IBM Consulting

Action for the Non-Proliferation of Identity

How governments and leading businesses can act to protect us all.

February 2023

Authors: Richie Paul, Kylie Skeahan, Sarra Swami, Eugene Hunt and Sameer Saini

Authors

Richie Paul
Partner, Enterprise Strategy
IBM Consulting
richiepaul@au1.ibm.com

Kylie Skeahan
Client Partner,
Government Transformation
IBM Consulting
kylie.skeahan@au1.ibm.com

Sarra Swami
Enterprise Strategy Consultant
IBM Consulting
sarraswa@au1.ibm.com

Eugene Hunt
Client Partner,
Government Transformation
IBM Consulting
eugene.hunt@ibm.com

Sameer Saini
Digital Trust Principal Consultant
IBM Consulting
sameer.saini@ibm.com

Executive summary

We all have digital identities. They are essential to our modern day-to-day activities. Most of us have more than a hundred discrete digital identities to access services from government departments, utility and telco providers, banks and financial institutions, real estate and property managers, even groceries, food delivery, and ride-sharing. To establish each of these discrete digital identities, we provide evidence that we are who we present ourselves to be [1]. As a result, documents that evidence our identity proliferates, and each provider that holds this information represents a potential vulnerability to be exploited by identity thieves.

A single breach in our network of 100+ digital service providers can lead to identity theft, financial fraud, and other types of abuse. The cost is high – ranging from loss of trust, reputational damage, financial penalties, ransoms, as well as the cost and opportunity cost of remedial actions.

The average cost to organisations who suffer a data breach is $4.34 million with some known to be 9 figures. 83% of organisations have had a minimum of one data breach [2]. 60% of breaches have led to price increases passed onto customers [3].

A new model for digital identity is available. Credential-based digital identity solutions allow individuals to use a single trusted digital identity to authenticate with multiple online services without the need to provide personally identifiable information 100+ times. Identity information is not shared, rather it is verified by a credential provider. The development of credential-based digital identity solutions and successful pilot implementations by leading digital governments and businesses provide demonstrable evidence of a simpler, better, and safer approach to digital identity that dramatically curtails the proliferation of personally identifiable information and the associated risks and threats.

Despite ground-breaking work, the uptake of credential-based digital identity solutions is very slow. The delay of economy-wide uptake of these solutions is influenced by several factors including:

- Regulatory changes regarding data security, data sharing, and privacy are complex to get right and enact. Once done, relevant legislative changes would typically serve as a catalyst for economy wide change.
- Business systems and process changes required to integrate digital identity solutions into existing workflows are complex, impacting systems, processes, and people.
- The digital identity network business model is embryonic – both services providers and consumers require choice, and a single centralised digital identity solution will not create economy-wide scale at pace. The business model for network players is not clear, and trust in network dynamics is not established (and regulatory changes are pending but remain unclear). Integrated global standards are a foundation for large scale digital identity solution investment.

Authors

Richie Paul
Partner, Enterprise Strategy
IBM Consulting
richiepaul@au1.ibm.com

Kylie Skeahan
Client Partner,
Government Transformation
IBM Consulting
kylie.skeahan@au1.ibm.com

Sarra Swami
Enterprise Strategy Consultant
IBM Consulting
sarraswa@au1.ibm.com

Eugene Hunt
Client Partner,
Government Transformation
IBM Consulting
eugene.hunt@ibm.com

Sameer Saini
Digital Trust Principal Consultant
IBM Consulting
sameer.saini@ibm.com

IBM believes that a trusted and decentralised digital identity network (that is a few-to-many-services pattern rather than a one-to-many services pattern) will accelerate adoption and scale. Digital identity credential providers that form this network would need to include:

- Varying approaches to identity holder consent (including real-time consent)
- Open digital identity verification exchange
- Identity consistency and accuracy across the network

To rapidly harden the protection of citizens' identities and allay the economic cost of identity fraud, swift action is required to:

- Halt the proliferation documents evidencing individuals' identity;
- Disarm government departments and businesses from the need or obligation to collect and retain documents evidencing individual customers' identity;
- Advance a decentralised digital identity network, with consideration for a common gateway that would both support a multi-provider network and limit the integration burden on government and business; and
- Accelerate the integration of secure digital identities into business as usual.

