

2023 Digital ID Bill

The 2023 Digital ID Bill describes a somewhat flawed hammer. We sometimes need a hammer, but we don't always want to be the nail.

Sezoo welcomes the opportunity provided by the Australian Government to provide our comments on the exposure draft of the 2023 Digital ID Bill ("the Bill") and Digital ID Rules.

As well as our overall comments in the pages that follow, we have detailed comments on the Bill content, including a suggested correction to what we think is a typo.

While recent Australian government initiatives in digital privacy and identity systems offer some improvements, we still have concerns with the content of the Bill and the narrow, singular and sustained focus that is given to "ID", as if Digital ID is the silver bullet for all our online ills.

Digital ID, as understood by this Bill will not prevent another major data breach, will not reduce the scams we suffer from, and will expose the Australian economy to fragility and new risks. In addition, the Bill provides no support for those people who are cared for by others and who care for others. Digital ID, as defined by this Bill, is focused on those who can represent themselves and provides no support for parents of children, the children themselves and cared for adults. It provides no support for those who have a duty and right to represent others, not just themselves. As such it provides no support for a third of all our lives and for the most vulnerable members of the Australian population.

We are not against digital identity systems. We support the fundamental need to have trustworthy digital identities to authenticate ourselves in digital interactions on the occasions that identification is required, and we recognise the absolute need for trustworthy sources of such identities.

The Australian government is the primary source of cardinal facts about the identity of Australian citizens and as such we recognise it as a critical authority on digital identity in our interactions with government services and private enterprises in Australia and elsewhere. As Australians, we want the Australian government to have a great digital identity system but this bill doesn't get us "to good", let alone from there "to great". We, the Australian people and the Australian government, must avoid locking in outmoded thinking and must look to better approaches.

We thank you again for the opportunity to respond and hope that our comments and suggestions can be used constructively in creating a better outcome for all of us. We would be happy to discuss these comments and suggestions further, and would be delighted to support the Australian Government in achieving a better outcome for all of us.

John Phillips
Co-Founder Sezoo

Jo Spencer
Co-Founder Sezoo



Overall Comments

Scope

The Bill is focused on providing legislation for digital systems that enable the authenticated and trustworthy identification of people seeking to represent themselves online. As such it is one of the necessary tools of any digital government toolbox, but it isn't the only tool, and authentication of people isn't the only work to be done to achieve and maintain a trustworthy digital environment. In fact, the overuse of identification and authentication significantly damages trust and risks causing harm.

Further, Digital ID, as defined by this Bill, is focused on those who can represent themselves and provides no support for parents of children, children and cared for adults. It provides no support for those who have a duty and right to represent others nor does it protect those who are dependent on others. As such it provides no support for a third of all our lives.

Non Neutrality

The Bill is not technology neutral, it includes elements that enshrine the current technical implementation (for example, sections 53 and 56 pertain to "exchanges" which are a feature of the current architecture not a requirement in law for a digital identity system). In addition, the Bill anticipates maintaining current interaction patterns (as implemented in TDIF) with a federated solution and hence the need for the IDP to be available to enable anyone to use an identity it provides.

Choice and migration between IDPs needs to be supported

It should be possible for people not only to choose from a list of IDPs, but also to choose on each occasion that they interact with a relying party which IDP they use. All relying parties (including government parties ideally) should offer a genuine choice of IDPs to the user.

In addition, we should minimise lock-in to an IDP, it should be possible for people to migrate from one IDP to another with minimal loss of privacy and service access.

[Note that these challenges are created by the federated identity model that is the basis of thinking in the Bill, and their resolution is made possible with the Verifiable Credentials model we refer to below.]

Fragility and Risk

The current approach creates fragility and risk in systems that are critical infrastructure. The fragility is that when an IDP is unavailable, no person who previously authenticated themselves to the IDP can use the IDPs services to prove their digital ID. This is wrong on several levels. The original service performed by the IDP is to authenticate the identity of the individual. This should be done to the level of authentication required/offered by the IDP and requested by the person. Once authenticated to this level, the IDP should provide **signed proof to the individual** of its determination. The IDP should



not need to be involved in the reuse of the “credential” it provides. This is important not only from a privacy perspective, but also security and resilience perspectives.

If the IDP that a person used to initially authenticate themselves to a relying party is unavailable, the person cannot interact with the relying party.

This makes IDPs attractive and hence vulnerable to cyber attack. Not only can significant economic distress be caused by taking them offline (and hence ransom be demanded), the data that they hold is highly valuable and a “honeypot for hackers”.

The fragility of the identity system defined by the Bill is amplified by the use of “exchanges”. If an exchange is brought down, none of the federated identity systems and relying parties that rely upon it can function. If an exchange is compromised (infected with software that captures and echoes the flow of data through the exchange), then significant amounts of data would be breached and other more insidious crimes committed.

Authentication should be Once and Done

One of the consequences of the current approach to digital identity, and the one that the Bill legislates for, is that a person’s identity is not only used to authenticate the individual during initial onboarding (for account creation etc.), but it is used in subsequent repeat visit “login” authentication.

