Whitepaper

Creating a Seamless Citizen Experience: The Future of Digital Identity in Government

Intermedium report
commissioned by Okta

Table of Contents

Introduction

Digital transformation has fundamentally changed how governments think about and deliver policies and core services. No longer an afterthought, a government's ability to offer user-friendly digital solutions efficiently and effectively is essential to meeting citizen expectations and building citizen trust of government.

The rise of cloud computing and the almost universal use of mobile devices has helped drive the ubiquitous take-up of digital services across all facets of life. Governments recognise they can assist citizens anywhere, any time for a fraction of the cost of a phone call or an in-person appointment. However, in this era of cybercrime and privacy concerns, implementation of appropriate digital identity systems by government agencies has been a major brake on the digitisation of government services.

Digital identity has long been recognised as a vital enabler of digital government. Getting digital identity 'right' in an environment of siloed government business systems, many of which are yet to migrate to the cloud, remains a complex and often intractable issue for governments and has led to years of delay, unnecessary expenditure, and risks to citizen data and privacy.

Resolving digital identity is a high order strategic issue. The most recent meeting of the Data and Digital Ministers Meeting reiterated a need for jurisdictions to collaborate, so Australians have "an easy, safe and secure way to prove who they are when accessing government services online[1]".

At the macro level, three issues need to be addressed before the availability of digital government services is widespread:

1. the cost of implementing digital identity citizen expectations around
2. the ease of use digital identity and the security & compliance
3. robustness of the digital identity system being used

Born-in-the-cloud Citizen Identity platforms, often termed customer identity and access management (CIAM), have already addressed these cost, expectation and security issues for many private sector organisations and, increasingly, for government agencies.

Cloud-based Citizen Identity platforms offer five key benefits. They:

1. Simplify the management of identities and access at scale, even in complex multi-cloud environments.
2. Are much less costly than building an in-house, proprietary system and reduce project risk through a faster, agile approach.
3. Cross-agency information sharing, end-to-end user visibility, data collection, joined-up services and proactive policymaking.
4. Help improve security maturity – including compliance with the 'Essential Eight' by providing multi-factor authentication MFA and monitoring specifically.
5. Adhere to regulation and policy for identity governance and administration including privacy compliance and records.

The Future of Digital Identity in Government

Common cloud Citizen Identity features

Multi-factor authentication (MA): Using two or more features in combination to prove someone's identity e.g. something you know (a password), something you have (a smartphone), something you are (biometric data).

Single sign-on (SSO): Use of a single identity to access all of an agency or government's services

Security Assertion Markup Language (SAML): A standard for exchanging authentication between organisations.

System for Cross-domain Identity Management (SCIM): A standard for automating the exchange of user identity data between services.

OAuth (Open Authorisation): A standard that allows apps to access user data while keeping authentication data (i.e. passwords) hidden.

In government, the use of digital identity to validate that an online user is who they say they are will typically involve traversing a complex web of applications, gateways, standards and processes. Traditional workforce identity and access management, covering a diverse range of applications and roles, was complex enough, but at least confined to the one agency, and relatively low numbers of users.

When the need to authenticate, authorise and identify users is scaled to millions of citizens accessing services from thousands of possible devices, in real time [2], oversight becomes difficult for in-house teams and often generates unacceptable levels of risk.

A cloud Citizen Identity solution helps eliminate this burden on agencies, allowing them to focus on improving the user experience.

Common technical issues in digital identity systems:

1. **Authentication**: To ensure only authorised individuals have access to certain services and information, a digital identity system must first be able to prove people are who they say they are. Multi-factor Authentication (MFA) is recommended as a gold standard by government security policy to ensure that systems are not compromised [3].
2. **User experience:** Business systems that require multiple accounts and passwords are likely to have poor navigation and other attributes that provide a poor user experience and lead to citizen dissatisfaction and loss of trust in government. Security may also be compromised through the reuse of passwords across accounts. Single sign-on (SSO) is the contemporary response to these concerns and is a core component of a cloud-based Citizen Identity platform.
3. **Complexity and integration:** Agencies supporting a range of services typically do so via siloed business systems implemented over time in response to new legislation or business requirements. This progressive implementation results in complex IT architectures that in themselves create maintenance and enhancement challenges, especially when technical expertise and resources are limited, as they are in the current overheated ICT labour hire market.

Cost of implementation

In the post-COVID 19 world of increased government debt, rising interest rates and demands for attention to neglected core services, such as aged care and emergency services, the imperative to ensure digital and ICT projects are delivered on time and on budget is greater now than ever before.

