ForgeRock

ForgeRock Comments on the: Digital Identity Legislation Position Paper

July 14, 2021

Global Headquarters 201 Mission St, Suite 2900 San Francisco, CA 94105 +1 415-599-1100

Disclaimer of Liability

While every effort will be made to ensure that the information contained within the document is accurate and up to date, ForgeRock makes no warranty, representation or undertaking whether expressed or implied, nor does it assume any legal liability, whether direct or indirect, or responsibility for the accuracy, completeness, or usefulness of any information.

Global Headquarters 201 Mission St, Suite 2900 San Francisco, CA 94105 +1 415-599-1100

Table of Contents

Global Headquarters 201 Mission St, Suite 2900 San Francisco, CA 94105 +1 415-599-1100

Summary

ForgeRock welcomes the opportunity to provide comments and share our views on the Digital Identity Legislation Position Paper as part of the public consultation phase.

At ForgeRock we strongly believe that people need to be able to safely and simply access the connected world. Behind this simple statement are some fundamental principles that need to be considered in legislation, regulation and technology solutions. This includes:

- Strong user centric privacy controls
- Strong means to verify a digital identity and who it relates to
- Strong means to verify attributes related to a digital identity
- User controlled means to manage how digital identities and associated identity attributes are used and shared
- Establishing trust between the digital identity ecosystem participants and its users
- Transparent accreditation and auditing of the digital ecosystem participants

Citizen access to Government services is increasingly becoming digitised and users are expecting a digital first experience. This expectation stems from not only wanting more convenient access to services but also to be able to access critical, identity based, services in situations where physical access is limited or restricted.

From a citizen point of view there will always be a choice of digital identity providers in Australia. A citizen will choose, based on aspects such as trust, convenience and availability. This creates a competitive tension between private and public digital identity ecosystems. It is not a given that a citizen will trust a public (Government) provider any more than a private provider. Allowing a citizen to choose an identity provider, as indicated in the position paper, is important as it provides an opportunity for specialisation and compartmentalisation.

A citizen may choose to use a certain provider for work purposes as it can assert business related attributes (e.g., being an accredited professional) and use another provider for private purposes as it can assert, let's say, lifestyle associated attributes (e.g., valid boating license). We anticipate that federal, state, territory and council level providers will, over time, be integrated and active participants in the digital identity system. It is encouraging that the position paper suggests leveraging the TDIF accreditation scheme.

In a digital identity ecosystem as envisioned in the position paper interoperability is critical. This applies both to how this regulation can work in harmony with local territory, state and industry sectors that may have more restrictive legislation and regulation in place. From a technical point of view we would like to stress the importance of using internationally accepted standards. Such standards are critical for citizen user experiences, ease of integration and thus the growth of the digital identity system as well as the ability to tap into existing digital identity expertise and experience.

Global Headquarters 201 Mission St, Suite 2900 San Francisco, CA 94105 +1 415-599-1100

We welcome, as outlined in the positioning paper, that expert advisory boards can be appointed by the Minister. We would encourage that a privacy and consumer advisory board is established in conjunction with a technical standards board that includes private sector experts. Relevant and related work being undertaken in organisations such as Kantara (https://kantarainitiative.org/) and the OpenID Foundation (https://openid.net/foundation/) should be leveraged. Active participation with and in such organisations will also be advantageous for the digital identity system roadmap and how its participants can innovate.

Another aspect of using industry accepted global standards is that we can anticipate the need for a global interworking aspect of the digital identity system. There are cases where people move between countries and digital identity cross border exchange standards can provide a convenient and secure way to improve the process of, for example, granting residency and citizenship. We can also envision that there are certain asserted attributes associated with an identity that conveniently can facilitate the process of travelling, e.g., proving vaccination status, visa eligibility etc. as required by border entry and exit policies and procedures. Cross border use cases are not only convenient for the users, they are also good for business making it easier to welcome visitors such as overseas students who also are going to be users of the digital identity system during their education. We envision that specialist identity exchanges may operate cross border focused services. Such identity exchanges may specialise in verifying and attesting attributes from countries or organisations they are peering with.

At ForgeRock we have experience with citizen identities, associated government services and identity ecosystems and believe that by focusing on the citizen experience, strong privacy & consent mechanisms in combination with accepted industry standards and public awareness and education will make the Australian Digital Identity System a successful one.

Global Headquarters 201 Mission St, Suite 2900 San Francisco, CA 94105 +1 415-599-1100

Specific Comments

Section 3.5 - Privacy and consumer safeguards

- It is encouraging to see that privacy and consumer safeguards within the TDIF are intended to become law by means of this Legislation, especially as it relates to how data can be used, who can use it, for what purposes, and how explicit consent can be gathered.

- It is equally important to ensure that there is clarity on what needs to happen, amongst the relevant participants, when a user revokes consent previously given. This also relates to the process associated with trustmarks and associated auditing. In simple terms, the revocation of consent should trigger, as permissible by law, for example the deletion of data, stopping the processing of such data and, ideally, a confirmation or certification that such data storage and use has been stopped (preferably with an indication of how it was used during the time of the active consent).

Section 3.5.1 - Security requirements

- It is expected that Australian Cyber Security Centre (ACSC) maintains a close and active relationship with cybersecurity industry participants, relevant standardisation organisations and Community Emergency Response Teams as relevant.

