COMMUNICATIONS ALLIANCE LTD

Communications Alliance submission

In response to the

Digital Transformation Agency

Digital Identity Legislation Position Paper

14 July 2021

Contents

1. Introduction

Communications Alliance welcomes the opportunity to provide this submission in response to the Digital Transformation Agency's (DTA) Digital Identity Legislation Position Paper.

Our members welcome any efforts aimed at contributing to voluntary enhanced security mechanisms in relation to identity establishment, verification and management. In fact, our members in the telecommunications sector already undertake substantial digital and non-digital identity verification/management for consumers of communications services, either against the background of legislative and regulatory requirements and/or as part of their own processes, designed to minimise fraud and to ensure that existing verified identities are managed securely.

As enablers of large parts of Australia's digital life, our members naturally take a keen interest in any systems that allow their organisations and their customers to further enhance their digital experiences, while simultaneously safeguarding privacy and maintaining security.

Against this background, we offer the following comments.

2. Additional checks for Relying Parties

The Position Paper envisages an accreditation process for Identity Providers (IDPs), Attribute Service Providers (ASPs), Credential Service Providers (CSPs) and for Identity Exchanges (IDXs). Communications Alliance supports rigorous accreditation standards for privacy and security to ensure the proposed framework can function appropriately and, importantly, gain and maintain user trust.

However, it appears that the same standards of rigour do not apply to admitting Relying Parties to the system. While this may be useful to attract Relying Parties to join the scheme and, therefore, increase reach/breadth, we believe that the current thresholds for onboarding Relying Parties may be too low and create the risk for malicious actors to become Relying Parties in order to avail themselves of User attributes that are envisaged to be available to Relying Parties under the scheme.

As currently proposed, Relying Parties are required to meet: 1) the onboarding data and technical rules; 2) a check in relation to national security (as defined in the Criminal Code); and 3) an assessment of whether they are fit and proper persons.[1]

We note that express user consent is required prior to enabling authentication to a service[2]. However, it is conceivable that malicious actors would also be able to elicit such consent from unsuspecting and/or vulnerable Users and, subsequently, be able to pursue their malicious activity relatively freely.

Consequently, we submit that Relying Parties ought to be subject to an additional layer of scrutiny. This could be achieved, e.g. by:

- A check of the company's history/longevity;
- Sighting of some minimum policies (e.g. data handling/privacy, security); and
- Evidence of compliance with relevant security and privacy standards as they apply to IT systems, data storage etc.

[1] Section 5.4.4, p.20-21, bullet points 1, 2 and 4, *Digital Identity Legislation Position Paper,* DTA, June 2021

[2] Section 3.5, p.9, fourth bullet point, , *Digital Identity Legislation Position Paper,* DTA, June 2021

3. Risks arising from unlimited scale

The Position Paper envisages that the number of Accredited Participants in the scheme is unlimited, presumably to maximise prospective consumer choice (and potentially to avoid dealing with the problem of setting an arbitrary limit to participation).

However, we are concerned that this may create an operationally overly complex or even unworkable scheme, which may also lead to barriers to join the scheme for Relying Parties and, therefore, have the counter-productive effect of reducing consumer choice.

The reason for our concern lies in the complexities that arise from the number of logical connections that Relying Parties are required to maintain with Accredited Parties: while the diagrams in Figures, 5 to 8 in the Position Paper indicate that it is expected that a Relying Party would only connect to IDXs, or even only one IDX, i.e. only maintain one or a very limited number of physical connections, the number of logical connections, or relationships, to Accredited Parties remains unlimited.

While technical standards will play a major role in the exchange of information (credentials, attributes, etc.) between the Participants, it can be expected that slight variations in the formats of exchange will occur. This, in turn, means that the onboarding of each new Accredited Participant will require testing with each Relying Party. The same would hold for a change or addition of new attributes etc. Given the sensitivity of the information transmitted, it also appears that such testing can also not occur in an offline environment with some preselected dummy or default entities, but instead must be done in an online 'real world' environment.

Importantly, with respect to the flow of Restricted Attributes, testing would also need to ensure that only those parties entitled to receive those Attributes actually receive them (e.g. only a hospital as a Relying Party should receive health attributes but not a telecommunications provider as a Relying Party)

We agree that it is desirable to allow for an approach that facilitates substantial consumer choice, and, in principle, we support the Interoperability Principle as an approach that does this. However, we also believe that the proposed approach bears the real risk of becoming unwieldly and overly complex or even unworkable. Consequently, we urge the DTA to give further thought to measures that would reduce the risk of 'scope explosion', be it through limitation in the scope of information permissible to be exchanged, of the technical variations permissible for exchanging those, limiting the number of Accredited Parties or otherwise.