[1] NPC 100 Point Checklist

[2] Statistics from the IBM's Cost of a Data Breach Report 2022

[3] Statistics from the IBM's Cost of a Data Breach Report 2022

What is digital identity?

Digital identity refers to the online representation of a person or entity.

A digital identity is required to interact with online service providers. Once registered with an online service provider, it is used to identify an individual to the online service provider (with a range of safeguards typically including at least password complexity rules and multi-factor authentication).

Centralised or decentralised – one secure digital identity to rule them all?

Instead of multiple digital IDs (requiring multiple submissions of documents evidencing identity), a Secure Digital Identity (SDI) issued by an Identity Service Provider (ISP) requires such information to be provided once. The ISP creates the individual's SDI, and this certificate is then used by the individual to prove identity with the various online service providers for which the individual wishes to register. The ISP provides a service that registers the individual, validates their identity through collecting and storing the necessary documents evidencing identity, and provides the identity authentication service to all online service providers that enable the individual to register for and consume online services without the need to resubmit to multiple online services providers the documents evidencing their identity.

In a centralised Secure Digital Identity model, one Identity Service Provider would register a user and issue a certificate that uniquely identifies that person. This Identity Service Provider provides a service that registers the user, validates the user's identity through collecting and storing the documents evidencing identity, and provides the identity authentication service to all online service providers that enables a user to register for services without the need to re-submit documents evidencing their identity to multiple online services providers. The service providers then allow users to access a range of applications, websites, or other systems with a set of credentials which verifies their identity.

While this improves the user experience, it relies on one organisation to offer the service of identity management and verification. In practice, there will be multiple "central" organisations who provide the same services, all requiring access to the same valuable user identity data.

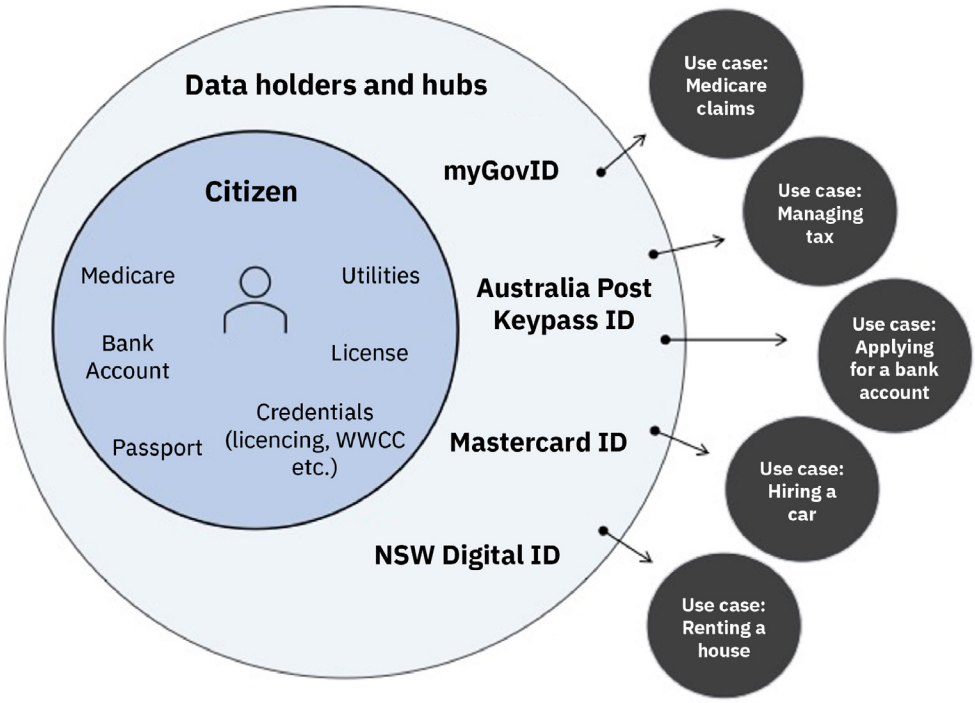
In a decentralised identity model, users receive credentials proving their identity from multiple issuers, such as employers, banks, and the government, and store them in a location of their choice, such as a digital wallet. The user can then choose to share just the minimum amount of information required for a transaction, and in most instances, this will require the sharing of credentials as opposed to identity data itself. The key is to move away from "sharing" identity data and rather "verify" it.