This means that the IDP and Exchange weaknesses that we highlight above are repeated for each and every interaction with relying parties.


If we need to prove identity when creating accounts (and certain sectors such as financial services justifiably demand strong identification of new customers), then this should be a once and done process. Once authenticated to the appropriate level, the customer should be issued with an account that they subsequently prove they have the right to access. They should not need to reprove who they are, but that they are the owner of the account.

Better Alternatives

The government should look to define a legal framework for Digital ID that is technology neutral and enables relationships between people to be proven. Beyond the legal framework, it should look to support the evolution of solutions and services using different models because the one certain thing about technology is that it will continue to evolve.

The current best practice globally is to enable trustworthy digital identities to be issued to people as decentralised verifiable credentials (VCs). This provides several benefits to government, individuals, and relying parties:

- 1) The same rigour and level of authentication can be used in determining the issuance of the digital identity as a verifiable credential. We still need IDP’s but now they issue VCs
- 2) The individual holds the VCs that they have been issued and can choose who to share, what to share, and when to share their digital identity or elements thereof without having to have the originating IDP part of the conversation or online and available at the time of use.

- 
- 3) The relying party can have the same confidence in the level of authentication as with the current system without needing to interact with the IDP who issued the VC to the user.

This is the approach that Europe is adopting with EIDAS v2.

This is the approach the NSW Government has pioneered with its world class Digital Identity and Verifiable Credentials program.

Encouragingly, while this may seem a significant change, the Bill need not be that far away from supporting this approach. The key step is to remove the technology dependencies currently embedded in the Bill and the implicit reliance on the current technology service design.



Specific Comments

Here we have used the term "Section" to describe the numbered paragraphs contained within the Bill.

Section / Part of the Bill	Sezoo Comment(s)
<p>Section 44 Restricting the disclosure of unique identifiers</p>	<p>We note this provides specific protection against "unique identifiers" and understand that this is in some way an attempt to address concerns of correlation. We argue however that this is largely irrelevant other than to provide the ability to deny that this system represents a national identity system (a new "Australia Card").</p> <p>If the AGDIS enables the unique identification of people it doesn't matter whether they are allocated a number or not.</p> <p>Rather than focus on unique identifiers, if the aim is to prevent correlation and activity monitoring, then this should be spelled out rather than identifying one way in which this risk can be prevented.</p> <p>While we have the option to use more than one provider, most will not (and systems that are "optional" often end up being unavoidable from a user's perspective, see for example India's Aadhaar).</p> <p>To avoid lock-in, as well as choice of IDPs for onboarding, the ability to migrate from one IDP to another should be included in the Bill. This ability must ensure minimal loss of service.</p> <p>If we always use the same AGDIS IDP every time we access a service, then the IDP (and the exchange) are privy to our every interaction. While we recognise that the Bill makes efforts to describe how personal information must not be retained, it would be better if it was never seen in the first place.</p>
<p>Section 51 Personal information must not be used or disclosed for prohibited enforcement purposes (a) and (b)</p>	<p>There appears to be considerable leeway offered here. Accredited entities might disclose information if they are satisfied that the enforcement body reasonably suspects that the person has committed an offence.</p> <p>This seems far too low a bar to provide adequate protection whereas (c) requires a warrant.</p>





Section / Part of the Bill	Sezoo Comment(s)
Section 53 Accredited identity exchange providers must not retain certain attributes of individuals	<p>Legislation should be technology neutral. Exchanges are an artefact of the current TDIF implementation, not an essential element of digital identity systems.</p> <p>We suggest that if this section is considered necessary it should be rewritten along the lines that all accredited entities in a digital identity system must only acquire the information required for them to perform their role and that they should retain this for the minimum period required for the transaction and allowed by legislation.</p>
Section 71 Creating and using a digital ID is voluntary (2) (a)	<p>Typo (we think). We think the sentence “the service provider access to another service; and” is at best confusing, even in context, and most likely a typographic error.</p> <p>We suggest that this should be: “the relying party provides access to another service...”</p>
Section 79 Accredited entities participating in the Australian Government Digital ID System protected from liability in certain circumstances [and sections 80, 81, 82 and 83]	<p>Liability is a critical issue for all parties in digital identity systems. A precondition of the trustworthiness of any identity system is to make it clear what happens if a relying party trusts (relies upon) the attestation of an identity provider or attribute provider about a person, and that attestation proves to be false. An obvious and frequently cited example is the financial sector’s requirement for licensed entities to meet their “Know Your Customer” obligations.</p> <p>As it stands, we don’t believe that the current text for this section makes it clear enough who bears the liability in such uses.</p>
Section 116 Digital ID Accredited Entities Register	<p>We support the inclusion of this section as it provides a description of one of the essential elements for trustworthy ecosystems, and it does so without specifying “how” this should be done.</p>
Section 138	<p>We note the inclusion in the Bill of the concept of fees by the regulator and welcome the protection afforded by 138(3) to the individual.</p>