December 17th, 2020

To whom it may concern

This response is submitted by Kantara Initiative.

Kantara is the leading global consortium whose mission is to grow and fulfill the market for trustworthy use of identity and personal data. To fulfill this mission Kantara operates an independent third-party conformity assessment program for the digital identity and personal data ecosystems. In addition to this Kantara has, since its inception in 2009, provided real-world innovation through its development of service assessment criteria for various certification schemes and specifications, such its Identity Assurance Framework (IAF), UMA 2.0, Consent Receipt, applied R&D.

Our interest in offering this submission is to help the Government of Australia to keep in mind, during the development of its Digital Identity Legislation, the importance of providing assurance as to the conformity of all parties involved in the requirements the Government has established for its Digital Identity Ecosystem, and how that assurance can be reliably delivered by proven means.

This submission was developed by participants in Kantara's Identity Assurance Work Group (IAWG). The IAWG consists of individuals from both the public and private sectors with extensive experience in the identity industry including assessing identity services for conformance to established requirements, developing requirements for identity services, and implementing and providing identity related products and services.

Kantara is therefore interested in working alongside the Government of Australia at key points in the development of its Legislation to provide a supporting assurance process. The Kantara assurance process is based on the experience of over a decade's operations and on the skills and understanding of our own subject-matter experts, some of whom have contributed to this response.

We invite the Australian Government's Digital Transformation Agency team to continue to keep Kantara apprised of its progress. We further suggest further call-ins during to continue to explore how Kantara might support the development of an assessment/certification component of the Government's Legislation.

Sincerely,

Ruth Puente

Ruth Puente
Director, Assurance Operations
Kantara Initiative

Consultation questions

1A) Are the matters above (legal authority, privacy protections, governance, amendments) relevant matters which should be included in the Legislation?

1B) Are there additional matters which should be considered?

> **Kantara Response**: Kantara suggests that the legislation include consideration of international interoperability. For example, Canadian companies operating in Australia, foreign individuals who act on behalf of Australians (e.g., a UK citizen with Power of Attorney for an Australian), or a service operating in the European Union being used by an Australian.

2A) What matters covered by the TDIF should be incorporated into the primary legislation?

> **Kantara Response**: Kantara is not familiar with the structure of Australian legislation. That being said, from what Kantara understands of the structure, it recommends that the necessity of the concepts that are included in 04 - Functional Requirements and 05 - Role Requirements be incorporated into Primary Legislation. For example, the need to conduct Privacy Impact Assessments should be part of the Primary Legislation.

2B) What matters covered by the TDIF should be incorporated into Operating Rules?

> **Kantara Response**: Kantara would recommend that the details associated with the concepts included in 04 - Functional Requirements and 05 - Role Requirements be incorporated into Operating Rules. For example, who is accountable for conducting Privacy Impact Assessments and how often they should be conducted should be incorporated into Operating Rules.

2C) What matters covered by the TDIF should remain as policy?

> **Kantara Response:** Kantara recommends that the remaining parts of the TDIF remain as policy.

3) Is a publicly available 'Digital Identity Participant Register' an appropriate mechanism to communicate who will be covered by the Legislation?

> **Kantara Response:** Kantara suggests that it depends on the functionality Australia wishes to achieve. In some ways, a Trust Mark (along the lines of an RCM) appearing on

a service would be of greater use to clients to reassure them (at the time of use) that a service is compliant. A RP could use a Digital Identity Participant Register to be assured that entities with whom they interact are compliant. A Participant Register could even be queried as part of the authentication process to provide real-time assurance that the Participant's registration remains valid as of the time of a transaction. Australia will need to determine if they wish the Digital Identity Participant Register to be static or dynamic, and if the same requirements apply to providers and consumers.

4) Are the proposed obligations on relying parties described above reasonable? Should there be any additional obligations?

