



The Australian Registrars' National Electronic Conveyancing Council (ARNECC) is the national peak body established to facilitate the implementation and ongoing management of the regulatory framework for electronic conveyancing of real property in Australia.

ARNECC is constituted under an Intergovernmental Agreement (IGA) among the State and Territory Governments. ARNECC membership comprises the Land Titles Registrars (or their nominee) from each Australian State and Territory.

The principal functions of ARNECC are to:

- Advise the State and Territory Governments on any proposed changes to the Electronic Conveyancing National Law (ECNL)
- Develop and publish Model Operating Requirements (MOR) and Model Participation Rules (MPR) as provided for in the ECNL
- Provide authoritative advice to the States and Territories about matters relating to electronic conveyancing
- Ensure that, as far as is practicable, business practices with respect to electronic conveyancing are consistent when implemented by the Registrars in each jurisdiction.

A key aspect of the national regulatory framework is a requirement for Subscribers (lawyers, conveyancers, financial institutions etc) to verify the identity of specified parties including their clients or mortgagors. In addition, Electronic Lodgment Network Operators must verify the identity of each Subscriber to their Electronic Lodgment Network, and Subscribers must verify the identity of some of their users. Because of this, ARNECC has observed and engaged with the Digital Transformation Agency (DTA) as it progresses proposals for Digital Identity Legislation. ARNECC's focus is to understand how the proposed digital identity processes would work and the security of the system in comparison to verification of identity (VOI) processes which Registrars currently require conveyancers and lawyers to use. The primary role of all Australian Registrars is to ensure the integrity of the land titles register in their jurisdiction and a secure VOI process is an integral part of the overall system.

With this in mind, ARNECC has reviewed the consultation paper and provides its comments in the table attached. Please note that these comments are general in nature and ARNECC is unable to provide specific commentary until a draft Bill is available.

ARNECC thanks the DTA for the opportunity to make a submission on the proposed Digital Identity Legislation and looks forward to future engagement.

ARNECC's Submission on the Digital Transformation Agency's Public Consultation Discussion Paper on Proposed Commonwealth Digital Identity Legislation

Page	Consultation Questions	ARNECC Response
9	<p>1A) Are the matters above (legal authority, privacy protections, governance, amendments) relevant matters which should be included in the Legislation?</p> <p>1B) Are there additional matters which should be considered?</p>	<p>1A) Yes</p> <p>1B) Yes:</p> <ul style="list-style-type: none"> • Include a statutory provision that allows a relying party to rely on a digital identity – see for example section 12 of the Electronic Conveyancing National Law which allows certain parties to rely on the digital signature of another party. • Enshrine the concept of a User being identified once, and that digital identity being relied on multiple times by multiple parties. • Permit a User to review the information held about themselves and request necessary changes if they are incorrect. • It is noted that enforcement provisions will be located in the Operating Rules, and penalty provisions will be included in the Act. It is queried whether the proposal to include enforcement provisions for the Oversight Authority in the Operating Rules should in fact be in the Act to ensure these provisions are not ultra vires. • The power to set security, fraud prevention measures and technical requirements in the Operating Rules. • Ensure appropriate and adequate resources for the permanent Oversight Authority – legislation on its own will be ineffective if the Oversight Authority lacks resources to ensure strict implementation and enforcement.
12	<p>2A) What matters covered by the TDIF should be incorporated into the primary legislation?</p> <p>2B) What matters covered by the TDIF should be incorporated into Operating Rules?</p> <p>2C) What matters covered by the TDIF should remain as policy?</p>	<p>2A) To be flexible in an area where technology can change rapidly, the primary legislation should be facilitative. The legislation should also contain adequate head-powers to enable all matters contemplated to be actioned through the Operating Rules and a review process for amending them.</p> <p>2B) The Operating Rules should cover the application process for accredited participants. General requirements or obligations as to the accreditation of entities in connection with the system including security, privacy, accessibility, usability, service operations, fraud</p>

