Australian Banking Association

SUBMISSION REGARDING THE DIGITAL ID BILL AND RULES 2023

DEPARTMENT OF FINANCE

10 October 2023

Australian Banking Association

Key Recommendations

The Australian Banking Association (ABA) welcomes the Government's plan to facilitate widespread adoption of Digital ID use in Australia through the implementation of a voluntary Accreditation Scheme (**the Scheme**) which evolves the existing Trusted Digital Identify Framework (**TDIF**).

A well designed and implemented Digital ID scheme will be a cornerstone economic reform that will deliver customers added security, protection, and peace of mind in the knowledge that they will have the ability to provide proof of identity without the risks associated with the loss of identity papers. This reform will enhance compliance efficiency and effectiveness, helping reduce cyber security risk. Significantly, it will offer a safe and simple consumer banking experience.

Scheme governance:

- We strongly recommend a simplified governance model with a single point of accountability for the scheme in total to the Minister.
- We recommend the government should consider ways to maintain appropriate oversight over the standards setter given the link to broader policy objectives around the need to ensure national security and cyber security.

Scheme uptake:

- We support a proactive approach by the Scheme's operators (the collective of the six governing bodies) to encourage and facilitate adoption of Digital IDs.
- We recommend the establishment of collaborative public-private 'task forces' as the most appropriate mechanism for achieving this outcome.
- We strongly recommend the Department of Finance consider mechanisms for providing assurance to banking relying parties that the Scheme is an acceptable mechanism for fulfilling their KYC obligations.
- We support a voluntary Scheme that permits Digital ID services to be delivered outside of the scheme.

Scheme phasing:

- We recommend that Phase 3 'Use their myGovID to set up a new bank account' should be moved to a new Phase 1(b) utilising the task force approach recommended in section 2 above.
- We recommend the Government consider the balance between maturing the system and ensuring a competitive level-playing field where private Digital IDs can compete with government Digital IDs. Consideration of this balance may require bringing the proposed phasing of private Digital ID issuers forward, when Treasury deems it appropriate.
- We encourage the publication of timelines against each phase as soon as possible to enable industry alignment with delivery timelines.

[redacted]

About the ABA

The Australian Banking Association advocates for a strong, competitive and innovative banking industry that delivers excellent and equitable outcomes for customers. We promote and encourage policies that improve banking services for all Australians, through advocacy, research, policy expertise and thought leadership.

Australian Banking Association

Australian Banking Association submission regarding the Digital ID Bill 2023

The Australian Banking Association (ABA) welcomes the Government's plan to facilitate widespread adoption of Digital ID use in Australia through the implementation of a voluntary Accreditation Scheme (**the Scheme**) which evolves the existing Trusted Digital Identify Framework (**TDIF**).

Australian bank customers have overwhelmingly shifted to digital banking with 98.9% of total transactions now being made via the online channel and banking apps. From FY2019 through FY 2022 online banking and app use increased by 26%. Further, chatbot interactions an emergent and growing channel, having seen a 559% increase in customer use between FY2019 and FY 2022.[1] All this to say that banking is digitising at pace which requires related functions, such as customer identification processes, to be similarly digitised.

Therefore, a well designed and implemented Digital ID scheme will be a cornerstone economic reform that will deliver customers added security, protection, and peace of mind in the knowledge that they will have the ability to provide proof of identity without the risks associated with the loss of identity papers. This reform will enhance compliance efficiency and effectiveness, helping reduce cyber security risk. Significantly, it will offer a safe and simple consumer banking experience.

The ABA makes the following recommendations to enable the efficient management and expedient take-up of the Digital ID Scheme. Thematically, our recommendations pertain to Scheme governance, uptake, and phasing.

