27 October 2021

Digital Transformation Agency
Via email to digitalidentity@dta.gov.au

Re: Cuscal response to the Consultation on Australia's digital identity legislation (Phase 3)

Cuscal Limited (Cuscal) appreciates the opportunity to respond to the above consultation paper issued by the Digital Transformation agency.

Background to Cuscal

For over 40 years, Cuscal has leveraged our assets, licensing, and connectivity to provide intermediary and principal outsourcing activities on behalf of our clients. We are an end-to-end payments specialist that services more than 100 established and challenger brand clients within Australia's financial system, including the majority of the mutual banking sector, and a growing number of FinTech and 'PayTech' enterprises. We enable their market connectivity so they may provide innovative products, business models, and drive improved customer outcomes.

We are an Authorised Deposit-taking Institution (ADI), the holder of an Australian Financial Services Licence, and an Australian Credit Licence for Securitisation purposes. Cuscal has Board representation with eftpos, NPPA, Australian Payments Network and participates in numerous industry committees. We are also the founder of 86400 (www.86400.com.au), a fully licenced mobile-led digitized bank, acquired by National Australia Bank.

The services that we provide to our client institutions include: card scheme sponsorship for issuing and acquiring, payment card issuing, card production services, digital banking applications, and access to domestic payment services using direct entry, BPAY and the New Payments Platform (NPP). We also act as settlement agent for many of our clients through our Exchange Settlement Account with the Reserve Bank of Australia (RBA).

As a fully PCI-DSS accredited ADI, Cuscal is uniquely placed to provide secure and robust capabilities that facilitate access to markets that would otherwise be beyond the reach of some organisations.

Cuscal plays a key role as a CDR intermediary in the Open banking ecosystem. To help our clients benefit from the CDR, while minimising their cost and risks, Cuscal is investing in a Collaborative Data Exchange. This technology platform helps CDR participants manage compliance obligations, provides consumers with best practise simplicity while remaining in control over the data they consent to share and a better secure digital experience.

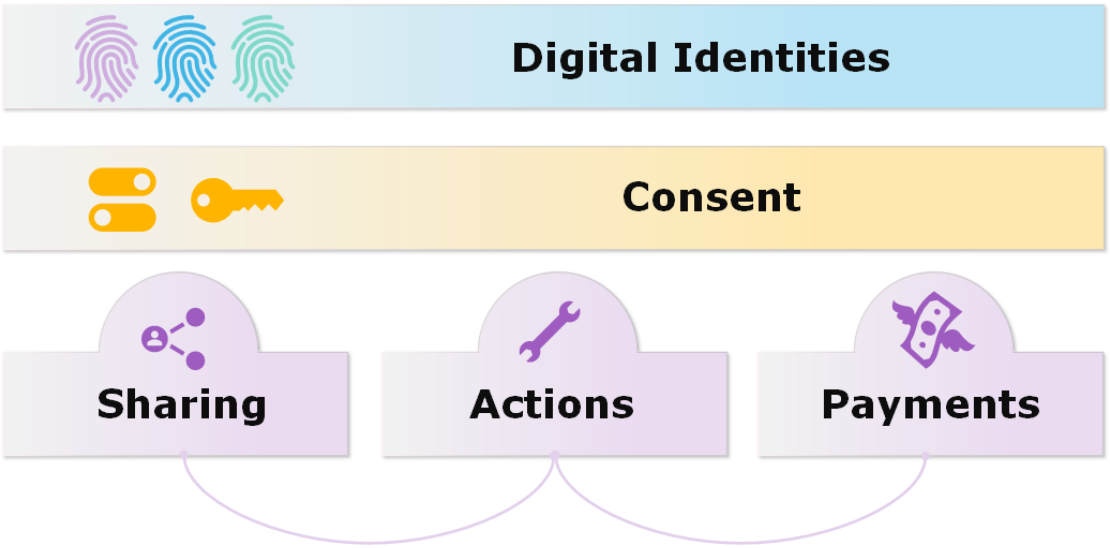
For further information on Cuscal and our services please refer to our website at https://www.cuscalpayments.com.au/

We welcome the introduction of the Digital identity legislation. We also believe it will emphasize Australia's position as a leader in embracing a strong digital identity framework that many countries have failed to achieve. The draft legislation has undergone multiple rounds of public consultations and Cuscal is aligned with the Privacy and consumer protections that are enshrined in the legislation. The recent developments in other areas of the digital economy such as Consumer Data right (CDR) has not been extensively reflected in the consultations. The CDR and the Digital Identity bill are complementary to each other for the development of a range of services that Australians can benefit from the comfort of their homes.

