sezoo

DIGITAL IDENTITY LEGISLATION PHASE 3 CONSULTATION

27 October 2021

Sezoo is pleased to provide a response for the phase 3 consultation on the Trusted Digital Identity Bill exposure draft (the Bill). As an Australian company founded with the mission to "radically improve trust in digital interactions for the benefit of all", we recognise the importance of this initiative for all Australians.

Recognising the amount of work preceding this phase 3 consultation, we have approached our review with two key focus points:

1. Does the Bill and supporting documents enable good, or risk harm? Here we are as much interested in direct as indirect impacts on participating people and organisations.

2. Does the Bill limit or prescribe technical solutions? Our position is that, to the extent possible, the Bill should not prevent new technology solutions nor prescribe current technology solutions.

Our review focused on three of the documents presented for the consultation:

1. Trusted Digital Identity Bill 2021 exposure draft
2. Trusted Digital Identity Framework (TDIF) accreditation rules
3. Trusted Digital Identity rules

Our response is organised in sections as follows:

- Key observations on the reviewed documents
- Future directions of digital identity systems
- Background to Sezoo

We have endeavored to keep our response brief and focused on these points as we recognise the challenge of reviewing what we hope are many contributions to the consultation. We would of course be happy to provide further explanation or participate in discussion on the points we raise. We are happy for this response to be shared publicly.

With Best Regards

John Phillips
Co-Founder Sezoo

Jo Spencer
Co-Founder Sezoo

Key observations

1) **Identity is always important, but not always needed.**
   While we recognise the need, at times, to "prove" identity to appropriate levels of confidence in order to initiate or complete a transaction, we reject the concept that this is prerequisite for all transactions. Some transactions demand identity to be proved, some do not. In almost all instances, it isn't the identity of an individual that is ultimately at question, it is the capability and rights of the individual, not who they are but what they are recognised as being capable of, their "credentials" in the general sense of the word[1]. Implementing systems and policies that insist that identity is part of every type of exchange erodes privacy, security and trust.

2) **The exposure draft includes terms that embed current technology implementations making the Bill date rapidly**
   The definitions section includes terms that are specific to the current implementation of TDIF (for example, the definitions of *attributes*, *credentials* and *identity exchange*). These embed current architecture and practices that are tightly coupled to the current TDIF implementation and make the Bill resistant to future developments. There are already better technology frameworks than those assumed by The Bill (see Future Directions of Digital Trust Systems below). The Bill should be technology neutral.

3) **This is about "Trusted Digital Identity", nothing more, or less**.
   The exposure draft defines a digital identity system to mean:
   "a system that facilitates or manages either or both of the following in an online environment:
   (a) the verification of the identity of individuals;
   (b) the authentication of the digital identity of, or information about, individuals."

   The Bill should be used for the purpose for which it has been defined, and no more than this. It does not, for example, provide a "fit for purpose" framework for credentials or digital trust in the general sense.

[1] Note that OIDC and the TDIF rules contain the concept of "credentials" and credential service providers, these should be understood as authentication or access credentials since the OIDC standard uses a narrow definition where a credential is " data presented as evidence of the right to use an identity or other resources" - https://openid.net/specs/openid-connect-core-1_0.html

4) **We need many trusted identities and many systems, not one.**
   A key benefit of the government bill and government defined system is to simplify and secure digital access to government services. This helps to fulfill a duty of government and the rights of its citizens. The use of the same system for commercial environments, and indeed, in the fullest implementation of the vision, to *all* Australian environments, is an overreach that would directly impact the privacy and security of Australian citizens - achieving exactly the opposite of the intended effect. Single system solutions of all kinds are vulnerable to attack, technically, socially, and politically.

5) **You don't need to 'blind' yourself to things that you didn't see, nor forget things you never knew.**
   The TDIF architecture, with its reliance on an identity exchange, creates privacy issues that it then seeks to overcome through rules (for example, no data is to be kept by exchanges) and/or through cryptographic techniques ("blinding" transaction enablers to the identity of the participants). An exchange is involved in every transaction, and the reliance on an identity service provider for authentication in every transaction creates a "call home" record - both are privacy eroding and unnecessary, and are required purely because of the current technical implementation.

