Digital Identity Legislation Background Paper

https://haveyoursay.digitalidentity.gov.au/digital-identity/news_feed/background-paper

3. What a Digital Identity is not

A Digital Identity is not a single, universal or mandatory number, or an online profile. User information remains private and protected. Users are asked for consent before any of their personal details are shared with the service they are trying to access.

I'm not sure if I agree with the "… or an online profile". The platform will have enough information and knowledge of the user to establish a profile of the person.

---

4. Benefits of the Digital Identity system

The Digital Identity system is designed to make accessing government and private sector services easier, faster and more convenient for Australian people and businesses.

It will safeguard privacy by sharing only relevant details (compared with handing over an identity document in person). It will strengthen the security of digital services and help prevent fraud and identity theft when Australians interact online.

The benefits of the Digital Identity system will allow the user the ablity to consent to allowing their information to the relying party. In sections 10…

Section 10 …. Consent

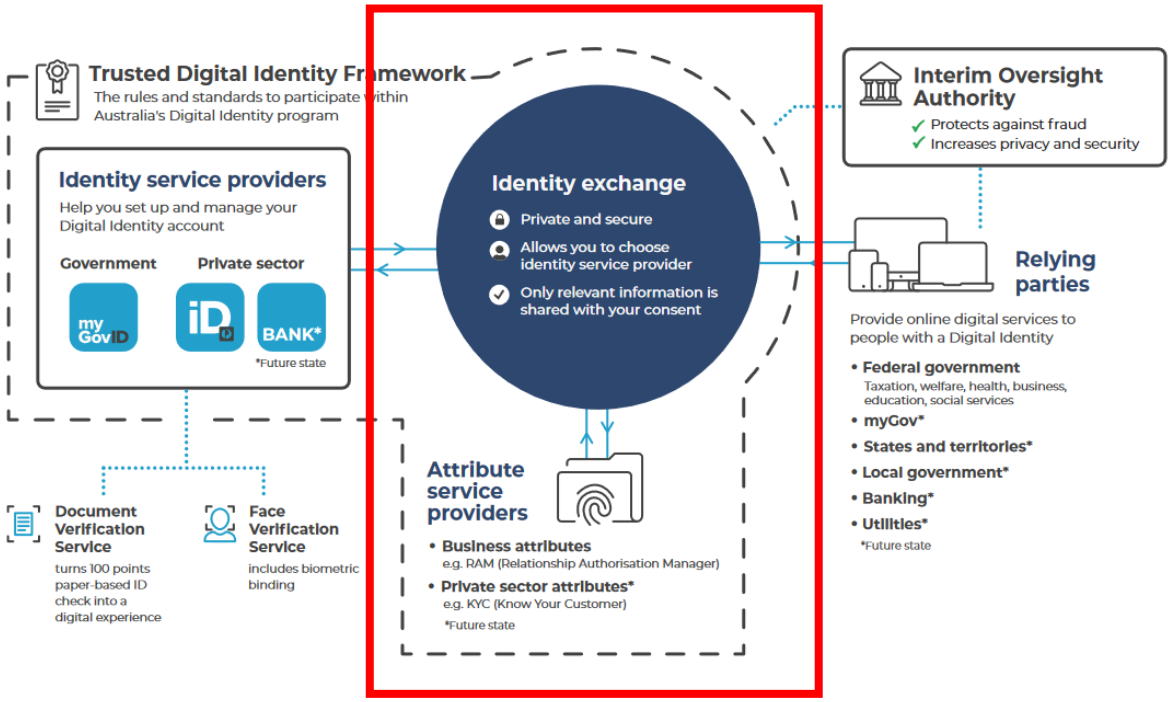
- **Consent** – consent is required at multiple occasions when a person uses the system. A person must consent to set up a Digital Identity with an identity provider. The person's consent must also be obtained by the identity exchange before their Attributes can be passed through to a relying party. Furthermore, Users can withdraw consent for their Digital Identity to be used at any time, and opt out of the system through a process which is easy to understand and access.

The system will provide the user with the capability to remove consent (as above). Further to this will it provide the user to ability/ capability to the Right to be forgotten and other rights related to the Consumer Digital Rights.

https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0

---

8. Digital Identity System



Where does the consent management sit? Is it in the Attribute service provider or the Identity exchange? In section "9. User journey across the system" is the sitting in the Attribute Verification Service.

---

10. Principles underpinning the Digital Identity system

The Digital Identity system is based on these core principles:

- **Choice** – creating and using a Digital Identity is voluntary. Users will have the option to select from multiple identity providers to verify their identity and access government and private sector services online.
- **Consent** – consent is required at multiple occasions when a person uses the system. A person must consent to set up a Digital Identity with an identity provider. The person's consent must also be obtained by the identity exchange before their Attributes can be passed through to a relying party. Furthermore, Users can withdraw consent for their Digital Identity to be used at any time, and opt out of the system through a process which is easy to understand and access.

Will the consent management require the user to re-consent when the relying party changes the terms of the consent. i.e. request of more information, more attribute than what was originally agreed to.

Digital Identity Legislation Consultation Paper

https://haveyoursay.digitalidentity.gov.au/digital-identity/news_feed/consultation-paper

Consultation questions:

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

No comment

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

No comment

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

No comment

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

- Requirement of the accredited replying party entities and approval must meet an Open Standard - TDIF or independent certification to exchange PII data. Re-certification must be completed annually or periodically.