Kantara Response: Kantara, not being familiar with other Australian legislation, wonders if RPs are already subject to data minimization requirements or requirements concerning the use, sale or transmission of collected personal information. This being said, Kantara is concerned that establishing obligations on (the anticipated) RPs outside of government might limit uptake. Small RPs might consider the cost of meeting those obligations might exceed the benefits they would realize from participation. Is it Australia's intention to exclude these RPs? In any case, Australia should keep in mind that each obligation imposed on any Participant imposes costs that may result in lower participation.

5) Are the concepts outlined above appropriate to include in a definition of 'Digital Identity' for the Legislation? Are there any additional concepts that should be included?

Kantara Response: Kantara suggests that the middle bullet ("will always be capable of electronic transmission or its equivalent") would be better worded as "will always be capable of electronic authentication or its equivalent". The concept of "electronic transmission of a digital identity" is challenging to understand.

6) Does the Legislation need to include a definition of Digital Identity information, or is it preferable to rely on the definitions of personal, sensitive, or protected information in other Commonwealth Acts?

Kantara Response: While Kantara is not familiar with Australia legislation, it believes that it is important that this new legislation remain consistent with other Commonwealth Acts. To that end, Kantara would suggest that the Legislation include a definition of Digital Identity with reference to the definitions of personal, sensitive, or protected information in other Commonwealth Acts.

Kantara is not a proponent of establishing a "standard set of Digital Identity Information". The issue that Kantara has observed is that any such set is not universal

across all instances. While not being a sufficient set can be overcome, the case where attributes in the set are not required is problematic as it usually violates the principle of data minimization.

7) What factors should be considered in the development of a charging framework for the system?

Kantara Response: Kantara endorses that users should not be charged to use or acquire their Digital Identities. Kantara suggests that consumers of Digital Identities (or attributes) (i.e., RPs or IdPs that are verifying an identity attribute) be charged by providers of those Digital Identities or attributes (IdPs or Authoritative Sources). Under this model, these consumers can determine the cost/benefit of acquiring the information. In general, Kantara also recommends that the business framework be designed wherever possible to promote competition amongst providers, to keep prices down while increasing service quality and User choice.

8A) What factors should be considered in the development of the liability framework?

Kantara Response: in Kantara's opinion, Government is uniquely responsible for developing the liability framework, so this may be the Government's most important contribution to the success of the system. For reference, Kantara was involved with the amendments to the Commonwealth of Virginia legislation which of relevance here:
https://law.lis.virginia.gov/vacode/title59.1/chapter50/
https://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-436/
https://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-437/

Kantara suggests that the framework's design goals should be: clear definition of the liability of all Participants (including the government) and Users; and effective delivery of recourse, especially for individuals. Kantara also suggests that the liability framework make maximum use of existing legal institutions rather than viewing the task as building a complete separate framework for identity related liability.

Finally, Kantara suggests that the financial liability of Users for losses incurred by fraudulent use of their credentials by another party be very low, very clearly defined, and be established in law. The credit-card system in the United States and in many other countries provides a model: credit-card holders are liable by law only up to a maximum of $50 for fraudulent use (by others!) of their cards, provided they report the loss of theft of the card promptly to their card issuer. Losses to fraud are shared between card issuers and merchants according to their contracts. The reason for this approach is that Users are

the least-sophisticated and most financially vulnerable actors in the system, but their adoption of the system is absolutely essential to its success.

8B) In what circumstances should Participants be held liable under the liability framework?

