

The global landscape of identity adoption

Adam Cooper

Expert Advisor to the World Bank, and the European Commission

May, 2025

|next
id

Digital Identity continues to evolve

*Digital Identity should be reusable and
widely accepted.*

*Digital Wallets continue to drive
innovation and standards.*

Use cases are driving agendas e.g. Age Verification and Cross-border Trade.

It's not just about citizens; it's about workforces and organisations too.

Regional approaches to Digital Identity

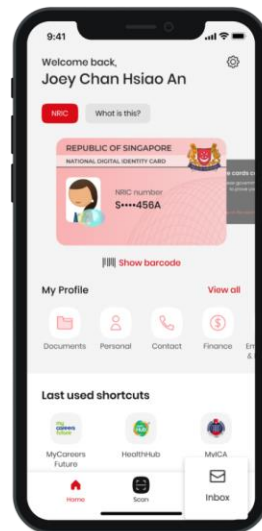
Apps and Decentralised Presentation of Credentials

Across Asia and the Pacific, countries are embracing Apps and Wallets to provide digital identity and access to wider public services.

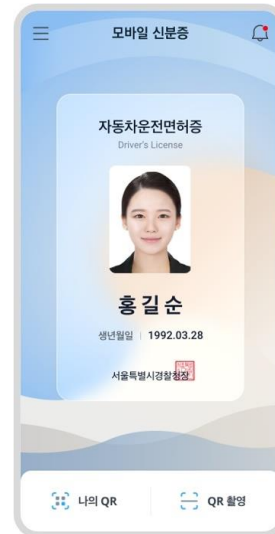
Bhutan



Singapore



South Korea



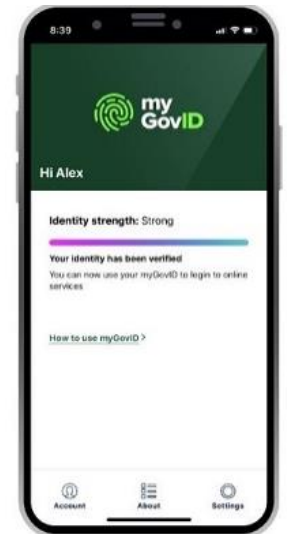
Thailand



Vietnam



Australia



European countries push forward with Digital Wallets and EUDI

The number of countries with advanced Identity Wallet projects continues to grow.

The EU Commission has published implementing acts for EUDI.

AT Austria BE Belgium HR Croatia

CY Cyprus CZ Czech Republic

EE Estonia FR France DE Germany

GR Greece HU Hungary IE Ireland

MT Malta NL Netherlands IT Italy

PL Poland PT Portugal ES Spain

RS Serbia CH Switzerland

GB United Kingdom

The rise of Digital Wallets globally

Canada / British Columbia

Licences e.g. digital lawyer member card from the Law Society of British Columbia
Person credential the BC Services Card app
Academic diplomas (education transcripts)

USA

Mobile Driver's Licences (mDL) issued by multiple states
Google and Apple providing mDL support in their wallets
RealID providing a legal framework for use of mDL and trust in issuance

European Union

Large Scale Pilots - over 250 private companies and public authorities across 28 countries.
Strong legal framework - eIDAS / EU Digital Identity Framework Regulation

Central and Western Asia

Many countries closely following the EU model e.g. Ukraine and Georgia.

South Asia

Bhutan NDI wallet holding ID and public and private sector credentials.

East Asia

Thailand and South Korea already have VC wallet solutions and others such as Singapore are following closely.