Theme 1: Scheme governance

1. Governance structure

We note with concern the proposed distributed governance structure for the Scheme. This includes six government departments or agencies undertaking 8 core functions (Box 1). The governance structure lays the foundations for success of the Scheme. It is critical for this framework to be set right from the Scheme's inception. Our considerations on the proposed governance structure are based on the banking sector's experience with the Consumer Data Right which is briefly summarised in Box 2. The ABA view is that the multi-player distributed governance model proposed for the Digital ID scheme will be subject to the same issues as the CDR's governance structure if the Government does not learn from past mistakes.

Distributed Governance of the Scheme

1. ATO
    a. MyGov ID provider
    b. Attribute service provider, relationship authorisation manager
2. Services Australia
    a. Exchange facilitating information flow between MyGovID and the relying parties.
    b. Administer/operate government digital IDs, system integrity and performance.
3. ACCC – ID regulator.
4. OAIC – privacy regulator.
5. Department of Finance – Support the Minister in managing the policy framework including the rules.
6. Data standards chair – sets the technical and data standards.

Box 1: The Scheme's proposed governance structure

[1] ABA, 2023, 'Bank on It: Customer Trends 2023' pages 12-15 (link)

A distributed governance structure implies a 'set and forget' approach to the Scheme as distinct from one which is to be actively managed. We question the ability of such a governance model to deliver on the Scheme's objectives. Whilst we note that this is government's preferred model, we strongly recommend a simplified governance model with a single point of accountability for the Scheme to the Minister.

We note, through engagement with the Department of Finance, that the governance structure is considered final. If a revision cannot be made, we strongly recommend that the government consider ways to maintain appropriate oversight over the standards setter given the link to broader policy objectives around the need to ensure national security and cyber security (refer to Box 2 for context from the CDR).

We urge incorporation of a mechanism for regular communication between the six government departments and agencies to facilitate early resolution of implementation issues, ongoing operational issues, responses to critical incidents, as well as strategic direction setting. This matter is expanded in Section 2.

ABA observations on the governance arrangements of the Consumer Data Right
In respect to the Consumer Data Right (CDR), the delineation of responsibility between the Department of Treasury (Treasury) as the Rule setter and the Data Standards Body (DSB) as the standards setter has not led to an optimal deployment of the CDR.

Broadly, there are two types of standards setting work undertaken by the DSB: (a) to ensure standards reflect strong security settings and that those settings are constantly maintained and upgraded; (b) to develop standards that provide the blueprint for how the CDR Rules are to be technically interpreted and deployed.
Whilst an argument can be made for an independent standard setter for security requirements, we are less supportive of the independence of the DSB under its second function. This position is based on the observation that many changes to the CDR standards are often put forward which are unaligned to the strategic policy direction of the CDR. Such changes are enabled because Treasury does not have direct responsibility or a sign-off responsibility. Two current examples are the DSBs considerations for tightening a 'Non-Functional Requirement' response time on requests from Accredited Data Recipients (ADRs) to 1 second and including non-digitised Pass Book accounts on the list of products for inclusion on the CDR.

The DSB is not required to undertake consultations in the form of per government agencies, this includes running options for change through GitHub, not undertaking a cost-benefit analysis of the proposed change, and not canvassing alternative options for managing the issue raised by ADRs (the 1 second NFR is an example). Further, the independence of the DSB means that Treasury is not formally able to question the need for such changes.

Box 2: CDR Governance structure

Finally, we note that reference is made to a 'Code' without further explanation. We seek clarity in respect to oversight of this Code.

Theme 2: Scheme uptake

2. Proactive approach to driving uptake

The ABA notes that the success of the Scheme is dependent on ongoing strategic oversight and direction setting by the Government. The ABA defines success as the extent of uptake of the Scheme.

Australian Banking Association

Therefore, the ABA supports a proactive approach by the Scheme's operators (which presently is the collective of the six governing bodies) to encourage and facilitate adoption of Digital IDs.

