Digital Identity in the UK: An Update

Campbell Cowie, Head of Policy, iProov

Proven market leadership at scale

Government Services

Government Digital Service

ID.me

IRS

Home Office

GOVTECH SINGAPORE

Australian Government
Australian Taxation Office

Borders & Travel

U.S. Department of Homeland Security

eurostar

Digital ID for Citizens

NHS

itsme

CA.GOV

State of California DMV Department of Motor Vehicles

id A service by

Banks & Financial Services

UBS

bradesco

EastWestBank

ING

Standard Bank

absa

bankaxept

Norway's national Bank ID

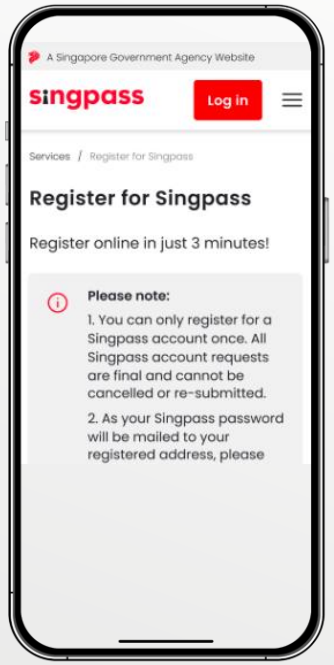
Biometrics for identity creation and assertion

Identity

Individual

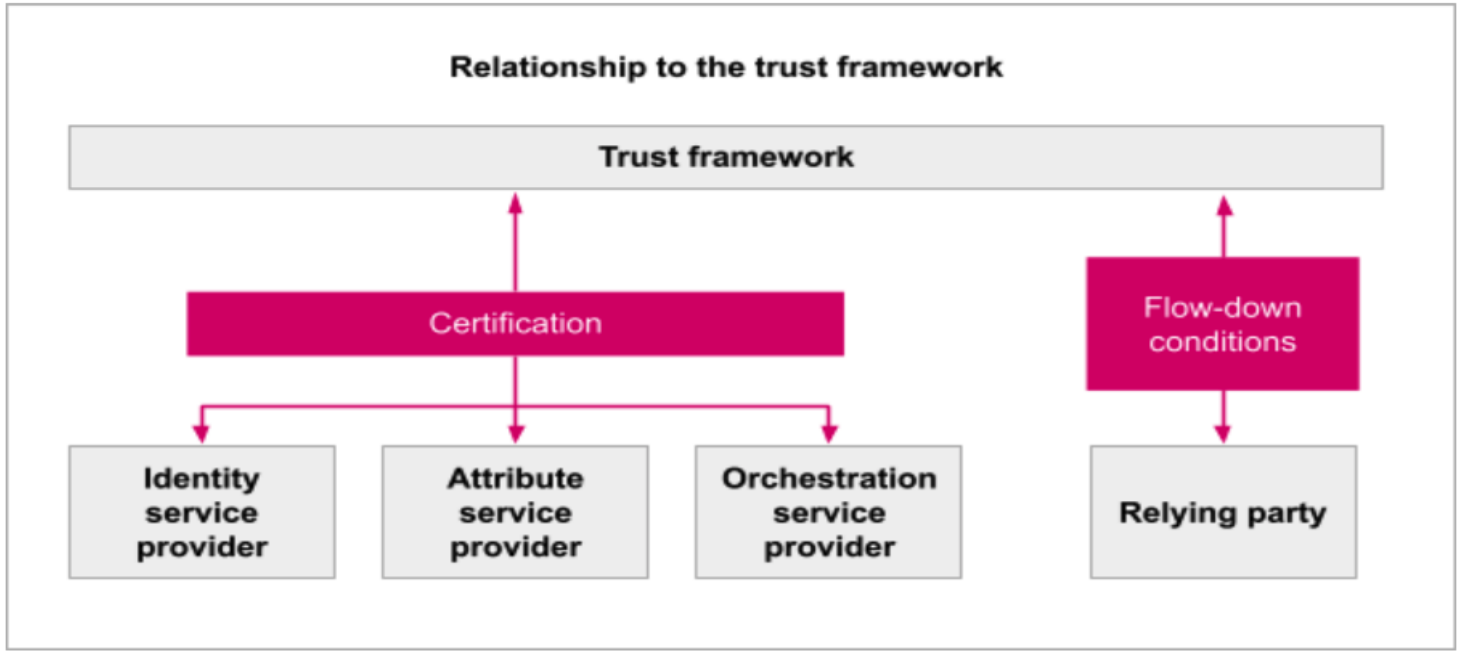
Biometrics connect the person to their government and digital identities

Biometrics are used in successful national Digital Identity programs



The UK Trust Framework is built around Good Practice

The UK Digital Identity and Attributes Trust Framework (DIATF) is a set of rules and standards for digital identity services that aims to make them more secure and trustworthy



DIATF focus is access to Government services – not a national ID scheme

Draft legislation is expected in October to place DIATF on a statutory footing, creating a formal ID framework, although not a national ID scheme. DIATF has 3 components:-