Global progress of digital identity

Leading up to today, digital identities were most often established using login credentials (that is usernames and passwords). These credentials prove you are you and are given to you after you establish trust through the provision of personal information. Today's challenge is that all services that add value to your life are digital. Having a trusted digital identity is a requirement to access what you need. So, each service you use - insurance, banking, telco, shopping, content streaming, social media all ask you to provide personal information to establish identity trust, they store that information and provide you a unique digital identity. We don't have one, we have hundreds. Our identity information is not stored in one place, it is littered all over the world.

Now and into the future, digital identities will be established through digital credentials. These will allow individuals to use a single set of credentials to access multiple online services, without having to create a separate digital identity for each service. To do this, a third-party identity provider will manage personal identity information and act as a trusted intermediary between the individual and the various online services. In this system, an individual's identity is verified by the identity provider, and a digital token is issued to represent their identity. This token can then be used to access multiple online services, without the individual having to enter their login information each time. This can be more convenient for the individual, as they only need to remember one set of login credentials, and it can also help to reduce the risk of identity theft or other security issues.

Current digital identity ecosystem interaction in progress in Australia



Global progress of digital identity

Case studies

Australian Government

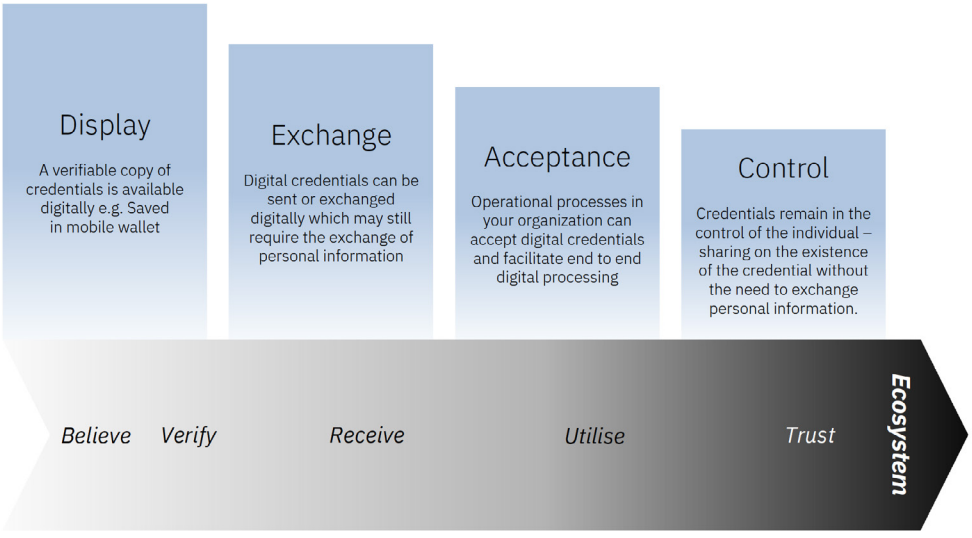
The Australian Government have made significant progress in offering a safe and easy way to verify identity online. The MyGovID digital identity service launched in 2019 and can be used to access 72 different government services today. The service uses encryption and cryptographic technology in addition to the security features in a user's electronic device, such as fingerprint or face, to verify identity. The user is in control and personal information is only shared with consent.

Different government services require different levels of identity verification to mitigate varying levels of risk. MyGovID offers users the ability to authenticate themselves up to three levels of identity strength – basic, standard and strong. The minimum identity strength needed by the user is determined by the government online service they want to access. This approach allows users to maintain control and supports incremental user adoption over time.

