



Western Australia Submission: Digital Identity Legislation Position Paper

Western Australia (WA) welcomes the opportunity to provide submission on the Digital Identity Legislation Position Paper (Position Paper). This response has been developed in consultation with the WA Digital Identity Ecosystem. However, WA reserves the right to alter positions made in this submission in response to changing circumstances in the WA context, and/or on reception of the draft legislation and its content.

Feedback is provided first generally, then in reference to specific sections of the Position Paper.

1. General Feedback

- State and Territory collaboration should be central to development of all secondary legislation and Rules, and sufficient consultation time should be built into each drafting process.
- Further collaborative work is required with States and Territories to determine the Charging Framework and Cost Modelling. While WA is providing representation on the Digital Identity Charging Framework sub-group, participation does not guarantee WA acceptance of a Charging Framework. WA supports the charging of private sector participants, but holds that States and Territories should not be charged for participation in the DIS.
- Should the Act be introduced, sufficient time should be provided to States and Territories to build capability and plan for implementation of the legislation.
- It is within the interests of the Digital Identity System (DIS or system) to minimise requirements placed on Relying Parties and Accredited Participants to onboard, in order to incentivise system use when there are competing digital identity platforms available on the market.

2. Specific Feedback

Section	Feedback
1. Introduction	Nil feedback.
2. Glossary of terms	2.0. <ul style="list-style-type: none">• At present participants in the system are “Accredited Participants” whereas other parties who are accredited under the framework but not using the system are “TDIF providers”. A change of terminology may clarify this aspect. For example:<ul style="list-style-type: none">- TDIF Accredited Parties: being any entity which is accredited as an identity exchange, credential service provider etc- System Participants: being those TDIF Accredited Parties who are part of the digital identity system.
3. Purpose of the Digital	3.0.

<p>Identity Legislation</p>	<ul style="list-style-type: none"> • It will be important to clearly present the difference between TDIF Accreditation and DIS participation and that TDIF Accreditation does not require DIS participation. <p>3.1.</p> <ul style="list-style-type: none"> • WA are in support of an independent Oversight Authority that is not shared by DTA or Services Australia. <p>3.4.</p> <ul style="list-style-type: none"> • WA acknowledges the future development of TDIF Rules. Can DTA please provide an indication of which Standards may transition into enforceable Rules? Mandatory Rules may affect the costs of accrediting and subsequent business decisions about becoming accredited or not. It is desirable to balance security and privacy compliance while incentivising onboarding and maturity to standards. • The issuing of Technical Standards should follow consultation with States and Territories. <p>3.5.</p> <ul style="list-style-type: none"> • WA acknowledges the intention to enshrine key privacy standards through Digital Identity Legislation. Can DTA please provide an indication of which Standards are intended to be enshrined. The movement of non-mandatory Standards into mandatory legislation will affect the business decisions of existing and future DIS participants. <p>3.5.1.</p> <ul style="list-style-type: none"> • TDIF Rules are “Disallowable Instruments” and subject to Parliamentary approval. At the same time, there is recognition of the “constantly evolving fraud and cyber security landscape” which continues to change at a rapid rate. By making the TDIF Rules “Disallowable Instruments” how will changes that need to be rapidly made to address this rapidly changing fraud and cyber security landscape be handled?
<p>4. Structure of the Digital Identity Legislation</p>	<p>4.0.</p> <ul style="list-style-type: none"> • WA acknowledges the intention that Rules may be added by the Minister that places additional requirements on Relying Parties. Can DTA please clarify what assurance Relying Parties will have those new requirements will not result in an excessive burden for Relying Parties to continue as participants in

	the DIS.
5. Scope of the Digital Identity Legislation	<p>5.2.</p> <ul style="list-style-type: none"> • WA supports the creation of multiple digital identities. <p>5.4.1.</p> <ul style="list-style-type: none"> • WA acknowledges that further work is planned to identify which components will apply to TDIF Providers versus Accredited Participants, and requests that States and Territories are collaborated with in that process. • The current set of bodies who will be allowed to be accredited is listed as “government body, company, trust, partnership or unincorporated association”. This list may not be broad enough to contain all entity types who might want to participate such as incorporated associations, cooperatives, etc. <p>5.4.2.</p> <ul style="list-style-type: none"> • It appears State and Territory governments may apply for accredited roles, thereby allowing for flexibility and economies of scale in some instances. Would it be correct that whole State governments can become accredited? <p>5.4.3.</p> <ul style="list-style-type: none"> • Please provide further insight to the ‘fit and proper person test’ criteria that may be used for State government applicants.
6. Governance of the Digital Identity system	<p>6.4.1.</p> <ul style="list-style-type: none"> • Work is being undertaken in WA to mature Privacy legislation and frameworks. As such, WA will reserve full analysis of the Information Commissioner’s role at this time and will liaise with DTA separately to ensure detailed analysis of the implications for WA. • It will be noted that it appears the Information Commissioner may have powers to investigate and sanction State and Territory agencies. The impacts of this will need to be considered before agencies seek accreditation. <p>6.4.2.</p> <ul style="list-style-type: none"> • The Minister will have responsibility to appoint at least one Advisory board to the OA. Please advise the minimum number of board members and the skills/representation that will be required.