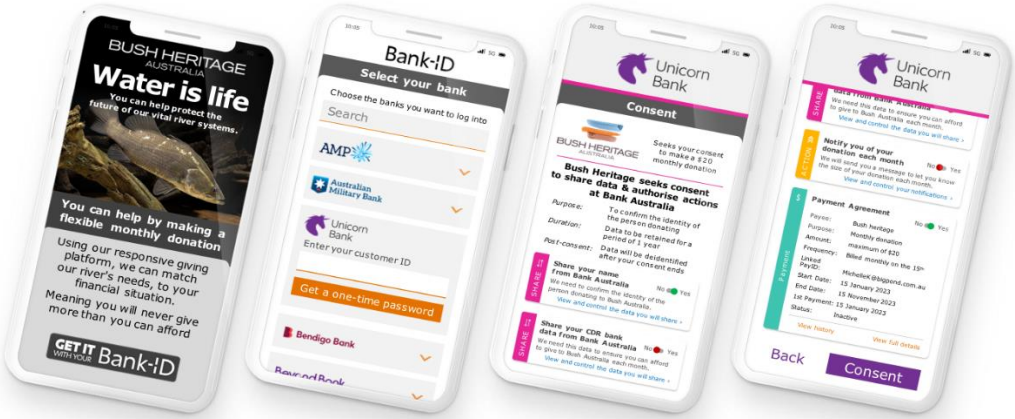
Our main focus in providing this response is to ensure government initiatives in digital identification are not fragmented and considers other regulatory programs that relies on digital identity. The digital identity is a whole of economy initiative and is instrumental in achieving the future directions of CDR.

Any cross overs and synergies that could be attained by considering these initiatives as interoperable is highly recommended. As the CDR is incrementally moving through the various sectors and the regulatory framework for the Australian payment systems is evolving, Cuscal believes that digital identity holds the key to create solutions that will meet value propositions for its users.

A visual representation of how Cuscal perceives digital identity to integrate with Consumer data right and unlock the potential of a fully digitized economy.



Digital Identity unlocks data sharing, actions & payments



Enabling Australians with a secure and convenient way to prove who they are online is critical for the success of such regimes. The CDR and digital identity systems are enablers and drivers of building trust and positive outcomes for consumers in a modernized digitized economy.

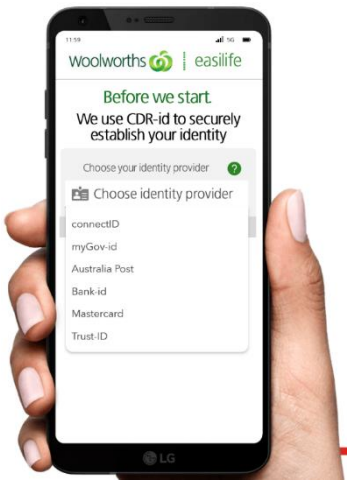
A. The aligned policy objectives between CDR and Trusted digital identity systems should drive the rules and accreditation process:

Digital Identity System policy objectives	Consumer Data right policy objectives
Key outcome is to deliver a broad range of benefits to consumers, business users, service providers and the broader economy	Consumer focussed and convenient experience for users
Restricted attribute defined	Inclusive for Vulnerable consumers
Greater participation from the state and territory governments and the private sector	Competitive and viable channel
Enshrine in law privacy and consumer protections to build confidence and trust in the government led digital identity system	Privacy & Security protections, to inspire trust and confidence
Establish a strong governance and regulatory regime	Government intervention where the private sector cannot be expected to otherwise provide outcomes

B. Recommendations on the current draft legislation to help achieve the policy objectives:

1. A uniform approach towards legislations trying to achieve similar objectives must be considered to reduce duplication of obligations, cost of participation, and provide clarity for regulated entities and the community. The CDR has developed accredited models for participation in the highly regulated CDR regime to enable a digitized economy. Enforcing another accreditation model does not add any increased value however it undermines the viability of similar regulated accreditation models passed by the Australian government in the interests of consumers. The objectives of CDR and that of the digital identity have synergies for secure data sharing and as such Cuscal proposes that the legislation should enable entities accredited by other government agencies such as ACCC (Australian competition and consumer commission) to participate and be recognized by providing a reduced scope assurance under the Digital Identity system.

   The CDR trust mark and Digital Identity is integrated in the below visuals to showcase how use cases may be developed in the future.