We recommend the establishment of collaborative public-private 'task forces' as the most appropriate mechanism for achieving this outcome, subject to competition considerations. The task forces would involve the relevant sectoral regulators and industry and will focus on driving adoption for specific use cases. In terms of the banking sector, we envisage two use cases: (1) AUSTRAC and industry working together on how to best utilise a Digital ID for Know Your Customer (**KYC**) and/or (2) the Australian Tax Office (**ATO**) and industry working together on how best to utilise a Digital ID for income verification. Additionally, Digital ID and KYC would be beneficial across the economy where it is used, for example mobile plan account opening in telecommunications.

3. Consequential amendments to the Anti-Money Laundering and Counter-Terrorism Financing Act 2006

The application of Digital ID in fulfilling KYC requirements is perhaps the Scheme's single most significant use case. However, it is unclear whether the Scheme will meet the requirements of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (**the AML-CTF Act**) and the Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1) **(the AML-CTF Rules).**

Given the significance of KYC to the take up of the Scheme, the ABA strongly recommends the Department of Finance consider mechanisms for providing assurance to banking relying parties that the Scheme will meet KYC obligations. This may include whether consequential amendments to the AML-CTF Act are needed and/or regulatory guidance by AUSTRAC in relying on Digital ID for KYC purposes.

4. Data settings to enable uptake

There are some potential impediments to the uptake of the AGDIS scheme.

The first impediment relates to the handling of AGDIS data offshore. There may be unintended consequences for data security as many large cloud service providers are located offshore; these providers often have stronger data and cyber security protocols. The draft provision may unintentionally prohibit entities from accessing these more secure services, ultimately increasing the risk of identity information being compromised. In addition to this, banks may have overseas-based employees performing roles such as investigating higher risk transactions involving failed matches. A prohibition on the transfer or handling of Digital ID information outside Australia may result in inefficiencies and suboptimal customer experiences.

The ABA notes that the draft Rules enable the Minster to grant an exemption to the requirement to hold, store handle or transfer data onshore. ABA recommends that legislation enable the Minister to grant class exemption in appropriate cases to improve efficiency of scheme administration and provide greater consistency across the scheme. ABA notes that for APRA-regulated financial institutions, CPS 230 provides a useful apparatus by which the Government can be assured of the security and oversight of offshore services.

The second impediment relates to compliance with recording keeping requirements including data destruction. The ABA notes that participants may have reasons to hold data for a longer period, for example, AML reporting entities may make risk-based decisions to hold some data for longer than 7 years to support AML decision-making and for record keeping purposes.

5. Voluntary approach to the Scheme

The ABA thanks the Department of Finance for their clarifications in respect to the voluntary nature of the Scheme. On the basis of responses provided by the Department of Finance at the *Digital ID Legislation Consultation webinar and live Q and A session* on 28 September 2023, our understanding for accreditation of private sector Digital IDs is as follows:

- There are two limbs to the provision of services under the Digital ID Scheme: the first pertains to whether the entity is an accredited entity (such as a bank); the second relates to whether the accredited entity is providing accredited services. This implies that accredited entities can provide both accredited Digital ID services and Digital ID services that fall outside the Scheme.
    - We are seeking clarification on whether the above implication is accurate. If so, we recommend making this (being the scope of accreditation) clearer as one of the only references to this appears to be section 31 of the Bill.
- The Trust mark is to be applied to the accredited service and therefore can only be displayed when an accredited service is being undertaken.
- Entities are encouraged to make clear the extent of their data environment to enable a clear delineation of the accredited service as distinct from other Digital ID services.
- Trust marks are clearly displayed in relation to the accredited services. If providing both types of services need to show which is accredited and which is not accredited – make it clear to the customer.
- This is a voluntary accreditation scheme, and the government is not seeking to stop innovation in digital ID services from taking place outside of the Scheme.

On this basis, the ABA supports the nature of the voluntary approach to the Scheme.

6. Related government reviews

ABA believes that the passage of the Digital ID Bill is a necessary but not sufficient step for the development and widespread adoption of a productivity and cyber security enhancing digital ID ecosystem. Other steps that need to be taken include:

- An alignment of the government's revisions to the Privacy Act 1988 (Cth), particularly the review agreed to in principle by the government in Proposal 21.6. This review is critical given that through the rollout of Digital ID, entities may now be relying on a centrally held digital records rather than collecting and retaining the underlying identity documents containing personal information.