NSW Government

In Australia, the state Government of NSW has reached a pilot stage with a new digital identity wallet. Complementing the existing Service NSW App which already stores digital copies of credentials such as licenses for driving. This new digital identity allows the sharing of verified credentials (without the need to share personal information and details) digitally. This approach builds on the broad acceptance and rapid adoption of the Digital Drivers Licenses in NSW. The Digital Identity allows a user to build a photographic reference (through taking a selfie) and ties to independent forms of identity e.g., Drivers Licensing and Medicare Card. Details and credentials are stored on a user's mobile device with only minimal information shared with Government or agencies. The solution has included next generation security features including two-factor authentication to protect the personal information and limits the personal information that is required to be shared to satisfy identity requirements with both government and private businesses.

Where is your organisation on the digital identity maturity ladder?



Effective mature digital credentials require both a capability within the organisation and in the ecosystem in which that credential is used. [2]

Case studies

United States of America

The US Government is working through the legislation to address concerns around government digital identity that have emerged after private services such as ID.me have launched. This is likely to limit the development of whole of government ID services but look to build on existing private digital identity services across the US.

Positive lessons can be gained from the use of digital credentials for the management of COVID19. The Excelsior Pass in NY state provided a digital wallet to support collection and sharing of health credentials such as COVID19 test results and vaccination status. This solution scaled to over six million users rapidly and was essential for the safe reopening of NY State during the pandemic. Using open standards, a targeted education and awareness campaign and thoughtful design of both the user application and verification solution, NY State was able to provide an effective digital solution. Detailed lessons learnt are available through this blueprint: https://covid19vaccine.health.ny.gov/excelsior-pass-plus

UK Government

The UK Government is working to avoid a fragmented approach to digital identities through the publication of the Digital Identity Attributes & Trust Framework [6] to establish a national approach to digital identities. The objectives of the framework were to provide citizens with greater control on how their information is used across Government and private sector organisations and provide a framework for trust to support reusability of identities across the UK. Key aspects of this program are a certification scheme designed for identity or attribute issuers and orchestrating parties to ensure identities can be trusted. This framework allows for multiple schemes to exist in which a user may choose to participate and create their identity – creating a decentralised approach to identities for users.

In addition, the UK Government has launched UK.gov One Login to replace existing sign-in routes and accounts allowing customers to establish a reusable digital identity with the UK Government. The Scottish Government is also piloting the use of a digital identity platform across the Government Agencies.

The UK's National Health Service, other parts of UK government, and IBM have also been exploring the use of decentralized personal data stores (Pods) that use the Solid Protocol, an open Web standard. When data is stored in someone's Pod, they control which organizations and applications can access it. They can grant or revoke access to any slice of data in their Pod as needed. The proliferation of personal data across organizations is reduced because applications access the same data from the Pod instead of requiring separate application or organization specific data silos. Consider an individual applying for a government service through a Solid enabled website – they can choose to store personal details (e.g. unemployment benefits) in their Pod. Subsequently the individual can grant a private sector application access to these same personal details from their Pod, saving time and preventing the duplication of their personal data.

Case studies

The EU

The European Union is exploring decentralised digital identity through several initiatives, including the European Self Sovereign Identity Framework (ESSIF). ESSIF aims to implement a generic self-sovereign identity (SSI) capability, allowing users to create and control their own identity across borders without relying on centralized authorities. The focus of the ESSIF is to enable identity holders to have control over their personal data and decide to whom and for what purposes they want to make their identity data available by means of digital credentials.

Pilot solutions have been tested in various countries, such as Estonia, Sweden and the Netherlands, to explore how SSI can be used to improve the delivery of e-government services, such as online voting, tax submissions, healthcare, and other administrative tasks. German financial institutions have trialed SSI solutions for digital identity verification and secure data sharing. These pilots have helped advance the development of standards which is a crucial element to enable interoperability between SSI solutions and drive greater adoption.

From this, multiple consortiums are forming across EU to pursue various use cases such as the POTENTIAL consortium on digital identity wallets which is across 19 EU countries.

Key takeaways

Australia must create confidence and transparency by establishing standards for the handling, collecting and storage of citizen data.

Digital solutions should easily integrate into the wider business systems in the economy.