- Would like to see that the "Authority" (regardless of interim or permanent arrangement) should be audited annually by external third-party assessor meeting a some public level of standard. i.e. NITS / CPS or GDPR level of posture

- Privacy protection and user control should have alignment to the Consumer Data Right - standards https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0

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

Working locally, thinking globally. Policy which are aligned to the Australia CDR or other ASEN Personal Data Protection Acts of our neighbouring countries.

CDR - https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0

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

A publicly available Participant list which makes up the core (involved in the creation, transmission, management, maintenance) and structure of the TDIF platform must be available, transparent for scrutinization and auditability.

Relaying parties need only to be disclosed to the participating user who have already consented to the use of their data.

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

The relaying party must be certified (TDIF or independently) to be accredited for trusting the PII data of the users. Similar to the requirements of PCIDSS, you can not handle this data unless you have or meeting a level of assurance.

Re-certification must be completed annually or periodically.

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?

The legislation will also need to set out the definition of what is PII and what is not PII data.

The legislation also needs to outline the relying party what will be their limitations, how to honour the limitation, their accountability, risk of breaking the trust and link to the penalties of the mandatory data disclosure laws.

- Purpose limitation
- Storage limitation
- Confidentiality
- Accountability
- Audit

User data rights and honouring the consent and the digital rights of the user if they choose to exercise their rights to the access of their data.

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?

YES. There cannot be any contradictions to over commonwealth acts on the understand what is classification of PII and other data.

I personally feel it is quite already distributed, however, each act is serving its purpose. The Digital Identity information could inherit the data classification of other acts, but however, its goal is to frame the how a digital identity is mastered and for what purpose, in this case to enable a digital economy and social services.

Breach of trust, privacy, availability or integrity must be met with penalty and loss of service by the TIDF.

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

This is an enablement platform which is also voluntary for the citizens to sign-up. The TIDF must be able to hit critical mass before is will become sustainable. The relaying parties need to see or understand the benefit. It should be run as a not-for-profit structure. The transactional model would work well on a pay per transaction basis.

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

The requirement of the express consent from an individual or their representative to use the system to authenticate and pass Attributes to a service. The right to be forgotten if the individual revokes their express consent and penalty if this is no honoured.

The requirement of the express consent from an individual if the purpose of the consent has change as per the relying party change of terms and conditions or intended purpose.

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

Choice should to be available for accessibility needs, deaf, blind or immobile.

The NIST standard states and provide description on the level of assurance which is required based of the proofing. If the verification of the identity for transaction which are managing sensitive or protective levels, yes. The choice must be available.

You must watch this. Australian computer hacker at a famous hacking conference on how to kill someone's identity on paper. https://www.youtube.com/watch?v=9FdHq3WfJgs

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?

I think it is best to define the assurance level and mandate the relying parties to verify base the transaction or level or risk, i.e. financial risk or personal health

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

The commercialisation or profiteering of the data should prohibited with strong penalties applied. The need to obtain the individual data is based of a need driven by compliance, i.e. KYC or other verification needs.

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

Yes. Data classification standards should be made available and clear just as in every private company.

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

Yes. The relying party needs to be accredited and have a need-to-know purpose for the attribute based of either compliance or legal requirement.

Restricted data which is shared to the relying party should / can be tokenised to protect it's value.

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

Storing biometric data must be handle in proper fashion. You can not change your biometric information after it is compromised, unlike a password. Such storage must be done using proper industry standards.

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

Sharing biometric data should be or could be done in a tokenised manager to protect is integrity from the outset.

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

Will there be provision for the use of biometric information if there is national security interest or criminal needs?

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

No. If so, then change it.

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

Yes. This is must!

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?

Yes. Also the legislation should deal Right to be Forgotten, Request suspension of processing.

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?

This is an enablement platform. For it to work, it must meet the needs of the relying parties, especially the Tax Office, Health and Banking institutions. Identity could be established when a baby is born, like medicare card….

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?

There needs recognition for the parent or guardian, individual who have power of attorney be it medical or full.

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

Yes. The accreditation requirement also must be tested, audited and/or re-new as with PCI DSS requirements.

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?

This must be directly linked to the CDR, consumer digital rights requirements or PDPA (Personal Data Protection Act) for ASEN neighbours. This is not the governments data, it is the individuals data, the individual should have the right to be forgotten, access, copy of their own data.

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

No comment

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?

No comment

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

No comment

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?

If the established independent bodies can fulfil the role of a independent oversight while maintain the integrity and trust of the citizens then don't re-invent the wheel.

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

No comment

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

Accreditation of the relying parties and the currency/validity of the accreditation. The audit results of the relying party.

Consent management, and the audit results of the honouring of consent

24A) What is the appropriate period for review of the governance structure of the Oversight Authority?
No comment

24B) Should the Oversight Authority be subject to accountability requirements beyond those in the PGPA Act?
No comment

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

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

They should also perform verification and verification re-check on the accredited participant to ensure they still operating as per agreements.

26A) What other committees or advisory structures do you think may be needed?
The CDR
https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0

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

No comment

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

Yes.

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

Please don't use a daggy Australian logo.

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… of course.

I'm not a lawyer, not sure what it should say. However, when dealing with data/information related to judicial proceeding the chain of evidence must be properly handled.

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

I think so. No business or entity should be exempt from the privacy act regardless of the revenue.

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

Accreditation of the participant must be met before allowing access to identity data. If there is gaps to the accreditation this must be able to be address via merits review. However, not at the risk of the privacy and integrity of the data.