March 16th, 2021

To whom it may concern

This response is submitted by Kantara Initiative.

Kantara is pleased to provide comments on the Government of Australia's Position Papers.

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 specifications, such as UMA 2.0, Consent Receipt, applied R&D, and its Identity Assurance Framework (IAF). More information is available at https://kantarainitiative.org/trustoperations/ or contact us at secretariat@kantarainitiative.org

As with our other submissions, our interest in offering this submission is to the Government of Australia is two fold. First to offer its expert advice to the Government while it is developing its Legislation and second to remind the Government, during the development of its Digital Identity Legislation, of 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 continues to be interested in working alongside the Government of Australia at key points in the development of their Legislation to provide a supporting assurance process. As the Government of Australia is aware, 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 continue to invite the Australian Government team to keep Kantara apprised of its progress. We further suggest further call-ins during which we could 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 Inc.

Comments on the Governance of the System Including Oversight Authority Position Paper

1. Kantara supports the establishment of an independent Oversight Authority. Kantara would suggest that the Oversight Authority be divided into two separate functions: Policy Authority and Operations Authority. The advantage to the Government is the traditional advantages that are gained from the separation of management and operations functions.
2. Kantara also supports the establishment of one or more trust-marks to indicate that participants have been accredited. Kantara also supports the use of different trust-marks for different types of entities but would recommend, as it has done with its own trust-marks, that the different trust-marks all be based on a common base trust-mark. The use of a common base trust-mark will encourage "brand recognition" with Australians.
3. While it does not have to be specified in the legislation, Kantara suggests that the Oversight Authority outsource the accreditation function.
4. In Kantara's opinion it would be advantageous to accredit RPs to a set of requirements as to how they interact with Users and other accredited participants. Once accredited, RPs could be granted a trust-mark to indicate to Users, and the other accredited participants, that the RPs meet the requirements to participate in the system.

Comments on the Liability framework Position Paper

1. The statement, "the onus of proof will be on the individual" seems to presume an equality of arms, which Kantara does not believe to be true. Kantara would suggest the following:
    - That references to users ignores the greater problems for those who are not users (i.e., not the ones conducting a transaction with a stolen credential) but whose identities have been usurped.
    - The (initial) relying party is paying for something, which could reasonably be transfer of (possibly limited) liability. It is not clear if there are any subsequent relying party costs, e.g. for courts.
    - Redress also needs to be available to non-users, for whom there is clearly no contract.
    - Assessors presumably have some liability, but are they part of the 'system'? If this differs from any other system then it needs to be identified. Kantara suggests that Assessors only be liable for fraudulent approval of a service or if they can be shown to be incompetent. Kantara also suggests that Assessors be required to carry appropriate insurance.
    - Kantara would suggest that liability for issuing a "bad identity" be considered. That is, the system issuing a fraudulent identity even though all TDIF requirements have been satisfied.
    - It would be helpful to all parties of the framework, and perhaps to participation, to have a breakdown of all main scenarios wherein a loss may be suffered, and where potential liability may fall in those situations.
    - Kantara notes that in the credit-card model, losses incurred from on-line transactions are divided on the basis of contracts between card issuers (i.e., credential providers) and Relying Parties (merchants), with liability of users (consumers holding credit cards) limited by statute (in the US) to $50.
    - Generic consumer protection legislation may over-ride DTA liability disclaimers, which can be counterproductive when encouraging use.
2. Kantara suggests that, from the perspective of non-government digital identity service providers or intermediaries (including identity credential providers, identity proofers, and identity attribute providers) as well as relying parties, liability falling on TDIF accredited registrants must be clearly defined so as to enable insurability. In addition, Kantara suggests that consideration should be given to providing liability limitations to non-government digital identity system providers to enable sustainable business models.

Because the public sector, including the Oversight Authority, enjoys sovereign immunity protections, the private sector providers will bear the burden of relying-party efforts to recover losses.

3. As an example of a statutory scheme that addresses liability for federated digital identity systems and identity trust frameworks, Kantara would recommend the Virginia Digital Identity Law (2015 and re-enacted in 2020), available at: https://lis.virginia.gov/cgi-bin/legp604.exe?151+ful+CHAP0483&151+ful+CHAP0483 and http://law.lis.virginia.gov/vacode/title59.1/chapter50/section59.1-550/. An explanatory article is available at: https://static1.squarespace.com/static/5feb9d8f175ffd115ab172d1/t/602807baebe5f9446eb96286/1613236154509/Virginia+Digital+Identity+Law.pdf.
4. If approvals or accreditations granted by other jurisdictions will be accepted, the legislation will need to address how liability will be handled.