Economic headwinds and labour constraints

ICT professionals are among the most highly sought-after and highly paid workers in Australia [4], with over 50% of workers ranking among the top 25% of earners . Despite this, demand across the country for these workers is strong – requiring the public sector to compete with high private sector wages, reducing the availability of the best talent.

Application developers have one of the highest occupational vacancy rates in the country [5] and many other digital and ICT roles are projected to become the most in-demand over the coming years, adding extra pressure to an already tight labour market.

ICT professionals familiar with government processes and requirements and with appropriate security clearances to work on government business systems are rare. This has resulted in an ever-increasing cost of ICT contingent labour hire in the public sector [6].

Competing policy priorities

Adding to these labour pressures is the need for governments to respond via appropriate policy initiatives to a diversity of issues arising from all sectors of society, the economy and the geopolitical situation.

Government across Australia allocated nearly $4.75 billion in their 2022-23 budgets to ICT and digital initiatives [7]. This funding is spread across 278 individual projects, with more than half of these falling into the $5m to $20m range. Project volumes and funding at this level places an enormous call on internal and external ICT resources, with agencies often competing against each other to obtain the digital resources they need.

Cyber security in particular has grown as a policy priority of its own, with $450 million from 2020-21 to 2022-23 in budget year spending on new and existing initiatives in state and territory budgets. Federal Government programs over the same period total over $780 million [8].

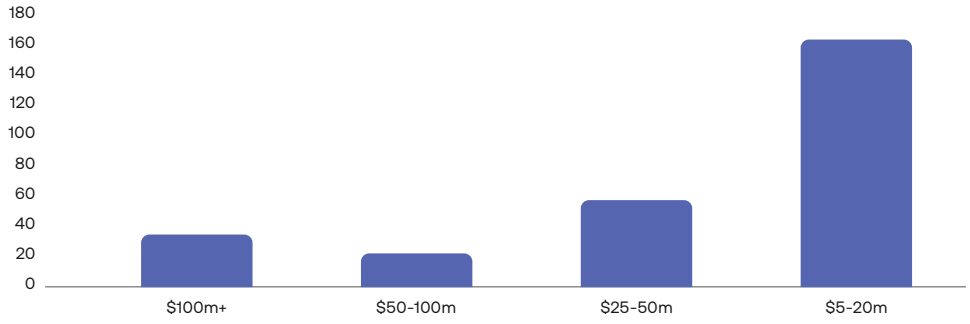
Cost of implementation (cont.)

The use of a cloud-based Citizen Identity platform can help alleviate the resourcing and cost pressures being experienced by agencies by removing complex integration and security issues associated with implementing a custom-built CIAM into already complex architectures and crowded project pipelines.

Software as a Service (SaaS) offerings account for almost 75% of agency cloud contracts [9]. SaaS is favoured, particularly by smaller agencies, due to ease of use, relatively inexpensive start-up costs, and the ability to scale and add value through analytics and information-sharing capabilities.

In an environment where an agency may be utilising a number of SaaS solutions, cloud-based Citizen Identity platforms with SSO capability are a natural fit to manage costs and ensure the productivity of staff can be enhanced, with a flow on benefit to citizens.

Chart 1: Number of 2022-23 budget-funded digital and ICT initiatives - Federal, State and Territory jurisdictions



Cost of implementation (cont.)

Reuse before Buy, Buy before Build

Whole of Government (WofG) architectures and digital service standards are increasingly being adopted by jurisdictions to control digital and ICT spending, increase speed and agility, minimise project delivery risk and join up services.

The Federal Government's WofG digital architecture requires agencies to reuse whenever possible, to design and build for reuse and to enable reuse for others when considering a new digital or ICT capability [10]. Building a solution in-house is now considered a last resort.

'Speed-to-market' is a key part of the cloud value proposition for private sector. In the absence of a commercial imperative, governments see value in cloud-based solutions responding to citizen needs as efficiently and effectively as possible.

Timely response to citizen needs becomes vital in crisis situations. For example, NSW is currently developing a single app for citizens that provides emergency information and risks by expanding its current Fires Near Me NSW app to other disaster types, such as floods and cyclones [11].

A key advantage of cloud Citizen Identity solutions is that once they have been adapted for one instance, they can be quickly reused across government services, agencies and potentially jurisdictions in an agile fashion.

