dspanz. digital service providers australia new zealand

217 Flinders Street
Adelaide SA 5000

info@dspanz.asn.au
dspanz.asn.au

16 July 2021

Digital Transformation Agency
50 Marcus Clarke Street
Canberra ACT 2601

Via email: digitalidentity@dta.gov.au

Re: Digital Identity Legislation Position Paper Submission

To Whom it May Concern:

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

We welcome the release of the new Position Paper and thank the Digital Transformation Agency (DTA) for taking the time to directly consult with DSPANZ on how Digital Identity will be used by Digital Service Providers (DSPs) in the lead up to its release.

Our submission covers the following points:

- The charging framework should be in line with the fee structures of existing providers to make costs affordable;
- Recognising or adopting the Security Standard for Add-on Marketplaces (SSAM) for relying parties would help reduce regulatory burden for DSPs looking to participate in the system;
- We support the interoperability principle but note that DSPs may have additional user verification requirements when acting as a relying party that are not covered by the TDIF specifications;
- There is an opportunity to align the Trusted Digital Identity Framework (TDIF) with New Zealand's Digital Identity Trust Framework; and
- Users should be made aware that they need to create accounts with each identity provider as well as verifying all of their identity documents to prevent their identity from being compromised.

DSPANZ would appreciate the opportunity to engage further on this submission. For further information, please contact Maggie Leese.

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

Yours faithfully,

Simon Foster,
President & Director,
DSPANZ

Formerly ABSIA

Digital Service Provider (DSP) use cases and impacts of the charging framework
We are pleased to see that the DTA is considering more business use cases for Digital Identity. However, this has the potential to considerably increase the number of identity exchanges with DSPs undertaking hundreds of millions of identity verification transactions per day. This means that the charging framework, if the costs are high, will be a barrier to entry for DSPs.

We are also concerned about identity exchanges with variable fees and DSPs needing to determine which identity provider is the cheapest as part of an application log in process. Choosing the cheapest option may mean that some DSPs will be required to compromise on cyber security. There may also be circumstances where a relying party cannot afford to use a particular identity provider.

We would like to see the charging framework fall in line with current providers including Google Cloud Platform (GCP), Facebook, Amazon Web Services (AWS), Apple and other similar providers to keep the costs affordable for DSPs and other relying parties. Find an outline of the costs for GCP below.

GCP Fee Structure

Tier 1 Providers:

- Email
- Phone
- Anonymous
- Social

Monthly Active Users (MAU)	**Price per MAU ($USD)**
0 - 49,999	0
50,000 - 99,999	0.0055
100,000 - 999,999	0.0046
1,000,000 - 9,999,999	0.0032
10,000,000 +	0.0025

Tier 2 Providers:

- OpenID Connect (OIDC)
- Security Assertion Markup Language (SAML)

Monthly Active Users (MAU)	Price per MAU ($USD)
0 - 49	0
50+	0.015

Moving forward, DSPANZ is happy to participate in roundtables or consultations to ensure that these use cases are accounted for.

Recognising or adopting existing security frameworks for relying parties

We would like to see the recognition or adoption of the Security Standard for Add-on Marketplaces (SSAM) for relying parties to meet the security requirements of participating in the Digital Identity system. The SSAM is a lightweight security standard put in place to increase the minimum levels of security amongst applications that connect to DSPs and ultimately through to the ATO. It has been adopted by DSPs and their add-on ecosystems. Adopting or recognising the SSAM, or similar existing standards. would make meeting security requirements much easier for relying parties rather than making them meet entirely an entirely new set of requirements and increasing regulatory burden.

As the custodian of the SSAM, DSPANZ would be pleased to provide more information about the standard and how it could be utilised.

Interoperability principle

We support the interoperability principle in that it gives flexibility for users to choose which identity provider they would like to use for different purposes. It will be important to ensure that the process is efficient and allows relying parties to be able to trust the process.

DSPs may have additional user verification requirements when acting as a relying party that are not covered by the TDIF specifications. For example, when consuming services from the Australian Taxation Office and data under the Consumer Data Right. We do positively note the inclusion of exemptions for some relying parties. However, it is critical that relying parties are not required to revalidate what solution is being used; who has verified the user's identity and whether two factor authentication has been used or not.

Interactions with other digital identity frameworks

We believe there is an opportunity to align the TDIF with New Zealand's *Digital Identity Trust Framework*. Aligning these two identity frameworks and ensuring they are interoperable would make things easier for participants operating across both systems.

Users needing to create multiple accounts and verifying all identity documents

Under the UK's digital identity framework, individuals are essentially required to create accounts with all identity providers to prevent their identity being compromised. We would expect a very similar situation to arise in Australia and this should be made known to users. Similarly, we see an issue with users needing to verify all of their existing identity documents with each identity provider so that any unused identity documents cannot be used to create a separate account for the same individual. Risk mitigation approaches to this problem should be investigated so that users can reasonably protect themselves.