Australian Information Industry Association

Submission to the Department of Finance

Feedback on Digital ID Rules, Digital ID Accreditation Rules and Accreditation Data Standards

28 June 2024

Introduction

The Australian Information Industry Association (AIIA) thanks the Department of Finance for the opportunity to comment on the draft Digital ID Rules, Digital ID Accreditation Rules and Accreditation Data Standards 2024 that will support the overarching Digital ID Bill. Please note that as well as broad member feedback, the AIIA's response is also informed by the member roundtable that took place with the Department of Finance on 5 June 2024 in Sydney and the subsequent online meeting between the Digital Identity cyber security team and members of AIIA on the 19 June 2024.

AIIA supports the implementation of a secure, voluntary Australia wide Digital ID scheme and framework. Our members highlight that the success of the Digital ID scheme relies on the trust of the Australian people which will be gained through the implementation of strong, real time cyber security measures. A significant challenge for the Digital ID scheme will be avoiding vendor lock in and remaining technology agnostic while maintaining strong controls for different entities, with different cyber security capabilities, seeking accreditation.

Australia has the benefit of being able to review the implementation of international systems such as those in the USA, Canada, UK, Japan and Singapore to learn from their experience. It will be important that the expansion of digital credentials in Australia is accompanied by public education around the use and protection of digital IDs. Additionally, it is imperative that the Government continue to consult with the ICT industry through the expansion if the Digital ID scheme to the private sector.

The AIIA views the digital ID system as creating a secure and trusted framework that will result in innovation and entrepreneurialism accompanied by a wave of new services and offerings. This has happened in other economies following the establishing of digital ID and payments (e.g. India). The interoperability requirement is an important pillar in the DI scheme rules that supports a system that fosters competition and innovation. The AIIA commends the Government's accelerated timeframe for private sector access and the substantial budget allocation for implementation.

As mentioned in AIIA's submission to the *Senate Economics Legislation Committee inquiry into the Digital ID Bill 2023 & Digital ID (Transitional and Consequential Provisions) Bill 2023*, for the Digital ID scheme to be a success and achieve widespread adoption, it must:

1. Gain and maintain the trust of citizens;
2. Incorporate strong privacy protections;
3. Have robust cyber security protections; and
4. Provide a benefit to the user or citizen by making the use of the scheme more efficient and easier or providing access to new innovative services.

General Comments

Security of citizens personal information

Trust in the Digital ID scheme will depend on the security and transparency of the scheme. To enhance confidence in the Digital ID scheme the Draft Digital ID Rules 2024 should address the cyber security of the Digital ID Government system. Privacy and security rules must address issues around functional creep, the misuse of personal data and security breaches building in safeguards to protect citizens while allowing user consent, control and oversight of confidential information. As part of protecting personal information, collection and retention of data must be minimised. Data collection and retention should be legislated to the bare minimum necessary for the specific purpose. Going forward consideration of how data will be treated when an organisation or citizen leaves the scheme, including data retention implications is required.

Consultation with industry may assist in safeguarding what will become the central access point to citizen digital identities. This key challenge of safeguarding digital identities can be addressed by

1. using phishing resistant passkeys, and
2. Digital ID based on verifiable credentials.

Over thirty percent of Australians have been a victim of identity crime, costing an average of $4,000 per incident. [1] There have been significant rises in the number of attacks using valid credentials and in phishing attacks in Australia[2]. Removing reliance of passwords can help avoid the security failures experienced by other national digital id schemes. Passkeys are phishing resistant as they are implicitly linked to a domain. This means passkeys created for instance for myGov can only be used to authenticate users on myGov, and not on fraudulent or other websites. Biometrics including facial recognition and a fingerprint prevent users entering passwords that can be copied for account takeover. Biometrics also mean users do not have to remember and re-use passwords that once compromised can be used to access multiple accounts.

Digital credentials can abstract confidential information and securely share it from wallet to validator. Digital credentials reduce the amount of confidential information shared, and to effectively execute identity theft, malicious third parties will need to acquire authentic digital credentials from the citizens' secured digital wallet.