Federated digital identity is taking a long time

The Federal Government has acknowledged digital identity as the key to unlocking the benefits of the digital revolution for almost a decade [12]. In 2018, then-Human Services Minister Michael Keenan announced the Federal Government's goal of being a top three digital government by 2025, declaring that digital identity was "absolutely essential" in achieving this end [13].

This led to the creation of the Trusted Digital Identity Framework (TDIF), an attempt at a nationally consistent digital identity ecosystem providing identities, credentials, attributes and an exchange.

Cost of implementation (cont.)

Despite multiple consultations and iterations of the TDIF and over $430 million in budget funding, uptake of the government's identity solution remains low, with only 10% of users linking their government-provided myGovID to their myGov account. Duplication of accounts has been noted as a common problem, with governance poorly understood and responsibilities for various functions split between four major agencies [14].

The importance of digital identity has also been underscored by the new Labor Government with the 2023 release of the myGov User Audit [15]. Faster adoption of digital identity was found to be "critical to improving government services and making broader digital interactions safe and more secure". It recommends urgently changing governance arrangements to support interoperability across Australian jurisdictions.

Citizen Identity solutions offer the ability for governments to address their digital identity requirements now. By utilising such a platform, governments can iterate to further services, while also providing a basis for a truly federated national identity system.

Citizen expectations

Although cost is always an important factor in government decision-making, the need to maintain and deliver core services while anticipating the future is at the core of the citizen-centric ethos that underpins a modern public service.

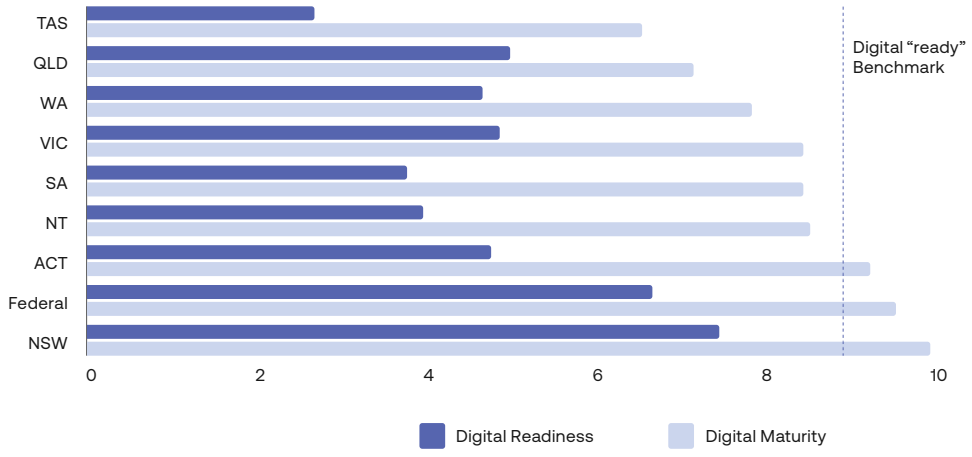
Citizens want an easy, convenient and seamless experience

Citizens are increasingly expecting that their governments can provide online services that work the way businesses do. However, despite considerable progress, nearly all Australians jurisdictions are not quite 'there yet' when it comes to easy-to-use, convenient and seamless services and getting digital identity right is proving to be key factor in achieving this end.

Many jurisdictions have reached a high level of digital government 'readiness' according to Intermedium's annual Digital Government Readiness and Maturity Indicator, which measures a government's policy, strategy, collaboration and processes that enable digital service delivery [16].

Nonetheless, few have made significant progress towards 'mature' digital and ICT environments characterised by citizen-centric, data-driven and platform-based service delivery.

Chart 3: Digital Government Readiness and Maturity Indices 2022



NSW leads heads and shoulders above other jurisdictions, and this is in no small part due to their focus on identity, evidenced by the availability of a multitude of digital licences and the ServiceNSW WofG app. The state is currently piloting digital ID and verifiable credentials, with roll-out expected later in 2023 [17].

Citizen expectations (cont.)

The ServiceNSW app, through which the NSW Digital ID will be available, stands out in comparison to other states, with over 8.7 million accounts (107% of total population) and a customer experience satisfaction rating of 94% [18]. Western Australia's app on the other hand only has accounts that equate to 35% of the population [19]. The Federal myGov app has been found to provide a suboptimal user experience, satisfying only 45% of users [20]. Recognising the NSW Government's success, the Federal Government has indicated it will partner with the state to improve its offerings.

