Microsoft

Microsoft submission to the Digital Identity Legislation consultation

Introduction

Microsoft welcomes the opportunity to respond to the Government's consultation on Australia's Digital Identity Legislation. We believe everyone has the right to own their digital identity, and the right for personal information to be stored securely and privately. The Government's Digital Identity Legislation provides both the privacy and security guardrails that are essential to building trust with citizens, businesses and governments.

We note that individuals can already use the Government's Digital Identity System to access 80 government services, which includes some of the most sensitive citizen data. As the back-end provider for many of these services, Microsoft commends the Government for enshrining consumer privacy and protections through legislation, and going beyond existing privacy legislation in areas including the management of biometric data.

The Government's measures to expand the Australian Government Digital Identity System to enable a broader range of participants—including companies and state and territory governments—is a welcome development. The legislation and associated accreditation frameworks will provide greater confidence for businesses and governments that want to participate in the scheme or be accredited for the services they provide under the Australian Government accreditation scheme.

This submission sets out: Microsoft's approach to decentralised digital identity management; our comments on elements of the legislation including holding information outside of Australia; comments on the Trusted Digital Identity (TDI) rules and the Trusted Digital Identity Framework (TDIF) accreditation rules; our position on the future uses of digital identity; and the legislation's interaction with other government reviews and processes.

We note that while the consultation provides the opportunity to comment on the exposure draft and associated instruments, the technical standards are yet to be released. Microsoft would welcome the opportunity to provide comment on those standards once released.

Microsoft's approach to digital identity

Microsoft believes everyone has the right to own their digital identity, and the right for personal information to be stored securely and privately. This identity should seamlessly integrate into daily life and give complete control over data access and use to individuals.

As our lives are increasingly linked to apps, devices, and services, individuals can be subject to data breaches and privacy loss. While we commend the Australian Government's Digital Identity System, we believe a standards-based decentralised identity system can provide even greater privacy and control.

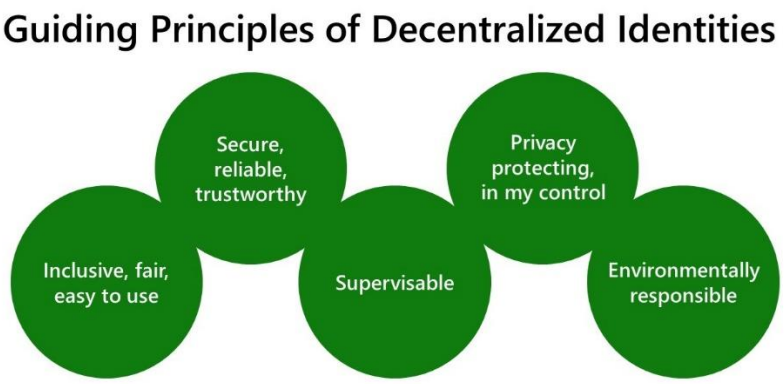
Over the past three years Microsoft has incubated a new set of decentralised identity technologies, including a public preview of our own our new decentralised identity system—Microsoft Azure Active Directory Verifiable Credentials.

Decentralised identity is a trust framework in which identifiers, such as usernames, can be replaced with IDs that are self-owned, independent, and enable data exchange using blockchain and distributed ledger technology to protect privacy and secure transactions.

In a decentralised ID landscape, a person's critical data is stored securely and released only when and how that person chooses.

Guiding Principles

Microsoft has published a set of guiding principles that we are using to guide our efforts in decentralised identity technology. Not all these principles will be achievable from the start, but we believe that all are necessary over time to realise the promise of decentralised identities:



Although Australia's Digital Identity Legislation is not a decentralised system, we believe the legislation broadly aligns with our own principles for identity management, and the legislation provides the framework for the introduction of decentralised identities in the future.

Microsoft believes that the Australian Government often performs the role as a technology leader in policy and standards development. While the TDIF is enabling legislation for a specific program, we believe that because of this leadership role, the TDIF core principles and standards are likely to be replicated more widely. As a major provider of identity management services in Australia we encourage the DTA to build in ongoing engagement practices that ensure the TDIF is aligned with other providers as identity practices evolve. This engagement, in particular during the rules development process, should ensure that the Australian market continues to adopt emerging security trends to and practices.