- **Certification** – accredited auditors must certify participating organisations
- **Standards** – DIATF sets out minimum requirements, including rules for privacy, data protection, fraud management and security
- **Updates** – updates will be managed by the governance body, as technology evolves

Controversially, direct regulation by Government rather than independent regulator

Key strategic questions remain unanswered

Regulatory Model

- Strong stakeholder preference for existing independent regulator (Ofcom) over Government oversight
- Role of Government in the market with OneLogin?
- Could OneLogin be a UK Digital Wallet?
- No enforcement framework yet and no performance KPIs.
- **No focus on Digital ID as a driver for economic growth**

Age Assurance

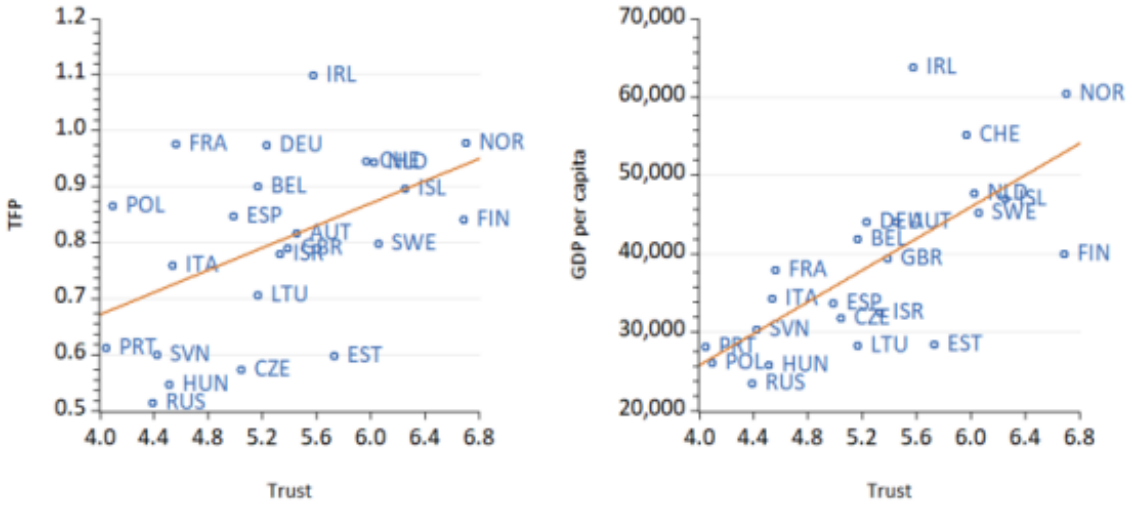
- Securing age-appropriate sales and protecting children online is critical
- Estimation vs verification a key decision to be taken
- Only verification underpinned by ID is accurate and legally robust
- Verifiable credentials offer privacy secure solution

Testing & Standards

- Should external lab testing be mandatory?
- How to move from lab-testing to real world application
- WCAG tests for accessibility
- AI model safety checks under development
- How to align UK standards to EU, US and ASEAN markets

Trust fuels growth through increased productivity

Research shows the causal relationship between trust and growth



Coyle, D & Lu, S (2020), *Trust and Productivity Growth - An Empirical Analysis*

How this happens matters

- Research shows digital transformation to be the spark for growth.
- However, anonymous digital transactions across remote supply chains can trigger costly compliance requirements.
- Asymmetry of information between trading parties creates a coordination problem

Trustworthy Digital ID lowers transactions costs

Trustworthy Digital ID is a powerful catalyst

To illustrate the magnitude of the potential impact of improved trust on growth, the World Economic Forum (WEF) estimates that (in 2019 values) **“a 5% point increase in digital trust results in an average increase in GDP per capita of $3,000”.** For example, the WEF impact estimate for Indonesia is $3640(US) in 2024 values - **an addition to GDP of $1tn and an incremental tax receipt of $100bn in 2024.**

But not all Digital IDs are equally trustworthy

Inclusive: System design identifies and mitigates barriers to access, usability and usefulness to create a service which is responsive to the needs of various users.

Useful: Users have a simple, convenient - verify once, use many times - experience that is reliable, trusted, and accepted for use across multiple contexts. This adds value to their everyday lives.

Accountable: Users and their data are kept safe through processes that ensure integrity, auditability, accuracy, and control.

Responsible: System design leverages open standards, decentralisation, cryptography and industry good practices to deliver a robust, secure, responsive, and sustainable service.

Transparent: Users have the right to understand how their data is used. They are able to choose why, when, and where it is used, with explicit consent or as permitted by law.

Fair: System design implements data-minimisation, privacy-by-design and user control to ensure that data is only used for legitimate, proportionate, and non-discriminatory purposes.