Other jurisdictions are even less mature with their service offerings, with fragmented services across multiple apps and frustrating experiences to authenticate oneself.

Key to NSW's successful approach has been its adoption of cloud Citizen Identity platforms, enabling citizens to authenticate easily while minimising the need to expose sensitive personal data to unnecessary risk.

Tell Us Once

A change in life circumstances often requires notifying many government agencies. The need to do so often comes at a challenging time for citizens, such as moving home or dealing with the death of a relative.

Tell Us Once principles have emerged as one of the key drivers of innovative and citizen-centric service delivery, ideally requiring citizens to update their details just once against a centrally accessible single source of truth.

Tell Us Once is one of the NSW Premier's Priorities, with 60 services available as of June 2022 [21].

A cloud Citizen Identity platform offers the potential to link a single user's identity to multiple services and agencies at scale, allowing for changes to be registered immediately across linked services.

New digital approaches require easy-to-use solutions

For almost two decades, governments in Australia have identified a need for 'joined-up' services and have long seen the value of digital government in being able to achieve this end [22]. Unfortunately, some projects fail to overcome technical hurdles and political realities when it comes to uniting siloed agencies and systems.

Citizen expectations (cont.)

Ease of use' is a key driver in the adoption of digital, cloud-based services in the public sector and there has been acceptance of the notion that government services should be designed in a way that makes sense to the user rather than to the bureaucracy. Achieving such ease of use requires grouping services around 'life events' such as the birth of a child. Commonly, these services utilise UX-design approaches as well as data analytics to assess the 'journeys' that citizens take throughout government to help ensure continuous improvements.

While Citizen Identity is a necessary element of contemporary digital and ICT architectures, a fully integrated system with end-to-end user visibility and data collection can help agencies proactively address citizen needs and evaluate policy effectiveness in real time.

Additionally, a 'single view of government' for the citizen opens the door to personalised services. This holds real promise for citizens in times of crisis – by enabling them to access all services in one place without the need to continually prove their identity or remember multiple passwords.

Cloud Student Identity at UTS: Providing security while scoring customer-centric goals

In 2018 a sophisticated cyber-attack on the Australian National University allowed access to nineteen years of personal information via a single phishing email [23].

This put the entire tertiary education sector on notice regarding their identity and access control systems. At the same time, the nature of university ICT architecture had significantly changed because of a widespread shift to cloud applications.

The University of Technology Sydney (UTS) decided to modernise its identity and access management systems, which were fragmented across various cloud and legacy applications, some requiring the use of a VPN to sign in [24]. Further iterations saw benefits for students and workers, leading to a reduction in complaints regarding remote access.

As a cloud Citizen Identity can centralise user information and act as a third-party intermediary between silos, this future may finally be realised.

Security & compliance

Cyber security is one of the key drivers of government digital policy. Heightened threat levels and mainstream attention to high-profile attacks has resulted in significant funding to upskill professionals to deal with cyber security threats and create cyber-resilient agencies.

The Australian Signals Directorate's (ASD) Essential Eight Maturity Model is a nationwide framework that prioritises a set of mitigation strategies to defend against known cyber threats. The Essential Eight calls for both MFA and monitoring of cyber incidents, features which are both generally offered by cloud Citizen Identity platforms.

A 2021 Australian National Audit Office audit report recommended that a number of federal agencies specifically improve monitoring efforts after finding they were inadequate [25].

Privacy

Case Study: The need for Multi Factor Authentication
A major WofG service delivery agency for an Australian jurisdiction suffered a significant breach of customer data due to a phishing attack.

The resulting audit found that the agency had not effectively handled personal information, storing scanned copies of citizen documents in the agency's CRM, leaving them vulnerable to hackers.

Other weaknesses in IT and security controls were found to have significantly contributed to the breach such as management and monitoring of role-based and user access. Notably, MFA features included with the CRM platform were not enabled which would have likely prevented the breach.

The agency implemented a cloud-based Citizen Identity platform to ensure it could digitise safely and at pace, without the need to worry about blind spots in privacy and security compliance.

Urged on by more frequent, widespread and damaging personal data breaches across the public and private sectors, legislators in Australia (and across the world) are seeking to mandate reporting of data breaches as well as increase punitive measures for organisations found to act recklessly.

Security & compliance (cont.)

Privacy obligations have been gaining traction as an area of significant policy reform, with the Federal, Western Australian and Queensland governments indicating substantial changes to their privacy legislation will be made.