Section 4 - Structure

- It would be expected that specifications are leveraging accepted and global de jure and industry standards published by organisations such as ISO/IEC, OpenID Foundation, Kantara and IETF. It is also important that resources are provided to maintain such specifications and provide sandboxes etc to facilitate interoperability testing, integration and associated growth of the system.

Section 5 - Scope

- "*...relying parties will need to offer a choice of identity providers.*"

  This is positive as it allows for choice of identity providers as it will facilitate competition, specialisation and user choice whilst the legislation provides governance principles and accreditations.

- *"...entities generating, transmitting, managing, using and reusing digital identities will need to provide a seamless user experience with the Digital Identity system (interoperability)."*

  This is positive as it puts emphasis on user experiences which is critical for adoption, trust and associated security. The interoperability aspect also indicates the

Global Headquarters 201 Mission St, Suite 2900 San Francisco, CA 94105 +1 415-599-1100

importance of using accepted standards.

- *"5.4.11 Principle of Interoperability: it is in violation of an identity provider's constitution to transact with a particular type of relying party, for example, a relying party in the gambling industry."*

  How is a "particular type" defined and are there any classification mechanisms, e.g., via the registry, that can be used at run-time or is it expected to be managed at onboarding time? Also, if a relying party changes its business, e.g., from providing only music streaming services to include gambling, is there a notification mechanism that a provider can leverage?

Section 6 - Governance

- "*6.4.2 Permanent Oversight Authority: a technical standards board made up of entities participating in the system, as well as key experts from the public and private sectors."*

  We would encourage the creation of a technical standards board and recommend that it should include participants from the private sector due to their skills and expertise in the Digital Identity space.

- *"6.4.5 Functions of the Oversight Authority: public education about Digital Identity, including conducting educational and consultative opportunities with other bodies on Digital Identity issues"*

  This is encouraging for not only the uptake and use of the system but also for general awareness of the value of asserted identities and attributes for trusted interactions.

Section 7 - Privacy and consumer safeguards

- *"7.4.6 ...require individuals to expressly consent before their attributes are shared with a relying party"*

  Protecting personal information has both technology, system and behavioural aspects associated with it. Technology can be applied to ensure that data is securely stored, transmitted, shared and managed. This includes using cryptographic means to protect the information as well as ensuring that explicit user consent can be applied as relevant, that a user can assert relevant data controls, can be notified of changes to T&Cs, data breaches or leaks, and make an informed decision on how to control his or her personal information. Community trusted and transparent audits, related to how system participants manage and use personal information, should also be considered as part of personal information protection so users can make informed decisions in regards to their personal information management. This also

Global Headquarters 201 Mission St, Suite 2900 San Francisco, CA 94105 +1 415-599-1100

relates to the concept of catering for several identity providers.

- *"7.4.1 ...create a voluntary system giving users the right to create and use a digital identity, including the right to deregister and not use a digital identity at any time"*

  It would be worthwhile to elaborate on what "deregistering" a digital identity means. There may be community expectations, along the lines of "right to be forgotten" such that deregistering a digital identity is expected to completely erase the digital identity and associated information. This has linkages to mandatory record keeping, data retention, as required by law etc. From a citizen service point of view deregistering a digital identity may also impact service delivery and associated processes, therefore it is important that proper notifications are provided outlining what the consequences of deregistering the digital identity is.

- *"7.4.12 ...default minimum age of 15 years for the use of a digital identity."*

  In a digital identity ecosystem we can expect that there are transactions related to someone under the age of 15. An example of this includes issuing school identity credentials, proving age compliance e.g., for playing an online game, getting a concession on public transport or similar. It is also worth highlighting that use of certain attributes, e.g., for age verification purposes, lean themselves well for zero knowledge proof protocols and associated data minimisation approaches.

  The concept of a default minimum age also touches on the concept of delegation and guardianship. We believe it important that provisions are established to ensure that it is indicated when someone is acting on behalf of someone else. This is critically important from an auditing, trust and record keeping perspective. For relying party applications knowing that some interaction is done on behalf of someone else can also drive conditional processing and user experiences.

  A guardianship, for age related or other reasons, should also be put in the context of what needs to happen when the guardianship is no longer in effect. For example, what will happen with identity related attributes and any guardian provided consent when a child becomes of legal age or a person is no longer a ward under a guardianship? A transfer of ownership and control over such attributes and consent needs to be catered for.

  Specifically, with respect to "default minimum age" it should be clear what processes and controls need to be in place to manage exceptions for using a digital identity. It can be suggested that it should be encouraged for citizens to be able to use the digital identity system at an earlier age.

Global Headquarters 201 Mission St, Suite 2900 San Francisco, CA 94105 +1 415-599-1100

Section 8 - Trustmarks

- It is important that the accreditation process is not a once off process but something that is done on a regular basis or triggered by certain events (e.g., change of ownership, change of outsourcing arrangements, change of directorships etc.). The “trust mark” should not only provide a “visual” indication but also be embedded in the digital interactions as far as practically possible.

Section 9 - Liability and redress

- *“9.4.4….ensure assistance is provided to Users of the system where there has been an inappropriate disclosure of information, identity theft, cyber security incident or system failure.”*

  A “notification” mechanism is a critically important part of the privacy safeguards in the system. It needs to provide enough details so a user can take appropriate actions to protect their personal information, update credentials, block payment instruments such as credit cards etc.

Section 10 - Penalties and enforcement

No comments.

Section 11 - Administration of charges

No comments.

Global Headquarters 201 Mission St, Suite 2900 San Francisco, CA 94105 +1 415-599-1100