Australian Privacy Foundation

https://privacy.org.au

Secretary@privacy.org.au

https://privacy.org.au/about/contacts/

13 August 2026

Submission to the Statutory Review of the Digital ID Act (2024)

About the Australian Privacy Foundation and this submission

The Australian Privacy Foundation (APF) is the nation's pre-eminent civil society body concerned with privacy. Our *Online Authentication of a Person's Identity and Attributes* policy statement is attached in Appendix 1.[1] The statement forms the basis of our response.

We appreciate your invitation to contribute to the Statutory Review of the Digital ID Act 2024 (the Act) on July 24, 2026.[2] However the short notice of around 4 weeks given for submissions is not an adequate period to enable civil society organisations to evaluate, discuss and draft a useful response. Nonetheless our submission follows.

The APF submission focuses on the development of a privacy-preserving Digital Certificate Framework embedded into the Act. Currently Australian organisations routinely collect, duplicate and retain personal information to meet regulatory requirements, facilitate business activities and for other operational purposes.[3,4] **We recommend a shift from Australia's current identity-based security model away from organisations and towards a Certificate system in which people have transparent, auditable and enforceable control over access to their identity attributes**.[5,1]

A short policy brief and technical design specification setting out the recommended Certificate Framework follows. The Certificates would be incorporated into the Australian Digital ID Framework.[6] We include a brief cost-benefit analysis and examine the relevant privacy, constitutional and surveillance concerns in the body of this submission.

Definitions

- Cryptocurrency: A digital asset that uses cryptography and encryption to secure and verify transactions- it only exists in electronic form.
- Blockchain ledger: Cryptographic digital ledger.
- Permissioned ledger : Closed resource requiring access authorisation.

- Relying party : Computer application that relies on information about an individual to provide a service.

- Centralised information repository : Concentrates data under a single management system, requires a single point of failure for access to all stored data.[1]

- Distributed information repository : Interconnected data management systems sharing resources without the need of a centralised information repository, eliminates the risk of a single point of failure.[1]

Overview of the APF recommendation

The proposed Digital Certificate Framework we recommend would be a unique, non-transferable, cryptographic credential issued after a person had completed the appropriate Australian Government Digital ID identity-proofing process. The credential would not contain a person's name, date of birth, biometric template, identity-document number or other personally identifiable information on the blockchain ledger.[5] Instead, it would work as a cryptographically verifiable identity pointer and access-control mechanism that connects to Government ID records. We contemplate a private or permissioned ledger rather than a public cryptocurrency network.

Under the recommended architecture:

1. A citizen could grant a government agency, financial institution or other authorised relying party access to only the identity attributes necessary for a particular transaction;
2. Consent could be limited by purpose, scope and duration;
3. Permission could subsequently be rescinded;
4. Each access request and disclosure could be recorded in a tamper-evident audit log;
5. Individuals could receive notice of who had accessed their information, when it was accessed and which attributes were disclosed;
6. Selective disclosure could permit verification of a fact, such as whether a person is over the age of 18 years, without disclosing the person's full date of birth or identity record; and
7. Law-enforcement or national-security access without consent would be confined to expressly defined statutory powers, supported where appropriate, by judicial warrants and independently auditable controls.

The APF recommends that privacy protections be embedded into the technical architecture itself rather than relying principally on privacy notices, organisational promises and retrospective regulatory enforcement. **We also recommend corresponding amendments to the Digital ID Act (2024) and the Privacy Act (1988) to control and rescind access to an individuals' personal information and mandatory cryptographic access logging.**[7,8]

Privacy and identity-security benefits

The APF proposal is intended to reduce the amount of personal information copied and retained across government and private-sector Frameworks. Currently, each organisation, such as health insurers, state, federal and territorial government services, banking and finance companies and smartphone applications, obtain and retain copies of driver licence/s card numbers, passports, phone numbers, email and postal addresses, Medicare card numbers or other identity documents despite the need to establish only a limited fact or facts about an individual, such as date of birth and/or account number. As cyberthreats continue to grow over time, sometimes involving international actors, regular data breaches are expanding.[9-12] Reducing this duplication of personal information stored by organisations would:

1. Diminish the number and value of centralised personal-information repositories available to attackers: centralised information requires a single point of failure for access to all stored data while distributed information repositories eliminate the risk of a single point of failure, thwarting unwanted access;[1,13]
2. Minimise the consequences of data breach by limiting the reusable identity information held by relying parties;[14]
3. Make stolen document numbers and biographical information less useful for malicious actors;
4. Allow individuals to readily identify unauthorised or excessive access;
5. Improve the accountability of relying parties to individuals through immutable or tamper-evident access records; and
6. Reduce reliance on indiscriminate biometric and public-surveillance Frameworks, such as storage of personal information or facial imagery on a blockchain, as a response to identity crime or other cyberthreats.[5]

The APF does not suggest that any technology can ever guarantee the complete prevention of data breaches, fraud or cybercrime. Endpoint security, credential recovery, software assurance, governance frameworks, key management policies, insider access and legislative safeguards - supported by transparent system audits - will remain critical components of data protection.