The Federal Government has signalled that the changes to the Privacy Act will likely increase agency compliance costs as well allow the Information Commissioner to independently investigate and order action against intransigent agencies.

A frequently proposed change is the creation of a statutory tort for invasion of privacy. If enacted, this could leave agencies liable to civil lawsuits for damages incurred because of a data breach [26].

Aside from the very real threat of compliance sanctions, the reputational damage incurred from significant privacy breaches can seriously impact citizen trust and hinder the ability of governments to keep pace with digital transformation.

In response to a volatile cyber threat landscape, the NSW Parliament passed laws strengthening the state's privacy enforcement regime. This included the creation of a mandatory notification of data breaches (MNDB) scheme, which will require agencies to maintain an internal register.

As with the Essential Eight, a cloud-based Citizen Identity is an obvious fit, allowing agencies to monitor access centrally and apply specific compliance controls across the whole organisation.

Utilising Citizen Identity will also help agencies respond to the future which will likely entail the hardening of security requirements, such as removing SMS authentication, and allowing for the adoption of new 'passwordless' factors such as biometrics and WebAuthn.

Conclusion

Digital identity will be one of the key drivers to the success of digital government in the future, with significant reforms expected to flow on from the federal myGov audit and from agencies and jurisdictions attempting to manage highly complex cloud and hybrid cloud architectures.

For governments serious about increasing their digital services as rapidly as possible, digital identity that is convenient, easy-to-use and seamless is an essential enabler.

While there are many approaches to citizen digital identity, agencies must consider four fundamentals of government administration – that of delivering core services, anticipating future needs, managing finances responsibly and growing the economy.

Cloud Citizen Identity solutions allow for an iterative and agile approach to building citizen digital identity, allowing agencies to minimise risks around upfront costs, project management and falling afoul of compliance standards.

The same key benefits that apply to SaaS applications generally, such as a centralised view of the citizen, superior data collection and analysis, ease of use, and a fast 'speed to market' also apply to cloud Citizen Identity platforms.

References

[1] https://www.finance.gov.au/sites/default/files/2022-11/data-and-digital-ministers-meeting-communique-41122.pdf

[2] https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model

[3] https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model

[4] ABS, Australian Census 2011, 2016, 2021.

[5] https://www.nationalskillscommission.gov.au/sites/default/files/2022-09/Job%20Openings%20and%20Replacement%20Rates%20by%20Occupation%20-%20September%202022.pdf

[6] Intermedium AnalyseIT tool

[7] Intermedium Budget IT tool

[8] Intermedium Budget IT tool

[9] https://www.crn.com.au/news/cloud-is-absorbing-msps-public-sector-market-reports-aws-584749

[10] https://www.dta.gov.au/whole-government-architecture

[11] https://www.linkedin.com/posts/victordominello_digital-technology-emergency-activity-7023389486482939904-bkOE

[12] https://treasury.gov.au/publication/c2014-fsi-final-report

[13] https://app.intermedium.com.au/articles/ato-keenans-challenge

[14] my.gov.au/content/dam/mygov/documents/mygov-useraudit-jan2023-volume1.pdf

[15] my.gov.au/content/dam/mygov/documents/mygov-useraudit-jan2023-volume1.pdf

[16] https://app.intermedium.com.au/system/files/publications/Intermedium-2022-DGRMI.pdf

[17] https://www.nsw.gov.au/nsw-government/projects-and-initiatives/nsw-digital-id

[18] https://www.service.nsw.gov.au/system/files?file=2022-12/service-nsw-annual-report-2021-22.pdf

[19] https://www.wa.gov.au/system/files/2022-11/AR_2021-22_Digital.pdf

[20] https://my.gov.au/content/dam/mygov/documents/audit/mygov-useraudit-jan2023-volume1.pdf

[21] https://www.nsw.gov.au/nsw-government/premiers-priorities/government-made-easy

[22] https://apo.org.au/sites/default/files/resource-files/2007-11/apo-nid1465.pdf

[23] https://www.abc.net.au/news/2019-10-02/the-sophisticated-anu-hack-that-compromised-private-details/11566540

[24] https://www.okta.com/au/customers/uts/

[25] https://www.anao.gov.au/work/performance-audit/cyber-security-strategies-non-corporate-commonwealth-entities

[26] https://www.oaic.gov.au/privacy/the-privacy-act/review-of-the-privacy-act/privacy-act-review-issues-paper-submission/part-11