Governments need to build incentives for issuers and verifiers, with clear and well defined requirements for operation.

[4] https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-beta-version

Complications and why digital identity solutions have not scaled

There are multiple identity services which have been developed internationally and within Australia, however, there are three key complicating factors which are affecting the ability to scale these solutions.

1. **Regulatory complexities**

   Often, changes in legislation are used to guide, accelerate, and scale economic change. In the case of digital identity, there are complexities in defining the standards that will govern the appropriate collection, storage, and use of user identity information. Factors including data sharing constraints, system security posture, privacy and user consent must be taken into consideration. Government's ability to align and inter-operate with the developing global standards for digital identity must also be managed.

2. **Scale of change to current business processes**

   The value of digital identity to the user is directly related to the volume of everyday services they can support with their credentials. The use of digital credentials therefore requires existing operational processes to change - not just of the issuer but anyone who wants to verify identity as part of their service. They must do this in a way that does not leave them exposed to security vulnerabilities, regulatory compliance risk or threat of a cyber-attack on their organisation.

   In Australia, early adopters of digital credentials such as the NSW Digital Driver's License have encountered issues when trying to use their digital credential outside of the NSW jurisdiction as a form of identity. The true value of the digital identity will only be realised once it is able to be shared digitally in a true digital end-to-end process and not just to take a paper copy of in lieu of a hard copy credential. These processes will also need

to have a mechanism to establish evidence of identify beyond capturing a number or details of a credential e.g., verified copy of birth certificate or driver's license number.

Many organisations have incorporated identity verification approaches such as two-factor and multi-factor authentication into business processes as an interim solution to improve end user experience and increase security controls, without integrating to complex real time identity verification services which leverage data stored outside of their organisation. This has slowed the scaling of Digital Identity solutions.

Credentials are issued by a broad range of organisations today and while a growing number of these are being issued digitally, not all are at that stage yet. Most government and private industry processes require multiple credentials, and it is challenging to migrate identity when a mix of digital and hard copy is required to be used.

3. **Unclear business model and incentives to play**

   While several players exist in the Digital Identity network today, the supporting business model is immature and unclear. Users need trusted and centralised identity issuers to drive adoption and scale. Identity issuers, particularly those which are non-Government, need incentives to develop, market and maintain their solutions. Today, issuers may have the ability to offer an improved user experience for select services. Tomorrow, the user will have greater choice in selecting their issuer of choice. The incentives for organisations to play in this space are not clear and the complexities of establishing trust and transparency in the network increases as decentralized Identity scales in the economy.

What needs to be done – success factors for scale

In order to scale digital identity solutions, reduce the proliferation of identity data and drive rapid user adoption, Australia must establish the following:

1. **Trust and Confidence**

   To establish confidence, Governments must establish standards for identity issuers, holders, and verifiers. All digital identity platforms and services must be transparent in their collection, storage, and usage of identity data. All business workflows that incorporate digital identity platforms must offer traceability and auditability of data flows.

   Key to establishing confidence for end users is building consent into the user journeys. This can be done in the form of real time consent approval messages which detail exactly what information will be verified using digital credentials and for what purpose.

2. **Interoperability**

   Digital identity solutions must easily integrate into business systems in the economy, offering integrated user journeys that allow the users to choose which credentials they use to verify identity.

   As the number of issuers and verifiers in the network increase, there must be system interoperability that supports the verification of identity without the sharing of data. For this decentralised model to scale, the network must avoid creating new silos of identity data.

3. **Business and Incentive Model**

   Today, Government-led centralised digital identity solutions are establishing the viability of credential based digital identity solutions. For a decentralised network to take shape and scale, participation for new and non-government players must be encouraged. For this to happen, clear incentives for issuers and verifiers must be established as well as clearly defined requirements for how they must operate to meet legislative standards.

Key takeaways

Australia must establish confidence though standards in order to create transparency in the handling, collecting and storage of citizen data.

Digital solutions should easily integrate into the wider business systems in the economy.

Governments need to build incentives for issuers and verifiers with clear and well defined requirements for operation.