6) **The Bill and the accompanying rules should enable a flexible ecosystem**
   Australia needs a digital trust ecosystem that is robust, economic, and designed to support multiple services with specific functional, commercial and technical needs. The ability for multiple services to coexist and coordinate within the governed technical ecosystem and governance framework is not articulated in the Bill and supporting documents. Commercial organisations will be unlikely to commit to being a service provider or a relying party (assuming they have a choice) under the current framework, and the commercial engagement with a government owned entity is unlikely to be preferred.

7) **The Bill and TDIF rules constrain the implementation solution.**
   The current TDIF design and the exchange dependency is fragile to change, will struggle to support transactions with different service levels, won't provide transaction throttling and prioritisation based on service distinctions, or flex and prioritise based on capacity constraints. Removing the reliance on exchanges is preferable, but would require fundamental redesign. While the current solution provides purely government services, this architecture may be acceptable. But the infrastructure necessary to support differentiated, commercial offerings requires considerably more design flexibility, "always on" and "service nuanced" change capabilities, and resilience, and these are not provided by the current system.

Future Directions of Digital Trust Systems

The fundamental technology underpinning the current implementation of the Trusted Digital Identity Framework is an OIDC-based, federated solution. The architecture that this technology imposes can be seen reflected in the concepts and terms used in the documents reviewed.

Whilst OIDC was considered best practice some 5+ years ago (when TDIF was first conceived), new practices and technologies have been developed since. The most significant developments in digital trust infrastructure in recent years has come from the area of "decentralised identity", particularly in those technologies associated with the "self-sovereign identity" model which is based on open standards from the W3C and DIF. Indeed, the OIDC standards bodies are drawing up extensions to OIDC to support Verifiable Credentials[2].

These decentralised technologies provide better security and privacy protections than the current TDIF implementations and naturally support multiple services and service versions in the same ecosystem. There will (no doubt) be further technology improvements that improve on these technologies and ultimately replace them. This constant evolution is the primary reason why we believe the legal framework (the Bill) should have **no** current technology related concepts embedded or referred to. Rather it should only use conceptual and/or logical constructs and terminology that defines ecosystems that provide digital identity services with trust.

We understand that knowledge of these alternative technologies and their growing use may not be widespread, and so we offer some examples of existing global initiatives below.

[2] https://openid.net/specs/openid-connect-4-verifiable-presentations-1_0.html

Examples of SSI based government and commercial systems

Europe has invested in SSI with its eSSIF-LAB[3] initiative (5.6 M€ among 62 projects), and earlier this year Germany announced two joint initiatives to develop cross-border decentralised identity systems, one with **Spain**[4], and one with **Finland**[5], in addition to its own initiatives (**Germany** already has a national SSI-based digital identity ecosystem that now involves more than 60 stakeholders from the private and public sectors).

Canada has been investing in SSI within its Pan-Canadian Trust Framework[6] and has government[7], and education[8] initiatives already in operation and many more critically important solutions currently in development[9].

The **USA** through the Department of Homeland Security was an original investor in these technologies, seeking a more secure way for US citizens to hold and share data about their identity. This work continues under the Silicon Valley Interoperability Program[10].

The **UK** Public Health System (the NHS) has been running a Passport system for its medical professionals to enable rapid and trustworthy and efficient staff relocation and authentication between hospitals during COVID-19[11]. The current evolution is to roll this model and approach out across the whole NHS for multiple staff verification purposes[12].

The **global** IATA TravelPass solution[13], designed to (re)enable international air travel as COVID-19 travel restrictions are eased, is built on this technology.

There is a vibrant community working on these technologies, and even well established major global corporations have declared their commitment, for example Microsoft is adding verifiable credentials to its Azure Active Directory solution[14], and IBM's Digital Health Pass provides the underlying technology for New York City's Excelsior pass[15]. Many COVID-19 vaccination certificate solutions use W3C Verifiable Credentials technology, including the SMART Health Card[16] solution that can now be added to the Apple Wallet in the US[17].