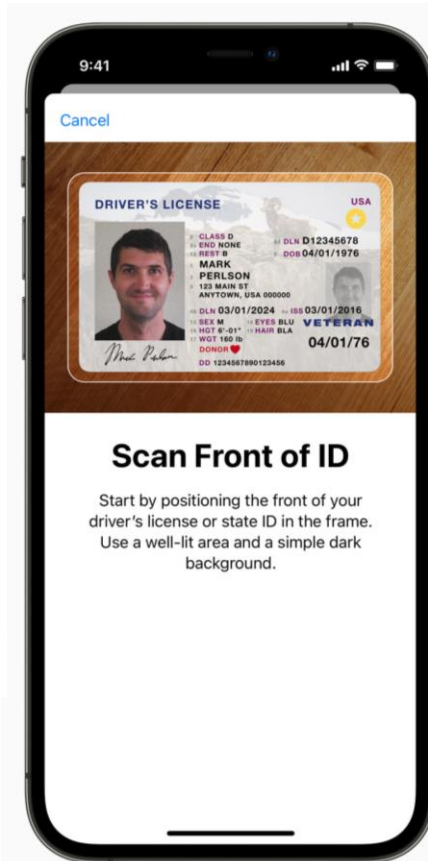
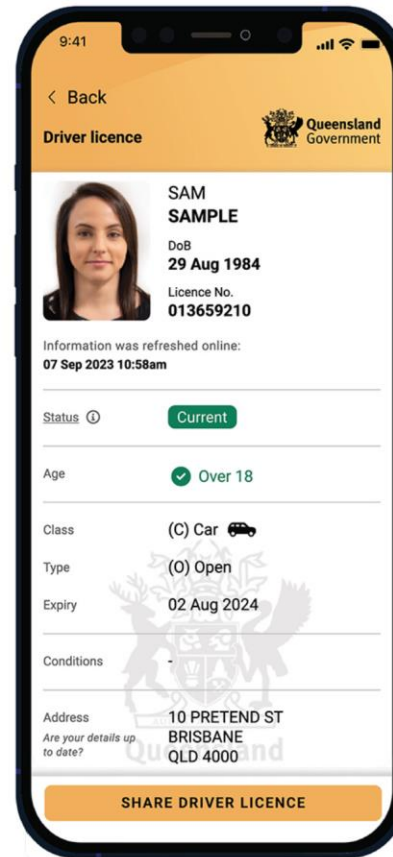
Australia

Digital ID Act 2024, established a legal framework for a national digital identity system that includes verifiable credentials.
Mobile Driver's Licence at state level

Mobile documents provide Digital ID by stealth

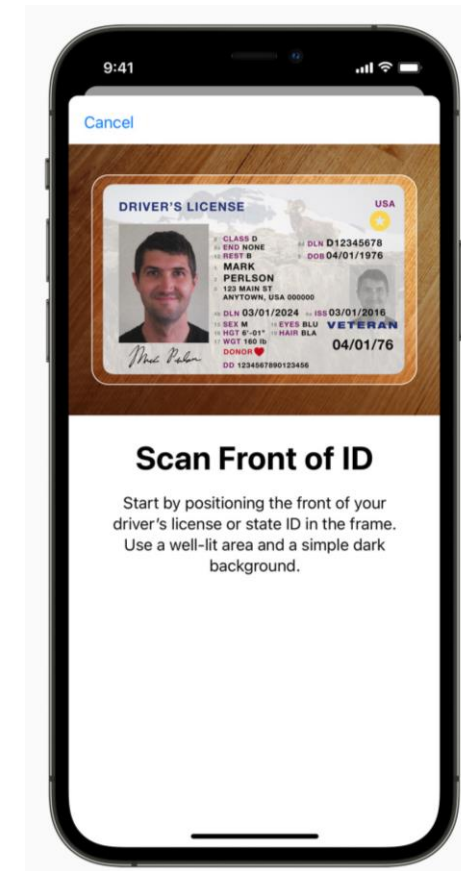
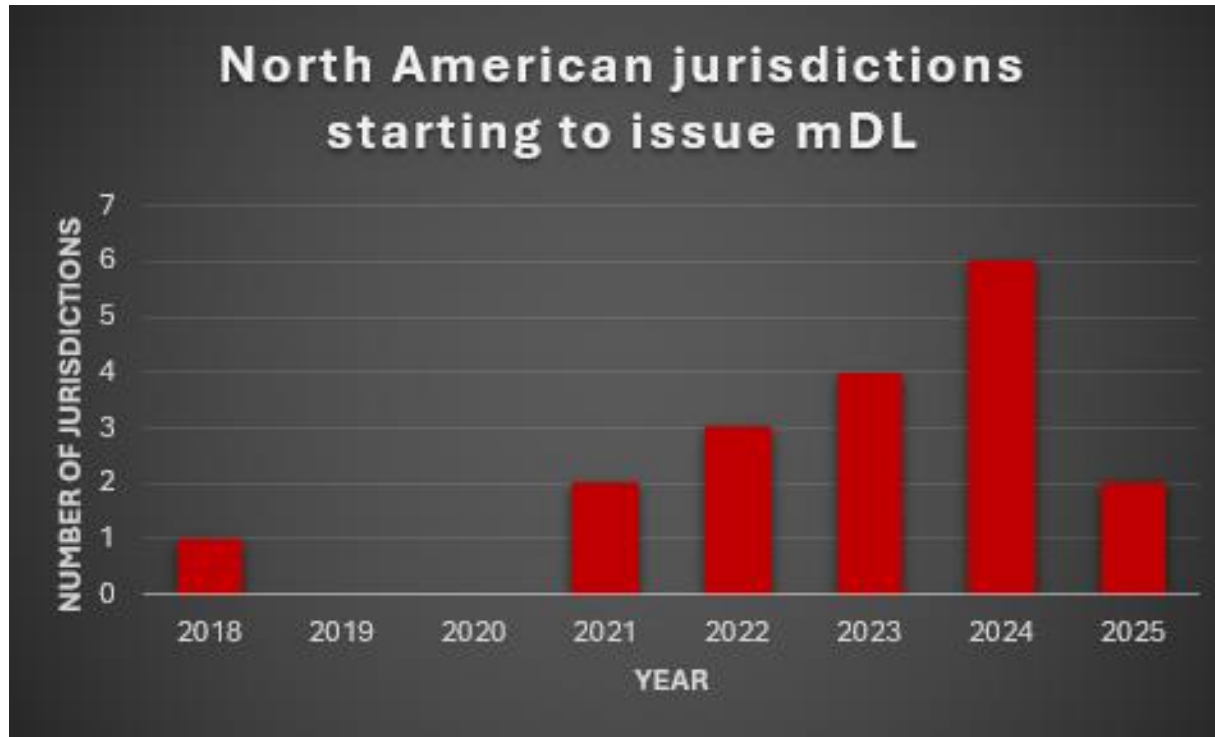
Countries where mDL has been adopted or physical ID can be transferred to digital wallets are seeing the rapid growth of de facto digital ID.

