Innovations Accelerated

Nikesh Lalchandani
Innovations Accelerated Pty Ltd
PO Box 304
Miranda NSW 2228
nikesh@iaccelerated.com

14 July 2021

Digital Transformation Agency
50 Marcus Clarke Street
Canberra ACT 2601

Dear Madam/Sir,

Thank you for the opportunity to provide a submission to the proposed Digital Identity Legislation that will eventually empower the Trusted Digital Identity Framework (TDIF).

My name is Nikesh Lalchandani, and over the course of several years I have had the privilege of developing and evolving Australia's digital systems, through the government and through my 11 year role at CBA in roles as Head of Payments Architecture, Head of Payments Innovation and Emerging Technology, and in other banks, including roles in all four majors, and Neo Banks such as Volt Bank and several others. I have represented the IT industry through the Australian Computer Society. These days I am an independent consultant with Innovations Accelerated and advise governments, banks and NBFIs on these topics and assist fintech start-ups. Through innovations accelerated me and my team have authored/published books on payments and digital identity. I have provided advice and architected digital identity solutions in banks and in government, completed postgraduate research in digital identity and participated in the establishment of international standards in digital identity. I have been involved in implementations of TDIF and can contrast the model with others in the world.

Digital identity is critical in the development of a digital economy, and I commend the Australian Government and the Digital Transformation Agency (DTA) for acting to enable it.

In the paper that follows, I make the following points:

1. That **digital identity** can facilitate better engagement and unlock value in the economy, it could be the next wave of the Internet, and bring stronger safety and security into both the physical and digital world. Digital identity needs to be led and shaped by government for so many reasons.
2. The approach however, that the DTA legislation and TDIF is taking is a proprietary solution based on a **legacy federated model**. It establishes a unique system that is untested in the world, and may not scale to meet the needs of the public and private

sectors. Entrenching the system in legislation and regulation could have the reverse intended consequence of preventing us implementing a good digital identity system and the legislation could push Australia's emerging digital economy into darkness.

3. **The digital world knows no borders**. A good solution should be built on or develop emerging global standards with global vendors – these are real and they exist.
4. A newer, **self-sovereign identity** paradigm is based on the philosophy that the individual controls their identity. It seems this principle is taking off in the global arena, and it is fair to assume that the principle could become a human right in the years to come – it is not fair to ignore it.
5. Three of **Australia's close allies are developing solutions in the self-sovereign space**, and are turning their backs on a federated model like ours. The US, through the department of Homeland Security (SVIP project). The European Union through eSSIF-Lab, and Canada through a number of initiatives including pseudo SSI - verified.me. South Korea has also expressed interest, as have other countries.
6. The **design and constructs of TDIF are problematic**. The Identity Exchange has central visibility of individuals and the authorities that issues credentials. The "wallet" is not clearly established in the TDIF paradigm. The likelihood that other countries adopt similar standards as TDIF are remote, so interoperability is unlikely, and it is unclear how many use cases can be implemented by TDIF.
7. Several private and government **institutions have voiced their concern of the TDIF model**. Many would prefer the implementation of the international standards. These organisations are reluctant to speak out.
8. **The Government and DTA should** urgently seek to validate how any digital identity framework can work with the emerging international standards, ensure that any steps taken legislatively would not prevent or dissuade the implementation of internationally aligned credentials by a third-party making use of TDIF, or by the government itself, issuing credentials on an international standard.

I submit this response out of a genuine interest to build a robust solution to digital identity that can catapult Australia to a leading position in the digital world. We still have time to take a global approach and invite the world's leading IT providers to build a solution that they can be taken globally. I urge readers to take notice as few responses would be as independent and have the expert insight that I will present to you.

1. Digital Identity Can Facilitate and Unlock Value in the Economy

Many of our current constructs, such as trusted parties and money were formed by a lack of trust in a globalising market. We trusted the coin more than our counterparty, a middleman more than a farmer. A universal network of communication, connecting the data of everyone, could have enabled better trust, and opened up more possibilities, but somehow

the Internet did not, and today it is a less-trusted environment, and individuals for the most part are unidentified, and undervalued.