Voluntary nature of the scheme

AIIA supports the implementation of the Digital ID scheme on a voluntary basis. However, members consider that there are additional factors that must be considered, such as:

1. After a period of time, we suggest five years after implementation, those major suppliers (for example those with market share of 20 per cent or higher) of services that require ID checks (for example real estate companies who control the rental market for many Australians) should be mandated to accept a digital ID under law;
2. Providing for a non-discriminatory 'right to be forgotten' allowing individuals to request that only data relating to the construction of their Personal Identity be deleted from the platform but not general data the person has provided to tech companies to receive tailored solutions and products;
3. Safeguarding against digital coercive control - aka technology-facilitated coercive control - in unique arrangements such as but not limited to conservatorship or guardianship abuse[3];
4. Allowing for end-of-life considerations and instructions and how this is managed by various regulators.

Interoperability

It is important to align multiple identification, health and skills credential systems to avoid creating separate and duplicative systems for users and limit the collection and storage of personal data. AIIA supports interoperability between the Commonwealth ID scheme and Healthcare Identifiers Service and other relevant credential platforms for example, working with children check and the proposed digital skills passport.

AIIA further suggests that there should be interoperability with State digital identities to minimise the number of digital IDs that citizens should have to establish and seeks understanding of when and how harmonisation and interoperability will be achieved.

---

[1] Australian Institute of Criminology, Identity crime and misuse in Australia; Results of the 2019 online survey, Statistical Bulletin 27

[2] Zscaler, Threatlab 2024 Phishing Report, IBM X-Force Threat Intelligence Index 2024

[3] See also discussions surrounding self-sovereign identity

Regulatory reform

As part of reaching the ability for departmental and Australia wide interoperability and in preparation for the expansion of the Digital ID scheme to encompass the private sector it is imperative that an expansive and regular review of existing legislation and regulations is undertaken. Data sharing, privacy laws/requirements and data retention laws for Commonwealth, state and even between departments, correspondingly need review and harmonisation where possible as a priority.

Oversight

The ACCC's role as an initial Digital ID regulator demonstrates a commitment to ensure that the interests of consumers are protected. However, there are concerns that the tech sector is becoming highly regulated by numerous government agencies that often do not talk to each other. In addition, this new obligation sits in the context of overlapping Federal Government incident reporting obligations in Australia, including but not limited to:

- Notifiable Data Breaches Scheme (Privacy Act): Companies must report breaches of personal information to the Office of the Australian Information Commissioner (OAIC), regardless of whether the breach is due to a cyber incident or human error (e.g., a data spill).
- If breaches of personal information results from a cyber incident, the company must also report to the ACSC.
- Security of Critical Infrastructure Act: Recently amended, this Act requires regulated entities to report cyber incidents to the ACSC, even if the incident does not involve personal information. If personal information is compromised, entities must also report to the OAIC.

This proposed new obligation which requires entities to report all cyber incidents (irrespective of the data or system impacted) to the Digital ID System Administrator, would mean that if they are impacted by a cyber incident affecting personal information, they would have to report to the ACSC, the OAIC and the Digital ID System Administrator. This is complicated and could potentially result in confusion, undermining the effectiveness of each reporting scheme.

Where possible Australia should streamline duplicative cyber incident reporting obligations by establishing a single reporting mechanism to a single agency, which will also provide a central point for monitoring policy progress. This will also provide a centralised mechanism for tracking malicious cyber incidents.

We recommend that all entities report to the Australian Signals Directorate (ASD)/Australian Cyber Security Centre (ACSC), regardless of the circumstances of the breach or the nature of the exposed/stolen information. This consolidation would reduce the regulatory burden on industry and enhance the efficiency of both public and private sectors in protecting our ICT infrastructure.

Accreditation Scheme and Digital ID Providers information sharing

As part of the interoperability and sharing of information between services, we seek an understanding of what elements of data will be shared. It is preferred that where an entity shares credentials, these credentials should only be transferred in an encrypted version, especially by or through private identity exchanges.

Members have highlighted that there needs to be greater articulation of the standards for protecting data at rest.