In parallel, Google is expanding mobile ID coverage. Others will follow.



Mobile documents provide Digital ID by stealth

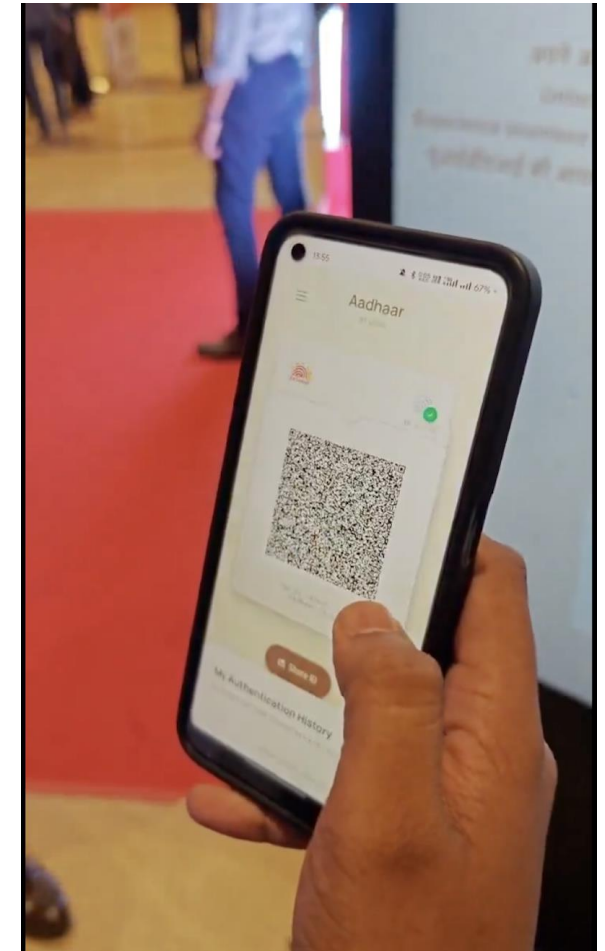
In the US 95.4 million people already have mDL (40% of the driver population).



Aadhaar continues to evolve

In April, the Unique Identification Authority of India (UIDAI), in collaboration with the Ministry of Electronics and IT, launched a new Aadhaar mobile app reducing the need for physical documents.