There are many other examples that we would be happy to discuss.

---

[3] https://essif-lab.eu/
[4] https://www.bundesregierung.de/breg-en/news/digital-identity-ecosystem-1947474
[5] https://valtioneuvosto.fi/en/-/10623/finland-and-germany-intensify-cooperation-to-promote-digital-identification
[6] https://diacc.ca/trust-framework/
[7] https://vonx.io/
[8] https://mycreds.ca/
[9] https://www.ontario.ca/page/digital-id-ontario
[10] https://www.dhs.gov/science-and-technology/svip
[11] https://beta.staffpassports.nhs.uk/about/
[12] https://www.digitalmarketplace.service.gov.uk/digital-outcomes-and-specialists/opportunities/15275
[13] https://www.iata.org/en/programs/passenger/travel-pass/
[14] https://www.microsoft.com/en-au/security/business/identity-access-management/verifiable-credentials
[15] https://covid19vaccine.health.ny.gov/excelsior-pass-and-excelsior-pass-plus
[16] https://smarthealth.cards/
[17] https://au.pcmag.com/iphone-apps/89717/apple-plans-to-bring-covid-19-vaccination-cards-to-wallet

Is a decentralised approach secure?

We understand that there is (and should be) a question about the security of any technology system aiming to provide a platform for trusted digital interactions. We offer two viewpoints: 1) Decentralised architectures are inherently more robust and secure than centralised systems; 2) The most secure systems undergo public peer review and scrutiny (as is the case with open-standards and open-sourced cryptographic libraries).

The fundamental architecture of the internet was designed around decentralised principles to make it resistant to attack. Decentralised systems provide resistance to single points of failure and denial of service attacks as well as offering better response to system load distribution (a concern with the current TDIF architecture that respondents expressed in the phase 2 round of consultation, notably Telstra and the Communications Alliance, both of whom understand large scale network performance).

The SSI technologies discussed in this section provide a decentralised model of authentication (proof request and response) with no need for exchanges, blinding, “call home", or identity providers being available 24/7. While providing the same or greater levels of security, this approach also prevents privacy breach, addresses correlation risk and negates the erosion of trust that having a third party involved in a transaction inevitably introduces.

The cryptographic techniques used within SSI frameworks rely on the same “asymmetric key” (public/private key) technologies that underpin all other current forms of online encryption and digital proofs but provide trustworthy mechanisms for decentralised key management. Most of the cryptographic techniques currently used in SSI rely on Elliptic-Curve algorithms and several quantum proof methods have been identified and are being explored. In addition, SSI includes techniques that enable selective disclosure (I can choose what parts I share from what credentials), as well as zero knowledge proof (I can prove I have something without disclosing any details, for example I can prove I have a driving licence). These developments are publicly shared and scrutinised by the community, enabling robust peer-review and preventing the “security by obscurity” path of proprietary solutions.

Primary versus secondary credentials

One of the design features assumed by the Bill and its supporting documents is that a “digital identity” is constructed from existing, physical, document artifacts, liveness checks and biometrics. In other words, existing documentation is used by a trusted third party to create a digital identity. Our preferred approach is that, to the extent possible, the digital processes follow established physical processes, the digital channel is an “and” to the physical channel. This is to make best use of **existing** governance, regulations, quality control processes, **and to prevent digital exclusion**.

In this model, our preference is that original documents are created in both physical and digital formats. Birth certificates, marriage certificates, death certificates, driving licences, business documentation, educational documentation etc. are all issued as both physical **and** digital artifacts by the originating organization. This creates a more trustworthy environment with a richer choice available to receiving parties and holders of credentials..

Secondary or “synthetic” credentials (those issued by a third party on the basis of checks that they make on primary credentials) are by definition one step removed from the original, causing problems with maintenance of currency, creating toxic data repositories of personal data and introducing significant questions of trustworthiness.