2. The CDR establishes a strict privacy framework for its participants to comply. In addition to the 13 Privacy safeguards that is required by the Accredited data recipients the CDR is established on a Data minimization principle. This means it limits the data collected to a specific purpose that is supplemented by an express consumer consent. There are clearly defined CDR rules related to Data retention and de-identification requirements to further secure the safety of the information held by accredited entities. Any data attached to CDR data is classified as CDR data thereby achieving a higher standard of security and protection for consumers. The digital identity legislation does not adequately cover non-APP entities under Part 2-Privacy of the draft bill and there is an opportunity to apply the privacy safeguards introduced by Office of the Australian Information commissioner (OAIC) to add additional trust and security in the system.

3. As the CDR expands and a range of functions are introduced strong authentication will be required to perform higher risk activities. It is acknowledged by both governments and industry participants that provision of identity is critical to implement a number of customer centric use cases. Initiating actions through CDR requires secure digital identity services. The Digital Identity accreditation model is well considered to support different identity services and should be interoperable with CDR and Payments accreditation models. Exclusions such as in the case of accredited credential providers may restrict use cases for consumers where credential can be applied for seeking customized services.

4. Digital Identity is evolving, and the accreditation should not be bound to TDIF specifically, which should be one of several digital identity frameworks designated by the minister. TDIF may not be fit for all uses that digital identity will be used for and consumers should have a free choice of digital identity frameworks.

5. The CDR legislation has adopted a tiered accredited that has obligation on accredited parties to protect consumer data, meet the Privacy safeguards, defined liability model, and Insurance requirements for redress. The TDIF accreditation has similar requirements and there is an opportunity here for businesses to take advantage of existing systems to comply without having to draw in more investments and incur additional compliance costs.

6. The consumer consent is termed as the bedrock of the CDR regime as it puts the consumer in control of their data with respect to whom they share and the period of sharing. It supports a transparent consent management process and achieves consumer experience via the dashboard functionality to put the consumer in control of their data. Leveraging CDR data standards setting capabilities to encourage consistent standards across the data economy will create efficiency and ensure consumer participation is simple across the various digital services.

7. The onboarding and accreditation process between CDR and Digital identity systems should be streamlined for entities. For e.g., the requirement under section 5 of the TDI rules around "fit and proper person" should be aligned with CDR as they are eligibility criteria for providing regulated services. The TDI rules incorporates additional conditions that may not be relevant in all scenarios such as past decisions regarding revocation and suspensions.

8. Adopting the technical standards set under the CDR by the Data standards body will help consumers with a consistent data sharing experience. This will also help remove any technical barriers for entities to participate in the digital identity systems. The consumer experience standards have been defined and built for consumer dashboards under the CDR. There is an opportunity to collaborate with the Data standards body that has widely consulted on user experience with industry and regulators. This approach will also help align complex scenarios such as interacting with Power of attorneys, legal guardians, secondary users etc.

9. The dispute resolution mechanism is not defined under the TDI rules and the accreditation framework. However, under the Consumer data right CDR participants are required to have an internal and external dispute mechanism as a requirement for accreditation. Since the objective of the digital identity system is to build consumer trust and transparency economy wide it should consider the need for a streamlined dispute management mechanism in place with complaints reporting requirements to the oversight authority.

10. The CDR rules requires entities applying accreditation to provide assurance certifications such as ASAE 3150 and other approved industry certifications that provides assurance on Information security standards. The cost of maintaining compliance across various digital services can be minimized for entities where such industry approved certifications are recognized under the legislations. The TDIF accreditation rules are granular in nature and could lead to excessive complexity and cost creating barriers for participation and harm consumer outcomes.

11. Digital Identity is moving internationally to models self-sovereign identity, and the proposed regulation does not recognise this. Otherwise, Australia many be left behind, making the Digital Economy 2030 goals harder to achieve.

The productivity commission report on growing the digital economy in Australia and New Zealand suggests the need to recognize digital identity services in both these jurisdictions to help streamline online Trans-tasman interactions. The New Zealand government in July 2021 agreed to establish a consumer data right framework that is expected to work alongside the Digital identity trust framework. New Zealand is adopting the Australian CDR model to build their consumer data right framework. There are considerable benefits with respect to interoperability should we follow the same path with respect to recognizing CDR under the digital identity legislation making it simpler for businesses and effective for consumers.

Cuscal believes there is greater efficiencies that can be achieved by setting a common data sharing practise. The standardization of rules and technical standards across consumer data right and the digital identity system will enable common service providers in the data supply chain to deliver better consumer experience. If we can be of any further assistance in the interim, please feel free to contact me at kmckenna@cuscal.com.au or (02) 8299 9000.

Yours sincerely,

Kieran McKenna

Chief Risk Officer