Towards decentralized identity

e.g. Singpass

Including Biometrics

e.g. eIDAS1, Azure AD

Including Biometrics

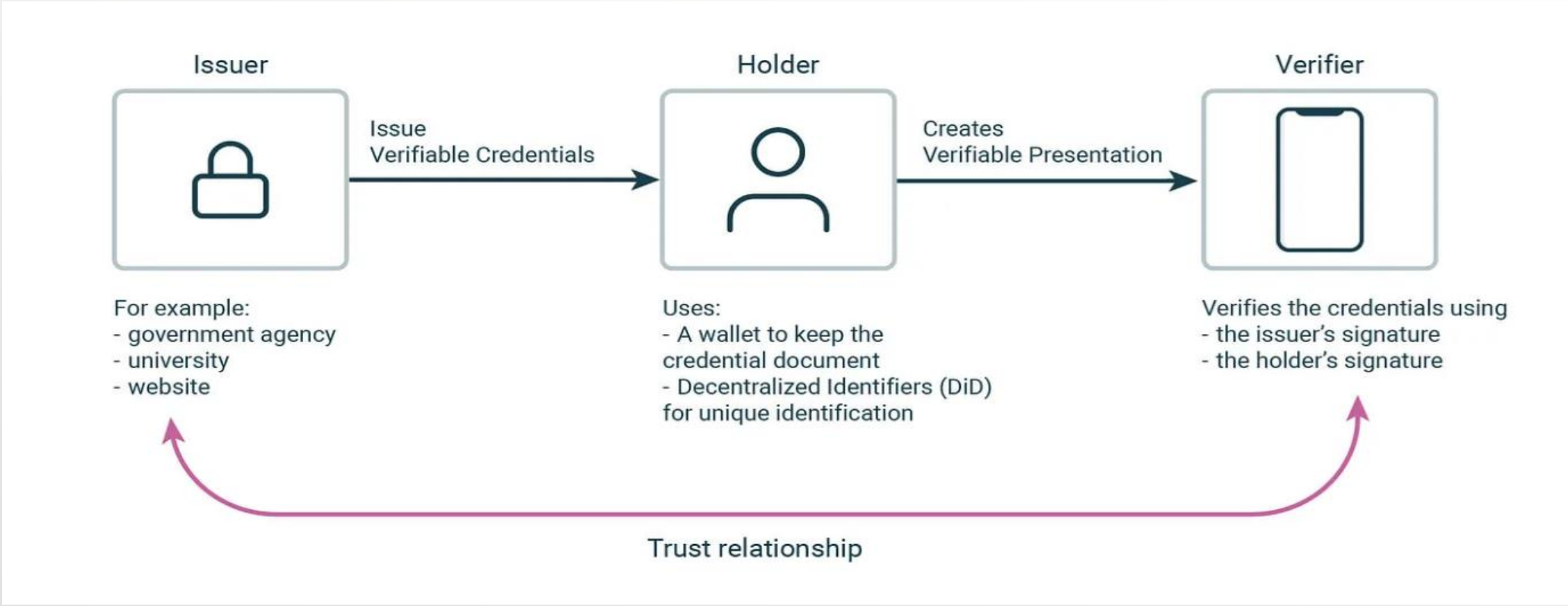
e.g. eIDAS2, CBP, mDLs, Ping

Including Biometrics

"Digital identity has evolved from centralised to federated models. Federated identity only addresses authentication—every other aspect of identity is still based on the centralised model. Beyond federated identity, a new architecture of decentralised identity is emerging."

https://www.citi.com/ventures/perspectives/opinion/digital-identity.html

The roles of a decentralised identity ecosystem



Disrupt the traditional identity ecosystem

Stakeholder	Traditional Identity System	Decentralised Identity System	Impact
Users/Individuals	Limited control over personal data, reliance on centralised authorities for management.	Ownership and control of data, ability to choose what to share and with whom.	Empowerment, increased privacy, and portability of identity across platforms.
Identity Providers	Dominant role in issuing and managing identities, potential for data breaches and misuse.	New competition from decentralised providers, focus shifts to value-added services like verification and authentication.	Evolving business models and the need for collaboration with decentralised networks.
Relying Parties	Reliance on centralised databases for identity verification, risk of fraud and data breaches.	Reduced reliance on centralised data, streamlined verification processes using verifiable credentials, increased customer trust.	Enhanced security, improved user experience, and potential for new revenue streams through data sharing agreements with users.
Data Brokers	Profit from collecting and selling personal data, potential for privacy violations and misuse.	Business model disruption as users gain control over their data, potential to pivot to data aggregators with user consent.	Necessity to adapt to a privacy-centric model, focusing on user-consented data sharing and value-added services based on anonymised data analysis.
Regulators	Focus on overseeing centralised identity systems and enforcing data protection laws.	Need to develop new frameworks for decentralised identity, balancing innovation with security and privacy protection.	Adaptation to new paradigms and challenges in regulating a decentralised, user-controlled identity ecosystem.

Closing comments….

1. **Biometrics with Liveness is a requirement for trustworthy identity schemes**
2. **UK lagging EU, US and many APAC trading partners**
3. **Evidence dictates that economic growth should be a high-profile goal**
4. **The more trustworthy the Digital ID the greater the economic impact**
5. **Trust cannot be asserted but is shaped by the trustworthiness of component parts, including the solution and regulation**
6. **Decentralised identity is lower cost, higher security and pro-privacy – more trustworthy**

iProov

Thank You

Real Person Right Person Right Now

Campbell.Cowie@iproov.com