Australia's Digital ID System

Key questions on the Digital ID legislation and Digital ID Rules

Your name	Nathan Kerr
Your organisation	One Click Verify
[redacted]	[redacted]

Page # of guide	Question	Your response
14	What other types of Digital ID service should be included in the legislation, either now or in future?	Over the years we have seen many advances in technology and with more publicly available Machine Learning commonly referred to as Artificial Intelligence the legislation and rules around specific types of digital ID services need to be able to evolve as technology and new needs arise. As an example the use of an Avatar within a metaverse may need to be added if the platform(s) wanted to participate.
14	Does the Minister's rule-making power to include new services over time provide appropriate flexibility to add new types of Digital ID services? If not, why not?	Providing a clear response can be challenging because the Minister's authority should be adaptable, allowing for the integration of new services into the system without unnecessary constraints. At the same time, it's crucial to prioritise data protection and security. This can be a complex task, particularly when dealing with emerging technologies that have not undergone extensive security and privacy testing. To address these complexities, it would be relevant to ensure that the Minister's authority is characterised by transparency. Additionally, establishing

Page # of guide	Question	Your response
		an industry stakeholder committee, similar to the Digital Partnership Office within the Australian Taxation Office, could be a valuable approach. This committee would operate under a defined charter and serve as a steward, facilitating collaboration among various stakeholders. For instance, the ATO Software Developers Group convenes regularly to deliberate on diverse topics that might impact both the government and private sector, specifically in the context of Standard Business Reporting (SBR2) system changes to comply with upcoming legislation, all aimed at achieving a shared objective.
16	Is the Regulator's power to impose conditions on accreditation an appropriate mechanism to balance the need to provide for unique characteristics of accredited entities with the need for a consistent set of Rules for the Accreditation Scheme? If not, how can the Regulator's power to impose conditions on accreditation be improved?	The regulator's power to impose conditions on accreditation can strike a balance between accommodating unique entity characteristics and maintaining consistency within the Accreditation Scheme. To improve this mechanism, it should prioritise clarity, transparency, stakeholder involvement, regular review, and a risk-based approach. The goal is to ensure that conditions are fair, relevant, and aligned with the scheme's objectives while allowing for flexibility when needed.
16	Is the application for accreditation process appropriate, or should other matters be included or some excluded?	The proposed application for accreditation process is appropriate, though per my previous comments (above) there should be stakeholder involvement via the formation of a stakeholder committee with government and private representation to address any future changes to the accreditation process.
17	Are the maximum penalties for failure to meet accreditation requirements sufficient to deter accredited entities from not meeting their obligations? If not, what maximum penalties would be an appropriate deterrent?	We do not believe the maximum penalties for failure to meet accreditation requirements sufficient for some of the larger body corporates who may participate in isolation. Though with many body corporates also covered under the The Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 and possibly the EU General Data Protection Regulation it may be sufficient deterrent.

Page # of guide	Question	Your response
21	Are the additional privacy safeguards sufficiently robust, clear and practical?	Yes, we believe the additional safeguards are sufficiently robust, clear and practical.
21	Is the rule making power to allow disclosure of biometric information to enable sharing of verifiable credentials (under specified circumstances) an appropriate exception to the restriction on disclosure of biometric information?	We believe that the collection of biometric data should be avoided entirely. Instead, we should establish a "Trust Framework" for accredited entities to provide attestation that it was performed to an industry standard, that would enable all participants to securely dispose of any biometric data. Allowing any form of data collection tends to result in data storage and misinterpretation of data retention requirements, which could potentially lead to more significant incidents like the recent data breaches witnessed in Australia.
21	Is the maximum penalty for a breach of a privacy safeguard sufficient to deter accredited entities from interfering with a person's privacy? If not, what maximum penalty would be an appropriate deterrent?	Yes, the maximum penalty for a breach is sufficient to deter.
23	What is the appropriate age at which a young person should be able to create their Digital ID? What factors should be considered?	The appropriate age should be 15 as this is the general minimum age a person can start working in Australia.
25	What other steps could the Government consider taking to ensure the AGDIS is ready for use by private sector relying parties and accredited entities?	There should be stakeholder involvement via the formation of a stakeholder committee with government and private representation to address any future changes to the accreditation process.
25	What factors should the responsible Minister consider prior to deciding to approve the AGDIS expanding into another phase?	It is pertinent that the Minister consult with existing industry participants, which most would be a Gateway Service Provider already consuming Document Verification Services and any change will possibly affect our businesses if we require to make any material changes.
26	How would phasing the rollout of the ADGIS affect the wider Digital ID services market in	One Click Verify are only able to comment as one of the 25 Gateway Service Providers though we would like to see a quicker roll out of this.

Page # of guide	Question	Your response
	Australia?	
27	Is the balance between voluntary use and the exceptions to voluntary use right? Are any additional exceptions appropriate?	We believe the balance to be correct at this current time.
27	Are the exemptions to the interoperability principle appropriate? Are any additional exemptions appropriate?	Yes though we would like to reiterate previous comments provided around the formation of attestation and a “Trust Framework” to prevent the collection of biometrics. The creation of a “Trust Framework” where accredited participants could accept another organisations attestation would reduce future data breaches.
29	Are the protections for the Australian community within AGDIS appropriate, or are additional protections needed?	One Click Verify believe this is a well-considered draft legislation of a extremely complex issue and commend everyone who has participated to get it to this form.
29	Are the protections for participants in the AGDIS appropriate, or are any additional protections needed?	One Click Verify considers this draft legislation to be well-thought-out, addressing an extremely complex issue. We commend everyone who has been involved in its development to reach this stage.
34	Noting the pace of technological change and the need for Digital IDs to stay protected by the latest developments, how can Data Standards provide an appropriate balance between certainty for accredited entities while maintaining currency?	We think this can be accomplished by requiring an IRAP Assessment for any participant categorised as Official:Sensitive. This would ensure that all participants adhere to the same controls (ISM). Additionally, since reassessment is mandated every two years, it would help maintain a level of currency for all organisations.
34	What would be an appropriate model for the Australian Digital ID Standards Chair and are there lessons that can be learned from the Consumer Data Right model?	One Click Verify have no opinion on CDR other then GDPR is a much easier and clearer system to manage and understand.