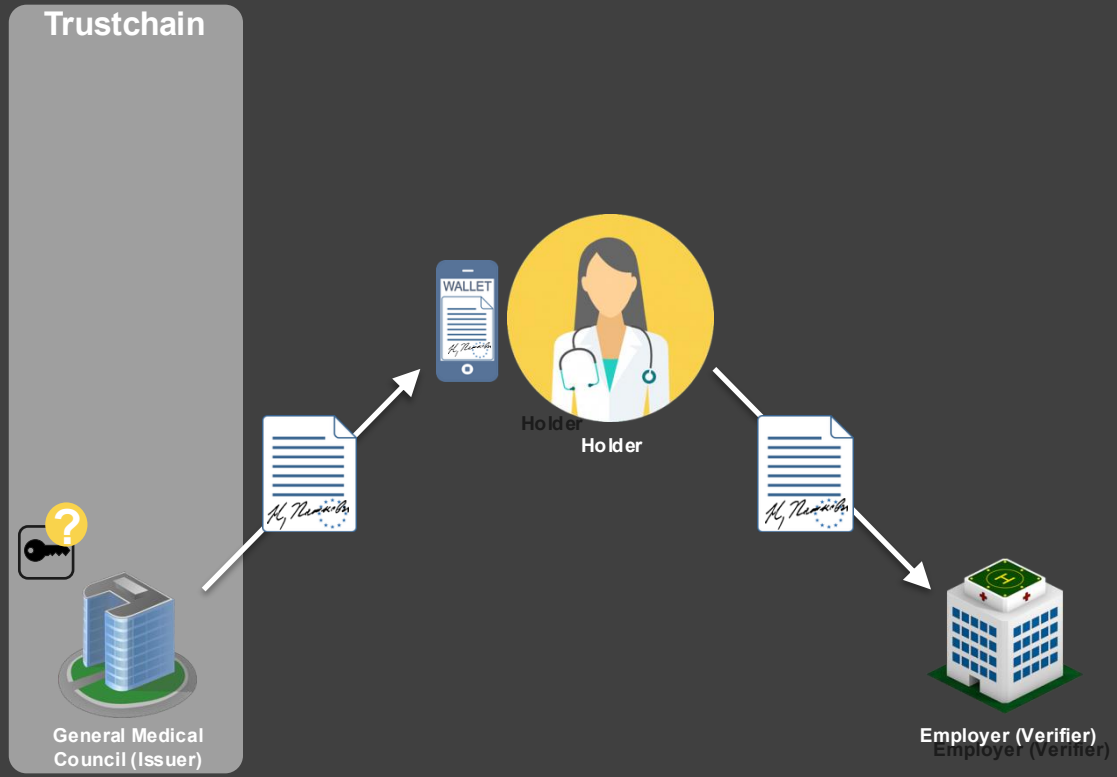
Use case: Medical licence



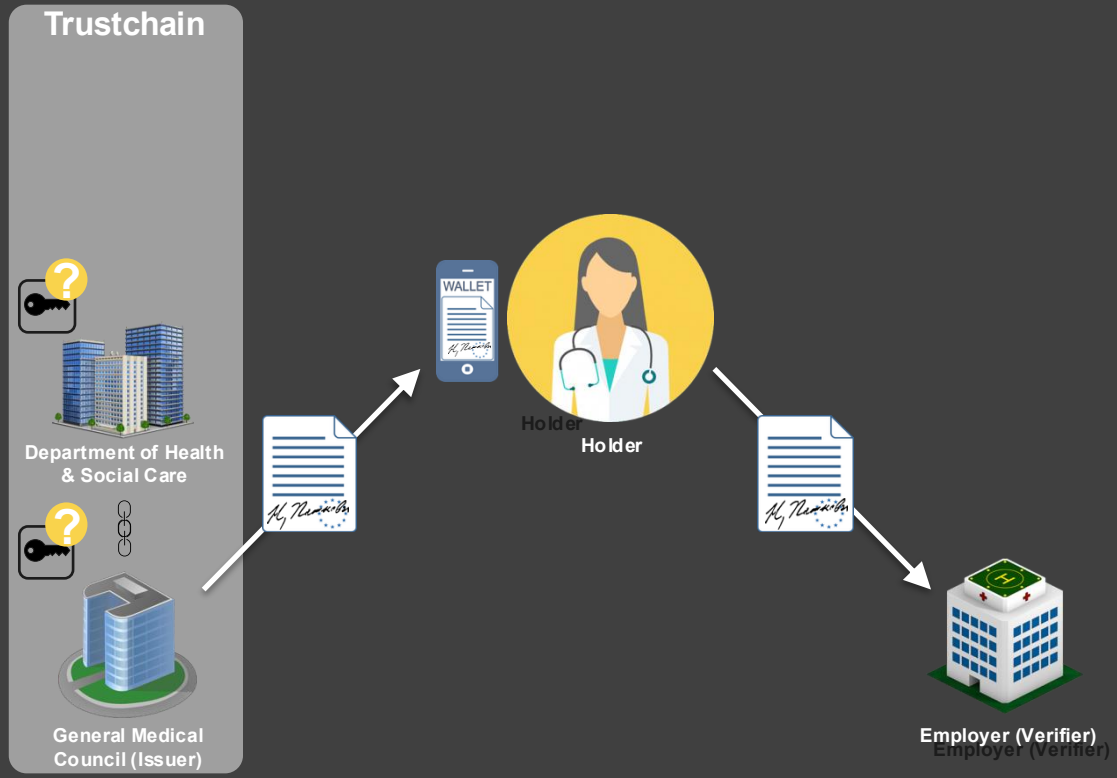
Use case: Medical licence



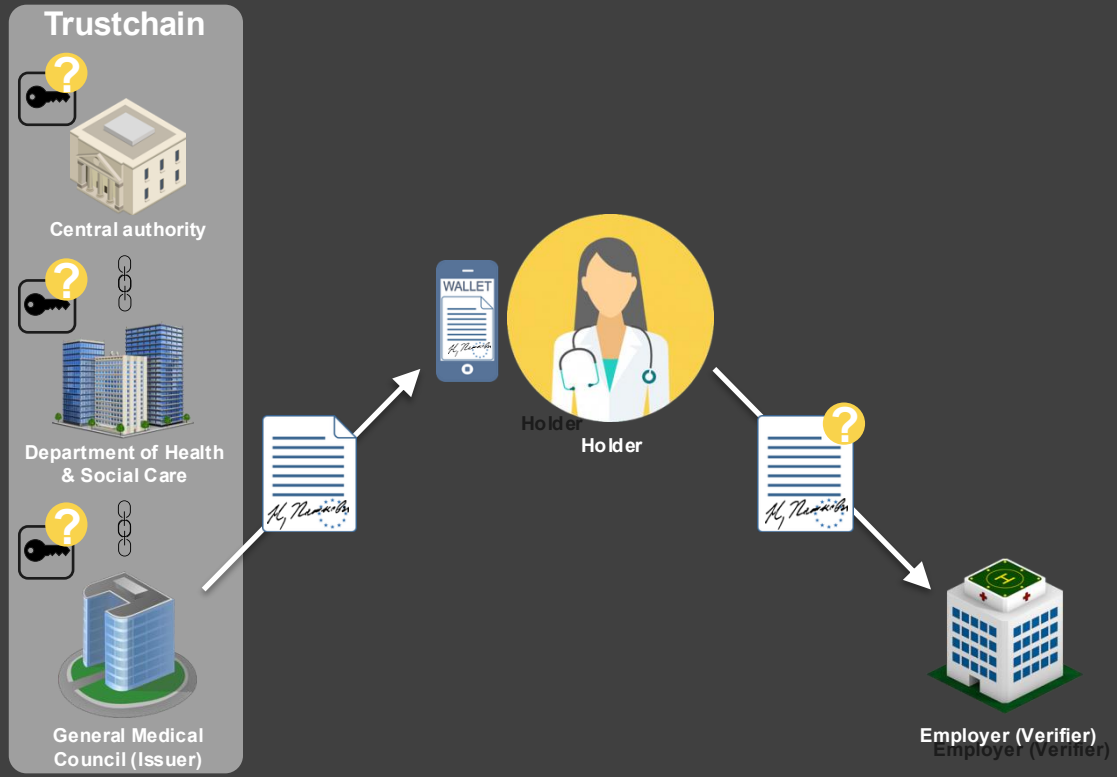
Use case: Medical licence



