Deloitte.

October 2023

2023 Digital Identity Bill and Rules Consultation

Deloitte Response

Executive Summary

Deloitte is pleased to submit items for consideration for the *Exposure draft of the Digital ID Bill 2023*. Ours is a team of identity and cyber professionals who carry out significant work across government and industry building and advising upon identity solutions, particularly for larger scale solutions in the citizen and customer identity domains. Our view is derived from first hand experience in how identity solutions are designed and used. We have recently helped several private sector organisations navigate the requirements of the Trusted Digital Identity Framework (TDIF), and we are strongly supportive of evolving this framework to provide robust but flexible protections for citizen data and online services across both government and private sector contexts. National cyber resilience requires government and industry partnering to solve data privacy and identity proliferation issues together.

We note that the private sector interest in TDIF is significant and that organisations are prepared to invest in scheme participation. This is good for the Australian identity landscape, where strong ground rules are needed to better protect the way that personal information is collected and handled in digital contexts. However, with investment comes a need for some certainty and a flexibility to evolve. We call out a couple of provisions in the Bill that, as currently worded, risk presenting as impediments to uptake and innovation, particularly around cyber threat provisions and the anticipation of particular technologies namely, verifiable credentials.

We also suggest that some thought might be given to the way that identities are strengthened with ongoing use. There is room to consider accommodating identities that are formulated much earlier in a citizen's journey, and taking on board some of the lessons learned internationally on how identities may be used for younger people.

Lastly, we are aware that there is currently some backlog in organisations interested in joining the TDIF community. While the introduction of this draft Bill sends a strong positive signal of the Commonwealth's continued commitment to maintaining a secure digital identity ecosystem, we believe there is an additional opportunity to provide reassurance to those organisations currently seeking accreditation. A clear transition plan for those organisations investing in accreditation would complement the commendable intentions of this proposed Bill.

Rob Parker
Deloitte
Partner, Cyber

Julie Gleeson
Deloitte
Principle, Cyber

Table of Contents

Our contributions and responses mapped to the consultation documents and guiding questions:

Withdrawal, Suspension and Deactivation

Digital Identity Bill Exposure Draft: Chapter 2, Part 2, Division 3, Section 25 and Section 26 (1) (b) and (c) and Division 5, Section 28

Reasonable Concessions for Cyber Incidents

The draft exposure bill has commendably focused on cyber security as a key risk to digital identity services, and we applaud the intent of having participating organisations understand the importance of their role in safeguarding citizen data. However, we believe the following provision impedes rather than assists with that intent. We recommend that it be reconsidered and reworded:

- Chapter 2, Part 2, Division 3 Section 26 (1) (b) and (c):
  The Digital ID Regulator may, in writing, revoke an entity's accreditation if:
  ...
  (b) the Digital ID Regulator reasonably believes that there has been a cyber security incident involving the entity; or
  (c) the Digital ID Regulator reasonably believes that a cyber security incident involving the entity is imminent;

In today's cyber threat context, most organisations are expected to experience a cyber security incident[1]. It, therefore, seems a harsh and arbitrary requirement to be able to revoke accreditation on this basis, and this would likely serve as a significant barrier to organisations considering accreditation. From our work across multiple organisations to date – both government and private sector - we are aware that the meaning and intent of TDIF are very well supported, but obtaining and maintaining accreditation imposes some cost. Investment is far less likely given the uncertainty that this condition would impose.

It is also important to acknowledge that revoking accreditation if a cyber security incident is *imminent* would do little to protect the identities of individuals at risk. Efforts would be much better placed working with the at-risk organisation to prevent that incident from occurring or at least limit damage.

A requirement to work with the Australian Cyber Security Centre (ACSC) or other appropriate cyber authorities in the event of an actual or suspected security incident that is likely to expose sensitive information (including end-user identities) would, in our view, provide better protection for citizens and align with bill's aim to *"protect privacy and security of personal information."*

As written, this requirement provides a strong disincentive for entities to acknowledge incidents and seek help remedying them.

There is room to reserve the right to suspend or revoke accreditation in the worst-case circumstances where an accredited entity poses a clear, systemic cyber risk to the wider Australian Government Digital Identity System (AGDIS) and has proven itself less than cooperative in working with the relevant authorities to mitigate those risks.

Accommodations for Verifiable Credentials

Digital Identity Bill Exposure Draft: Chapter 3, Part 2, Division 2, Section 46 (2) (a)

Future-proofing the Digital ID Bill: Technology Agnosticism

We commend the draft exposure bill for anticipating that the digital identity landscape is changing and will likely continue to evolve, aligned with technological changes and in response to a changing threat landscape.

A forward-looking legislative framework is required to accommodate ongoing evolution. However, we recommend that, as much as possible, the bill remains agnostic regarding technology choice.

Specific reference to verifiable credentials in *Chapter 3, Part 2, Division 2, Section 46 (2) (a)* may unintentionally stymie future innovation and prevent the uptake of other technologies over time. These technology-specific considerations may be better placed in the *Accreditation Rules* that can be evolved and updated without the need for parliamentary approval.

We acknowledge that verifiable credentials will very likely play a significant role in the immediate future –and we strongly support the TDIF evolving to accommodate this model, which puts users in much greater control over the information they share.