	<p>6.4.3.</p> <ul style="list-style-type: none"> • Will legislation also make provision for the Minister to terminate employment of the person appointed to be the OA under circumstances in which they fail to adapt to changing best practice in the sector and damage the competitiveness and security of the DIS? <p>6.5.2.</p> <ul style="list-style-type: none"> • Delegation of powers can have significant ramifications. WA requests that the identification of which powers the Minister and OA be permitted to delegate be determined through consultation with States and Territories. <p>6.6.1.</p> <ul style="list-style-type: none"> • Please clarify when a TDIF provider can be off boarded.
<p>7. Privacy and consumer safeguards</p>	<p>7.1.0.</p> <ul style="list-style-type: none"> • Inclusion of 'accessibility' safeguards suggests all participants will need to provide minimum levels of accessibility. If so, please provide an indication of what these safeguards are intended to be? <p>7.4.11.</p> <ul style="list-style-type: none"> • Further input from WA Health is required to assess the needs of younger citizens. <p>7.4.12.</p> <ul style="list-style-type: none"> • While WA supports accessible and inclusive system design, enshrining the following requirements in law is likely to be onerous and quickly outdated: <ul style="list-style-type: none"> - use of clear, concise and plain English that is accessible across all devices and browsers - usability testing with a range of individuals who require additional accessibility requirements. <p>Requiring compliance with specified accessibility guidelines and standards is sufficient.</p> <p>7.4.14.</p> <ul style="list-style-type: none"> • WA acknowledges provision in the Privacy Act (Act) for States and Territories, on request to and approval by, the Minister to come under the Act. However, work is being undertaken in WA to mature Privacy legislation and frameworks. As such, WA will reserve full analysis of the application of

	<p>privacy laws at this time and will liaise with DTA separately to ensure detailed analysis of the implications for WA.</p> <p>7.4.15.</p> <ul style="list-style-type: none"> While alternative data breach reporting schemes is outlined for States and Territories, further clarification is required for jurisdictions that lack a Privacy Act and Privacy Commissioner. Given work is being undertaken in WA to mature Privacy legislation and frameworks, WA will reserve full analysis of data breach reporting at this time and will liaise with DTA separately to ensure detailed analysis of the implications for WA.
8. Trustmarks	<p>8.0.</p> <ul style="list-style-type: none"> WA notes the intention to develop trustmarks for improved clarity of the system and to incentivise increased maturity and compliance.
9. Liability and redress framework	<p>9.1.</p> <ul style="list-style-type: none"> Will a timeframe be placed the ability to seek redress? <p>9.3.</p> <ul style="list-style-type: none"> WA notes the intention to develop a Liability & Redress Framework that provides DIS Participants the right to seek loss or damages where another Participant has breached the system's rules. WA requests that States and Territories be collaborated with in development of Redress Mechanisms to help recover losses or damages resulting from cyber crime and identity theft. <p>9.4.4.</p> <ul style="list-style-type: none"> Please note that the intended Redress requirements can add significant responsibilities for State bodies. This creates operational matters that will need to be carefully considered by State bodies before considering application for accreditation and may be a barrier to onboarding.
10. Penalties and enforcement	<p>10.3.4.</p> <ul style="list-style-type: none"> Please see feedback to section 7.4.15 regarding notifiable data breaches. <p>10.3.5.</p> <ul style="list-style-type: none"> Please advise if it is envisaged that a State body could be prosecuted under the Criminal Code in relation to information that the body acquires through an identity exchange, potentially from a private sector or interstate State body? How will crossover between State and Territory laws be determined?
11.	11.1.

Administration of charges for the Digital Identity system	<ul style="list-style-type: none">• Further collaborative work is required with States and Territories to determine the Charging Framework and Cost Modelling. While WA is providing representation on the Digital Identity Charging Framework sub-group, participation does not guarantee WA acceptance of a Charging Framework. WA supports the charging of private sector participants, but holds that States and Territories should not be charged for participation in the DIS.
--	--