Deloitte.

Digital Identity Legislation Consultation Paper

Deloitte Response

Deloitte.

Deloitte Risk Advisory Pty Ltd
ACN 611 748 184
8 Brindabella Circuit
Brindabella Business Park
Canberra Airport
Canberra, ACT, 2609
Australia

Phone: +61 2 6263 7000
www.deloitte.com.au

Deloitte Submission

Please find attached the Deloitte submission for the Digital Identity Legislation consultation paper. We have responded with observations on some of the questions, in areas where our experience provides us with strong insight and where were have a firm point of view that we believe may present some value to the digital identity ecosystem.

Julie Gleeson
Director
Cyber
Deloitte Risk Advisory Pty Ltd

Trevor Hancock
Specialist Leader
Cyber
Deloitte Risk Advisory Pty Ltd

Copyright Deloitte 2020

The entity named herein is a legally separate and independent entity. In providing this document, the author only acts in the named capacity and does not act in any other capacity. Nothing in this document, nor any related attachments or communications or services, have any capacity to bind any other entity under the 'Deloitte' network of member firms (including those operating in Australia).

Liability limited by a scheme approved under Professional Standards Legislation.

Member of Deloitte Touche Tohmatsu Limited

Consultation Response

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

It is Deloitte's view that yes, based on the purpose of the proposed legislation, the legal authority, privacy protections, and the establishment of permanent governance arrangements are critical to the success of any newly defined legislation, and that this in partnership with the amendments to other legislation is the minimum required to ensure the success of any Australian citizen identity ecosystem.

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

Considerations on how identities are bound to individuals

In terms of identity binding, the current legislative and policy focus is almost exclusively on strength of proofing - including facial biometric authentication in the enrolment mix. x

There is currently no equivalent focus on identities in use. Arguably, this is the real arbiter of how strong an identity really is. While strong initial proofing remains critical, this is a point in time exercise and can never definitively prove that that same individual to whom the credential was issued (at the time of proofing) remains the same individual in possession of that credential.

Identity in use frameworks support the progressive strengthening of the identity ecosystem by considering how an identity is built up over time as it is used in different contexts.

Someone applying for a *working with vulnerable people registration* for example with an identity credential is much more likely to be the person claiming that right (and attribute) if there is a consistent history of that identity being used in similar contexts, over a period of time. An identity credential that has never been used in that type of context before carries more risk.

This suggests the legislation and the supporting policy framework should consider how identity providers might preserve the currency of identities. This might include consideration of how the use of Attributes contributes to the picture of identity in use and overall strength.

Considerations related to identity fraud control mechanisms

Noting the need to balance privacy requirements, the legislation should consider how information might be shared across the ecosystem so as to enable investigation of suspected digital identity fraud events, as well as the processes covered around the investigation and remediation of actual digital identity fraud events. This will be critical to ensuring ongoing trust in the digital identity ecosystem and will allow both ecosystem providers and relying parties to manage the risk of fraud earlier.

Deloitte understands that the intent of the "*Double Blind*" concept provides citizen privacy protections, around providing the ability for a citizen to obtain services from a relying party without sharing with that relying party which identity provider is providing the citizen's digital identity; and for the citizen to use their digital identity, without necessarily advising their identity provider with details on which relying parties the citizen is obtaining services from.

Our view is that the provision of a central fraud management party within the ecosystem (possibly the Oversight Authority or an Identity Exchange provider, if not a standalone entity) would allow the intent of the "*Double Blind*" concept to be maintained, while providing the ability for providers within the ecosystem to share analytical data from any engagement, and allow the ecosystem to manage the risk of fraudulent use of ecosystem before the fraudulent event.

This consideration includes the legislation and/or supporting legislative instruments and then policy providing for the ability to share fraud related information. These should also impose obligations upon participants to support fraud control activities.

For example:

- All stakeholders should have the legislative ability to share identity fraud related information (including relevant information associated with the use of those identities) with the central fraud management party, who can then share sanitised data with relevant stakeholders within the eco-system so that suspected and actual digital identity fraud might be flagged, investigated and remediated, while maintaining the privacy of the citizen.
- Noting the existing intent to impose obligations on Relying Parties to inform the central fraud management party of security or fraud events impacting the system, this should also be extended to include instances where instances of digital identity fraud are suspected.
- All providers within the eco-system should carry obligation to inform the broader ecosystem when digital identities are known or are suspected to be fraudulent. This is to ensure a fraudulent digital identity rejected in one context cannot then simply be re-presented in another context.
- The Oversight Authority (or similar) should have the authority to force an identity provider to invalidate an identity in cases of actual or strongly suspected digital identity fraud.

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

As defined in the structure of the legislative framework, Deloitte agrees that the primary legislation should focus on providing the authority for the ecosystem to support citizens digitally interacting with relying party services in a secure manner. In Deloitte's opinion, the criticality of the primary legislation is to not only cover the provision of a digital identity, and the manner in which that digital identity is tied to an actual physical being, but should ensure that it provides similar authority on the security of the digital identity through the lifetime of the physical being.