Action plan

Leading Governments and private organisations should continue to accelerate the enablers of change that are required to realise a scaled, decentralised approach to managing digital identity.

To make whole of economy progress, swift action to is required to:

- Halt the proliferation of individuals identity;
- Disarm government departments and private sector organisations of their customers identity information;
- Advance a decentralised digital identity network; and
- Accelerate the integration digital identities into business as usual

Identity Non-Proliferation

Accelerate the changes to regulatory settings that are required to direct and influence the market toward the credential based digital identity approach. This includes updating policies and standards that incentivise the continued investment in credential based digital identity solutions and encourage their adoption.

Identity Disarmament

Perform a rapid assessment of current state identity storage and manage security risks. A planned reduction in customer's identity data storage should be defined in line with updates to existing customer identity policies and procedures.

Decentralised digital identity network advancement

Digital identity solution providers should advance the development of the decentralised digital identity network. Enhance solutions to enable varying approaches to identity holder consent, interoperable digital identity verification exchange inside the network and identity consistency and accuracy across the network.

Trusted adoption of digital identity solutions

Define a strategy for the integration of credential-based digital identity solutions into government and business workflows to replace the need for storing and managing customer's identity. Redefine the digital journeys for your customers and how you interact with them.

Understand how to participate in the decentralised digital identity network. Will you be a credential issuer, holder, or verifier? How will your participation in the network improve the efficiency and security of your own operations, as well as make your customers more secure.

The right partner for a changing world

At IBM, we collaborate with our clients, bringing together business insight, advanced research, and technology to give them a distinct advantage in today's rapidly changing environment.

IBM Consulting

IBM Consulting is a new partner for the new rules of modern government. Our specialisation is to co-create strategies that can be acted upon and to design innovations that transform experiences.

IBM Consulting combines its unique specialist skills in security technologies and techniques, digital credential solutions and digital platform architecture design to rapidly advance our clients' maturity and readiness for a digital identity future. The experience gained in implementing advanced digital identity solutions for Governments and leading global organisations ensures our advice is relevant and practical for the task at hand; be that

- A rapid identity data security assessment
- Detailed design of new digital identity platforms, or
- Transformation of processes with next generation digital identity embedded

IBM Consulting's Security Services

With the industry's broadest portfolio of consulting and global managed security services, IBM Security™ Services delivers industry-leading assessments and security strategies to many of the world's largest enterprises, including critical strategies such as zero trust. As a trusted advisor, IBM Security Services can help you quantify and understand your risks, extend your team resources, help detect and respond to threats, and unify your organization on security priorities to accelerate your business transformation.

IBM Center for the Business of Government

Through research stipends and events, the IBM Center for The Business of Government stimulates research and facilitates discussion of new approaches to improving the effectiveness of government at the federal, state, local, and international levels.
For more information, visit businessofgovernment.org

The right partner for a changing world

IBM Institute for Business Value

For two decades, the IBM Institute for Business Value has served as the thought leadership think tank for IBM.

What inspires us is producing research-backed, technology-informed strategic insights that help leaders make smarter business decisions.

From our unique position at the intersection of business, technology, and society, we survey, interview, and engage with thousands of executives, consumers, and experts each year, synthesizing their perspectives into credible, inspiring, and actionable insights. To stay connected and informed, sign up to receive IBV's email newsletter at ibm.com/ibv. You can also follow @IBMIBV on Twitter or find us on LinkedIn at https://ibm.co/ibv-linkedin.

Related from IBM Insititute for Business Value:

The next evolution of digital identity

Authors

Richie Paul

Partner, Enterprise Strategy
IBM Consulting

richiepaul@au1.ibm.com

Kylie Skeahan

Client Partner, Government Transformation
IBM Consulting

kylie.skeahan@au1.ibm.com

Sarra Swami

Enterprise Strategy Consultant
IBM Consulting

sarraswa@au1.ibm.com

Eugene Hunt

Client Partner, Government Transformation
IBM Consulting

eugene.hunt@ibm.com

Sameer Saini

Digital Trust Principal Consultant
IBM Consulting

sameer.saini@ibm.com