Digital identity today is mediocre, insecure and inconvenient. The average person needs to maintain 100s of logins and passwords, the compromise of any one of which could open the door to identity theft, and loss of savings.

In the simple case of single-sign-on, we surveyed respondents and discovered that the largest cohort supported a government based single-sign on – as shown below.

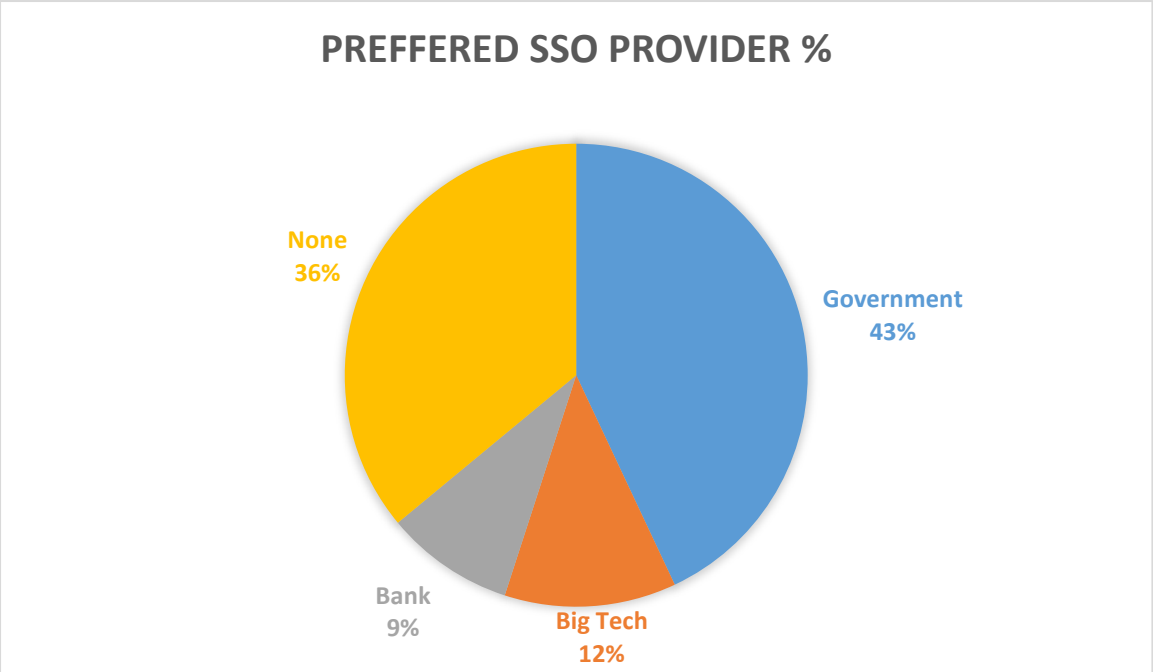

Figure 1 Government is the most trusted entity in Identity (~100 Respondents to a survey conducted by Innovations Accelerated)

Many identity documents are issued by government, and it makes sense that a solution to the digital identity problem is solved by government.

Digital identity means so much. Besides single-sign-on, it means that in the physical world a digital copy of a credential, displayed on a phone suffices instead of a physical one. It means that a credential can be checked for fraud. It means that credentials can be exchanged online without needing to physically interact, it means a holder can be biometrically validated even if online. Your age can be checked at a pub without sharing a name, a bank account can be opened online. Benefits can be handed out in real time. A sheep farmer in a small town can feel comfortable sending a sample to a buyer in the city without payment.

Digital identity extends not just to people, but parties or even "things". "Complete information" that could be partially provided by digital identity is a necessary ingredient of a true free market.

So at the outset, digital identity is a worthy cause, and the DTA is doing the right thing pushing it.