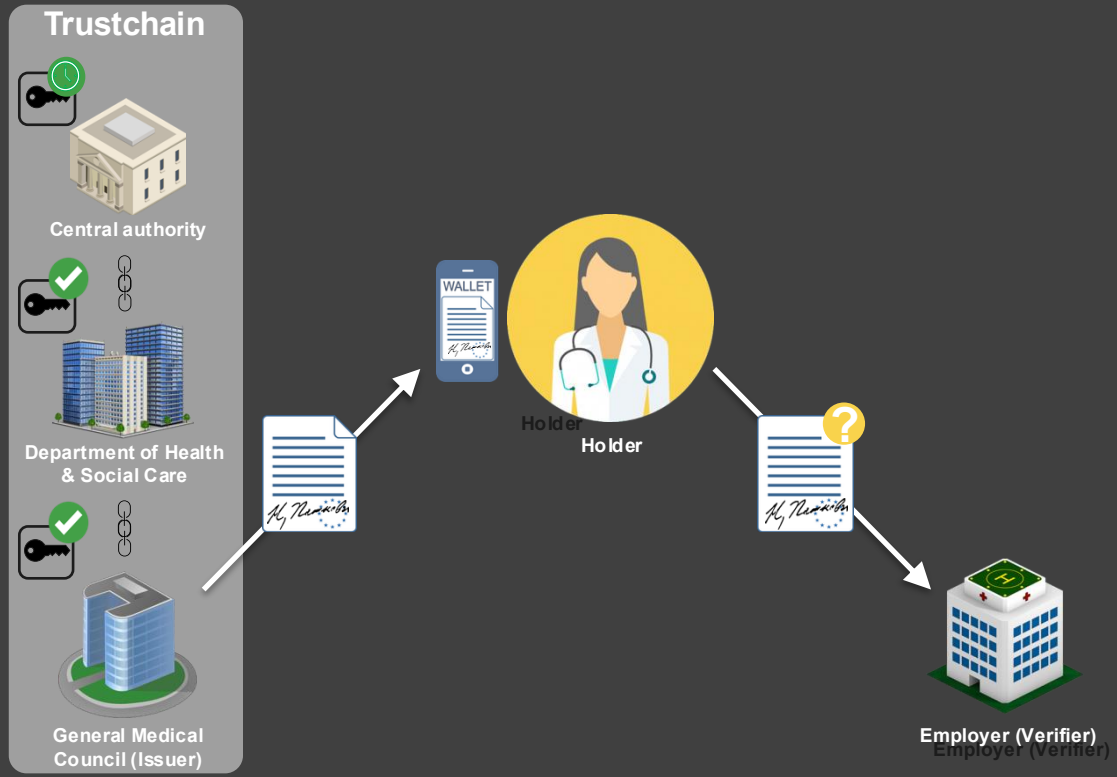
Use case: Medical licence



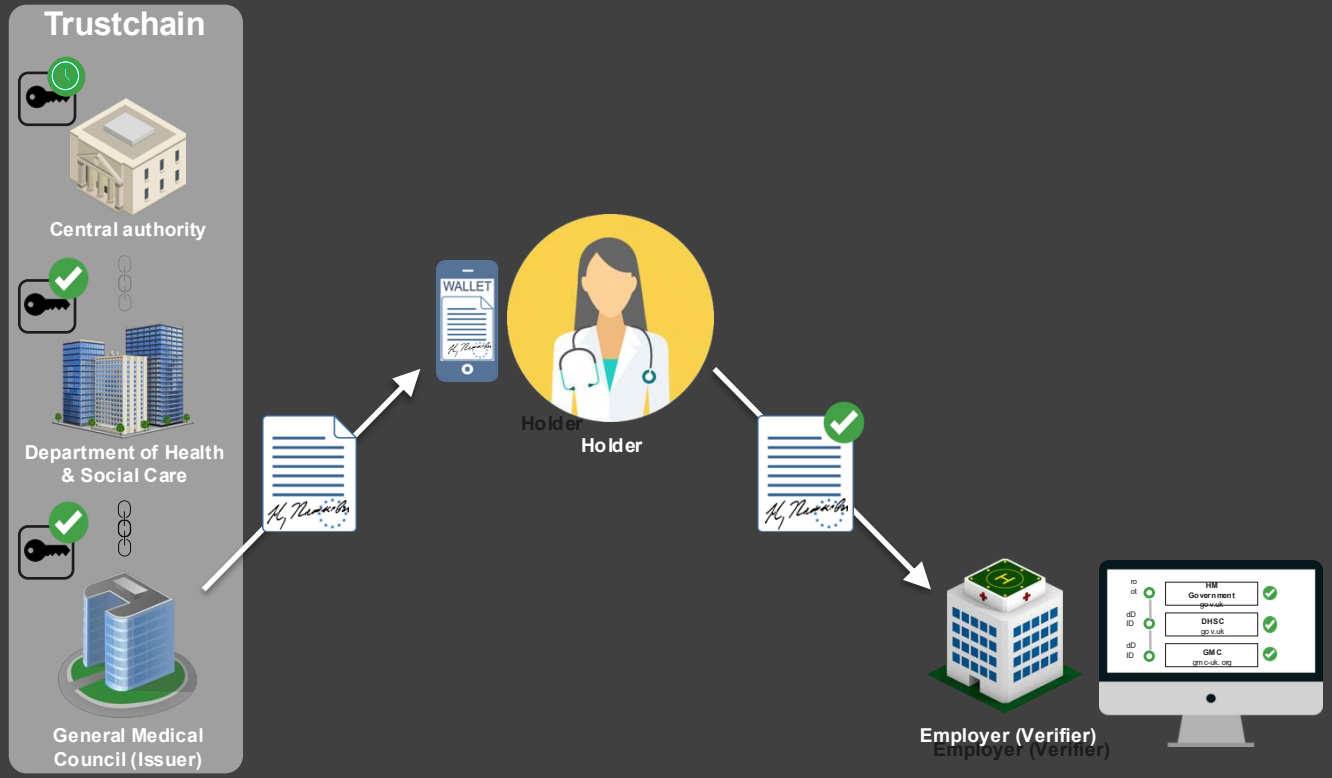
Use case: Medical licence



Use case: Medical licence

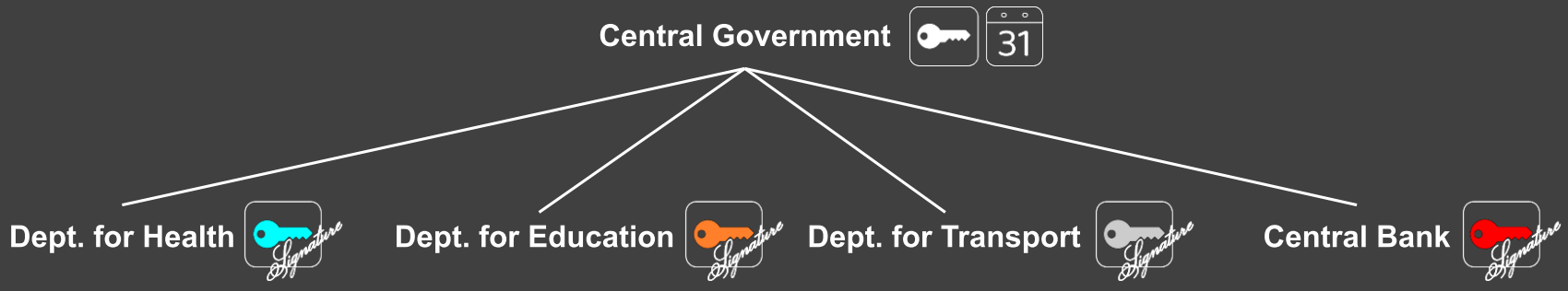