Kantara Response: Kantara suggests the following as a possible approach that could be adapted to the specifics of Australian institutions. Participants should of course be held liable for criminal acts like fraud or gross negligence resulting in harm. The framework Participant agreement should be viewed as a contract between the Government, Participants and Users. Enforcement of obligations undertaken by Participants will also be required, presumably by some combination of fines, removal from Participant status, or additional obligations (e.g., more-frequent audits or reports.) Financial losses or harms to Users or to other Participants demonstrably resulting from failure of a Participant to perform their framework function(s) according to their obligations or to take other reasonable measures to protect identity data should be actionable via the courts by the injured party or parties. (In some jurisdictions only the Government can impose a fine or initiate legal action based on failure to meet identity related obligations; in some jurisdictions the liability of an identity-services-provider is limited to implementation of government-defined practices that may not add up to effective protection of identity information or credentials). Users would of course be liable for their own criminal actions on-line, and Australia might consider imposing basic obligations on Users (e.g., prompt reporting of compromised credentials, no credential-sharing) by specifying that Participant IDPs included them in their standard Subscriber Agreement.

8C) What remedies and/or redress should be available to aggrieved Participants and Users for loss or damage suffered as a result of their use of the system?

Kantara Response: Kantara suggests that any Financial losses or harms to Users, or to other Participants, demonstrably resulting from failure of a Participant to perform their framework function(s) according to their obligations or to take other reasonable measures to protect identity data should be actionable via the courts by the injured party or parties. (In some jurisdictions only the Government can impose a fine or initiate legal action based on failure to meet identity related obligations; in some jurisdictions the liability of an identity-services-provider is limited to implementation of government-defined practices that may not add up to effective protection of identity information or credentials.)

8D) What other best practice mechanisms and processes should be considered to support Users when things go wrong?

Kantara Response: Kantara recommends that it should be possible for those Users (and non-Users) who find that someone else has managed to get an account in their name with a different provider be able to find out what has been done in their name so that it can be rectified. This requires considerable record keeping (an obligation on relevant Participants) and precludes strict double-blinding (which also causes challenges for any accounting.) To make this support for Users effective, the framework should include an obligation on Participants promptly to notify affected individuals of a likely compromise of their credential or their information.

9A) Should the proposed privacy and consumer protections listed above be enshrined in primary legislation?

Kantara Response: Kantara is not sufficiently familiar with how Australia uses primary legislation vs. legislated "Operating Rules" vs. non-legislative rule-making to offer a suggestion. This being said, Kantara notes that these protections could be incompatible with the principle of user choice. If, for example, a user wants a single identifier which would not offer the same threats as the use of an address or the complications associated with multiple names, then Kantara believes that option should be available. It should also be noted that there are cultures (e.g., indigenous Australians) where the use of the name of the deceased is taboo but where there is no ancient tradition concerning the use of other identifiers.

9B) Are additional protections required? If so, what?

10A) Should the Legislation include rules around the extent of choice available to Users to verify their identity?

Kantara Response: Kantara supports the concept of User choice in terms of verifying identity. That being said, while Kantara recognizes that Government is the primary authoritative attribute provider, the solution should not preclude external bodies from becoming authoritative providers of attributes they have verified with Government.

10B) Should any types, or all types of relying parties be obliged to provide an alternative identity verification mechanism, and what exceptions should be available?

Kantara Response: If by "alternative identity verification methods" Australia means verification methods for those who do not wish to conduct electronic transactions then Kantara recommends yes, there should be alternative methods that are probably in use today. However, if Australia means alternative methods to be used to conduct electronic transactions then Kantara recommends no. Kantara recommends, if it is possible, that

alternative electronic identity verification methods be allowed (i.e., use of different verification services).

The demand for relying parties to be participants (rather than everyone using services covered by law) has not been explained, and it would severely limit adoption and not provide small business and charities with the facility to make the online checks they need to, typically for compliance with obligations rather than any inherent business need.

11A) What types of profiling of behavioural information should be prohibited and allowed?

Kantara Response: Kantara expects this to be covered in other Australian legislation. Kantara suggests that the conduct of privacy impact assessments should be part of legislation rather than it being prescribed *ab initio*. Kantara also recommends that a definition of "profiling" be included in future drafts of the plan.

11B) Should a public register of Attributes be maintained?

Kantara Response: Kantara supports maintaining a list of attributes that prescribes formatting and allowed values. However, Kantara has security concerns about maintaining a list of attributes values.