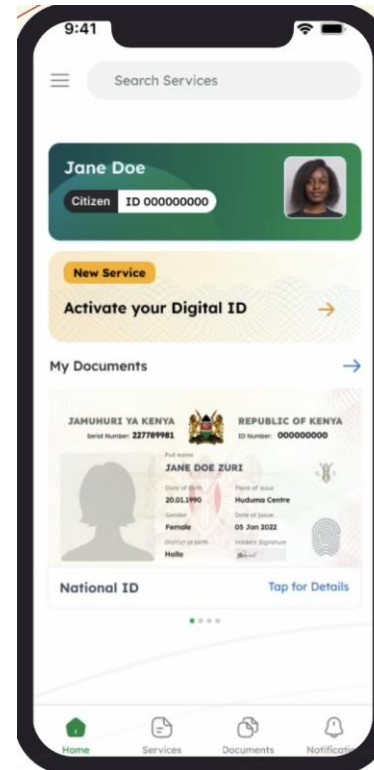
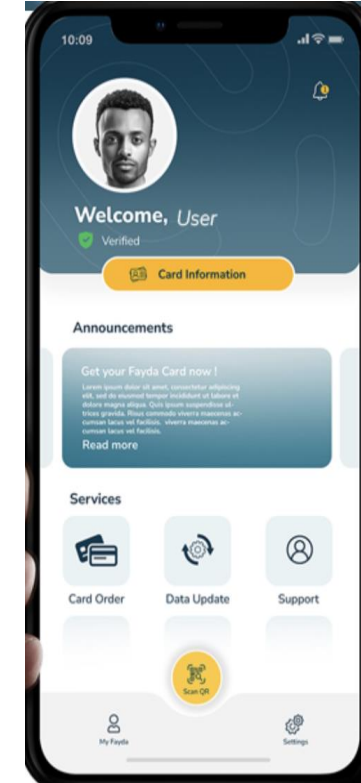
- Facial Recognition Authentication
- QR code based verification
- Enhanced privacy controls
- Consent based data sharing



Multiple African countries implementing Digital ID

Digital ID apps are being developed across Africa based on underlying national ID systems.

The potential for digital transformation is huge.



Interoperability is driving legislation

Cross-border interoperability and use cases such as international trade are driving forward legislation.

ASEAN and the African Union are both pushing forward with initiatives such as the AU Interoperability Framework for Digital ID, and the ASEAN Digital Masterplan 2025.



Building successful digital identity systems

Understanding user needs

Real user needs are from people and the services they want to access.

Digital identity should not be a barrier to service delivery.



Enrolment and identity proofing

For an individual to obtain a digital identity they must first provide evidence of their real-world identity that can be verified.

Biometrics help individuals to reach the highest levels of trust.

NIST Special Publication 800-63A

Digital Identity Guidelines
Enrollment and Identity Proofing

Paul A. Grassi
James L. Fenton

Privacy Authors:
Naomi B. Lefkowitz
Jamie M. Danker

Usability Authors:
Yee-Yin Choong
Kristen K. Greene
Mary F. Theofanos

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-63a>

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Official Journal of the European Union L 235/7

IMPLEMENTING REGULATION (EU) 2015/1502
of 8 September 2015
laying down technical specifications and procedures for assurance levels for electronic identification and trust services for electronic transactions in the internal market
(Text with EEA relevance)

Official Journal of the European Union,

Regulation (EU) 2014/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 2002/43/EC of 15 June 2002

Regulation (EU) 2014/2014 provides that an electronic identification scheme notified pursuant to Article 8(3) of Regulation (EU) No 910/2014 shall be subject to assurance levels low, substantial and high for electronic identification means issued pursuant to Article 8(3) thereof.

Technical specifications, standards and procedures is essential in order to ensure interoperability of the assurance levels and to ensure interoperability when mapping the assurance levels of electronic identification schemes against the assurance levels under Article 8(3) of Regulation (EU) No 910/2014.

Regulation (EU) 2015/1502 has been taken into account for the specifications and procedures set out in this Regulation. However, the content of Regulation (EU) No 910/2014 differs from that in relation to identity proofing and verification requirements, as well as to the existing Member State identity arrangements and the existing tools in the EU for electronic identification. Therefore the Annex, while building on this international standard specific content of ISO/IEC 29115.

Regulation (EU) 2015/1502 is based on an outcome based approach as being the most appropriate which is also specified in the terms and concepts. They take into account the aim of Regulation (EU) 2014/2014 to specify the terms and concepts. Therefore, the Large-Scale eIDAS project developed by it, and the definitions and concepts in ISO/IEC 29115 should not be used when establishing the specifications and procedures set out in this Regulation.

In an aspect of evidence of identity needs to be verified, authoritative sources such as registries, documents, bodies inter alia. Authoritative sources may be different in a similar context.

Regulation (EU) 2015/1502 and verification should take into account different systems and practices, and assurance in order to establish the necessary trust. Therefore, acceptance of electronic identification means should be made conditional upon confirmation that those procedures fulfil the requirements foreseen for the corresponding assurance level.

(1) OJ L 257, 28.8.2014, p. 73.