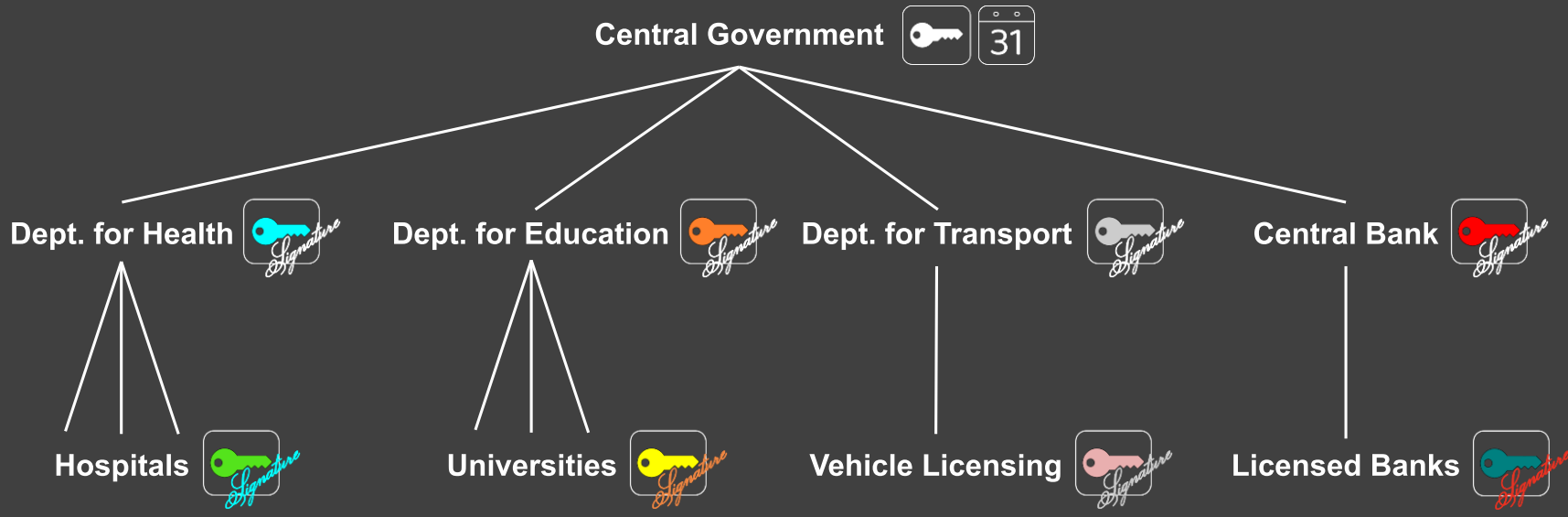
Use case: Medical licence

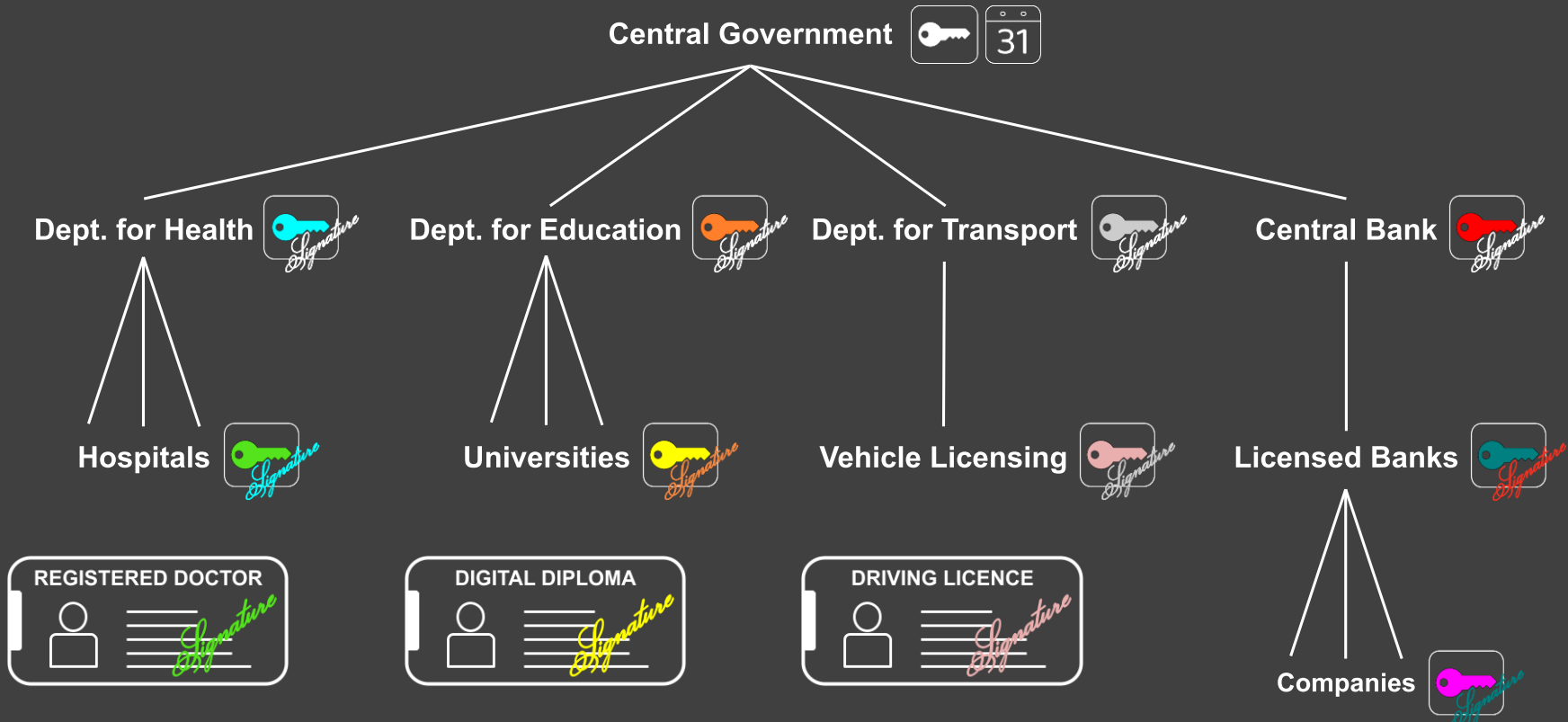


Decentralised Public Key Infrastructure

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

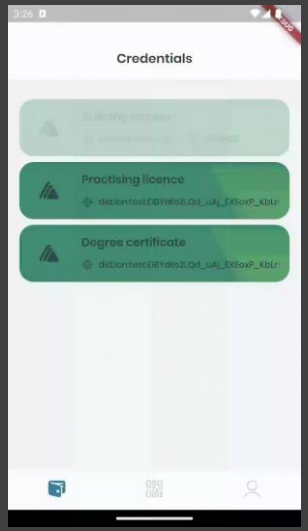

Central Government
31
Dept. for Health
Signature
Dept. for Education
Signature
Dept. for Transport
Signature
Central Bank
Signature

