

# DIGITAL CREDENTIALS: DIVERSITY, UNDERPINNINGS & THE LATEST ADDITIONS

May 2025

Dr Peter Waggett

---

---

# About Me

Director – Research IBM UK

- PhD in Rocket Science from Mullard Space Science Labs
  - Failed Astronaut
  
  - Focus on Identity for over 25 years
    - Chair of ISO Cards and Personal Identification Group SC17
    - BSI Chairs of IST/17 and IST/44
    - Convenor of EU National Critical Infrastructure Panel - Biometrics
    - Editor of ISO Standard on Biometric Vocabulary and BSI Code of Practice
    - Member of UK' s Biometric Assurance Group and Biometrics and Forensic Ethics Group
-





# Promise of Digital or Verifiable Credentials for Personal Identification



Digital Representation of a Person



Similar Use Cases to Physical Credentials for Identification, Authorization and Authentication



Can be Stored and Displayed on Smartphone or Edge Device or Accessed on Cloud

# Centralized Digital Identity Systems

Corporate Systems  
(supervised or self declared  
enrolment) e.g.

- Amazon
- Facebook

National Systems (typically  
supervised enrolment using  
'breeder' documentation or  
information) e.g.

- India
- Estonia
- Nigeria
- Singapore
- Sweden
- Netherlands
- Denmark
- Belgium

# Centralized Digital Identity Systems Advantages

Large Take Up and Utility (e.g. over 93% of Indian Population Covered)

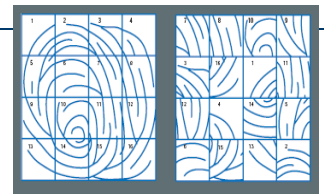
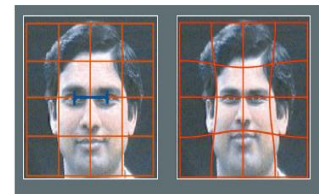
Citizen Benefits Targeted and Distributed Quickly

## Reducing Costs and Complexity

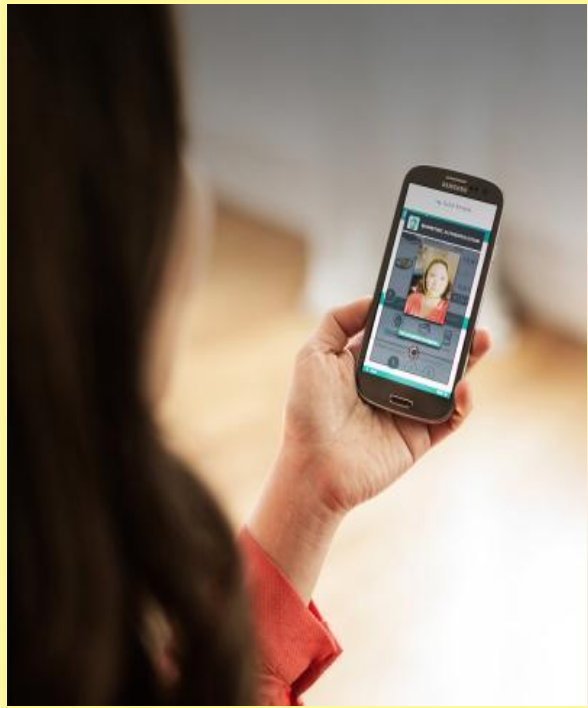
- Indian Aadhaar System has Reduced Benefits Fraud by over \$1B pa
- Indian Aadhaar System has Reduced Banking Onboarding Costs by over 99%
- Estonia Estimates that Eid Digital Identity System has Saved 2% GDP pa Over Use of Physical Credentials

# Centralized Digital Identity Systems Challenges

- Corporate Systems
  - Security Vulnerabilities
  - Data Sharing and Privacy e.g. Cambridge Analytica
  - Ethics
- National Systems
  - Security and Process Vulnerabilities
  - Data Sharing and Privacy
  - Ethics
  - May be Biometrics Based That Cannot Easily be 'Reset'



## Decentralized Digital Identity Systems



Storage of Verifiable Credentials in Digital Wallets Rather Than Centralized Government Controlled Data Stores or Monetized Data Silo's