2. The Proposal Could Entrench Australia in a Legacy Federated Model.

Federation is regarded as a good thing. In digital identity, it is highly regarded as well. It is better than a siloed model where everyone is left for themselves, and is the logical path forward from no or limited digital identity.

TDIF dates to 2015-2016, at a time in which most countries, in the absence of any broader system, implemented their own solutions.

The world has moved on from federated, and it could be safe to say new implementations have greater scope: decentralized identity, user centric identity and self-sovereign identity to name a few. A view of the evolutionary continuum of digital identity models is shown below.

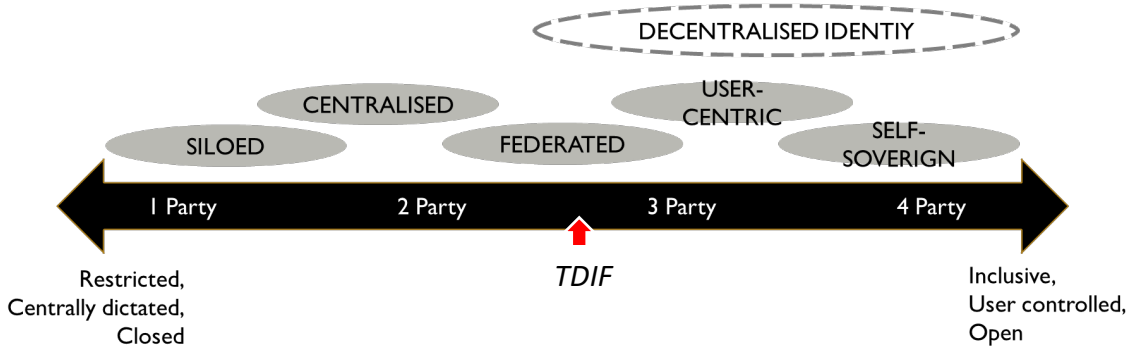

Figure 2 Continuum of Digital Identity Models

Phase two proposes to place restrictions on how information between participants in digital identity can be used.

If there is no way for a relying party to validate an identity outside TDIF, if there is no way for a person to share a credential outside TDIF, and if a relying party is restricted in how it can deal with TDIF information, this could restrict the flexibility of digital identity in Australia. If the restrictions are too tight, then it could lock Australia into a dark ages of digital identity as the rest of the world is free to move forward.

If legislatively TDIF is mandated and water tight, and it is too hard to use, and impossible to share credentials outside the framework, we will be in a worse position we are without a

digital identity solution. It is unclear what principles and guardrails are being applied to TDIF legislative changes to prevent such a reality.

The approach of TDIF has been superficially tested. Australia Post's use of TDIF creates another credential effectively outside TDIF as a Digital ID, and a Keypass. It is safe to assume other entities will do the same. TDIF is not being used as an ecosystem.

TDIF introduces terms and entities that are unfamiliar to the industry. Few industry partners have a clear idea how they will bridge TDIF. There is the Credential service provider, that holds logins, the Identity provider that provides identity credentials, the attribute service provider that provides non-identity attributes (can there be such a thing?), an Identity exchange provider that allows relying parties to be hidden from issuers (is this really necessary when it is often obvious who the issuer is?) creating a powerful entity that has knowledge of individuals, issuers and relying parties.

The paradigm is not a natural one, when compared with the more elegant and simple models put forth by the W3C.

I have been at many a meeting with sophisticated organisations, where experts have struggled to understand the TDIF model. It is safe to say the unnecessary complexity would be an inhibitor to adoption and the "build it and they will come," in this case could be wishful thinking.

The presence of restrictive legislation also acts as an inhibitor. Within government, agencies would be reluctant to go out-of-bounds, and a general fear-factor could prevent even non-government institutions venturing into the digital identity space if too restrictive.