Legislative Framework

While Microsoft welcomes the introduction of the Digital Identity Legislation, we have comments on a number of aspects of the legislative framework. Microsoft welcomes the interoperability obligation in s. 33 of the Bill. By ensuring participating relying parties provide choice of accredited identity service providers, we believe individuals have greater control over their own data, which in the long term will build trust in the use of digital identities. Noting that Government is often seen as a policy leader we would make the following points:

1. Holding digital identity information outside of Australia

We note s.31 of the Bill provides the power for the TDI Rules to prohibit the (either absolutely or unless particular circumstances are met or conditions are complied with) the holding, storing, handling or transferring of such information outside Australia.

Microsoft believes there are many important use cases that often require handling or transferring data outside of Australia. Although the government can write these data requirements into legislation, we believe that doing so does not increase security and has the potential to stifle innovation. To that end, we believe legislative prohibitions should be avoided where possible.

While under traditional IT and data centre models data locality is seen as a security control, hyper-scale cloud providers such as Microsoft can provide significant cyber security improvements regardless of the physical location of the data, this ability to host identities securely regardless of geoboundry enables new use-cases on a global scale without compromising security.

2. Additional Privacy safeguards

Microsoft believes that privacy is a fundamental human right. As people live more of their lives online and become more dependent on technology, it is increasingly important to protect that fundamental right.

Microsoft also believes that privacy is the foundation for trust. When using technology, trust is created when people are confident that their personal data is safe and they have a clear understanding of how and why it is used.

Microsoft welcomes the inclusion of additional privacy safeguards in the TDIF. We believe the following provisions enshrine greater privacy protections and will help to build trust in the TDIF: the deletion of biometric information of individuals; a prohibition on data profiling; and ensuring digital identity information must not be used for prohibited enforcement purposes.

In keeping with good privacy practices, we believe providers should retain only necessary data, for the shortest time possible.

3. The use of framework legislation to enable disallowable rules

Microsoft is concerned with the trend of implementing high-level overarching framework legislation that underpins codes, rules and instruments. We do not believe that this has led to the best possible public policy outcomes and reduces accountability and review of Government power. The ability to greatly increase the scope and requirements of this legislation through a disallowable instrument could lead to unforeseen requirements and use cases.

Microsoft strongly supports a legislative approach that is targeted, proportional and uses rule making processes exclusively to ensure that legislation remains current with technological development.

Trusted Digital Identity Framework (TDIF) accreditation rules

In reviewing the TDIF accreditation rules, we want to highlight some of the challenges with reporting requirements. The accreditation rules state that accredited entities must produce an annual report at least once a year "in an open and accessible manner a transparency report that includes information on requests by an enforcement body or the Oversight Authority for access to digital identity information held by the entity in connection with the services for which the entity is accredited to provide."

In some instances, there are restrictions on the types of information that providers can disclose. For instance, national security legislation prohibits providers from disclosing certain types of requests from law enforcement agencies. We would encourage the DTA to consider these limitations when assessing accredited entities' ongoing compliance with the TDIF accreditation rules.

Future uses of TDI and other Government reform processes

We encourage the DTA to consider the implementation of the TDIF in the context of other government consultations and reviews. As mentioned above, Microsoft is concerned with the trend of implementing high-level overarching framework legislation that underpins codes, rules and instruments. For instance, the TDIF provides the Minister the power to make changes to the TDI rules without consultation. Given the Government's role as a technology leader in policy and standards development, we strongly encourage the DTA to continue to ensure the TDIF is aligned with other providers as identity practices evolve.

We also note that some aspects of the TDIF may conflict with other government reforms. For instance, the data encryption requirement under the TDIF sits in contrast with the data access requirements in the recent *Online Safety (Basic Online Safety Expectations) Determination 2021*, which requires providers of encrypted services to "take reasonable steps to develop and implement processes to detect and address material or activity on the service that is or may be unlawful or harmful."

Further, it is not yet clear how the TDI will interact with the *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021*, which requires age verification for the use of social media services. We would encourage the government to ensure that the future uses of the TDI maintain the privacy of individuals and do not impede the rights of individuals.

Conclusion

Microsoft thanks the DTA for the opportunity to provide comment on the TDIF framework and accreditation rules. When the technical standards are released we would be happy to meet with officials to discuss the standards, if required.