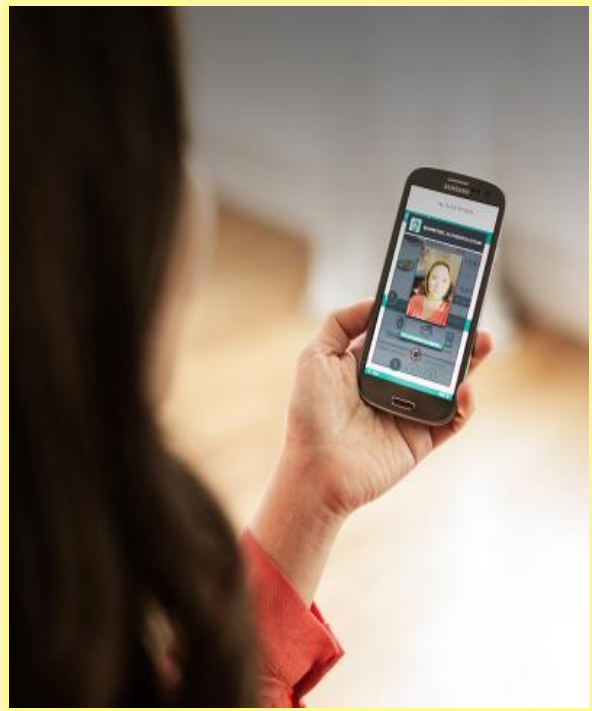
Many use Decentralized Identifiers (DIDs) to Allow End to End Cryptography Without Need for Third Party Involvement

Storage of Cryptographic Key Pairs can Enable Off-line Operation

Can Allow for Selective or Minimal Disclosure

'Self-Sovereign Identification'

## Decentralized Digital Identity Systems Advantages



Non Correlatable IDs

Machine Readable Verifiable Credentials

Open and Interoperable

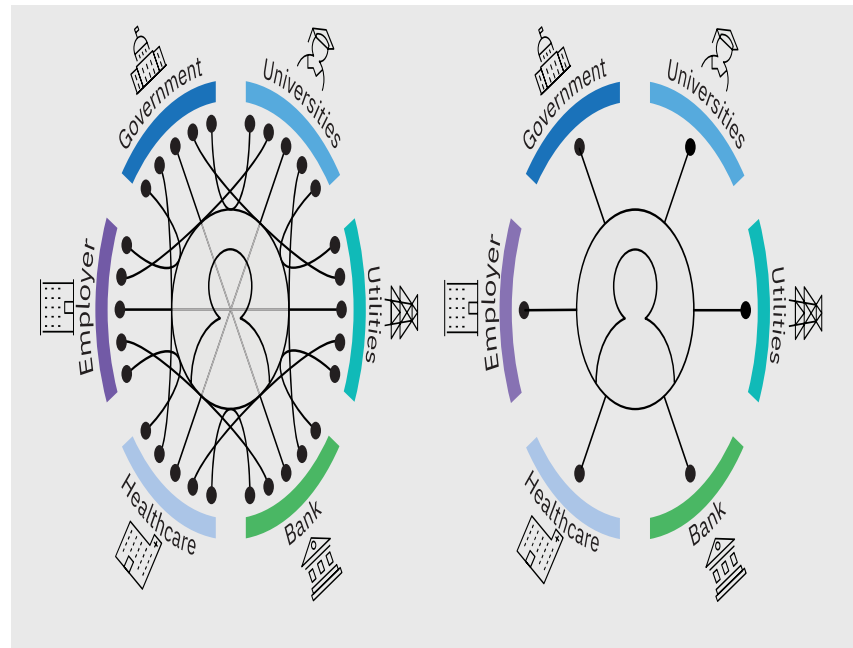
Off-line Bilateral Communications

User Friendly Wallet Apps on Common Devices

# Where Will Distributed Credentials be Most Valuable

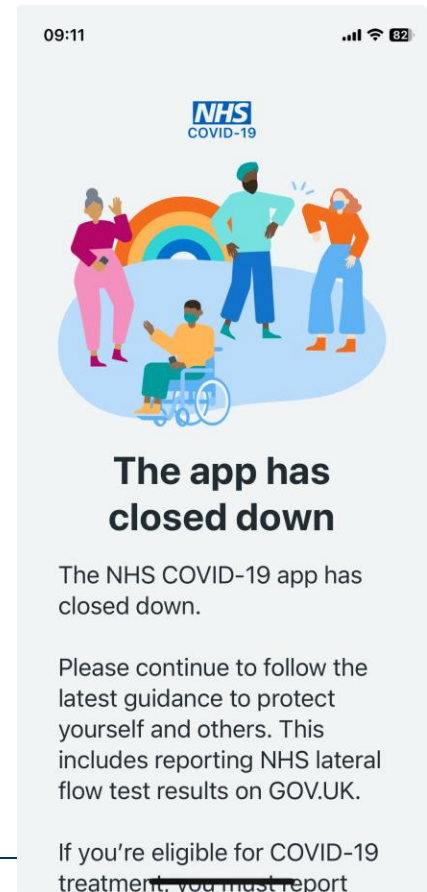
verifiable credentials and digital wallets are appropriate for:

- fast, machine-verifiable exchange of identity-related information without the direct interaction of issuers and verifiers,
- centralized identity management systems present privacy and security concerns
- centralized identity management systems fail to achieve adoption among a diverse array of stakeholder due to a lack of trust or a fear of concentrated market power.



