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

25 June 2024

Department of Finance
One Canberra Avenue
Forrest Act 2603

Via online form.

Re: Digital ID Rules, Digital ID Accreditation Rules and Accreditation Data Standards

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 government's gateway 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 updated draft Digital ID Rules, Digital ID Accreditation Rules and Accreditation Data Standards.

At a high level, our submission provides overarching feedback on private sector participation in the Australian Government Digital ID System (AGDIS) and specific commentary on select rules, including:

- DSPANZ is concerned that the two year delay for private sector participation in the AGDIS will create a compliance deadline for DSPs, with customers expecting this functionality in software.
- Without a clear indication of the charging framework and the Australian Taxation Office's (ATO) stance on interoperability, it will be challenging for DSPs to appropriately budget and plan for utilising digital ID in two years.
- As the Department of Finance (the Department) considers how individuals acting on behalf of businesses will work within the digital ID system, we expect that RAM will become accredited within the AGDIS.

- The Department should look to reduce the compliance burden in meeting the digital ID rules by leveraging and recognising existing security frameworks and reporting obligations.
- The Digital ID Rules and Accreditation Rules should state minimum and maximum record retention periods.
- The Department should align review periods and enduring consent timeframes with the Consumer Data Right requirements.

DSPANZ welcomes the opportunity to provide further feedback on our submission. We look forward to participating in future consultation on relying parties participating in the AGDIS and the charging framework.

Please contact Maggie Leese at maggie@dspanz.org for more information.

Yours faithfully,

Signed by:
Matthew JR Prouse
3C91E097E2F48F0B

Matthew Prouse,
President & Director
DSPANZ.

General Comments

Private Sector Participation in the AGDIS

DSPANZ supports opening the Australian Government Digital ID System (AGDIS) to private sector participation. However, we are concerned that this two year delay for the private sector will create a compliance deadline for DSPs, with customers expecting this functionality in software.

DSPs are managing several projects that are increasing compliance costs and limiting their capacity to develop new products and services for customers. In particular, DSPs are expected to deliver Payday Super from 1 July 2026 in a considerably short timeframe.

Considering this ongoing compliance work, DSPs will find it challenging to meet the technical and operational requirements needed to participate in the AGDIS by late 2026. These changes will fundamentally impact their development roadmaps as much of this work relies upon the availability of entity verification and authentication solutions.

The charging framework and consultation on private sector participation are not expected until next year, which adds further complexity to DSPs participating in the AGDIS in two years.

DSPANZ recommends that the Department of Finance (the Department) consult further with DSPs to understand these unique challenges and ensure that all stakeholders are well supported when the AGDIS opens to private sector participation.

Charging framework

The charging framework will determine how DSPs can leverage digital ID as relying parties within the ADGIS. With the Department indicating that charging is not expected to be included in the rules until 2025, DSPANZ is concerned about the short period between releasing the charging framework and the AGDIS opening to private sector participation.

Many DSPs want to leverage digital ID to meet their privacy and security obligations, which 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 in* processes or performing specific actions within software.

DSPs are expected to drive millions to billions of transactions annually through this use. For this reason, DSPANZ continues to advocate for the charging framework to align with existing services provided by Twilio, Google and Amazon.

DSPs may face further challenges if the Australian Taxation Office (ATO) exempts itself from the interoperability principle and requires government-operated digital IDs for interactions with its digital services. If DSPs are required to support interoperability for their customers

and use a separate service to interact with the ATO, they could be charged twice for the same interaction.

Without a clear indication of the charging framework and the ATO's stance on interoperability, it will be challenging for DSPs to appropriately budget and plan for utilising digital ID in two years.

DSPANZ strongly recommends that the Department provides clarity on the charging framework well before it is finalised in late 2025.

Verifying Individuals Acting on Behalf of Businesses
DSPs rely on machine to machine credentials, the ATO's Relationship Authorisation Manager (RAM), to verify that individuals are authorised to act on behalf of a business within software.

While there has been no indication that RAM will be part of the AGDIS, we expect that it will be accredited as the Department considers how individuals acting on behalf of businesses will work within the digital ID system.

DSPANZ recommends that the Department consults with the ATO and DSPs to understand the impacts of RAM joining the AGDIS.

Interoperability
There is an expectation that the ATO will seek an exemption from the interoperability requirement and require myGovID, or government-operated providers, to interact with their digital services. However, there has been no confirmation from the ATO about whether they will seek an exemption. The longer this is unclear to DSPs, the more significant the cost and timeframe impacts.

As mentioned in our feedback above on the charging framework, there are additional costs and complexities for DSPs that interact with government services and the private sector.

Change management in the system
The Department must recognise that they are now operating a distributed digital ID network and its associated constraints, especially when managing changes throughout the system.

For example, introducing technical or policy changes across the digital ID system will only happen as fast or slow as the entire ecosystem can make this change.

DSPANZ recommends that the Department adopt a change management process to update the rules and technical requirements and ensure that changes can be implemented smoothly across the ecosystem.