Comments on the Administration of Charges for Digital Identity Position Paper

1. Kantara finds the phrase, "to prove their identity through this legislation" is ambiguous and would suggest that it be expanded and clarified.
2. Kantara suggests that the First Charging Principal – no amortization of development costs – should only apply to the federal government, otherwise it discourages commercial suppliers from joining later. Assessment costs might need to be handled separately rather than viewed as 'development' as they are not just 'up front'.
3. Kantara notices that the discussion draft talks of a single system, but different aspects, and thus costs, fall to different players especially in repair, fraud prevention, detection, prosecution, etc. Kantara suggests that the government consider reviewing this concept.
4. Kantara notices that Charging Principal 3 says that the government would only charge RPs. That is, users/people will not be charged. Kantara believes that checks that are mandated by legislation or regulation should be free. Service providers abroad can reasonably be expected to make free age-verification checks, and Australian providers should not be disadvantaged.
5. Access charges under APP 12 suggest that organisations could charge but agencies could not. But an organisation cannot impose upon an individual a charge for the making of the request to access personal information, although there would seem to be an identifiable cost for checking the identity.
6. Kantara notes that, unlike the EU, Australia has an opt-out for vexatious requests, limiting the scope of the cost for handling malicious subject access requests, so that should not be a problem.
7. In line with Charging Principal 4, Kantara suggests that the initial content of subordinate legislation giving Charity or other exclusions should be identified up front.
8. The discussion draft sounds as if the government, and not the market, is setting a pricing structure. Kantara suggests that, while the government could recommend a charge, the market should be allowed to competitively set the price.
9. It is unclear if the charge model is per check or per successful check or per month or per calendar year or per subscription year. In Kantara's opinion this could lead to anomalies for any annual submissions. Kantara notes the successful charging model used in Canada where the federation policy authority is charged a fee by the provider participants when a credential is issued and the same fee again on the annual anniversary of the credential being issued. There was no charge to individuals. The federation policy authority charged participating RPs based on an appropriate basis to cover the cost of operating the federation.
10. The justification on charging to the public reads oddly when users are not directly charged.
11. If an IP3 service costs more than an IP2 service, who determines which one is used in a case when Level2 is all that is required but a user only has signed up with a provider offering Level3? (This is a fundamental question that the gov.uk Verify model failed to address.) Kantara recognizes that this is a challenge. Kantara suggests that the charge be based on what is needed not what is being supplied.

12. Note "the charges should correspond with the usage volume of the Relying Party". Is bulk charging by number of users, or number of transactions? For example, once a RP knows someone is over 18 then they can use that for every purchase if they keep an account, but some models expect payment every visit to the shop (if not every bottle). This will make a significant difference to the volume of transactions and the pricing.
13. Kantara suggests, based on its experience, that Assessor charges be established by negotiation between the Assessor and the participant being assessed rather than dictated by the government.

Comments on the Privacy and Other Safeguards Position Paper

1. Kantara suggests that, to reduce the bureaucratic burden on businesses, the Government consider, rather than providing exemptions to requiring an alternative channel to the digital channel, the legislation specify which monopolistic / essential businesses are required to provide an alternative channel.
2. Kantara questions whether, from an optics perspective, Government agencies should be exempt from the biometric requirements. While there may be existing legislative regimes and protections in place to safeguard agency use of biometrics, the perception to users that government agencies are exempt could be detrimental.
3. When deciding whether an attribute should be restricted, Kantara suggests that the legislation should require the Oversight Authority to consider and document the rationale for making an attribute restricted. Kantara would further suggest that the list of restricted attributes, and the rationale for them being restricted, be published in a publicly viewable register.
4. Kantara supports the prohibition on creating a single identifier for individuals but wonders if a User could choose to reuse an existing one. That is, an identifier that is already in their possession.
5. Kantara understands the requirement for accredited participants to seek express consent when users are using the system. However, Kantara suggests that care be taken on how this is implemented. (i.e., care be taken not to establish something akin to the EU Cookie Monster). Kantara would suggest utilizing an approach along the lines of its Consent Receipt Specification. The government should be aware that this specification is undergoing a revision to become the Advanced Notice and Consent Receipt Specification.
6. Kantara recommends that, as it has observed in other jurisdictions, care be taken with accommodating what might be considered by some to be "cultural idiosyncrasies". For example, Kantara is aware that Australian aboriginals have an aversion to using the name of someone who is dead.