Page	Consultation Questions	ARNECC Response
		<p>prevention measures and technical integration matters should be included in the Operating Rules while more specific technical requirements could be included in the TDIF.</p> <p>It might also contain provisions for Users in terms of what steps they'll need to follow to establish a Digital Identity (as technology requirements may change) and who can rely on the Digital Identity. While the primary legislation may establish this by class, it's possible that the scope of those relying on the Digital Identity could change rapidly and therefore some provision to facilitate this should be contemplated for inclusion in the Operating Rules.</p> <p>2C) See response under 2B) above.</p>
12	3) Is a publicly available 'Digital Identity Participant Register' an appropriate mechanism to communicate who will be covered by the Legislation?	<p>From the perspective of property transactions, conveyancers, lawyers and financial institutions will need to be a relying party for a conveyancing transaction. For both electronic and paper conveyancing transactions, each transacting party must have their identity verified by their conveyancer, lawyer or financial institution. If they are not represented, they must have their identity verified at Australia Post. There is some variance between each jurisdiction's legislation, however, they are closely aligned. It is unclear how such a Register would affect relying parties to a conveyancing transaction. Is it envisioned that each individual relying party would be entered on such a Register? ARNECC queries the usability and efficacy of such a Register to the conveyancing industry. More detailed information about what is proposed and how it would be used may assist.</p>
13	4) Are the proposed obligations on relying parties described above reasonable? Should there be any additional obligations?	<p>They seem reasonable except for keeping contact details up-to-date. It is unclear why this is a requirement and more details about how contact information will be used would assist here.</p>
14	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?	<p>The concepts appear appropriate, however, ARNECC will be in a better position to assess whether 'allows a person to access or interact with services offered by relying parties' captures the process for a conveyancing transaction set out in the response to question 3 once draft legislation is available. We would also query whether the definition needs to encompass the process required to establish a Digital Identity.</p>

Page	Consultation Questions	ARNECC Response
14	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?	It would be preferable to rely on existing and well understood terms. However, where additional information is required that is unique to the Digital Identity Legislation, consultation on any additional proposed definition/s should occur.
15	7) What factors should be considered in the development of a charging framework for the system?	As a relying party, Registrars would expect the User to pay, not the Registrar, but perhaps the fee will need to be passed on. Conveyancers, lawyers and financial institutions will most likely pass on the fee to their clients/customers. If governments are considered 'relying parties', details about the overall financial impact on government entities is necessary to avoid unintended consequences. Even if, as stated in the paper, the intention is that Users should not have to pay, it is likely that governments would either pass on the costs or avoid becoming a relying party where the financial impact is too onerous. This aspect will require significant fleshing-out before ARNECC can appropriately consider any legislative proposal.
18	<p>8A) What factors should be considered in the development of the liability framework?</p> <p>8B) In what circumstances should Participants be held liable under the liability framework?</p> <p>8C) What remedies and/or redress should be available to aggrieved Participants and Users for loss or damage suffered as a result of their use of the system?</p> <p>8D) What other best practice mechanisms and processes should be considered to support Users when things go wrong?</p>	<p>8A) Liability should be apportioned in accordance with existing common law principles that consider the extent to which each party was able to safeguard against error or fraud, as well as in line with existing statutory law. For example, liability is apportioned between 'concurrent wrongdoers' in accordance with state apportionment legislation such as the <i>Civil Liability Act 2002</i> (NSW) and the <i>Wrongs Act 1958</i> (Vic). Relying parties should not have any liability.</p> <p>8B) As 8A.</p> <p>8C) Indemnity should be based on apportionment of the blame. It is noted that it is intended for Identity Providers to be the first port of call for any User who has their identity stolen and that the identity provider should 'make good' and return the User to the position they were in prior to the theft occurring. ARNECC queries if this is to extend to any financial loss suffered and reputational damage, and how this would be quantified and facilitated.</p> <p>8D) There should be a requirement that adequate insurance is held by all Participants, other than relying parties.</p>