3. Digital World Knows No Borders. Our Solution Should be International.

At home, on the Internet, we may use a Samsung phone, a Google/Android device or an Apple iPhone, to access the Internet. Microsoft Edge, Google Chrome and Apple Safari provide are our instruments. Engaging these vendors in something as important as digital identity is important. We know Apple and Google have wallets, and indeed Google, and most of the big techs have fully federated their IDs so that a user can use a Google, Facebook or Linkedin login to access an online shopping store.

Microsoft, IBM, and Mastercard have signed up to enable a common interoperable standard of digital identity and exchange. In the light of these realities – international providers interested and willing to cooperate on a universal solution, we should look at true partnerships to establish a global solution.

Credentials are not unique to Australia. drivers' licenses, passports, visas, airline tickets, digital vaccinations are international problems and solutions. Education credentials such as

certificates, degrees and micro-credentials are parts of digital identity that we need to validate from overseas, and Australia exports to the world. What sense does it make to develop our own standard?

But does such a standard exist? It does and it is robust. Perhaps one of the most impactful standard bodies of recent times, the W3C has published a "Verifiable Credentials" (VC) data model and APIs and "Decentralized Identities" called DIDs that are similar to URLs but rather than refer to organisations, they refer to individuals and even things. These standards are supported by international industry grouping together through the Decentralized Identity Foundation and Trust over IP Foundation. A community of corporate, and government organisations sharing a common vision. Australia should be part of that vision.

The model is supported by a large body of academic work, solving hundreds of problems. It can be applied to unlock the ability of blockchain and the Internet of things to universally access resources, and most importantly, recognise individuals. The movement is so important and profound some call it "rebooting the web" giving everyone a voice, presence and identity on the web that they can control.

We need to be part of this, and not develop our own solution.

4. The New Self-Sovereign Paradigm is Important, Even if Aspirational

Since the 1980s Banks have put in place the 100 point check. Meticulous over 4 decades they have obtained the identities of almost all Australians. For them identity is an asset. The big banks retain these identities more abundantly than smaller banks, and thus are able to continue to maintain to a large extent dominance. Indeed, recently a "Buy Now, Pay Later" provider was seen offering $10 discount on purchases to new customers – in this particular instance the figure provides a good indicator on the value of a digital identity. So financial institutions see digital identity as an asset.

Governments on the other hand see digital identity as something they issue. Passports, citizen certificates, birth certificates, drivers' licenses, and Medicare cards feature prominently on lists of documents required to establish identity.

So who owns identity?

Self soverign identity (SSI) philosophy puts the individual in control of who and what people can see. Issuers give the individual credentials. The individuals can share them with relying parties as they choose. They can also choose how they are authenticated. This is a simple paradigm, and almost universally preferred at least aspirationally. It is very different to TDIF and the proposed legislation.

The principles of digital identity that are most cited in this regard are those of Kim Cameron (https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf) and Christpher Allen (http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html). SSI is not a religion, it is a common sense human digital right, and it is easy to see how it may be intrenched in our rights in the future. In the second appendix, we assess TDIF against these emerging principles.

5. Don't Listen to the Community – Listen to our Allies.

The work of W3C, DIF and ToiP are not the work of crazies. The US Department of Homeland Security's Silicon Valley Innovation Program (SVIP) and the Next Generation Internet initiative of the Eurpean Union on European Self Soverign Identity Framework Lab (NGI eSSIF-Lab) have funded many of the vendors and initiatives to date in this space. The time for implementation is now. Cannada, South Korea numerous European countries are implementing pieces of SSI.

Initiatives such as Good Health Pass, and IATA are also adopting elements of the standards.

While there may be initial nervousness in a full implementation of a decentralized model, many organisations such as Mastercard are marrying some federated control with using the SSI constructs. We should be doing the same.

6. The design and constructs of TDIF are problematic

There are so many technology standards that even despite the best intents, did not pick up. Sony's Betamax videos, and digital tapes are classic examples.