    Without consequential and simultaneous privacy reform, uptake by the private sector will be challenged. Under retention laws, businesses have increasingly been required to capture, process and store Australians' personal and sensitive information. This has been partly exacerbated by complex legislative requirements that mandate what type of information can or must be collected, for how long it must be held and when it can be destroyed.

    Further, such lack of alignment will support common interpretation of privacy obligations. At present, some privacy obligations receive differing/ inconsistent treatment across the economy. One such example is the approach to accepting digital drivers' licences for identification purposes. Consideration should be given as to how the private sector can attest and timestamp receipt of a digital driver's licence, within a retention framework calibrated for the digital world.

- Proactive review of other legislation imposing identity or credential verification obligations to ensure that they facilitate use of a digital ID.

- Alignment with the Modernising Business Communications strategy of the Department of Treasury to ensure that the digitisation of business communications can adopt the Scheme.

Theme 3: Scheme phasing

7. Proposed sequencing of launch phases

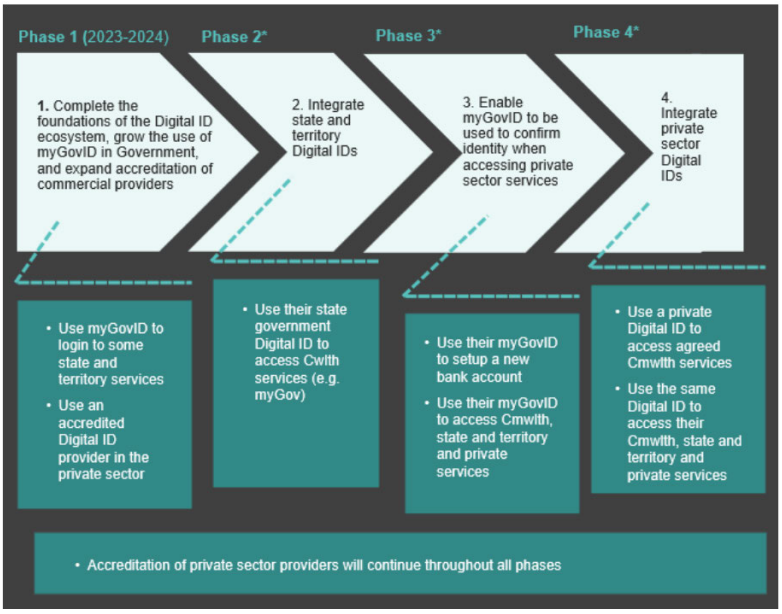

Figure 1: Proposed Phases of the Scheme, from Your Guide to the Digital ID Legislation and Digital ID Rules p 25

Whilst we appreciate an ordered and sequenced approach to the roll out of the Scheme, we consider the proposed phasing will not encourage early and large volume take up. Early and large volume uptake is important to the Scheme's success and its future development trajectory. It will also confirm the trustworthiness of the Scheme thereby encouraging further uptake. As an example, we note that the lack of prioritising key use cases for CDR, in part has resulted in its low uptake by Australian consumers.

Therefore, whilst the ABA encourages the Government to progress as rapidly as possible through the proposed four phases of the rollout, we strongly recommend the following:

First, that Phase 3 'Use their myGovID to set up a new bank account' should be moved to a new Phase 1(b) utilising the task force approach recommended in section 2 above.

Second, whilst the security of and trust in the Digital ID ecosystem is of the utmost importance, the ABA recommends the Government consider the balance between maturing the Digital ID ecosystem and ensuring a competitive level playing field where private Digital IDs can compete with government Digital IDs. Consideration of this balance may require bringing the proposed phasing of private Digital ID issuers forward, when Treasury deems it appropriate.

Third, we encourage the publication of timelines against each phase as soon as possible to enable industry alignment with delivery timelines.