Nominee Arrangements

While acknowledging that the initial rules will not incorporate rules relating to nominees, the AIIA wishes to highlight the importance and complexity of nominee arrangements in the context of acting on behalf of individuals using digital IDs. The complexity and legal implications of managing responsibilities and financial matters for individuals, especially in cases of disability or incapacity, or after death, are yet to be investigated.

Accessibility

The potential impact of digital ID on vulnerable groups, such as people with disabilities and language barriers needs to be considered and addressed, with a focus on the needs for these communities. The preferred and best case would be a system accessible to all, however in the meantime there must be accommodations and alternative means for people to verify their identify. A digital identity that fails to ensure all have access may increase digital and economic exclusion or reliance on paid agents to access a critical government service, namely the Digital ID. The latter sets up potential claims of discriminatory practices.

Security requirements

Given the sensitivity and personal nature of the data involved and the need to maintain public trust it is imperative that security standards built into the scheme are best practice and reflect the most robust options available. The overall scheme will be as secure as its weakest link. It is essential that the system builds in strong authentication and data protection.

It is recommended that the Digital ID scheme approach to security should be expanded to an all-hazard approach that includes management of risk across cyber, physical, natural hazard, personnel and supply chain areas. Additionally, cyber security risk should be managed and assessed in real time on all forward-facing internet assets and assets held in cloud environments. The effective management of cyber risks in real time can be enhanced with the use of machine learning and artificial intelligence tools that are more responsive than humans in large-scale automated attacks.

While requirements for entities to adopt protective security controls under frameworks such as ISO 27001 and Essential Eight are noted, the Department may wish to align its cyber security requirements with those mandated for systems of national significance under the Critical Infrastructure Act 2018 (SOCI). This could require all entities to:

- Develop and maintain an incident response plan (IRP) for the system and relating to any cyber security incidents. The IRP should be reviewed when there are system updates and following any significant network changes and reviewed annually to stay up to date. The Government should also have the ability to request a copy of this IRP and any subsequent updates. This is a particularly important measure given entities have incident reporting obligations under the posed rules.
- Conduct regular cyber security exercises to test the effectiveness of the IRP. The findings from these exercises should be reported to the Digital ID scheme regulator. Consideration should be given to external evaluations to ensure thoroughness and objectivity.
- Carry out regular vulnerability assessments to identify and mitigate potential security risks proactively. Again, a vulnerability assessment report should be supplied to the Digital ID scheme regulator.

Members have drawn attention to the challenges and limitations of the Essential 8 Maturity Model, particularly in the context of government entities achieving Maturity Model 2. They highlight the difficulties in meeting the maturity model and suggest potential options for grading it differently.

Members have also questioned the record-keeping obligations of the scheme and requested that Government provide more detail on the information to be held, including log keeping, monitoring anomalous behaviour and interactions with other regulatory regimes.

Cyber Security Uplift

As stated in previous consultations, it is imperative that legislation enhance and underscore the importance of cyber security for all entities involved in the Digital ID scheme. Specifically, the Australian Government can drive and incentivise the widespread adoption of relevant cyber security principles across all the digital ID providers in line with international standards and best practices.

Conclusion

The AIIA thanks the Committee for the opportunity to share the tech industry insights and the opportunity to comment on the draft Digital ID Rules, Digital ID Accreditation Rules and Accreditation Data Standards that will support the overarching Digital ID Bill. We are keen to discuss the content of this submission. Should you have any questions, please contact Ms Siew Lee Seow, General Manager, Policy and Media at siewlee@aiia.com.au.

Yours sincerely
Simon Bush
CEO, AIIA

About the AIIA

The AIIA is Australia's peak representative body and advocacy group for those in the digital ecosystem. Since 1978, the AIIA has pursued activities to stimulate and grow the digital ecosystem, to create a favourable business environment for our members and to contribute to Australia's economic prosperity.

We are a not-for-profit organisation to benefit members, which represents around 90% of the over one million employed in the technology sector in Australia. We are unique in that we represent the diversity of the technology ecosystem from small and medium businesses, start-ups, universities, and digital incubators through to large Australian companies, multinational software and hardware companies, data centres, telecommunications companies and technology consulting companies.