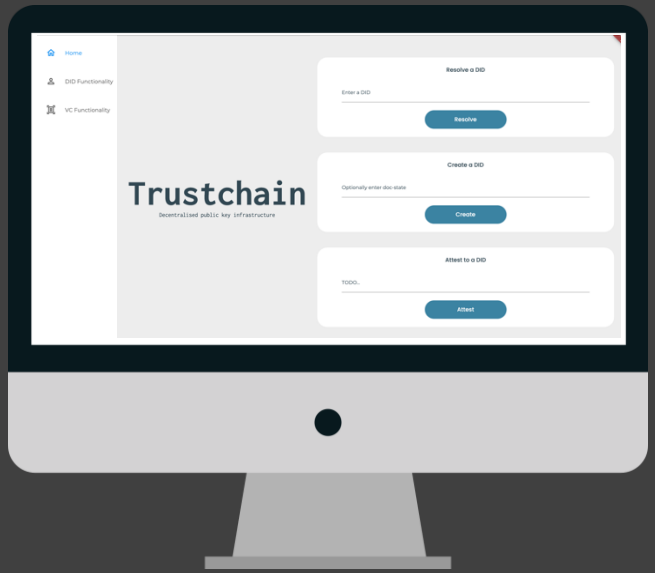

Central Government
31
Dept. for Health
Signature
Dept. for Education
Signature
Dept. for Transport
Signature
Central Bank
Signature
Hospitals
Signature
Universities
Signature
Vehicle Licensing
Signature
Licensed Banks
Signature


Central Government
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
REGISTERED DOCTOR
Signature
DIGITAL DIPLOMA
Signature
DRIVING LICENCE
Signature
Companies
Signature

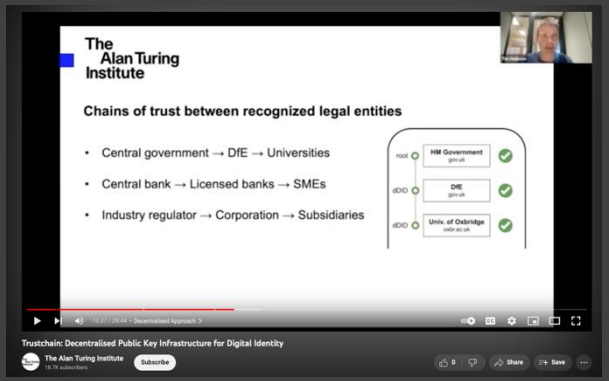
Trustchain resources

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[6], 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.

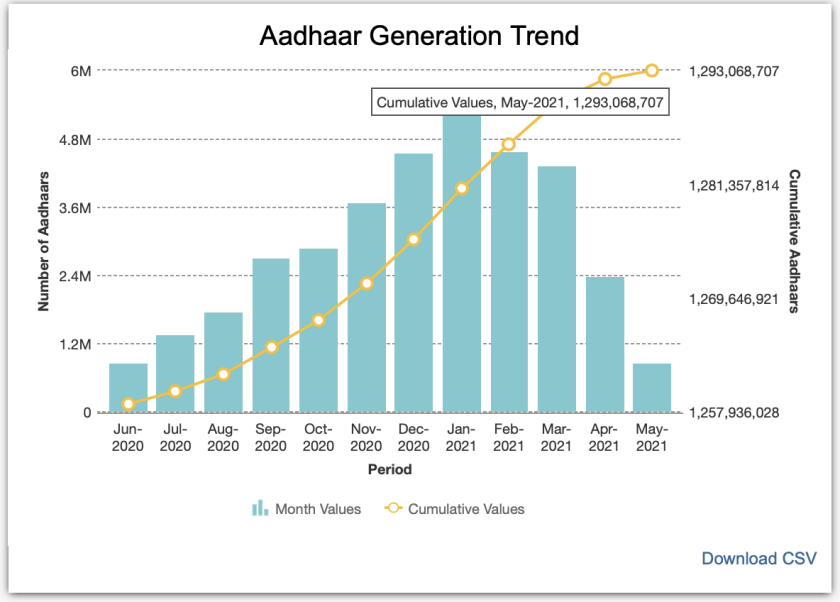
- New work using DAGs and Mysteci platform promising…

The Alan Turing Institute



SIMple ID

Can basic mobile phones display QR codes for digital identification?



Daily Authentication Trend for Transactions

Demographic Authentication Trend

Total Transaction	11,432,955,673

Biometric Authentication Trend

Total Transaction	41,772,861,733
Fingerprint Authentiction	40,857,370,044
Iris Authentications	909,900,669