EUDI and mDL standards are ready - the challenge now is use cases

ISO has produced standards for mobile driving licences (mDL).



W3C has defined the Verifiable Credentials (VCs) Data Model.



DIF created the DID specification.



And, the OpenID Foundation have developed protocols for VC issuance and VC presentation.

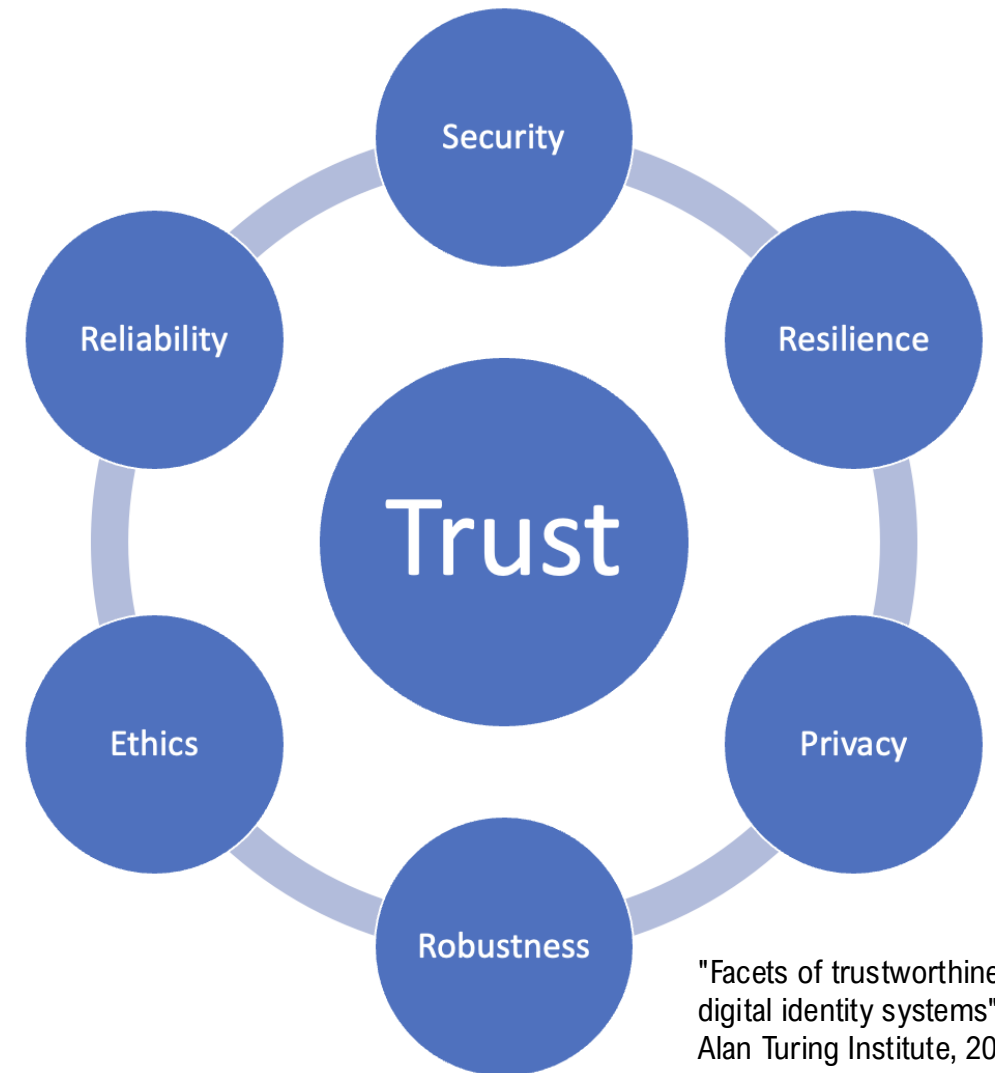


A trusted identity ecosystem

Consumers must be assured that the identity ecosystem is safe, resilient and reliable.

To ensure trust all parties in an identity ecosystem must agree to certain rules e.g. a trust framework.

Standards, certification, and assurance processes play a vital role.



"Facets of trustworthiness in digital identity systems", Alan Turing Institute, 2021

The role of biometrics

We began with inclusion and usage

*We began with inclusion and usage,
now the concern is protecting identity
against attack.*

Deepfakes and AI generated fake documents are a major threat.

*Digital ID needs digital evidence from
trusted sources.*

Governments have a key role: they issue strong evidence of identity.