In the case of TDIF, in technical circles the complexity of the parties, who does what, the standards make it almost impossible for developers to understand. They have more trouble explaining it to their bosses. Then there is accreditation. CSP, IdP, ASP, IdX, RP. Imagine a board-level discussion for a would be implementer, wishing to invest the money to get accredited. Many would-be implementers will walk away from the challenge.

What the industry calls IDP, TDIF calls CSPs. IDPs and ASPs are the same thing but treated totally differently. What are the standards for ASP exchange? What is an IdX? Are common confusions that are not easy to resolve.

TDIF attempted to solve the privacy problem where an issuer should not know how an individual uses a credential, nor should a relying party know about the individual or the issuer, through an "Identity Exchange". Many feel this is an unnecessary construct, and particular where there is limited competition means this new entity becomes all-knowing by design (though by policy this may be restricted, as advised in section 7.4.9 of the position paper).

The problem of multiple IdXs is illustrated in figure 8, page 29 of the position paper – and this could add to the usage difficulty.

Despite introducing a new industry/role of the IdX, TDIF fails to adequately cater for the individual holder or wallet and leaves it up to the parties. This is a major oversite, and without a consistent approach, could render the whole environment unusable.

A good way to ensure complete coverage is to walk through how scenarios would operate over the system: (e.g.)

1. User shows proof of age to shopkeeper
2. User buys alcohol online
3. Single sign on to private web sites using government login
4. User leaves/arrives Australia with a digital passport
5. User shows education credentials to a prospective employer
6. User applies for a loan with one-click by sharing their data and credentials
7. Individual receives digital credential reference from their ex-boss.
8. Local netball club issues “player of the month” credential. Their IT budget is $5 pa.
9. User sends money to another digital identity. Identity is checked for money laundering/terrorism financing ties.

The double-blind approach of the IdX may make sense to some.

To a lay person it does not matter who knows, just that someone knows, so once again TDIF becomes a central hub for identity exchange, a big brother that may be tracking our movements, this is a technical reality, despite efforts to avoid this perception.

The problem is solved in the old paper world by issuing papers and giving them to the individual. The government does not know and most often cannot know how a passport is used, nor for over 100 years, has it cared.

In the emerging international standards, a similar paradigm is used. The credential is issued to the individual and after that point, the issuer does not know how it is used. The difference is there is no central party that does know, unlike the IdX or CSP in the TDIF model.

Further the entry bar for each participant is substantial. Getting TDIF accreditation is not easy, and will dissuade many.

The alternate model from the W3C uses a “zero trust” paradigm, which is perhaps more secure. The model allows anyone to participate and security and authenticity should be implemented by the participants.

There are obvious concerns that many feel nervous about, to do with opening up the network, so some level of federated control could be warranted in the early days, but there should be a roadmap to a simpler solution, with less governance (see W3C model below, courtesy W3C):