11C) Should there be additional restrictions on access to Restricted Attributes?

Kantara Response: Kantara is not clear as to the definition of Restricted Attributes.

12A) Are there any other safeguards on Biometric information that should be included in the Legislation?

12B) Are there any that have been proposed above that should be modified or excluded, and if so, why?

13A) Do you agree with the proposed approach for Biometric Information?

Kantara Response: Kantara makes no comment on how the balance with the need for prevention and detection of fraud is addressed, but notes that the lack of 'one to many' matching use cases relating to multiple asylum seekers and organised crime have led to an unacceptably high and visible failure rate in other countries.

13B) Will the limitations on Biometric Information overly constrain innovation or rule out legitimate future use cases?

14A) Should the Legislation specifically provide a mechanism requiring an individual's consent before the User transacts with a relying party?

> **Kantara Response:** Kantara recommends yes, whenever consent is the legal basis for processing. Kantara would also recommend that Australia include the concept of Consent Receipts in the legislation. As mentioned previously, Kantara would be pleased to discuss its Consent Receipt Specification referenced in ISO standards, further with the government.

14B) Should the Legislation specifically provide an opt-out mechanism enabling individuals to opt out of the system after they have created a Digital Identity?

> **Kantara Response:** In Kantara's opinion, an opt-out mechanism should be provided. Kantara, as part of discussions concerning consent receipts, would also be pleased to discuss the revocation, or opting out, of consent. Kantara also suggests that Australia might want to consider implementing the concept of the "right to be forgotten" in its legislation.

15) Should there be a minimum age set for a person to be permitted to create their own Digital Identity? If so, what should it be?

16) How should the Legislation cover situations where a person lacks capacity, is not capable, is too young or lacks interest or motivation to engage personally with the system?

17) Should the requirement for a PIA remain in TDIF accreditation requirements or should it be required in the Legislation or Operating Rules?

> **Kantara Response:** Kantara notes that wherever specified, PIAs must be kept as live documents, adaptive to changing threats, so the mechanisms for changing them must be considered and may impact the answer.

18) In addition to the right to privacy and anti-discrimination in relation to accessibility and disability, how should the Legislation safeguard and ensure the enjoyment of Australians' human rights?

19) Is the proposed approach to accessibility and usability practical and appropriate? Should any other considerations be taken into account?

20) What additional mechanisms, including penalties and redress mechanisms, should be included in the Legislation to prevent disclosure or misuse of personal or other information?

> **Kantara Response:** Australia has existing legislation addressing disclosure or mis-use of personal information, so any additional legislation should only address gaps (if any) in coverage of the particular ways identity information is collected, used and protected to achieve the goals of data minimization, transparency, User control and effective redress.

21) Should the Legislation include provisions to enable the disclosure of information in specified circumstances? If so, what should those circumstances be?

22A) Are there established independent bodies that could fulfil the role of an independent Oversight Authority for Digital Identity, or is a new independent body required?

> **Kantara Response:** Kantara recommends that the Government establish an Oversight Authority for Digital Identity within the Government. This body would have accountability for the proper operation of Digital Identity in Australia. It should be noted that the establishment of this body does not preclude it from outsourcing functions to the private sector.

22B) What is the optimal structure of a new body?

23) What type (or types) of information should be required to be publicly reported by the Oversight Authority, to increase transparency in the system?

> **Kantara Response:** Kantara recommends that participants should be required to report adverse events (e.g., breaches) to the Oversight Authority and that the Oversight Authority, in addition to reporting these events to the public, should be responsible for investigating and reacting to these events (e.g., shutting down a service that has been breached).

24A) What is the appropriate period for review of the governance structure of the Oversight Authority?

24B) Should the Oversight Authority be subject to accountability requirements beyond those in the PGPA Act?

25A) Are the roles and functions outlined above appropriate for the Oversight Authority?

25B) Are there any other functions that should be undertaken by an Oversight Authority? If so, what?