The APF therefore recommends independent architecture reviews, privacy-impact assessments, threat modelling, source-code auditing, controlled testing and appropriate statutory governance to strengthen all data breach risk mitigation efforts.[1]

The proposed Digital Certificate Framework system could materially reduce Australia's attack surface while limiting the usefulness of information obtained by malicious actors if a breach occurs. [13] It's combination of data minimisation, distributed rather than centralised information repositories, selective disclosure and cryptographically controlled verification could reduce both the volume of sensitive information exposed and the potential value of compromised data.

The APF recommendation could also generate substantial economic efficiencies by reducing the need for governments and businesses to maintain thousands of fragmented, unconnected digital data silos and their associated privacy and security infrastructure.[15]

Conclusion

This Statutory Review of the *Digital ID Act 2024* provides an important opportunity to strengthen the standard of Digital ID protection and Digital Certificate management in Australia. Consistency with the APF's *Online Authentication of a Person's Identity and Attributes* policy is crucial, as demonstrated above.

The Act should be sharpened in scope and, most importantly, supported by an appropriate legislative framework that gives Digital ID Certificates clear legal force and a predictable, transparent, precise and enforceable application. This would better serve the Australian public interest by supporting a coherent national approach to digital identity and critical infrastructure, rather than perpetuating the current trend towards incremental and increasingly fragmented digital systems.

Contact: Dr. Juanita Fernando, Vice-Chair, Australian Privacy Foundation.

Phone: 0408 131 535

References

1. Australian Privacy Foundation. (APF) Online Authentication of a Person's Identity and Attributes – APF| Policy Statement. https://privacy.org.au/policies/online-authentication/. 27 May 2017.
2. Digital ID Act Statutory Review | Digital ID System. https://www.digitalidsystem.gov.au/have-your-say/digital-id-act-statutory-review.
3. Office of the Australian Information Commissioner (OAIC) Privacy guidance for organisations and government agencies | OAIC. https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies.
4. Office of the Australian Information Commissioner (OAIC) Guide to securing personal information | OAIC. https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/guide-to-securing-personal-information.
5. Nabben, K. The government wants to expand the 'digital identity' system that lets Australians access services. There are many potential pitfalls – Australian Privacy Foundation. https://privacy.org.au/2021/10/27/the-government-wants-to-expand-the-digital-identity-system-that-lets-australians-access-services-there-are-many-potential-pitfalls/ (2021).
6. Digital ID | Digital ID System. https://www.digitalidsystem.gov.au/.
7. Attorney-General's Department. Privacy Act 1988. https://www.legislation.gov.au/C2004A03712/latest/text (2026).
8. Federal Register of Legislation. Digital ID Act 2024. https://www.legislation.gov.au/C2024A00025/asmade/text (2026).

9. Oates, D. ATO admits identity loophole exposed by the ABC tops half a billion dollars. ABC News (2023). https://www.abc.net.au/news/dan-oakes/5618988 (30 October 2025)

10. Apro, Zolli. Breaking Australia - “The MyGov Hack” - A National Security Alarm Bell | LinkedIn. https://www.linkedin.com/pulse/breaking-australia-mygov-hack-national-security-alarm-apr%C3%B3-6owqf/. (October 28, 2025)

11. Office of the Australian Information Commissioner (OAIC) Infographic:Medibank data breach: alleged timeline. https://www.oaic.gov.au/__data/assets/pdf_file/0037/228979/Medibank-data-breach-alleged-timeline-infographic.pdf

12. Office of the Australian Information Commissioner (OAIC) Latest Notifiable Data Breach statistics for January to June 2025 | OAIC. https://www.oaic.gov.au/news/blog/latest-notifiable-data-breach-statistics-for-january-to-june-2025.

13. Bhatnag, A. Centralization vs Decentralization: A privacy-perspective. Cloaked https://www.cloaked.com/post/centralization-vs-decentralization-a-privacy-perspective (2024).