4. Identity fraud and security

We have previously pointed out that if successful, the implementation of the Trusted Digital Identity Framework (TDIF) will increase the use of digital identities (IDs) by Australians substantially. Eventually, the use of a digital ID will become the norm. For the TDIF to build trust, it is key that fraudulent identities are not created and that each verified identity is indeed representing the person that they purport to be.

Consequently, we are pleased that the Position Paper now indicates that the TDIF rules will contain "requirements that align with security advice, guidance, policies and publications developed by the Australian Government"[3] to ensure that all TDIF applicants adhere to minimum security standards, in order to protect identities and prevent fraud and other security breaches.

It also appears useful to allow the Oversight Authority to coordinate the sharing of information between Participants to support each other during and in the aftermath of cyber security/fraud events.

[3] Section 3.5.1, p. 10, *Digital Identity Legislation Position Paper,* DTA, June 2021

To further strengthen to framework, we believe it will be necessary to give consideration to an appropriately resourced and well-functioning process/agencies, headed by the Commonwealth, to investigate security breaches and fraud reported to it by Participants, including Relying Parties. While such processes/agencies currently exist in theory, in practice they often prove difficult to use and appear under-resourced to effectively investigate fraud-related matters currently referred to them.

5. Public consultation on technical standards

The Position Paper proposes the "*Minister be given power to issue technical standards relating to how technology in the system works.*" and that specifications will be Notifiable Instruments.[4] The Position Paper notes that a Technical Standards Board will develop and write the standards and that "*Participants will have the opportunity to provide feedback … through their membership of advisory boards*".[5] We are concerned that such instruments will only be notifiable, thereby not mandating the opportunity for public consultation. We consider it would be appropriate, in all cases, for public consultation on a final draft of any Technical Standards or rules ahead of the Minister making the instrument. This would also afford the opportunity for potentially affected parties who are not members of the appropriate advisory board(s) to comment.

6. Accredited Participants wishing to simultaneously operate outside the TDIF

There is a lack of clarity (or possibly ambiguity) in the Position Paper for the specific scenario where an IDP and an IDX are both Accredited Participants, and they wish to simultaneously operate outside the system for some transactions. The Position Paper states that the Digital Identity Legislation will "…*not prevent Participants performing roles in the system from participating in other digital identity systems or being accredited under other digital identity frameworks* ***simultaneously*** *whilst participating in the Digital Identity system*."[6] (emphasis added). This position seems to be reiterated further along in the Position Paper where it says "*Participants who choose to connect to multiple digital identity systems will need to put in place technical and business solutions to demonstrate how they will meet their obligations under the Legislation. This includes being able to clearly delineate which digital identity activities are conducted through the Digital Identity system and* ***through another digital identity system***." [7] (emphasis added).

However, the very next paragraph in the Position Paper then says: "*We have provided some example transactions below where participants may participate in multiple digital identity frameworks*" and importantly, every one of the examples that follow (Figures 5 to 8) show that where both the IDP and the IDX are Accredited, then the transaction falls under the legislation. Where the confusion arises in these figures is that while the figures do show an IDP or IDX conducting transactions outside the system, it is only in the context of the other party not being accredited within the system.

Assuming that we are correct in understanding that it is permissible for an Accredited IDP and IDX 'pair' to conduct transactions that are outside the system while simultaneously conducting other transactions that are within the system, then we propose this is clearly spelt out in the legislation, including the "delineation" that is required to demonstrate which transactions are inside, and which transactions are outside the system.

[4] Section 4, p13, *Digital Identity Legislation Position Paper,* DTA, June 2021
[5] Section 6.4.2, p.34, *Digital Identity Legislation Position Paper,* DTA, June 2021
[6] Section 5.4.1, p.16, *Digital Identity Legislation Position Paper,* DTA, June 2021
[7] Section 5.4.13, p.26, , *Digital Identity Legislation Position Paper,* DTA, June 2021

7. Liability, limitations and exclusions

The liability arrangements are key to entities' participation (both Accredited and unaccredited) in the system, and it is vital that potential entrants understand all possible liability scenarios prior to making a decision to participate in it. Communications Alliance notes that the Position Paper makes it clear that "*There will be a liability framework in the Legislation and Accredited Participants will not be financially liable for losses suffered provided they have acted in good faith and complied with the legislative rules and requirements relating to accreditation and the system*."[8] We agree with and support this proposal. We also assume this extends to the scenario where a fraudulent ID is used (by a malicious actor), assuming of course that the Accredited Participant has acted in good faith and complied with the legislative rules and requirements of the system.