Page	Consultation Questions	ARNECC Response
W	<p>9A) Should the proposed privacy and consumer protections listed above be enshrined in primary legislation?</p> <p>9B) Are additional protections required? If so, what?</p>	<p>9A) The proposed list appears reasonable and specific to the digital identity framework. While privacy protections may exist in other pieces of legislation, these could be amended without regard to impact on the Digital Identity Legislation. It is therefore worth considering if this is an avoidable risk or would constitute unnecessary replication of existing protections. Additionally, in line with best practice legislative drafting, the primary legislation should include sufficient head powers to enable the drafting and implementation of appropriate Operating Rules.</p> <p>9B) Additional protections may be identified once a draft Bill has been produced. One possible addition is to require two pieces of biometric information in the creation and access of accounts, rather than just one (eg. face and fingerprints).</p>
21	<p>10A) Should the Legislation include rules around the extent of choice available to Users to verify their identity?</p> <p>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?</p>	<p>10A) No comments.</p> <p>10B) No comment as ARNECC would determine any such conditions for the conveyancing industry through legislation it controls.</p>
23	<p>11A) What types of profiling of behavioural information should be prohibited and allowed?</p> <p>11B) Should a public register of Attributes be maintained?</p> <p>11C) Should there be additional restrictions on access to Restricted Attributes?</p>	<p>11A) Checking for unusual behaviour (ie requests for identity verification which do not fit the norm) will be a useful fraud mitigation tool.</p> <p>11B) A public list of Attributes may be useful for all relying parties to understand what pieces of information are available to verify identity and whether these Attributes are restricted or not.</p> <p>11C) It is possible that an Australian Registrar will require access to information contained in Restricted Attributes should litigation arise where verification of identity is contested (ie in claims for compensation under the Transfer of Land Act 1958 (Vic) and corresponding Acts in each Australian jurisdiction). There should perhaps be provision in the Act to enable Registrars to easily access Restricted Attributes in such circumstances, or by order of a court.</p>

Page	Consultation Questions	ARNECC Response
25	<p>12A) Are there any other safeguards on Biometric information that should be included in the Legislation?</p> <p>12B) Are there any that have been proposed above that should be modified or excluded, and if so, why?</p>	<p>12A) No comment</p> <p>12B) ARNECC notes that lawyers, conveyancers and banks are required to retain and produce documentation to show they have followed rules requiring them to verify the identity of clients or mortgagors. ARNECC understands that deletion of biometric information after use will safeguard that information but queries whether there will be some record kept by the relying party that the process was followed and the outcome of that process.</p>
27	<p>13A) Do you agree with the proposed approach for Biometric Information?</p> <p>13B) Will the limitations on Biometric Information overly constrain innovation or rule out legitimate future use cases?</p>	<p>13A) Detection of potential identity fraudsters should be a valid use of Biometric Information.</p> <p>13B) Limitations on the use of biometric information are necessary, especially when the system is at the development stage and remains untested. Any constraints that present in the future can be addressed through review and revision (if necessary) at the appropriate time.</p>
27	<p>14A) Should the Legislation specifically provide a mechanism requiring an individual's consent before the User transacts with a relying party?</p> <p>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?</p>	<p>If a User opts out, the information should still be accessible without consent if there is a court order or investigation by a law enforcement agency or regulatory body.</p>
28	<p>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?</p>	<p>No comments.</p>
29	<p>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?</p>	<p>Lack of interest or motivation (number 3) should not be relevant factors, however, 1,2 and 4 seem appropriate. ARNECC suggests that there could be penalties attached to deter any fraudulent behaviour.</p>

Page	Consultation Questions	ARNECC Response
		Some land titling legislation and other Acts in Australian jurisdictions contain provisions for how lawyers and conveyancers should deal with legal capacity issues and therefore this is not an issue for direct consideration by ARNECC. One issue that continues to present, however, is the difficulty some clients have in verifying their identity due to issues such as old age, health, disability or cultural barriers. To achieve inclusivity and assist such members of the public to create a Digital Identity, which may be a necessary precursor to engaging in a property transaction, it is suggested that the legislation should empower the Oversight Authority to provide reasonable assistance.
30	17) Should the requirement for a PIA remain in TDIF accreditation requirements or should it be required in the Legislation or Operating Rules?	The requirement for a PIA should be part of the Operating Rules, to be submitted as part of the application process.
30	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?	No comments.
31	19) Is the proposed approach to accessibility and usability practical and appropriate? Should any other considerations be taken into account?	No comments.
32	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?	<p>Australian Registrars will comment on the adequacy of any privacy protections when a draft Bill is provided for consultation. Until specifics are proposed, it is difficult to estimate the impact on land titling systems. However, for those States and Territories which have privacy legislation, those State and Territory relying parties should only be subject to their own privacy laws.</p> <p>Service providers should be subject to penalties for failing to meet and continue to maintain any security requirements set by the Operating Requirements or TDIF.</p>
32	21) Should the Legislation include provisions to enable the disclosure of information in specified	Australian Registrars protect the integrity of the land titles register in their jurisdiction. It's conceivable that Registrars will need to access Digital Identity information for a range of functions including compliance examinations, or in the event of claims for compensation or

