dspanz. digital service providers australia new zealand

217 Flinders Street
Adelaide SA 5000

C/- Hudson Gavin Martin
Level 16 45 Queen Street
Auckland 1010

hello@dspanz.org
dspanz.org

18 January 2024

Senate Standing Committees on Economics
PO Box 6100
Parliament House
Canberra ACT 2600

Via email: economics.sen@aph.gov.au.

Re: Digital ID Bill 2023 and the Digital ID (Transitional and Consequential Provisions) Bill 2023

To Whom It May Concern:

The Association of Digital Service Providers Australia New Zealand (DSPANZ) welcomes the opportunity to submit this on behalf of our members and the business software industry.

About DSPANZ
Digital Service Providers Australia New Zealand is the gateway for the government into the dynamic, world-class business software sector in Australia and Aotearoa New Zealand. Our members range from large, well-established companies to new and nimble innovators working at the cutting edge of business software and app development on both sides of the Tasman.

DSPANZ broadly supports the Digital ID Bills and the intent to allow private sector entities to participate in the Australian Government Digital ID System (AGDIS) and leverage myGovID.

In this submission, we provide feedback on the following:

- A voluntary system for non-business individuals will create significant cyber security risks for individuals who do not have a Digital ID. The Department of Finance should consider options to protect individuals from identity theft and fraud.
- The interoperability principle may be challenging for some relying parties to support, depending on the chosen fee structure for the AGDIS.
- For Digital ID to be an interoperable economy-wide system, government agencies (particularly the ATO, Department of Education, Department of Foreign Affairs and Trade and Department of Social Services) should not be able to exempt themselves from accepting any Digital ID providers accredited within the AGDIS.

DSPANZ has previously raised the opportunity to create a Digital Economy Regulator - a central source for security, certifications, data standards, and other requirements for market participants who leverage Commonwealth Government APIs and digital interactive services.

A Digital Economy Regulator could cover entities interacting with AGDIS, CDR, ATO, ABRS, ASIC and Fair Work Commission services. DSPANZ believes this would reduce the overlap in security and data requirements and the overall costs of leveraging these government services, in this case, participating in the AGDIS.

DSPANZ welcomes the opportunity to provide further feedback on our submission. Please contact Maggie Leese at [redacted] for more information.

Yours faithfully,

[redacted]

Matthew Prouse,
President & Director
DSPANZ.

Voluntary Use

DSPANZ would like to emphasise that creating a voluntary system for non-business individuals will create significant cyber security risks for individuals who do not have a Digital ID. To protect themselves against identity theft and fraud, individuals should register with at least one Digital ID provider. With the AGDIS intending to create a marketplace of Digital ID providers, individuals will likely need to register with every service provider available to protect themselves best. This may be arduous and costly for identity providers and require constant vigilance on the part of individuals to ensure they have registered an ID with every accredited provider.

The Department of Finance should consider options to prevent individuals from needing to take the above steps to protect their identity. For example, an individual could choose to only register with a single government or commercial identity provider and prevent their identity documents from being used to register their digital identity with any other service provider. This consent model would be consistent with the 'voluntary' principle and ensure individuals have sovereignty over their identity.

Interoperability

Potential Use Cases and Charging

When the AGDIS is opened to private sector participation, the interoperability principle may be challenging for some relying parties to support, depending on the chosen fee structure for the AGDIS. If there are high or variable fees between providers, it may become expensive for some relying parties to participate.

Many Digital Service Providers (DSPs) want to leverage Digital ID to meet their privacy and security obligations, such as the ATO's DSP Operational Security Framework. These obligations typically fall into two main categories:

- **Identity verification:** verifying entities during sign up processes such as registering or purchasing DSP software products.
- **Ongoing authentication:** verifying entities during sign on processes or performing certain actions within software.

DSPs leveraging Digital ID for ongoing authentication would generate millions of transactions each day. For example, if Digital ID were leveraged to authenticate users before they could process payroll within software, this would drive four billion transactions each year (the number of Single Touch Payroll events received by the ATO each year).

DSPANZ recommends aligning the fee structure with existing services provided by Twilio, Google and Amazon and applying the fee structure across the AGDIS rather than allowing individual providers to set their own fees, considering the number of Digital ID transactions DSPs are expected to generate. The Department of Finance should make it as easy as possible for relying parties to support the interoperability principle and avoid unexpected high costs throughout the system.

For example, the Verify service provided by Twilio starts at USD$0.05 per successful transaction. Twilio can be used in the following processes:

- Onboarding and signup
- Logging in
- Transacting
- Managing accounts
- Confirming number and email owners.

However, we recognise that identity verification (as part of account origination or sign up) and ongoing authentication (as part of account access or sign in) are different processes and that a fee structure may need to differentiate between them rather than setting a standard fee to cover all types of Digital ID transactions.

Government and Interoperability

For Digital ID to be a truly interoperable economy-wide system, government agencies (particularly the ATO, Department of Education, Department of Foreign Affairs and Trade and Department of Social Services) should not be able to exempt themselves from accepting any Digital ID providers accredited within the AGDIS.

DSPANZ is concerned that government agencies will seek exemptions and only accept myGovID or other government issued credentials for certain interactions.

For example, the ATO could apply for an exemption and only allow myGovID to access their online services. A DSP would need to support multiple experiences or workflows to manage interactions that require myGovID separately from other authenticated sessions that relied upon accredited third party IDs.

Moreover, the complexity for users will result in higher costs, less efficiency and potentially broken user experiences. Considering the potential costs for relying parties and Digital ID being free for individuals, relying parties, including DSPs, will ultimately pay the cost of an exemption.

This problem could be exacerbated by the need for DSPs to pay to use both a commercial identity solution and myGovID for a single interaction. This may result in DSPs only using myGovID for all interactions and imposing the full cost of support and maintenance onto the government. It will also weaken the market potential of the Australian Digital Identity ecosystem.

If one government agency is granted an exemption, this will create a precedent for other federal or state government agencies to follow, meaning the entire system is no longer interoperable. Further, requiring individuals to maintain several specific Digital IDs to access different government services will ultimately burden them and move away from the intent of Digital ID.