The Position Paper then goes on to propose that "… *the Legislation will enable the Minister, if needed, to make rules to provide limitations on the liability that would otherwise arise from non-compliance with the legislative rules and requirements*", however, "*there is no intention to have those rules when the Legislation commences*…".[9] This amounts to an uncapped liability on Accredited Participants for possible non-compliance with the rules. Bearing in mind that non-compliance is, in all likelihood, unintentional (Accredited Participants will not be deliberately setting out to avoid comply with the rules), an uncapped liability is concerning and potentially a disincentive to participation for Communications Alliance members. Section 9.4.2 of the Position Paper proposes to 'solve' liability through a statutory multiparty contract. While we support the use of a statutory multiparty contract as the mechanism for Accredited Participants to be contracted to supply services to the system, we consider it does not address the concern of uncapped liability. The absence of any principles or rules to limit the liability through this contractual mechanism is concerning, especially where participants include Government agencies who are similarly eligible to recover loss or damages in the event of an incident.

Communications Alliance also notes that the Oversight Authority and its staff are to be excluded from liability.[10] Due to the high risk that any identity system will be a target for malicious actors, Communications Alliance suggests the following broad principles should be adopted for the creation of the Digital Identity Legislation:

- The benefits of the framework will be shared by Users, Participants and by Government. Hence, the downside risks should also be shared, meaning all participants and Government should bear some liability.
- Accredited Participants should not bear unlimited liability for loss and damage flowing from their non-compliances – liability for such losses and damage should be capped from the outset as part of the statutory contract.
- Regarding section 9.4.3, we consider the Commonwealth should bear some liability for its participation in the framework. Its employees should not be immune from liability: they would be covered by the Legal Services Directions, which provide for the Commonwealth to give or fund legal assistance to an employee who has acted, or is alleged to have acted, negligently, i.e. failed to exercise the legal standard of 'reasonable care' owed in the circumstances, unless the employee's conduct involved serious or wilful misconduct or culpable negligence.

8. Risk of overlapping or conflicting privacy requirements

The Position Paper states that "… *the Bill will include privacy safeguards additional to those in the Privacy Act.*"[11] The Position Paper then goes on to say "*The Legislation is not intended to*

[8] Section 9.3, p. 59, *Digital Identity Legislation Position Paper,* DTA, June 2021
[9] Section 9.4.2, p.60, *Digital Identity Legislation Position Paper,* DTA, June 2021
[10] Section 9.4.3, p.61, *Digital Identity Legislation Position Paper,* DTA, June 2021
[11] Section 6.4.6, p.38, *Digital Identity Legislation Position Paper,* DTA, June 2021

duplicate or conflict with established principles in existing legislation, for example, the Privacy Act".[12] Communications Alliance members have concerns about the creation of privacy obligations across multiple legislative instruments as it creates a risk of overlapping and possibly conflicting obligations on scheme participants, both Accredited and unaccredited such as Relying Parties.

We appreciate and support the DTA's desire to leverage existing legislation where possible as it builds consistency and reduces red tape, as the DTA correctly observes in section 7.1. However, we hasten to add that creating separate legislative instruments requires a lot of care, and must be considered through the lens of each type of participant, and specifically through a wide range of Relying Parties. We recommend the DTA should engage with stakeholders to consider implications of the proposed 'additional' privacy obligations prior to releasing the exposure draft of the Digital Identity Bill, to ensure privacy obligations captured in the Bill are workshopped and analysed thoroughly.

We also note the *Privacy Act 1988* is still under review.[13] While the Position Paper seeks to assure stakeholders that "*The Legislation will also be developed in a way that recognises the potential changes being made to broader privacy protections as a result of the review of the Privacy Act currently underway…*"[14], we remain concerned that the revised *Privacy Act 1988* may contain changes that may not align well with the digital ID framework. We believe that it would be prudent to delay the final development of the privacy regime of the Digital Identity legislation until after the review of the *Privacy Act 1988* has concluded to avoid the need to amend the newly-minted Digital Identity Legislation shortly after it is made.

9. Conclusion

Communications Alliance appreciates the consultation the DTA has undertaken so far and looks forward to further engaging with the Agency and all relevant stakeholders in this important process, to create an effective and efficient expanded voluntary digital identity framework for Australia.

For any questions relating to this submission please contact Christiane Gillespie-Jones on 02 9959 9118 or at c.gillespiejones@commsalliance.com.au.

[12] Section 7.1, p.44, *Digital Identity Legislation Position Paper,* DTA, June 2021
[13] https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988
[14] Section 7.1, p.44, *Digital Identity Legislation Position Paper,* DTA, June 2021

Published by:
COMMUNICATIONS
ALLIANCE LTD

Level 12
75 Miller Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
E info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507