26A) What other committees or advisory structures do you think may be needed?

26B) Which other organisations or bodies could supply members of the Privacy Advisory Committee?

> **Kantara Response:** Kantara cannot offer specific advice on which Australian bodies are appropriate, but notes that since privacy requires striking a balance and being seen to do so, it is essential to have representation from fraud investigation, law enforcement, and prosecution experts (both criminal and civil) as well as public interest groups.

27) Should the record keeping requirements be outlined in the Legislation? If so, what should they be?

> **Kantara Response:** Kantara has no specific advice on record keeping requirements other than establishing a record retention duration that is consistent with other Australian legislation (e.g., legal evidence requirements) and referencing existing international record keeping standards.

28) What best practice models should be considered for the protection and use of the trust mark?

> **Kantara Response:** Kantara assumes that it would follow normal 'Standards Australia' processes for development and indication of compliance and would avoid inventing anything new. It is the national body representing ISO after all.
>
> In accordance with ISO/IEC 17065 'a certification body shall exercise the control as specified by the certification scheme over ownership, use and display of licenses, certificates, marks of conformity, and any other mechanisms for indicating a product and/or service is certified. Incorrect references to the certification scheme, or misleading use of licenses, certificates, marks, or any other mechanism for indicating a product and/or service is certified, found in documentation or other publicity, shall be dealt with by suitable action. Such actions can include corrective actions, withdrawal of certificate, publication of the transgression and, if necessary, legal action'.
>
> In terms of best practices and alignment with ISO standards, Kantara uses the following specifications that govern the use of the Kantara Approved Services Trust Mark/Approval Mark:

A. The Approval Mark must only be used to identify Approved Services Service Provider per the Kantara Approval and License Agreement. Further, the underlying KANTARA INITIATIVE Approval Mark must not be used standing alone but must always be used in the appropriate Approval Mark as set forth in paragraph E below.
B. The Approval Mark must not be used in a manner that would imply that the Service Provider is sponsored or endorsed by, or affiliated with, the members of Kantara Initiative.
C. The Approval Mark must not be used in a manner that would imply that goods or services provided by the Service Provider (other than the Approved Services) are sponsored or endorsed by, or affiliated with, KANTARA itself or its members.
D. The Approval Mark must be utilized in the provision of the Approved Services (including on software screenshots), on packaging for the related products and in marketing activities, including marketing presentations, corporate marketing collateral, and corporate websites in which the Approved Services are identified as part of the "Kantara Initiative Approval System".
E. Electronic art of the Approval Mark must be used as provided; changes in color, design, or proportions are not allowed. Electronic art is provided for reproduction purposes only. The Approval Mark can be reproduced in black and white; reverse; and/or full color. Finally, representations of the Approval Mark are shown and should not be reproduced.

When reproduced in full color, the following colors should be used:
<....>

Full color usage of the Approval Mark should appear as follows:
<....>

Do not condense, expand or distort the logotype in any way (see examples below). Do not position the Approval Mark within a contained space or position or place a border around the Approval Mark. Do not place the Approval Mark in a patterned background or add graphic elements to the Approval Mark. Below are examples of improper use of the Approval Mark: stretched, overlapping another graphic, directly abutting another graphic (should have at least .25 inch or 20px margin), and color change. It is very important to observe the correct scaling procedure when enlarging or reducing digital files of the logotype.
<.....>

29) Is the proposed approach appropriately balanced to achieve the objectives of the system?

30) Should the Legislation specify whether and how audit logs from the system can be used in court as evidence? If so, what should the Legislation say?

31) Is the proposed approach appropriate to achieve a high degree of consistency of privacy protections?

32) Should the Legislation specifically provide that additional administrative decisions relating to the system be subject to merits review?

401 Edgewater Place, Suite 600 Wakefield, MA 01880, USA
Phone +1 781-623-3094
Email: secretariat@kantarainitiative.org