OTP Authentication Trend

Total Transaction	1,538,732,976

Total Authentication Transaction **55,050,306,429**

04 June 2021

Fair Price Shops


Photo: Reuters

- 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



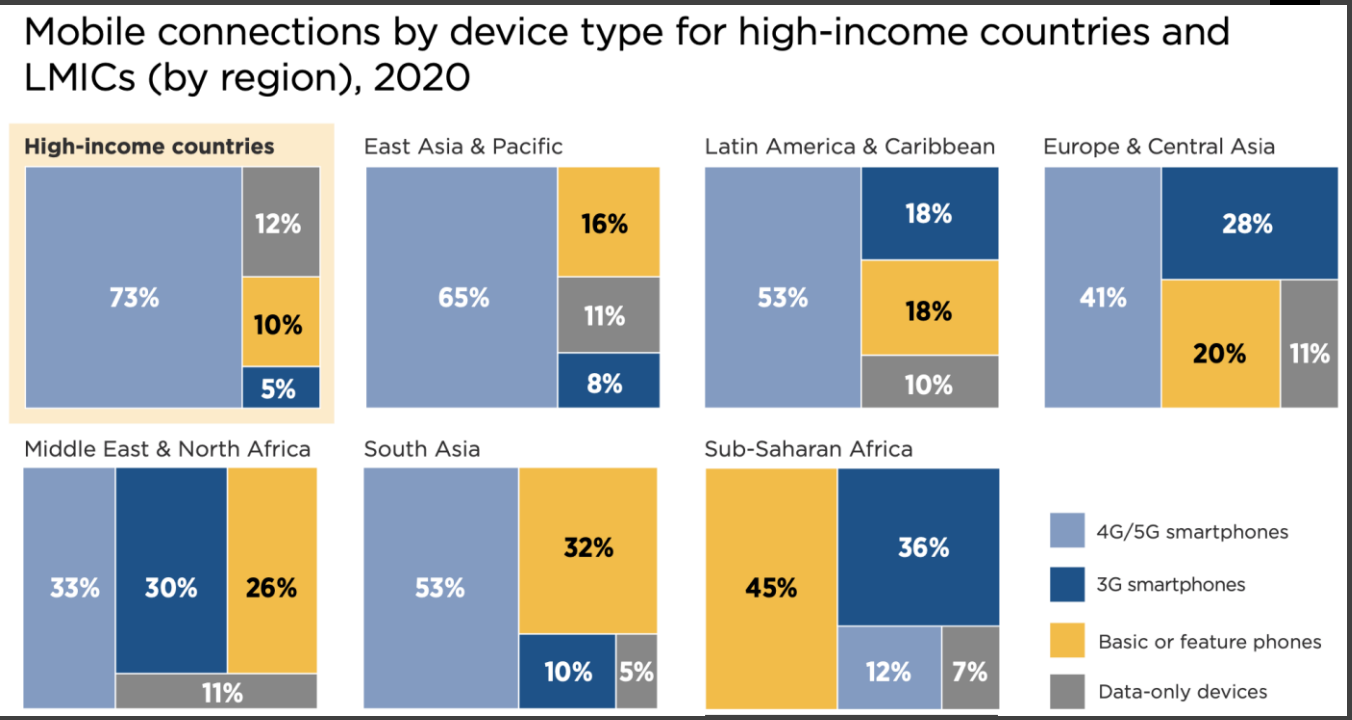


or



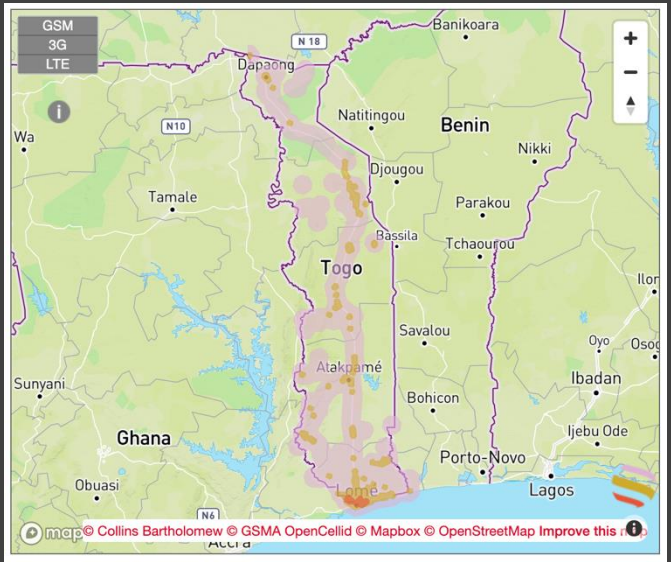
The Alan Turing Institute

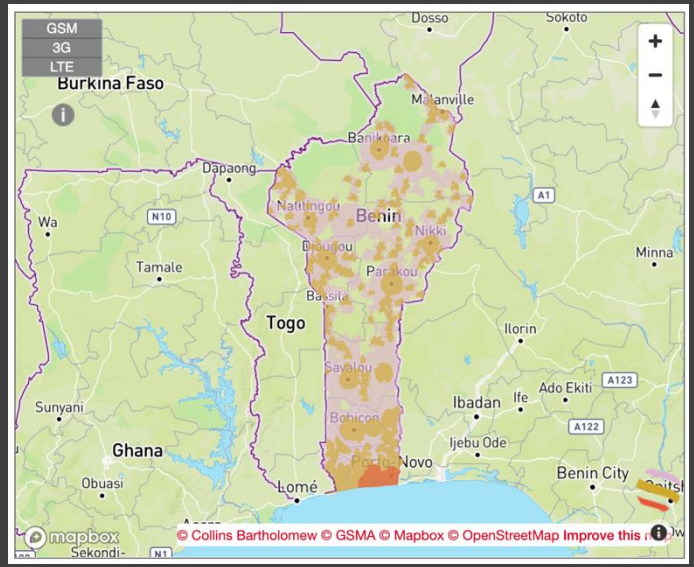
Mobile connections by device type for high-income countries and LMICs (by region), 2020