Page	Consultation Questions	ARNECC Response
	circumstances? If so, what should those circumstances be?	other legal action. The legislation should therefore facilitate disclosure of information to Registrars in line with their statutory functions and duties.
34	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? 22B) What is the optimal structure of a new body?	No comments.
34	23) What type (or types) of information should be required to be publicly reported by the Oversight Authority, to increase transparency in the system?	<p>Australian Registrars allow conveyancers, lawyers and financial institutions to verify the identity of their clients by applying a VOI Standard that Registrars deem acceptable. Should Registrars endorse use of a Digital Identity as an acceptable means of verifying client identity, they would be interested in any information that could assist in understanding and improving any security issues. As such, ARNECC would be interested to understand the:</p> <ul style="list-style-type: none"> • number of data breaches or other security incidents and resolutions • accuracy rates of biometric algorithms • number of successful and unsuccessful proofing requests by Users, with unsuccessful transactions categorised by the reason for non-completion (for example, failed document verification, failed biometric verification). <p>ARNECC would also be interested to know the number of fraudulent transactions and service availability measures. De-identified case studies may also assist Registrars to better understand such issues so they can ensure the security and integrity of the land titles registers.</p>
35	24A) What is the appropriate period for review of the governance structure of the Oversight Authority? 24B) Should the Oversight Authority be subject to accountability requirements beyond those in the PGPA Act?	No comments.

Page	Consultation Questions	ARNECC Response
36	<p>25A) Are the roles and functions outlined above appropriate for the Oversight Authority?</p> <p>25B) Are there any other functions that should be undertaken by an Oversight Authority? If so, what?</p>	<p>ARNECC considers the range of roles and functions proposed to be appropriate. However, ARNECC does not consider that the Oversight Authority should have the power to investigate relying parties, or to initiate enforcement action against them. This is on the basis that relying parties will not be holding any Digital Identity information except the attributes used to make a request. The Oversight Authority should have these powers in relation to Users in case of fraudulent Users.</p>
37	<p>26A) What other committees or advisory structures do you think may be needed?</p> <p>26B) Which other organisations or bodies could supply members of the Privacy Advisory Committee?</p>	<p>As the peak body for a nationally consistent electronic conveyancing system, it is possible that ARNECC would be interested in committee involvement. This would be as a conduit to ensuring Digital Identity laws and processes remain appropriate to land titling systems and the ongoing protection of land title registers, which comprises Australia’s greatest assets—land. ARNECC can provide further comment on this aspect once more details of the regime are settled and consulted upon.</p>
37	<p>27) Should the record keeping requirements be outlined in the Legislation? If so, what should they be?</p>	<p>Conveyancers, lawyers and financial institutions are required to retain supporting evidence for seven years. ARNECC therefore supports the proposal to require record keeping for seven years, which should be calculated from when the Digital Identity was last used. As stated above, a record that biometric information was produced and verified, and the outcome of the verification, should be retained for seven years from last use.</p>
38	<p>28) What best practice models should be considered for the protection and use of the trust mark?</p>	<p>ARNECC considers that best practice security measures (eg. security measures applied to currency) should be applied to the trust mark to prevent fraudsters adopting the trust mark and tricking Users into disclosing identity information, which could be used for criminal activities. Other measures proposed in the consultation paper appear appropriate.</p>
40	<p>29) Is the proposed approach appropriately balanced to achieve the objectives of the system?</p>	<p>This is unlikely to be a major issue for Registrars, as the Commonwealth cannot legislate in relation to land. There may, however, be some indirect impact on the land titling regulatory framework and ARNECC will provide any comment on this once a draft Bill is available.</p>

Page	Consultation Questions	ARNECC Response
40	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?	Audit logs should be admissible as evidence and the legislation should facilitate Registrars accessing these logs easily.
41	31) Is the proposed approach appropriate to achieve a high degree of consistency of privacy protections?	As individual jurisdictions have differing privacy regulations, ARNECC cannot easily comment on the appropriateness of the proposed approach. Once a draft Bill is available, individual Registrars may need to seek their own legal advice about the impact on their jurisdiction in order to provide appropriate comment. However, for those States and Territories which have privacy legislation, those State and Territory relying parties should only be subject to their own privacy laws.
42	32) Should the Legislation specifically provide that additional administrative decisions relating to the system be subject to merits review?	No comments.