Australian Information Industry Association (AIIA) Submission on the 2023 Digital ID Draft Legislation (and Rules)

October, 2023

About the AIIA

The Australian Information Industry Association (AIIA) is Australia's peak representative body and advocacy group for those in the digital ecosystem. We are a not-for-profit organisation to benefit members, and AIIA membership fees are tax deductible. 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.

The AIIA represents the depth and breadth of Australia's innovation technology companies. Given the numbers of tech professionals employed by these companies, the AIIA represents a significant portion of the 900,000+ workforce of the Australian technology sector.

1. Introduction

The Digital ID Bill of 2023 presents an ambitious framework aimed at modernising identity verification in the digital economy. While the AIIA lauds the Australian Government's proactive stance in securing digital identities, this evaluation will critically assess its potential impact on the ICT industry and stakeholders.

The voluntary nature of the system is important, however, there should be options for those in the community who can't access a digital ID. The user experience (UX) for the digital ID "front door" needs to be invested in a priority in any design and roll-out by government. Further, the mobile phone should be seen as the primary vehicle for using the Digital ID and designed to work on 4G networks or higher and work on all operating systems. We have seen through the Indian Aadhaar digital ID system that it achieved almost universal adoption and bridged the significant digital divide by having the smart phone on a ubiquitous mobile phone network as the primary access and use of the digital ID that allowed for services to be developed over the top of the framework.

The AIIA notes that over 10 million Australians are already using the government's digital ID (MyGovID) so there is an excellent platform and trust in the digital identity tools, the challenge for government remains around that seamless customer and citizen experience and "front door" to government service delivery. Without ongoing investment by governments, the benefits will not be realised.

As part of the Digital ID legislation and framework entering Parliament, the Government needs to include a response to the myGov user audit report in which the Thodey Review correctly claimed that it should be seen as a critical platform or asset of government and should be subject to commensurate investment – government will need to allocate funding in the next federal Budget.

Consideration also needs to be given to implementation and detailed use cases: for example, end-of-life and the 'right to be forgotten'. There should also be consideration to a 5-year timeframe after implementation whereby major suppliers (for example those with market share of 20 per cent or higher) of services that require an ID check (for example real estate companies who control the rental market for many Australians) to be forced to accept a digital ID under law.

The AIIA views the digital ID system as creating a secure and trusted framework that will result in innovation and entrepreneurialism of 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 rules that supports a system that fosters competition and innovation.

2. Voluntary Accreditation Scheme

Advantages: The scheme offers an avenue for ICT providers to achieve government recognition, fostering trust among consumers[1]. This voluntary scheme can also help foster innovation by not forcing a one-size-fits-all approach. However, history suggests that "voluntary" systems can result in fragmented adoption.

Concerns: Too stringent requirements could stifle innovation. A study on Estonia's e-ID system demonstrated that balancing security with ease-of-use was critical for uptake[2]. Only **14 out of 27** EU countries have reportedly notified eID schemes under eIDAS as of 2020[3].

Recommendation: An agile framework that allows for iterative improvements based on industry feedback will encourage participation and innovation.

3. Australian Government Digital ID System (AGDIS) Expansion

Advantages: Extending AGDIS to the private sector can streamline online services, providing a potential economic boost similar to India's Aadhaar system, which added up to 1.2% to their GDP[4].

Concerns: The phased approach can create fragmentation, leading to incompatibility issues observed in the early stages of Canada's SecureKey Concierge[5].

Recommendation: Maintain continuous dialogue with ICT providers to ensure seamless integration across systems.

4. Data Protection and Privacy

Advantages: The legislation builds upon the protections in the Privacy Act 1988. While the intent is commendable, relying solely on punitive measures may not guarantee compliance. The stringent measures reflect the EU's General Data Protection Regulation (GDPR), acknowledged for bolstering public trust[6].

Concerns: Over-regulation could increase operational costs. SMEs in particular may struggle with compliance, as seen in the aftermath of GDPR where 74% of SMEs reported significant implementation costs[7]. In the **U.S.**, states like California have enacted strong privacy laws (e.g.,

[1] UK Gov. (2018). Trust in Digital Identities.

[2] Riso, B. (2015). Estonia's E-Residency: A Model for the World?

[3] European Commission. (2020). Status of notified eID.

[4] World Bank. (2019). The Aadhaar Effect.

[5] McMahon, R. (2017). Canada's Digital ID Divide.

[6] EUR-Lex. (2016). GDPR and its Impact.

[7] Business News Daily. (2019). GDPR's Unintended Consequences.

CCPA). Yet, reports suggest that many companies struggle with compliance due to the complexities involved[8].

Recommendation: Consider tiered compliance pathways based on company size, ensuring smaller players aren't disadvantaged.