GSMA, 2021

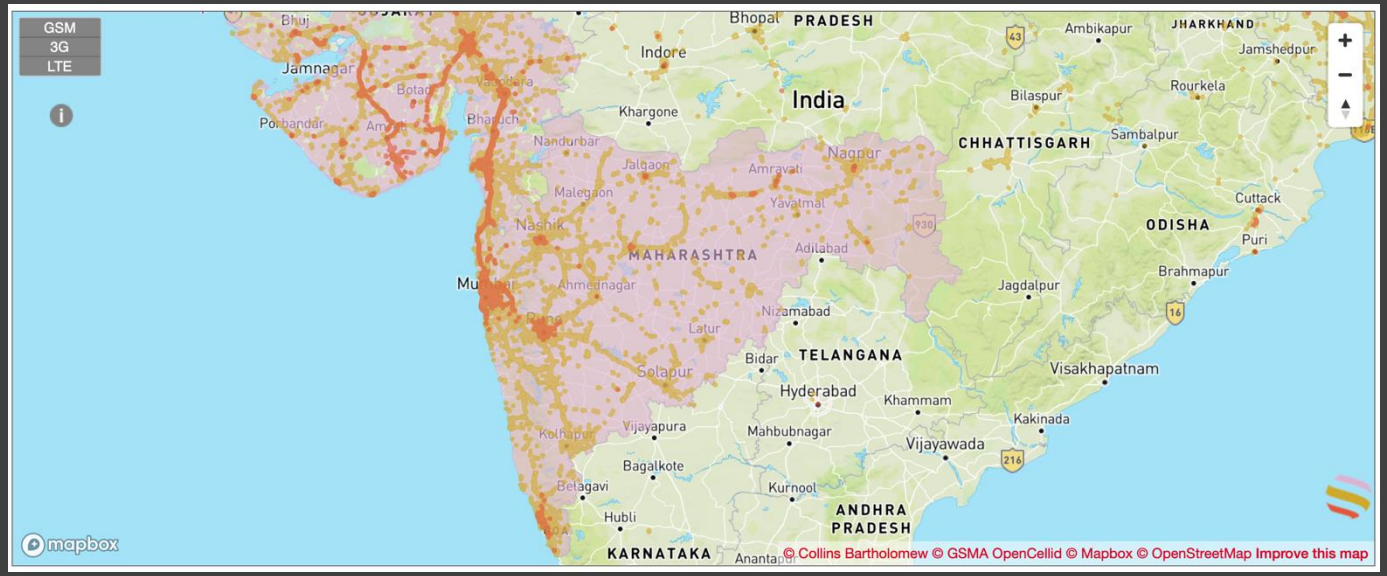
The Alan Turing Institute





The Alan Turing Institute

4G



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



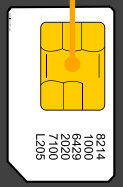
https://www.cl.cam.ac.uk/~rja14/DigiTally/

The Alan Turing Institute



System

- Proprietary
- **Not developer friendly**



Outputs

- Screen (low res.)
- Sounds
- Vibrations
- Cellular

Inputs

- Text
- Microphone
- Cellular

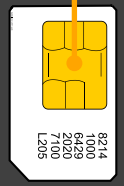
https://www.cl.cam.ac.uk/~rja14/DigiTally/

The Alan Turing Institute



UICC (System 2)

- Somewhat developer friendly
- Secure Hardware
- Dedicated cryptographic co-processor
- Can be Java-based
- **Card Application ToolKit**



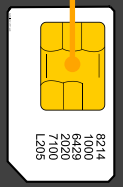
https://www.cl.cam.ac.uk/~rja14/DigiTally/

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

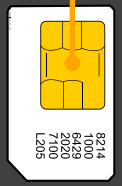
https://www.cl.cam.ac.uk/~rja14/DigiTally/

The Alan Turing Institute



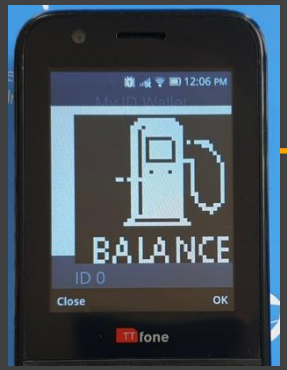
Card Application Toolkit

a.k.a. the STK!



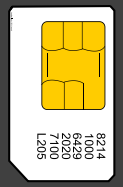
SET UP MENU
GET INKEY
GET INPUT
DISPLAY TEXT
PLAY TONE
SEND SHORT MESSAGE

INCLUDE ICON



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

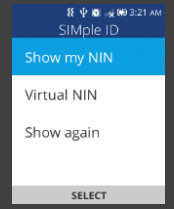
The Alan Turing Institute

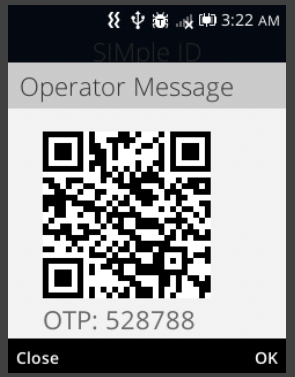




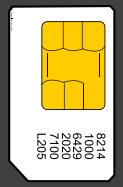
SIMple-OTP provides a standard OTP authentication and runs between the resident R, the UICC U, the requesting entity V and the issuer I. To begin, R has the PIN *pin* and U has the UID *uid* and OTP parameters (k_{OTP}, c). I has private signing key $k_{I\text{sig}}$, the CIDR containing unique residents' UID *uid* and OTP parameters (k_{OTP}, c) linked in the SIMple-Personalise phase.

1. The resident R sends the PIN attempt pin' to the UICC U.
2. If $pin' \neq pin$ then authentication fails. Otherwise U computes the OTP $hotp = \text{HOTP}_{k_{\text{OTP}}}(c)$, increments the OTP counter c, and then sends the authentication message $m_{\text{auth}} = (uid \parallel hotp)$ to V.
3. V sends m_{auth} to the issuer I (e.g., using the SA-UA network).
4. I uses *uid* to look up the resident's eID record of the OTP parameters (k_{OTP}, c) and computes the OTP response $hotp' = \text{HOTP}_{k_{\text{OTP}}}(c)$. If the OTP is correct, i.e., $hotp' = hotp$, then I computes the response message $m_{\text{resp}} = \text{SIGN}_{k_{I\text{sig}}}(\text{“}yes\text{”})$ and increments c. Otherwise, I computes $m_{\text{resp}} = \text{SIGN}_{k_{I\text{sig}}}(\text{“}no\text{”})$. I sends m_{resp} to the requesting entity V.
5. V verifies the signature on m_{resp} and, if successful and the message is “yes” then authentication succeeds. Otherwise authentication fails.



