10 October 2023

Department of Finance
One Canberra Avenue
FORREST ACT 2603
AUSTRALIA

Sent via submission portal

Subject: Submission to the Department of Finance on the *Digital ID Bill 2023*, *Digital ID Rules 2024*, and *Digital ID Accreditation Rules 2024*

Dear Sir/Madam,

We welcome the opportunity to comment on the Draft *Digital ID Bill 2023* (Draft Bill), *Digital ID Rules 2024* (Draft Rules) and the *Digital ID Accreditation Rules 2024* (Accreditation Rules).

The .au Domain Administration Limited (auDA) is the trusted administrator of the .au country code Top Level Domain (ccTLD). The .au ccTLD is part of Australia's critical infrastructure, supporting more than 4.2 million .au domain names. auDA is endorsed by the Commonwealth Government to deliver a secure, accessible and trusted .au domain for all internet users under its Terms of Endorsement.

In performing its functions, auDA seeks to serve the interests of the internet community as a whole and takes a multi-stakeholder approach to its work, ensuring that the views of all interested parties are heard and reflected it our outcomes.

Operational use for Digital ID - registering a .au domain name

To maintain trust and confidence in the .au domain, auDA requires domain name registrars who offer .au domain licences to the public to validate the identity of those seeking to register a .au domain and confirm they have an Australian presence. For certain namespaces in the .au a registrant can validate their identity using identity documents such as a driver licence or Australian Passport. Accordingly, a voluntary, secure and trusted mechanism for individuals to reliably and digitally verify their identities is of interest to auDA.

We understand there will be further opportunities for detailed comment as the phased expansion of the Digital ID system takes place. Thus, in this response, we only provide high-level comments and suggestions.

Voluntary scheme

We support the voluntary nature of the system. Alternative options should be provided to members of the public who cannot or decide not to register and use a Digital ID.

Human-centricity and digital inclusion

We believe it is essential to create a user experience that is designed with Australians' needs in mind. A human-centric design means that all Australians who opt into the system must be able to easily navigate and access services without encountering barriers or difficulties.

We agree in principle with the accessibility and usability requirements set out in the Accreditation Rules. It is our understanding that the Department actively engages with community and consumer advocacy groups to ensure the needs of marginalised and vulnerable groups are considered in the system's design. The effectiveness and suitability of the accessibility and usability criteria should be monitored and re-assessed throughout the phased expansion and amended if required.

Security and privacy

As outlined in our Public Policy Agenda, auDA considers security and privacy as essential elements in improving the digital lives of Australians and protecting and preserving our nation's digital infrastructure.

The Draft Bill, Draft Rules and Accreditation Rules have the potential to significantly raise the security of Australians' Digital IDs and preserve the privacy of our personal and most sensitive information. We endorse the requirements for security and privacy safeguards and agree that a minimalist approach to data collection and retention provides useful additional layers of security and privacy.

In our view, strong security and privacy safeguards and requirements enhance Australians' trust in the Digital ID system, a prerequisite for a successful implementation and large-scale uptake of the system.

We also support that the Digital ID system should be a key pillar of the upcoming 2023-2030 Australian Cyber Security Strategy to build Australia's resilience to cyber threats and identity fraud at an ecosystem level.

Phased approach to implementation of the system

We support, in principle, the phased expansion of the Digital ID system with an initial focus on maturing the foundations of the system and growing the use of myGovID within government, followed by integration of state and territory Digital IDs, culminating in economy-wide Digital ID enabling use of government Digital IDs for private sector services, and lastly private sector Digital IDs for government services.

We believe that the design and issuance of Digital ID solutions should be driven by innovation and competition, consistent with the strong privacy and security requirements discussed above. Generally, private sector technology solutions constantly evolve and innovate to respond to individuals' needs. We believe that Australians could benefit from the earlier integration of accredited private sector Digital ID services in government services (currently Phase 4).

Small business

To accelerate Australia's digital transformation, the government should ensure that small businesses are considered throughout the adoption phases of the Digital ID system and supported in implementing technology likely required to cater to customers using Digital ID solutions. Impact assessments and further engagement and consultation with small business and small business advocacy groups will support the Department in assessing the extent of support small business need.

Emerging technologies

As the Digital ID system matures, multiple Digital ID solutions deploying new digital technologies may emerge. In the long term, this may see the Digital ID landscape composed of a range of accredited and non-accredited participants and introduce greater Digital ID complexity for Australians.

The governance arrangement for Digital ID should consider how different models of identity from various emerging service providers will be managed and how they will interface with the Australian Government Digital Identity System (AGDIS).

Digital ID Data Standards

We welcome the requirement that all Data Standards associated with the Digital ID system are subject to consultation periods of at least 28 days. Data Standards should be sufficiently flexible and technology-neutral to cater for emerging technologies that may underpin future Digital ID solutions.

Multi-stakeholder approach

Multi-stakeholder engagements including *all* relevant stakeholders throughout the phased expansion of the system is crucial. It is important to establish effective cooperation between the Digital ID regulator (and Services Australia where relevant),

policymakers, industry, the technical community, academia and the general public, to ensure the effective implementation by exchanging experiences and best practices.

A multi-stakeholder approach led by the Digital ID regulator could help minimise fragmentation and obstacles and achieve the greatest acceptance of Digital ID among Australians.

Summary

We believe that a trusted Digital ID system is a critical component of a trusted internet. We reiterate our support for a national Digital ID system that will assist our nation in improving the privacy of personal information and the security of identity information.

auDA would be pleased to engage further with the Department on the issues canvassed above. If you would like to discuss our submission, please contact auDA's Internet Governance and Policy Director, [redacted]