As DSPANZ has mentioned in previous submissions to the Department on digital ID, we support establishing a "Digital Economy Regulator". This regulator would be a central source for security, certifications, data standards, and other requirements for market participants who leverage Commonwealth Government APIs and digital interactive services such as

Digitial ID. A Digital Economy Regulator would be beneficial in supporting change management in the digital ID and other similar ecosystems, such as the Consumer Data Right and ATO's DSP ecosystem.

Digital ID Rules

Rule 3.3: Applications for approval to participate - relying parties
We are seeking feedback on how to achieve this coordinated response in future phases of the AGDIS rollout, where non-Government organisations who may not have large fraud and security teams may find these requirements difficult to meet.
The Department should look to reduce the compliance burden in meeting the digital ID rules by leveraging and recognising existing security frameworks and reporting obligations. For example, DSPs already meeting the ATO's DSP Operational Security Framework or Consumer Data Right requirements could have these recognised and only need to meet the digital ID requirements that are not aligned.

The rules also contain several reporting and notification requirements that could be simplified to reduce the burden of complying with several different timeframes. Further, security reporting requirements should align with or rely upon information sharing from the Office of the Australian Information Commissioner or the Australian Cyber Security Centre to reduce the overall reporting burden for participants.

As mentioned in our feedback above, DSPANZ believes that establishing a Digital Economy Regulator would help reduce the compliance burden for DSPs and other participants in these digital ecosystems.

How would you consider clarifying these rules for non-government organisations while still maintaining strong minimum security and fraud protections for individuals who may use their digital ID to access that relying party service?
Under this rule, the requirement that the entity's governing body approve these plans may not translate well for non-government organisations without defined governing bodies.

In line with our feedback to the above question, DSPANZ recommends leveraging and recognising existing security frameworks and reporting obligations and exploring how a Digital Economy Regulator can reduce the compliance burden across different digital ecosystems.

Rule 4.2: Cyber security incidents and digital ID fraud incidents
Do you have any suggested changes to this rule supporting the relevant regulator in accessing the necessary information to undertake investigations into cyber security or fraud incidents that could occur within the Australian Government Digital ID System?
DSPANZ recommends aligning the reporting timeframe with the requirements of the Notifiable Data Breach scheme.

Rule 6.2: Record keeping requirements for accredited entities

Is 6 years an appropriate timeframe to retain the logging and transaction information required by rule 6.2 in the proposed Digital ID Rules in relation to transactions and personal information on the Australian Government Digital ID System? What do you consider an appropriate minimum timeframe for the retention of this type of information?

DSPANZ recommends that the Department consider the other information and documentation accredited entities must retain to demonstrate compliance with the rules under the relevant record keeping requirements. For example, the accreditation rules require records of decisions, investigations and responses to digital ID fraud incidents and data breaches.

Digital ID (Accreditation) Rules

Should the Accreditation Rules set out a maximum data retention period for an individual's personal information? For example, that an accredited entity must delete personal information after a period of time if an account becomes dormant. What should that period of time be?

DSPANZ believes defining minimum and maximum data retention periods is essential to helping accredited entities manage the privacy and security risks of retaining personal information. These retention periods should follow the logging record keeping requirements under the rules.

Rule 4.10: Advice to individuals

While this requirement directly applies to accredited entities, this rule seems to require relying parties to inform their customers, given that the individual is not directly interacting with the accredited entity.

Rule 4.22: Cryptographic standards

DSPANZ questions whether the specific version of TLS should be stated in the rules. The wording for this rule could leverage the wording used in the Information Security Manual (ISM), stating that accredited entities must implement the latest version of TLS.

Rule 4.41: Enduring consent

Do you think the rules should set a timeframe for enduring consent to expire? What should that timeframe be?

The Department should align the enduring consent timeframe for digital ID with the Consumer Data Right - 12 months.

The Department must also consider how enduring consent will work for individuals acting on behalf of businesses. Again, we suggest following the Consumer Data Right requirements, which provide 7 years for business consumers.

Rule 4.35: Record keeping

DSPANZ recommends including a minimum retention period for this requirement.

Rule 4.42: Data minimisation principle
While we support this rule, which allows relying parties to minimise the amount of data they collect, we recommend that the Department undertakes specific consultation before the AGDIS is opened for private sector participation to understand how this information exchange works in practice and the associated costs.

It is worthwhile noting that DSPANZ has published a data minimisation and retention best practice guide for DSPs.

Rule 4.47: Record keeping
DSPANZ recommends including a minimum retention period for this requirement.

Rule 6.1: General requirements
To reduce the compliance burden for accredited entities, the Department should align the review periods with the Consumer Data Right requirements. The Consumer Data Right requires a review after 12 months in the first year of accreditation and then every two years.

The Department should also align the timeframe for accredited entities to share their annual reviews with the regulator to the Consumer Data Right, which provides participants 3 months.