



Australian Government

**Digital
Identity**

Digital Identity Working Group

**Digital Identity and Verifiable Credentials in
centralised, decentralised and hybrid systems**

Matt Sedgwick, Head of Digital Identity

12 September 2022



Background

- The Digital Identity Working group was formed to develop pathways to enable mutually recognised and/or interoperable digital identities, to enhance trade opportunities.
- In 2021, we sought to understand how digital identity is being used globally to respond to and recover from an international pandemic.

Focus of 2022



Supporting verifiable credentials

How digital identity systems are being used to support trustworthy, high-value verifiable credentials.



Enabling Interoperability

What we need to do to make sure these verifiable credentials can be interoperable between countries.



Verifiable credentials

- Digital Identity is going beyond the ‘who I am’ to ‘what I can do’:
 - I can drive a car
 - My educational qualifications
 - I am first aid certified
 - I have clearance to work with vulnerable people
 - I have been vaccinated

A photograph of a crowd of people, mostly young adults, looking down at their smartphones. The background is blurred, showing more people and what appears to be an outdoor setting. A solid blue horizontal banner is positioned in the lower-left quadrant of the image, containing the word "Findings" in white, bold, sans-serif font.

Findings



Design

- Decentralised architectures used to support the issuance, storage, and presentation of verifiable credentials
- The role of digital wallet providers in the digital identity system is essential
- The market for distributed and decentralised technologies is maturing



Policy

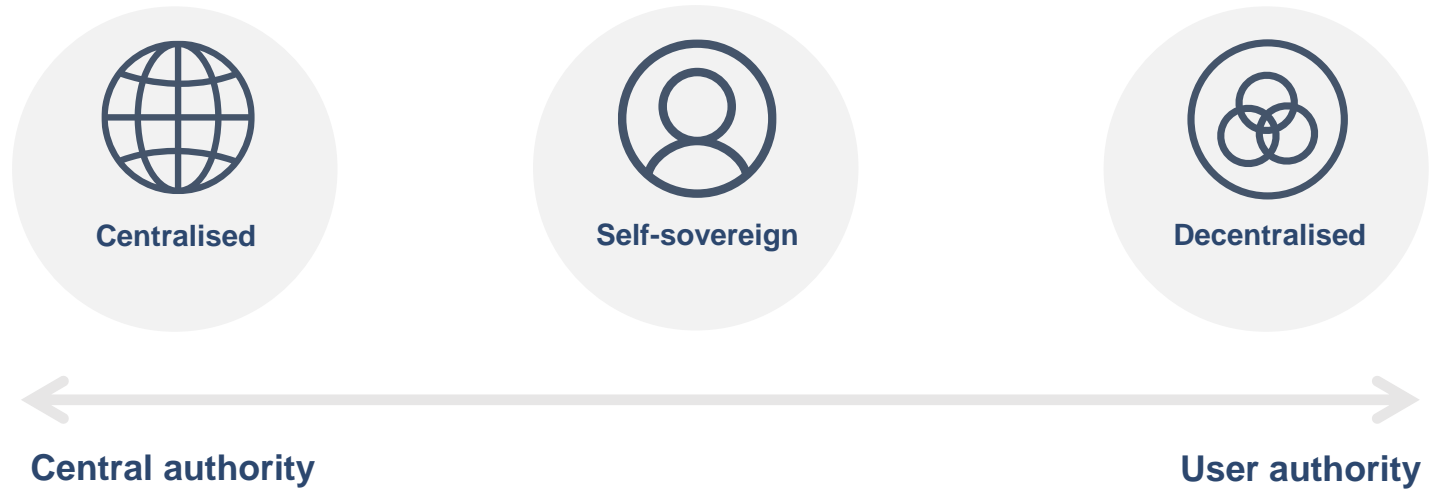
- Use cases clustered around the employment, healthcare, finance and professional sectors
- EU directives and regulations have increased the expectations of scalable digital identity systems
- Digital vaccination certificates have increased acceptance of digital credentials



Standards and interoperability

- Alignment of standards and levels of assurance is required for international interoperability pilots
- Technical standards are still maturing

Digital Identity models



There is a lot of interest in decentralised models, however at present these have not been applied fully to government services.

- | | | |
|---|--|--|
|  <p>Centralised approach led by government.</p> |  <p>Centralised approach led by government for citizens, hybrid approach in partnership with the private sector for businesses.</p> | |
|  <p>Centralised approach, led by government with individual programs between federal and provincial governments.</p> |  <p>Hybrid digital identity approach, led by government with participation by private sector identity and credential providers.</p> |  <p>Hybrid approach, led by central government with additional private sector identity providers.</p> |
|  <p>Centralised approach led by government.</p> |  <p>Hybrid approach, led by government running for public services supported by multiple private sector eID providers.</p> |  <p>Hybrid approach, led by central government with additional private sector identity providers.</p> |



Trust and issuers

Verifiers need to know that:

1. The individual presenting that credential is who they say they are
2. The credential has been issued by an appropriate and trustworthy organisation within that country
3. An acceptable level of evidence was provided by the holder prior to it being issued



Australia

- Hybrid digital identity approach
- National Verifiable Credentials Working Group established, spanning Commonwealth and state and territory jurisdictions.
- Digital driver licences
- Medicare cards
- Concession cards



Canada

- Centralised digital identity approach
- Federal leadership involving the National Standards and Digital Trust Infrastructure to support domestic and international interoperability of digital identity documents.
- Joint principles between Canada and European Commission for digital credentials and blockchain established.
- Small business owner opening a business bank account
- Cross-border acceptance of diplomas
- Greenhouse gas emissions tracking



Estonia

- Hybrid digital identity approach
- Participation in the European Digital Identity Wallet pilot project for early adoption of the renewed eIDAS regulation and for enabling the cross-border use of digital credentials.
- Mobile driving licence
- e-Health and sub use cases (e.g. e-prescriptions)



Israel

- Centralised digital identity approach
- The different use-cases are part of a pilot/ POC undertaken by the Israeli National Digital Agency, looking at the concept of VC, e-wallets and blockchain. The results will determine how to proceed.
- Land surveyors
- Blind person certificates
- Foreign volunteers
- Foreign workers stay permits
- Employee cards
- Air crew certificates
- Vehicle inspector / garage certifications



United Kingdom

- Hybrid digital identity approach
- The UK Government Digital Service is focused on developing the MVP for 'One Login for Government' before prioritising some further use cases for verifiable credentials: enabling for the use of digital identity across multiple government services.
- COVID-19 vaccination status



Singapore

- Centralised digital identity approach
- Explore potential collaboration opportunities with interested partners.
- Starting with issuing government data as verifiable credentials but future plan is determined based on use case needs.
- Opening bank accounts
- Applying for work permits
- Passports
- Driver licences
- COVID-19 vaccination status
- Education qualifications



New Zealand

- Hybrid digital identity approach
- Identity Check
- Verifiable Identity Check (VIC)
- Both will be driven by the Department of Internal Affairs, in collaboration with other government agencies.



For more information, visit

digitalidentity.gov.au