Biometrics and Verifiable Credentials

The exposure bill proposes specific privacy safeguard exemptions for verifiable credentials. Specifically, *Chapter 3, Part 2, Division 2, Section 46 (2) (a)* would permit an accredited entity to collect, use or disclose biometric information contained within a verifiable credential. While efforts to accommodate future verifiable credentials into the Australian digital identity landscape are admirable, this may introduce new risks in managing biometric information.

Previously, most biometric authentication use cases in the Australian digital identity ecosystem occurred on-device – i.e. validating that a biometric bound to a device matches the user presenting themselves for authentication, with the biometric data never leaving that device. In this model, authentication is performed with the cryptographic keys that are unlocked once the biometric is validated. While off-device biometric "matching to the source" authentication was possible, its uses were limited by strict provisions within the TDIF – specifically PRIV-03-08-01.

The on-device validation use case translates easily to the verifiable credential world. However, off-device authentication presents new opportunities and risks. For example, new third-party biometric verification services may emerge that exploit the fact that accredited user-controlled wallets are granted carte blanche permission to disclose biometric data. While these third-party biometric services might introduce useful new use cases - e.g. medical personnel presenting a biometric from their wallet to be verified by a security camera before entering an operating room - they are not without risk. New biometric verification services would increase the movement of biometric information throughout the environment, potentially enlarging the risk of unintentional exposure or exfiltration of biometric data that is difficult to reset or recover once compromised.

We recommend reconsidering if the proposed "disclosure" exemption for verifiable credentials is robust enough to provide confidence to users of Australian digital IDs.

Digital IDs for Young People: Factors to Consider

Digital Identity Bill Exposure Draft: Chapter 2, Part 2, Division 4, Section 27 (2) (i)

Context

While the existing legislative landscape may complicate the development of digital IDs for young Australians, the cost of inaction is potentially high. As digital natives and prolific consumers of digital services, young people are increasingly exposed to the risks of weak digital identities. A 2021 UNICEF report found that children tend to collect digital identities at various stages of childhood – if not through formal e-government initiatives, then via private sector services.[1]

Consequently, if the government does not make appropriate concessions to expand the eligibility of digital IDs to young Australians, this cohort will continue to be pushed towards low-assurance, low-security forms of online identification, which generally take a reductive, compliance approach to important issues like informed consent.

Australian Considerations

We recognise that the proposed bill has granted the Minister flexibility to make rules specifying the appropriate age for children to create a digital ID. This is a strong step in the right direction. We also note, however, that there are residual challenges specific to the Australian legislative landscape to be overcome. In particular, the *Privacy Act 1998* and the *Discrimination Act 2004* present conflicting guidance on the age of informed consent and the need to provide young people with access to government services.

While this space is still evolving (notably with the pending outcomes of the review of the *Privacy Act 1998*), it is important to note that Australia is not the first to navigate this issue, and there are lessons to be learnt from established international precedent.

International Precedent

International examples can provide useful precedent to shape Australia's approach. Notably, the European market has developed particularly advanced models for providing children with secure, privacy-preserving digital IDs.

The European Commission as part of the planned *European Digital Identity Wallet* is encouraging its Member States to "issues electronic IDs to monitor under the age of 18, to strengthen effective age verification methods."[2] This is intended to provide EU-wide recognised 'under/over age X' proof of age based on data of birth in a privacy-preserving manner. Belgium, following this guidance, has introduced "Kids-ID" – an electronic identity document for Belgian children under the age of 12. Its primary use case is as a travel document for trips within the EU. However, children from the age of six can use it for online authentication. This approach of gradually increasing use cases as a child develops is underpinned by a strong core identity and robust legislative controls that would be useful to consider as part of Australia's approach to digital IDs for young people.

An Opportunity to Strengthen Identities Through Ongoing Use

We note that the strength of a digital identity increases with use. There is a higher risk associated with someone presenting an identity for the first time, for example, than there is for someone who has consistently used that identity in the same or similar contexts over time.

Allowing students, for example, to commence their identity journey early and then build on it over time could provide significant longer-term benefits in combatting identity fraud. For example, if someone presenting their qualifications is already known through their identity to have studied the appropriate courses, this presents much less risk than someone relatively unknown claiming that same qualification.

References

[1] Australian Bureau of Statistics. "Cyber security incidents double between 2019-20 and 2021-22." *ABS Media Release*, 22 June 2023. https://www.abs.gov.au/media-centre/media-releases/cyber-security-incidents-double-between-2019-20-and-2021-22.

[2] Pelter, Z., Bryne, B., Meyerhoff N., and Mercy E. Makpor. "Government Digital Services and Children: Pathways to Digital Transformation." *UNCIEF Office of Global Insight and Policy*, United Nations University, 2021. https://www.unicef.org/globalinsight/media/1481/file/UNICEF-Global-Insight_e-gov-services-rapid-analysis-2021.pdf.

[3] European Commission. "New European strategy for a Better Internet for Kids." *European Commission: Press Corner*, 2022. https://digital-strategy.ec.europa.eu/en/policies/strategy-better-internet-kids.

[4] Government of Flanders. "Kids-ID: Electronic identity document for children under twelve years of age." *Vlaamse Overheid*, 2023. https://www.vlaanderen.be/en/kids-id-electronic-identity-document-for-children-under-twelve-years-of-age.

Deloitte.

Rob Parker, Partner
Deloitte Canberra Cyber
robparker@deloitte.com.au
+61 423 213 112

Julie Gleeson, Principal
Deloitte Canberra Cyber
jgleeson@deloitte.com.au
+61 414 966 073