# Early Activities – Covid Driven Emergency Responses

- Covid Emergency Forced Rapid Responses that were Invaluable at Time but Have Not Persisted; Mainly Due to Immature and Non-Standard Technical Approaches
- Citizen Take Up Rates Were High and App was seen as Valued
- Utility Under Trying and Constantly Changing Requirements was Proven



# Current Activities Include:

- EU Digital Identity Wallet
    - Scope to Cover:
      - E-Government Services
      - Banking
      - Employment
      - Education
      - Healthcare
      - Travel
    - Initiated in 2021
    - Enabled by 2014 eIDAS Regulation
    - Under Development – Available 2026?
-

# Decentralized Digital Identity Systems Challenges



Complex Legal Frameworks Need Extensive Correlation



Take Up and Adoption Rates



Business Models to Support Their Operation



Not Global – Yet!

# ISO SC17 and Identity

- Bank Cards
  - Passports and Travel Documentation
  - Driving Licences
  - Drone Licencing
  - Underlying Infrastructure Elements
-

# ISO SC17 and Identity

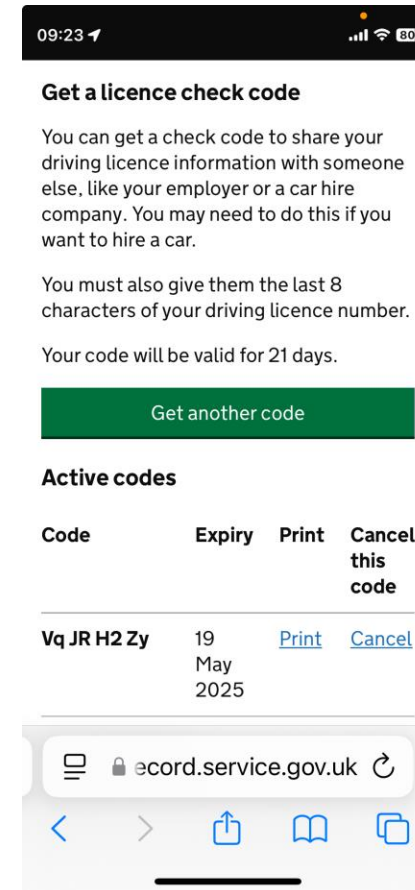
- Widely Accepted Standards and Infrastructure
- Supporting Evolving Requirements and Capabilities
- For Example, Bank Cards
  - Early Developments (1920s -1950s)
    - Limited Acceptance to Ubiquity
    - Paper to Cardboard to Plastic
  - Mid-Century Advancements (1960s-1970s)
    - Unique to Standardised to Competition
    - Offline to Electronic via Magnetic Stripe
  - Modern Era (1980's to Present)
    - Single Use Cases to Multiple
    - Enhancement Security e.g. Chip and Pin
    - Supporting Online, Mobile Wallets, Crypto and Contactless

# Major SC17 Initiative on Digital Credentials – Towards a Global Mobile Driving Licence Credential

- The Mobile Driving Licence (mDL) is a Major Global Initiative to Pilot a Digital Credential under the ISO 18013 Set of Standards
  - Digital Version of Traditional Driving Licence Stored and Selectively Accessed on a Mobile Device (e.g. SmartPhone)
  - Based on Existing SC17 Infrastructure Standards
-

# Driving Licence Use Case Example

- Hiring a Car in UK
- Claimant Needs to Provide Code Generated Using:
  - National Insurance Number
  - Driving Licence Number
  - Address Post Code
- Only Valid for Limited Time
- Needs Online Connectivity



# mDL Capabilities and Advantages



**Secure:** Encryption and Other Security Features on Mobile Device Provide Lower Risk of Counterfeiting and Identity Theft



**Convenient:** Allows Easy Sharing of Information for e.g. Hiring a Vehicle or Interaction with Law Enforcement



**Flexible:** Allows Selective Sharing



**Interoperable:** Common set of ISO 18013 Standards for Multiple Interactions and use Cases

# mDL Outstanding Activities

- Test and Accreditation Activities
- Business Models for Adoption