Biometrics allow us to verify identity, provide unique ID, and prevent fraud.

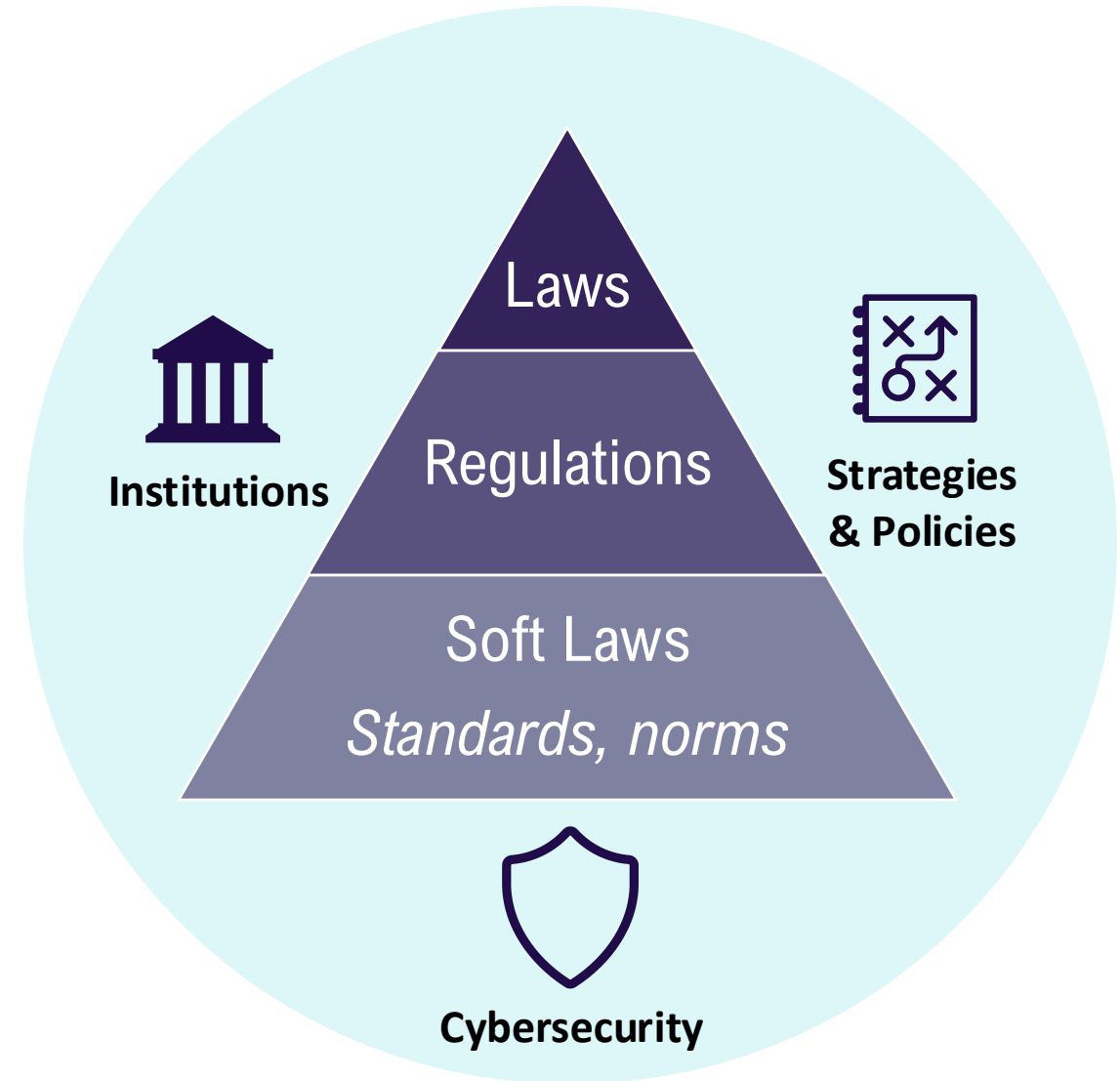
*Biometrics allow us to verify identity,
provide unique ID, and prevent fraud.*

*But only if we implement them
responsibly.*

Safeguards and Biometrics

Biometric data is highly sensitive and unique to individuals.

Security, Privacy, and Ethical considerations must be part of any system design and ongoing governance.



A closing thought

Doing things digitally makes the chance of industrialised attack more likely.

*Digital Identity is Critical National
Infrastructure.*

Digital Identity is CNI not just DPI.

Adam Cooper

```
|next  
|id
```

Thank you!