Comments on the Scope of the Legislation and Interoperability with Other Systems Position Paper

1. The process for handling exceptions would seem much more onerous than imagined since it would need every RP to review every change to suppliers. It could involve legal challenges relating to barriers to trade and add delays if there is an appeal process from those who have been excluded despite passing the required independent assessment of suitability. Kantara has the following comments on the proposed exceptions:
    - Kantara suggests that the exception, "it is not possible for a relying party to source identity provider services at a particular level of assurance from more than one identity provider," is a logical consequence of the level demanded rather than an exception.
    - How could any "legitimate security concerns warranting a monopoly arrangement" only apply to just one RP?
    - Kantara believes that and exception based on "if the relying party's services are vital to uptake of the system, and a monopoly could be justified on the basis that it promotes greater uptake of the Digital Identity system" would likely be challenged in court by those excluded as providers, both on grounds of fairness and not serving their 'customers'.

- If a system – even if it is being modified to implement new business practices or technological systems – is compliant with the defined interface standards, what does it matter what technology is used.
- It is Kantara's believe that granting an exemption to a service that is a monopolistic arrangement used as a transition mechanism to facilitate a jurisdiction or sector (such as the banking or electricity sector and/or a state or territory jurisdiction) participate in the Digital Identity system gives "first entrant advantage" to one provider and is potentially unethical, and could be open for corruption.

2. Kantara would suggest that the impacts on the use of multiple levels have not been fully considered. (Kantara ignore anything at LoA1 (self-asserted) since, by definition, where self-asserted suffices, involvement of and payment to any third party is unnecessary.) Kantara notes that there are three models with different features, which were and are challenging for eIDAS:
   - Just highest needed,
   - Just Lowest needed (even if branded 'substantial'), and
   - two or more-or-less defined points.

   One can see these in Estonia, NZ, and UK (talk but not in action) respectively.

   The UK two-level approach, articulated in GPG43 (sic), aimed to mirror the distinction between the civil balance-of-probabilities and the criminal beyond-reasonable-doubt thresholds, noting that most interaction with the public sector is covered by criminal law, not contract. With only 40% of those who attempted able to be identified at the lower level (unchanged over 8 years), the higher level is out of sight. The distinction is over-simplistic as it is rare for any case to have just a single piece of evidence, and also crimes can occur where there is a contract. GPG43 is also clear about separating out the requirements for identification of those new or moving online from re-authentication of an existing 'customer'. These may have been conflated.
3. Kantara wonders who would bring prosecution? Kantara suggests that it is not realistic to expect the regulator to be 'judge and jury'? This model, common in Napoleonic law, has recently been used for privacy commissioners in Common Law countries, but is not without issues and would need justification. Kantara would also suggest that the legislation should also be clear on the use of fake ID when the information presented is correct. For example. when a fake driving licence (cheaper than a real one) is used to give the correct birthday (but not for driving).
4. Kantara notes that there is precedent in the US under 'safe harbor' and 'privacy shield' for voluntary application of laws, (where there is a cost for the stick you could be beaten with, but only available if providing services into Europe). The policy on who can opt in needs to be clearer as there is a real chance that large US and Chinese providers would want to opt in, and maybe a few registered in the Cocos (Keeling) Islands or other external territories.
5. Kantara would suggest that the exclusion of occasional relying parties would seem to be a missed opportunity.
6. With respect to Multiple Identities, Kantara notes that the description appears to allow one person to use a number of different identities with a provider (e.g. with names before and after marriage, legitimately associated with different current addresses), and also to use as many providers as wanted, with many concurrent accounts being possible. This leads to perverse incentives as the user is not paying, is onerous for relying parties, and raises difficulties for fraud detection and error correction.
7. In Kantara's opinion, the connections described between exchanges, and whether these brokers are working for the IdPs or the RPs is not clear. As such, Kantara suggests that, in order not to confuse users, the description be enhanced so that exchanges offer users choice.
8. The discussion paper appears to encompass a federated approach with the private sector. However, in Kantara's opinion, this is not clear. Kantara recommends that it is important to clarify the overarching intent.
9. While Kantara recognizes the need for inclusion of disadvantaged communities, Kantara recommends care be taken with respect to granting exemptions to services that are slightly deficient in meeting the specified requirements just so a service can support a specific community. The granting of a trust-mark to such a

service would indicate to all Australians that this service meets all TDIF requirements which the service, if it is deficient in order to support a disadvantaged community, it does not.

10. Kantara suggests that the legislation address how non-Australians can participate in the system. That is, if and how non-Australian Users can access and use the system, how non-Australian RPs can be involved, or how non-Australian supplier participants (e.g., attribute verifiers) can participate.
11. Kantara suggests that the legislation address transportability of accreditation. That is, if approvals or accreditations granted by other jurisdictions will be accepted.