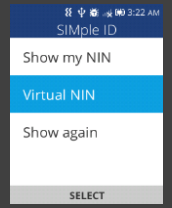


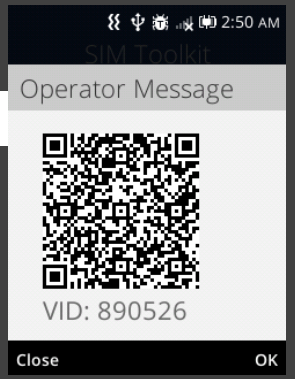
The Alan Turing Institute



SIMple-VID provides authentication with improved privacy using public key encryption to hide the resident R's UID *uid* from the receiving entity V. This phase is run between R, the UICC U, V and the issuer I. To begin, R has the PIN *pin* and U has the UID *uid* and OTP parameters (k_{OTP}, c). I has private signing key $k_{I\text{sig}}$, private decryption key $k_{I\text{enc}}$, the CIDR containing unique residents' UID *uid* and OTP parameters (k_{OTP}, c) linked in the SIMple-Personalise phase.

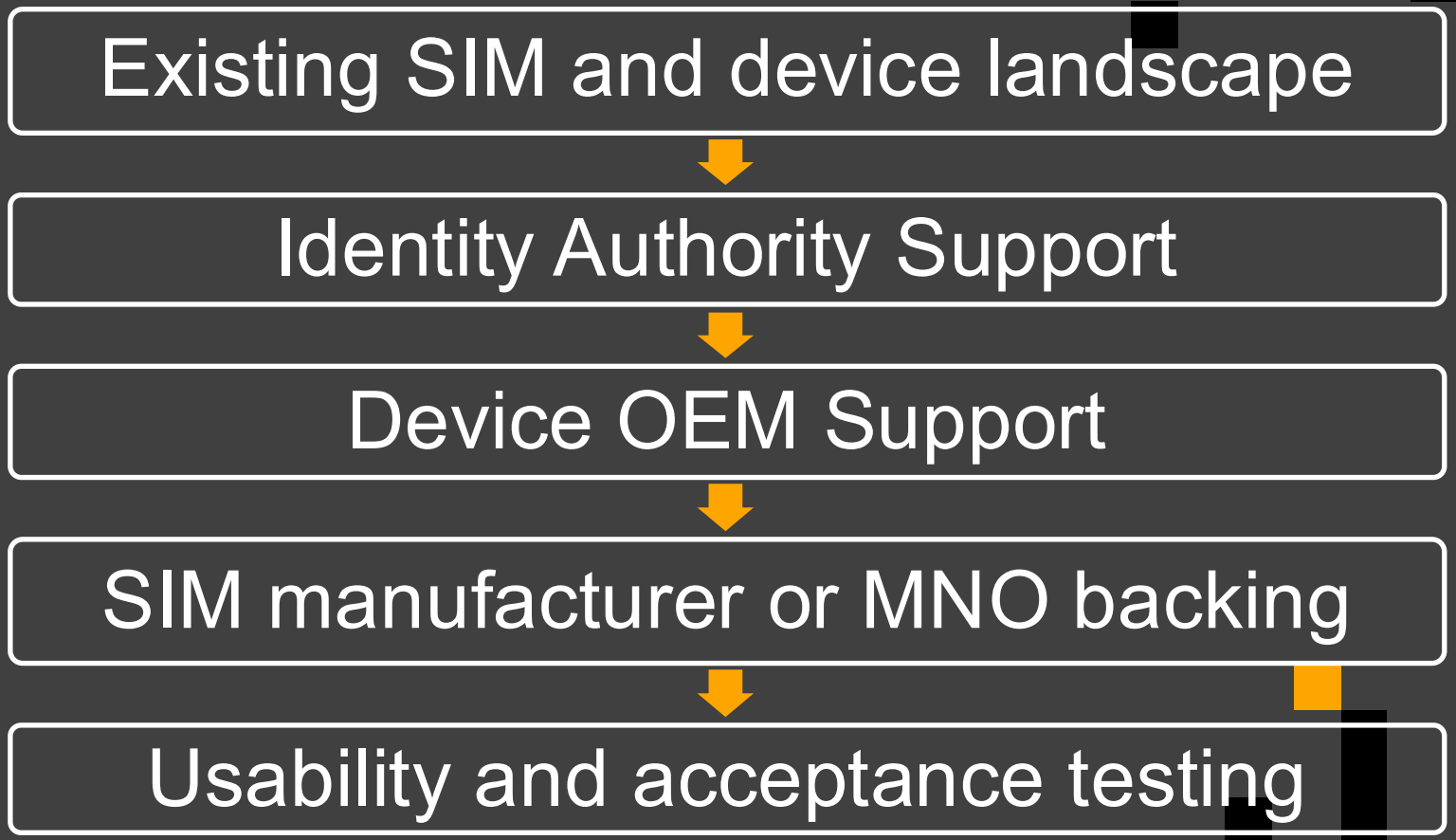
1. The resident R sends the PIN attempt pin' to the UICC U.
2. If $pin' \neq pin$ then authentication fails. Otherwise U computes the OTP $hotp = \text{HOTP}_{k_{\text{OTP}}}(c)$, encrypts the authentication challenge $c_{\text{chal}} = \text{ENC}_{P_{I\text{enc}}}(uid \parallel hotp)$ using the public key of the issuer I and increments the OTP counter c. The UICC U sends c_{chal} to the receiving entity V (i.e., it is shown as a QR code).
3. V sends m_{auth} to the issuer I (e.g., using the SA-UA network).
4. I recovers *uid* and *hotp* by decrypting c_{chal} using the private encryption key $k_{I\text{enc}}$. Next, I runs Step 4. from the SIMple-OTP phase.
5. V verifies the signature on m_{resp} and, if successful and the message is "yes" then authentication succeeds. Otherwise authentication fails.





The Alan Turing Institute

Deployment considerations



SIMple-ID – Standards

Standards

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

Impact/Adoption

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

Example standard QR Codea

The next phase - wallets

