Digital Identity Legislation Position Paper Submission

Information Identity and Aravena Global Solutions thanks the DTA for the opportunity to make this combined submission on the Digital Identity Legislation Position Paper.

It is clear that this paper, unlike the previous calls for submissions, does not seek respondents to answer questions in relation to Digital Identity systems/frameworks or the suggest legislation but rather seeks to feedback on the DTA proposed position. As such, the feedback provided has naturally tended to be more a focused review on what is being presented rather than generating more wide-ranging responses. However, whilst specific feedback has been provided (essay style) we have attempted to also identify areas that have not been clarified or requires improvement that could be included in the proposed legislation so that it achieves an outcome that we are all desiring.

Again, we thank you for this opportunity and we are happy for the submission to be made public, including any Personal Information herein.

Response

Accredited Participant & Participant– is limited to only those that are on-boarded to the Digital Identity System or participating in the system, noting that TDIF Providers are also proposed to be accredited. As such their does not appear to be a defined term that covers both Accredited Participant and TDIF Provider.

However, it is clear from the review that such a term is required, as throughout the Paper the term Accredited Participant, or Participant, is used somewhat generically and as such it is confusing as to whether, or which parts, the Legislation will not apply to TDIF Providers as well (noting that Accredited Providers are on-boarded to the Digital Identity System whereas TDIF Providers are not). It may be more applicable to use a term generic term in many of these instances, as 5.4.1 indicates most of these areas are included in the Legislation provisions. The concern is this confusion will flow into the proposed Legislation and the subsequent arrangements.

Some examples are:

a) 3.5.1 (Security Requirements 4th para) – indicates that Legislation will permit the OA to coordinate sharing of information between Participants, however, 'Accredited Participants' are only those on-boarded to the Digital Identity System (not TDIF Providers). As such, does this mean that the legislation will not cover/permit TDIF Providers in this sharing of information? As such, are they exposed to a) fraud risks, b) TDIF accreditation compliance risks if they do share information?

b) 5.3 (What's Changed since the Consultation Paper? 4th para) – '… it is now proposed to focus on the Accredited Participant generating the Digital Identity …. ' this would also apply to a TDIF Provider.

c) 7.4.2 (Safeguards on biometric information 3rd bullet) ' … prevent Accredited Participants from sending ….' this should also apply to a TDIF Provider.

d) 7.4.15 (Data Breaches) & 8.1 (Trustmark) – no mention of applicability in relation to TDIF Providers

Credential - Definition of Credential is at odds with NIST SP 800-63-3, which may cause confusion and lead to reduced acceptance in the community, especially in the provision of technical capabilities

Digital Identity System – provides the impression that a Participant has to both 'collect and validate attributes of individuals', based on definitions of Attribute Providers Identity Exchanges, and Credential Service Providers they don't appear to be 'collecting and validating attributes of individuals (ie. APs – verifies specific attributes they don't collect, IDX convey, manage and coord the flow of attributes and assertions they neither collect nor validate).

5.4.1 (Scope of the Legislation) – does not include in Fig 2 Relying Party implications (though 5.4.14 identities that some will be applied). As such, it is not clear how the legislation provisions, especially those relating to Penalties, Liability and Redress, are applicable to Relying Parties – or whether they are proposed to be. Whilst it is noted that other Legislation (Privacy, Corporate, etc) are/may be applicable it is difficult to identify at this point the impacts for Relying Parties and is therefore of concern.

5.4.5 Participant Register and TDIF List – displaying date of accreditation, and subsequent renewals

To be on either list/register an organisation will have to be accredited against the TDIF. It is clear that undertaking such an activity is costly and involves meeting the minimum standards as defined in TDIF. In addition to TDIF, some organisations may participate in other accreditation schemes (ie. CSP may also be a participant in the Microsoft Trusted Root Program). In such cases, there is normally overlap in accreditation requirements and the potential for those organisations to use TDIF accreditation (or parts of it) in their accreditation to other schemes. As such, it would be preferable that any public Register or List also include the latest Accreditation date (initial or renewal) and perhaps the date/duration that it is accredited for, eg. Accreditation Date –12 Jul 21, Accreditation Expiry - 12 Jul 23. In addition, it is noted that 6.4.5 (Functions of the OA) also includes an indication that the OA may publish 'accreditation summary reports' the inclusion of these reports (or links) within the Register/List may also be invaluable to organisations participating in other schemes.

5.4.6 (Defining a Digital Identity) – limits the definition of a digital identity to one provided by an IdP listed on the Participant Register. Does this mean an TDIF IdP Provider (ie. not an Accredited Participant) cannot provide a Digital Identity? If so, it is difficult to understand the implications on the use of the Digital Identity outside the System & therefore how the Legislation applies to the TDIF IdP Provider. In addition, this statement contradicts the definition as defined in the glossary.

5.4.7 (Defining Digital Identity Information) – The internationally used the concept of Personally Identifiable Information (PII) appears to be very similar to what is proposed to be in defined in Digital Identity Information. As such, why is Australia creating another term that has potential to cause confusion between countries, accreditation schemes and technical providers? This has the potential to be an impediment to the 'cross accreditation' or acceptance of a Australian Digital Identity on an international basis. As such, it is suggested that alignment of terms (or at least acknowledgement of a relationship) would improve international acceptance of Australian Digital Identities.

6 (Governance of the Digital Identity System) – There is some concern with the potential for 'tension/conflict' by establishing governance arrangements where two parties are accountable for differing portions of the arrangements (ie. between OA and Info Commissioner in relation to Privacy and accreditation – especially as states & territories have local privacy legislation). The previous

Digital Identity Consultation Paper (Dec 20) indicated that several privacy and consumer protections would be included in the legislation

- ensuring the system remains voluntary, not mandatory
- prohibition on the commercialisation of personal information and profiling of individuals
- restrictions on the creation and use of a single identifier for the whole system
- restrictions on the use and retention of Biometric Information to those required for verification on the system
- requiring express consent from an individual or their representative to use the system to authenticate and pass Attributes to a service.

Due to the potential for tension/confusion might it not be possible for these aspects to be included in updated to the relevant legislation (ie. Privacy Act) in relation to use/involvement in a Digital Identity System/Environment or aligned to the Act? (Noting that one of the key principles (7.1) was building on existing laws.) As such, the existing rights of the Information Commissioner are still applicable, and the OA can utilise these in their role.

6.6.3 (Continued Use of Digital Identity in offboarding context) – whilst the paper claims that this 'is a relatively simple step' for the User it will be important that:

a) they have choice in their Accredited Provider (especially IDP)

b) they do not have to re-undertake the Identity Proofing process, including re-providing biometric information, with the new provider (to achieve the same level of identity)

As such, it is envisaged that any off-boarding arrangement may need to occur over a period, which will be interesting if the Provider has been compromised in relation to trust – especially as the new Provider will need to potentially accept the old Provider credential to establish their credential with the User. This aspect does not appear 'simple' nor is it clear in the TDIF how this is managed.

7.4.12 (Accessible and inclusive website design) – noting the multicultural and diverse nature of the community, there is a concern that the Bill may be drafted that Providers must only use English ('.. clear, concise and plain English ….). It is important that this limitation is not mandated - should be possible to not only have English but other languages as the Provider wishes.

7.4.14 (Application of Privacy Laws) – for the avoidance of doubt is it correct that private entities (that may only service a relevant state or territory) would have to comply with the Commonwealth Privacy Act? This section appears to be limited to States & Territory Government entities, whereas RPs are subject to privacy laws that apply to them providing their services.