14. Office of the Australian Information Commissioner (OAIC) Relying parties privacy obligation when handling personal information | Digital ID System https://www.digitalidsystem.gov.au/digital-id-accreditation/privacy-materials-for-accredited-entities/relying-parties-privacy-obligation-when-handling-personal-information. (November 2024)

15. Ardagna, C. et al. ENISA Threat Landscape 2024. European Union Agency for Cybersecurity https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024. (2024)

Appendix 1: APF Policy Statement

Online Authentication of a Person's Identity and Attributes

Version of 27 May 2017

For the last two decades, governments have been trying to establish online mechanisms whereby a person can affirm to a government agency that they are who they say they are, or that they have a particular characteristic (over 18, over 65, recipient of a disability pension, etc.).

Many of the proposed schemes have been extraordinarily privacy-invasive, because they would expose a vast amount more personal data than is justified, and to far more than just the relevant government agency.

The APF has made submissions in relation to many of the projects that have been initiated and later withdrawn. Those submissions are indexed here, including the most recent specific submission. They have been drawn on in order to express this short statement about how any such project should be approached.

The APF proposes the following as necessary minimum principles for any Online Authentication Framework:

PROCESS

1. An Open, Participative Design Process

Any such scheme must not be conceived behind closed doors and must not seek 'security through obscurity'. It must involve and engage all relevant parties, including and especially representatives of and advocates for people, and information flows about the project must be open to all parties. Greater detail on the characteristics of an appropriate process are in the APF's Policy Statement on Meta-Principles for Privacy Protection.

2. Comprehensive and Inclusive PIA

A Privacy Impact Assessment process must be intrinsic to the project, must be well-informed, must engage closely with advocacy organisations, and must result in not only a public report but also in a register of the privacy issues identified, and the specific features of the design that address those issues. Greater detail on the characteristics of a PIA process are in the APF Policy Statement on PIAs.

DESIGN

3. Minimisation of Exposure of Personal Data

Where all that is functionally necessary is confirmation that the person has a particular characteristic, attribute authentication should be performed, and the person's identity should not be declared.

This can be achieved by the individual using a pseudonym but signing the assertion that they are making (e.g. 'I am a citizen or permanent resident') in a manner that can be recognised by the authentication service provider that the individual nominates, and only by that provider. The organisation that seeks assurance provides the assertion details to an authentication services provider and receives no data back other than a yes or no (or a 'badly formatted request' response).

4. Subject to the Individual's Consent

The act of disclosure to the enquirer must not be based on the assumption that the enquirer is behaving appropriately. The individual must control the what and when of disclosure, in relation to each requested data-item.

5. Many Alternative Providers of Authentication Services

A centralised scheme is under no circumstances acceptable, because it concentrates power and will be abused, whether the operator is a government agency, a corporation or a 'public-private partnership'.

A scheme must feature a sufficient number of providers of authentication services, such that people have a choice, and can use multiple of them.

Financial institutions are in a strong position to provide such services, because they already conduct sufficiently strong registration processes to pre-authenticate their clients.

6. Two-Sided Authentication

Trust-building is a two-way street. People must also be able to assure themselves that they are dealing with the government agency that they think they are communicating with.

7. Secure Transmission of Personal Data

Contemporary good practices must be applied, and specified minimum, baseline standards must be mandated.

8. Secure Storage of Personal Data

Contemporary good practices must be applied, and specified minimum, baseline standards must be mandated. See APF's Policy Statement on Information Security

9. Safeguards, Controls and Sanctions

The scheme must be designed to detect errors and abuse, with criminal offences and substantial sanctions enacted and applied to persons or organisations that fail to comply and that perform acts that breach security or privacy.

10. Tight Controls over All Access Other Than by Consent

All forms of data access other than with the individual's consent, by any organisation, including and especially by law enforcement and national security agencies, must be subject to a properly managed judicial warrant scheme, including online application by appropriate agencies to judges, but without exceptions for any agency or circumstance.

11. Certification

The security and privacy aspects of the scheme must be subject to review and public reporting by suitably qualified third parties that have not been involved in the scheme's design. This must include point-by-point evaluation of the extent to which the privacy issues identified by the PIA have been actually addressed.

REVIEW

12. Audit

The operation of the scheme must be subject to ongoing audit and public reporting, and periodic review, in order to ensure the identification and management of issues that arise, and the adaptation of the scheme to new needs and challenges.