5. Australian Digital ID Regulator Role

Advantages: Centralised oversight can streamline processes and standards. This model mirrors Singapore's Smart Nation Initiative, which witnessed high industry engagement[9]. The ACCC's role as an initial Digital ID regulator demonstrates a commitment to ensure that the interests of consumers are protected. This model draws parallels with the UK.

Concerns: Potential bureaucratic slowdowns. The AIIA reminds the government of the early struggles of the UK's Verify system where the central oversight mechanism was criticised for its inefficiency[10]. However, its effectiveness has been debated due to issues like the complexity of the registration process and lack of universal recognition[11]. The tech sector is becoming highly regulated by numerous government agencies that often do not talk to each other. In relation to privacy and cyber security there must be coordination of policy and regulatory approaches to ensure red-tape and compliance burden across the economy is minimised.

Recommendation: Regular audits to ensure the Regulator remains effective and agile.

6. Civil Penalties and Enforcement Powers

Advantages: Ensures industry accountability. New Zealand's RealMe service is a prime example of strong enforcement leading to broad public acceptance[12].

Concerns: Overzealous enforcement might deter new entrants, leading to monopolistic tendencies in the market.

Recommendation: Clear guidelines, coupled with an initial grace period, can help companies acclimatise to the new regulatory landscape.

7. Powers of Minister

Concerns: Concentration of power could result in potential misuse or lack of industry representation in decisions. The lack of clarity in the initial drafts of South Korea's Digital ID law led to industry pushback[13].

Recommendation: Establish an advisory council, including AIIA representatives, to ensure industry concerns are considered in decision-making processes.

8. Conclusion

The AIIA believes that while the Digital ID Bill of 2023 has significant potential, its success hinges on continuous collaboration with industry stakeholders and investment in the "front door" and ensure

[8] Bloomberg Law. (2020). A Year Into CCPA, Companies Still Struggle With Compliance.

[9] Smart Nation Singapore. (2020). Digital ID Progress Report.

[10] National Audit Office. (2019). UK's Verify Program: A Review.

[11] House of Commons. (2019). GOV.UK Verify: a secure way to prove your identity online?

[12] NZ Government. (2018). RealMe: A Public Trust Case Study.

[13] Kim, S. (2020). Digital ID in South Korea: Industry Views.

the citizen's user experience (UX) is world class. This will require new and continuous investment from government.

AIIA feedback on the Rules

- Work with industry to ensure clarity and transparency on the definition of System Information (eg does this include metadata)? Will the CI / SoNs Act be amended in the future to include the Australian Government Digital ID System and providers and if so will the step-in powers apply?

> *(2) In this rule:*
> ***system information*** *means information generated, collected, held or stored by the entity in relation to the Australian Government Digital ID System.*
> *(3) The entity must not do any of the following, or cause or permit another person to do any of the following:*
>
> 1. *(a) hold, store or handle system in formation at a place outside Australia; or*
> 2. *(b) transfer system information to a place outside Australia for storage or handling,*
>
> *unless the entity holds an exemption granted under subrule (5) in respect of the holding, storage, handling or transferring of the system information and the entity complies with any conditions on the exemption.*
> *(4) Subrule(3) does not apply in relation to:*
> *(a) a request by the individual to whom the system information relates, being a request made from a place outside Australia; or*
> *(b) transferring information to:*
> *(i) verify the identity of an individual; or*
> *(ii) authenticate the digital ID of, or information about, an individual, where the verification or authentication is to occur at the place outside Australia.*
>
> 4. *(5) On application by an entity mentioned in subrule (1),the Minister may grant, in writing, the entity an exemption in respect of the holding, storage, handling or transferring of the system information at a specified place outside Australia.*
> *Note: See Part 5 of Chapter 8 of the Act for matters relating to applications.*

- For security breach reporting it would be helpful to understand whether a breach or incident will also require reporting to other government agencies (e.g. ACSC, Privacy Commissioner) or just the Digital ID Regulator as indicated in the rules (it is important that providers understand and know their obligations). To clarify that the breach reporting requirements apply to "participating entity" is the Digital ID provider – however what if the breach is discovered by someone other than the provider (for example a cyber security provider or a financial institution)? It seems it does not apply to a "participating relying party" as SS 13 (3) in relating to digital ID fraud an accredited entity or relying party must report fraud incidents to the Digital ID Regulator. Note reporting timeframe is no longer than 24 hours after the breach or fraud is detected.

> *Part 4. 12. The entity must notify the Digital ID Regulator, in accordance with this rule, of any cyber security incidents that occur in relation to:*
> *(a) the entity's accredited services provided within the Australian Government Digital ID System; or*
> *(b) for a participating relying party—services received by the entity within that System.*

- The rules refer to records being held for 7 years for an entity in use (or suspended) and for 3 years for an accredited entity whose approval to onboard has been revoked (3 years after record

was created or 3 years after last used). The AIIA would appreciate understanding the grounds for the discrepancy in timeframes.