SSI models allow the use of verifiable credentials issued by the primary credential issuing organisation to be used in a real time proof of capabilities for every transaction. This fundamentally enables better processes, such as customer due diligence for banking and finance KYC/AML, which can be performed using trustworthy credentials, directly.

Can SSI support the required levels of identity proofing?

Previous conversations conveyed to us indicate that a particular concern held by some in the government is that SSI technologies do not provide and/or cannot support the levels of identity proofing required by the Bill.

Notwithstanding the general argument that levels of proofing are a blunt and often inappropriate instrument in establishing trusted relationships (see comments from Lockstep Consulting in phase the 1 consulting period[18]), to some extent this is a rather odd concern, as the levels of identity proofing described in the TDIF rules appropriately consider organisational and/or process steps rather than technology requirements. SSI (and OIDC) are enabling technologies for these steps, and don't provide these solutions inherently, as a part of their technology standards. Nevertheless it is important to consider if alternative technologies (to the current OIDC model used by TDIF) can support the defined identity proofing levels.

The "Trusted Digital Identity Framework Accreditation Rules 202x" document includes a definition of 6 levels of proof for identity (IP1, IP1 plus, IP2, IP2 plus, IP3, IP4).

Items 7 and 8 of the final level, IP4, require physical presence to complete the process of checking the person's identity. Clearly this is not an online transaction and as such is not enabled solely by digital technology. Neither an OIDC based federated model, nor an SSI based decentralised model have anything to say about physical presence checks.

For the other levels (IP1-IP3), SSI can support the process as well as, and often better, than other technology platforms. Document exchange, verification, and credential issuance can be performed as well under an SSI enabled system as they can within an OIDC enabled system. Indeed it is increasingly common for OIDC implementations to consider SSI enhancements to address OIDC technology limitations and add value to solutions[19]. Further evidence of this shift is given by the new OIDC standards being developed to enable better integration with, and use of, SSI capabilities[20].

Both SSI and OIDC provide mechanisms to encrypt communication between participants in the process of confirming an identity proofing level. Approaches such as liveness checks and biometric authentication mechanisms are additional to the base framework provided by an OIDC federated model and the SSI model. It is common practice for SSI Wallets to include biometric access and verification mechanisms, using the native security model of the holder's device (typically their mobile phone), access to the controlling mobile application and reverification during sensitive transactions.

[18] https://www.digitalidentity.gov.au/sites/default/files/2021-01/consultation01-lockstep.pdf
[19] https://auth0.com/blog/verifiable-credentials-with-auth0-and-mattr/
[20] https://openid.net/specs/openid-connect-4-verifiable-presentations-1_0.html

Background on Sezoo and its founders

Based in Melbourne, Victoria, Sezoo was founded in 2021 by John Phillips and Jo Spencer, in collaboration with the expert Management Agency, 460degrees[21], that they both work for.

Sezoo is the culmination of several years of work by John and Jo in promoting better models for digital trust both in terms of technology and organisational approaches. Sezoo's mission is to "radically improve trust in digital interactions for the benefit of all".

Since 2018, the founders of Sezoo have worked in digital trust with a number of organisations including start-up companies, international organisations, national and state government bodies, and national payments scheme operators.

In addition they have chaired global initiatives on topics such as digital models of guardianship, co-authored publications on the future of trust in the financial sector, and authored a chapter for the world's first book on "Self-Sovereign Identity".

John

With a professional career focused on helping organisations understand and benefit from emerging technologies in sectors as diverse as Space and Defence, Government, Education and retail, John was invited to write the "explaining SSI to business" chapter of the recently published Self-Sovereign Identity Book[22].
https://www.linkedin.com/in/11dot2/

Jo

A recognised global expert in payment systems, Jo has designed and built mission-critical market infrastructures (including NPP) and co-authored several publications on the use of SSI technology in financial services[23]. Jo was involved in the initial development of frameworks such as TrustID by the Australian Payments Network.
https://www.linkedin.com/in/jospencer-1pg/

[21] https://www.460degrees.com
[22] https://www.manning.com/books/self-sovereign-identity
[23] https://mattr.global/wp-content/uploads/MATTR_FinancialServices.pdf