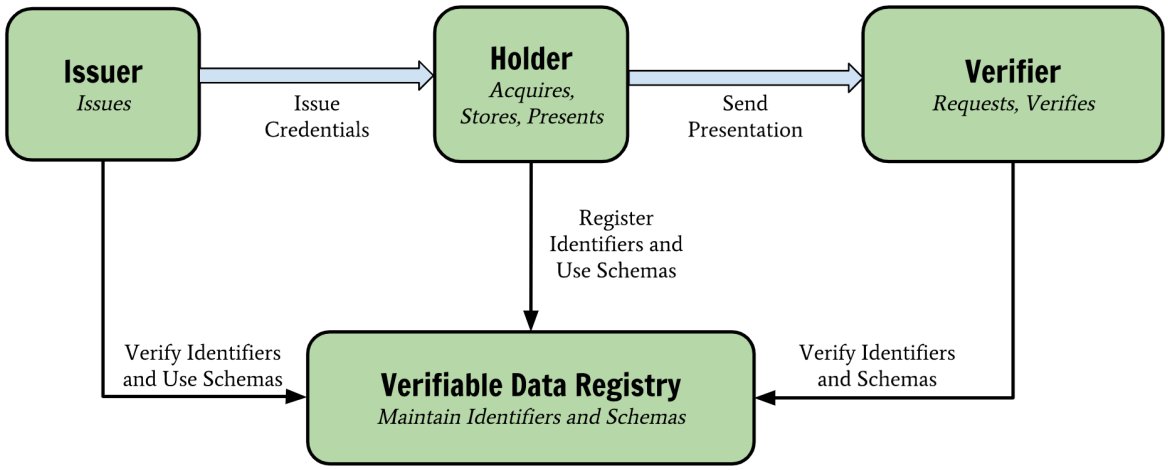

Figure 3 W3C Verifiable Credential model - a simple approach to the problem.

If all this is too complicated, that is my point. The complexity of TDIF could act as an inhibitor to implementing good Digital Identity in Australia, and unlocking the value that this brings.

7. Concerns are Shared by Many

As a consultant to leading organisations, I have had the good fortune of interacting with government, semi government and private institutions. My relationship with banks goes back decades and continues to this day.

The sentiments I express here are almost universally felt. Many organisations are reluctant to voice their concerns due to the need to maintain close ties with the DTA and government. Many are attracted by the possibilities of a more internationally aligned initiative - these include federal government agencies.

At the same time there is reluctance to publicly criticise, as mentioned before, as a solution to digital identity is important and any effort has value. The government should drive it. DTA looks like the best home for the initiative. The danger is that the government abandons the cause, or goes back to the drawing board for 5 years. At the same time the legislation could entrench TDIF and prevent a government-led implementation of a SSI model that would be more internationally aligned, and more open to adoption in Australia.

8. Conclusion and Recommendation

Something is better than nothing, and stopping TDIF could make matters worse.

The government should philosophically and strategically align with an aspiration to implement open, self-sovereign digital identity. There is considerable and almost universally positive/constructive literature on the topic. There should be a roadmap to implement the international standards especially the W3C VC and DID standards.

Second that legislative changes should not impinge on the federal government (and other entities) implementing TDIF alternatives such as SSI in the immediate future. It is refreshing to see that "There has been no change to the position that the Document Verification Service (DVS) and Face Verification Service (FVS)".

Third that TDIF issuance should not be mandated for any government (or non-government) credential.

Fourth that freedom should be given to relying parties, when acting with the express authority of the individual, to use credentials as they see fit, including to represent it alternatively.

Fifth that use of digital identity information especially by relying parties should be governed by privacy law. Some consideration should be given to some provisions of the GDPR regulations of the EU which are being held up as the high bar of privacy, at least to the extent that digital identity information should not be shared with jurisdictions with a lower privacy tolerance than Australia, that information used be for a proper consented purpose, deleted when no longer required, explicit consent, and recourse when information needs to be removed or has been misused.

Minor feedback is provided in an appendix to this submission.

Finally, as always, I offer my advice and services at no cost to the DTA if they wish to discuss this in further detail.

I do commend the DTA for championing the problem of digital identity.

Yours sincerely,

Nikesh Lalchandani

Nikesh Lalchandani
Principal Consultant

1. Appendix: Minor Feedback on the document

Page	Section	Comments
Page 20	Section 5.4.3	The onboarding process is onerous and a barrier of entry. The DTA should consider an aspirational target of more open participation.
Page 21	Section 5.4.6:	Digital Identity definition here is inconsistent with the industry use of the term. A digital identity often said to be a persona (or representation) that is presented online and may differ in different situations. Digital identity includes attributes from an ASP but here they are defined as IdP attributes only.
Page 24	Section 5.4.11:	This greatly limits what is possible with the digital identity implementation – it is suggested there is only one scheme possible under TDIF.
Page 27	Figures 5 & 6	What is indicated here is an all-or nothing approach. An IdP cannot issue credentials elsewhere using the IdX, they need to adopt another standard. So basically IdP credentials on network, cannot be taken off network. This prevents coexistence of models unless the IdP specifically implements them, which would be highly unlikely in practice effectively locking the agency into TDIF
Page 28	Figure 7	As per previous, an Attribute service provider is unable to use any TDIF infrastructure if providing information to an external RP.
Page 29	Figure 8	Figure alleviates the previous two issues, but is contradictory – when the legislation is written explicit permission should be given to an accredited IdX to exchange to non-accredited IdP, ASP and RPs. It is ok to put restrictions on any trust mark.
Page 30	Section 5.4.14	Relying party obligations could be quite restrictive and act as a barrier. Ideally relying parties should be subject to privacy safeguards as strict as Australia. “comply with conditions governing when and how they may use or share attributes” is not sufficiently defined
Page 30	Section 5.4.15	Machine-to-machine credentials is poorly handled by the TDIF model. In the W3C model, a DID allows machines