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

Given the fact that the Operating Rules and other legislative instruments are the tools to legally bind the operation of the ecosystem to the rules within the primary legislation, Deloitte suggests that it is critical to ensure that these rules cover the creation, use and lifecycle of the digital identity.

Additionally, Deloitte notes that in a typical digital identity use case, there are risks associated with the creation of the digital identity (identity validation), the use of the digital identity (authentication) and the actual digital transaction or interaction with the relying party undertaken by the digital identity (authorisation). The Operating Rules need to have the breadth of coverage to provide risk management to mitigate the risk of fraudulent events before the risk is realised, as well as coverage to recover, remediate and learn from a fraudulent event.

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

Deloitte sees the TDIF ecosystem as a distributed model, with multiple parties potentially involved in any digital service obtained (i.e. the citizen with the digital identity, the identity provider, the identity exchange, the relying party, the fraud management party and the oversight authority). Based on this model, Deloitte suggests the policy component of the legislative framework needs to be quite descriptive, so that any participant wishing to join the ecosystem is well aware of their obligations with ensuring the validity of both the citizen's digital identity and the digital services being provided.

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

The Digital Identity Participant Register sounds like a good method of communicating the entities of the accredited participants and relying parties within the TDIF ecosystem. Deloitte would recommend that an

internal register be maintained within the ecosystem (possibly with restricted access to the central fraud management party or the Oversight Authority) that shares where the ecosystem participants are providing similar services to other parties.

This will become particularly crucial if the TDIF ecosystem grows to include more commercial organisations. For example, if a commercial organisation joins the TDIF ecosystem as an Identity Provider, they will likely offer their identity services to other organisations who may be outside the TDIF ecosystem to ensure the commercial viability of their services.

Deloitte views this information as being critical, because if a fraudulent event occurs in these other organisations, the digital identity itself could be compromised, which could also compromise the TDIF ecosystem.

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

As per Question 1B, relying parties should hold obligations to inform a central fraud management party or the Oversight Authority in the event of *suspected* identity fraud events.

This is important in terms of providing the Oversight Authority the ability to detect patterns of anomalous behaviour, which is always an essential part of effective fraud detection and management.

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

The success or failure of a digital ecosystem is based on usage. While Deloitte acknowledges the risks associated with services only being provided digitally, if the processes supporting the creation of a digital identity limits a citizen's ability to obtain such an identity, there is also risk in limited take up by relying parties providing their services through the TDIF ecosystem if they are mandated to manage multiple channels of validating a citizen's identity.

Deloitte would like to see the legislation provide coverage to mitigate the limitations for citizens to obtain a digital identity. For example, supporting carers, power of attorneys or using identity validation through elders in indigenous communities could provide other methods to support a citizen obtaining digital services from a relying party, in cases where the standard processes for obtaining a digital identity may be limiting for that citizen.

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

Profiling of behavioural information is an interesting case study: there are privacy ramifications that need to be protected, while limiting the behavioural information can pose security and fraud risk to the ecosystem. Deloitte suggests that while individual providers within the ecosystem and the relying parties should gather behavioural analytics, they should be restricted from individually creating profiles to benefit themselves, so as to maintain the citizen's privacy.

In parallel, these providers should be mandated to share these behavioural analytics with the central fraud management party or the Oversight Authority, so that the ecosystem can maintain the ability to manage the risk of fraud.

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

Yes. In addition, Deloitte suggests that there should be authenticated access to an individual's attribute list, which provides the citizen with the ability to see where they have consented to an attribute being shared with

a relying party, and additionally provide the citizen with the ability to manage the consent throughout the life of their digital identity within the ecosystem.

Question 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?

The success of a digital service capability is the ability of the system to be as widely accessed as possible, as such Deloitte recommends, similar to areas covered in Question 10A), that the system support the ability for an identity to have a "*managerial role*", to support carers, power of attorneys or other relationships to ensure that no citizen is denied access to the digital services supported by the ecosystem.

Question 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?

Yes. In the TDIF ecosystem, multiple parties will play a role in managing a digital service or transaction being undertaken by a citizen with a relying party. Should this service provision or transaction be deemed fraudulent, and the relying party requires legal proceedings to recoup financial losses, the ability for the lawyers involved in the court proceedings to tie the actual physical person of interest with the fraudulent event will rely on the ability for appropriate digital forensics to link:

1. the digital identity verification audit logs,
2. the digital identity use (authentication) audit logs,
3. the consent to obtain any specific attributes, and
4. the actual fraudulent event (authorisation with the relying party).

Deloitte recommends that the Legislation needs to provide coverage to ensure that the integrity of both the system configuration (i.e. accuracy of timing and details within audit logs), and the audit logs themselves, to ensure that there is both a linkage between the ecosystem providers and the relying party and an appropriate validation that the logs have not been altered.

While Deloitte recommends that the Legislation provides coverage, it is important to not be too specific on the technical controls, so as to ensure that the Legislation stays valid with technology or court requirements changes.