		to act on behalf of individuals, or on behalf of things, with optional step-up.
Page 46	Section 7.4.2	The use of biometrics could help aged/lost/disadvantaged individuals be identified without data. The DTA should consider an opt-in, well defined one-to-many search. Fears of Biometrics should be reduced given the widespread use of them in social media and on modern tech.
Page 48 Page 51	Section 7.4.3 Section 7.4.5	While cross-organisational tracking should be restricted, and no national identity should be instituted, the government should look at an RP-specific individual ID to help to track within an RP meaning additional information requirements could be reduced, improving privacy and solving the customer uniqueness/de-duplication problem for many organisations.
Page 48	Section 7.4.3	"de identify" data should be qualified – as it is possible to reverse engineer aggregated data to obtain personal information. De identity is easy to say, hard to do.
Page 53	Section 7.4.9 Section 7.4.10	The need for the IdX to purge data, conflicts with the need for a log history. This problem could be alleviated somewhat through the adoption of the W3C Wallet/Holder who acts on behalf of the user.
Page 54	Section 7.4.11	Acting on behalf of another, including acting on behalf of a company are complex and worthy of further elaboration at this stage and should be designed.
Page 57	Section 8	In the end the security of the system is expressed to the user as a trustmark. Trustmarks can be forged, and most users are unaware of sophisticated compromise attempts. They will tend to trust the RP. In the end, all this boils down to a trustmark (that doesn't exist today), it is worth considering if this level of governance was required in the first place?

See:

https://www.digitalidentity.gov.au/sites/default/files/2021-06/digital-identity-legislation-position-paper-2021-06-10.pdf "Digital Identity Legislation Position Paper" Version 1801.

2. Appendix: Comparison of Cameron's and Allen's principles with TDIF & Proposed Legislation

Allen's Principles	Details	Cameron's Laws	Details	TDIF
1 Existence	The identity exists independently of the digital world, which can only ever contain a subset of attributes			**Yes**
2 Control	Users must control their identity	**1 User Control and Consent**	Technical identity systems must only reveal information identifying a user with the user's consent.	**No**
3 Access	Users must have access to their own data			**No**
4 Transparency	Systems and algorithms must be transparent			**No**
5 Persistence	Identities must be long-lived			**No**
6 Portability	Information and services about identity must be transportable			**No**
7 Interoperability	Identities must be as widely useable as possible	**5 Pluralism of Operators and Technologies**	A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.	**No**
8 Consent	Users must agree to the use of their identity	**1 User Control and Consent**	see above	**No**
9 Minimalisation	Disclosure of claims must be minimised	**2 Minimum Disclosure for a Constrained Use**	The solution which discloses the least amount of identifying information and best limits its use is the most stable long term solution.	**No**
10 Protection	The rights of users must be protected			**Yes**
		3 Justifiable Parties	Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.	**No**

		4 Directed Identity	A universal identity system must support both “omni-directional” identifiers for use by public entities and “unidirectional” identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.	**No**
		6 Human Integration	The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks	**No**
		7 Consistent Experience Across Contexts	The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.	**No**

See:

Kim Cameron (https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf)

Christopher Allen (http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html)