Feedback on the proposed Digital ID legislation

Introduction

The recent wide scale disclosures of people's personal information has highlighted the need for changes to the way we identify ourselves online. The status quo is not working and the problem will continue to get worse as more of our day to day interactions with Government, businesses and other citizens take place online.

The current approach is ad-hoc and inconsistent and relies on each organisation establishing the identity of people interacting with their online services. Typically this involves people providing copies of some physical documents (or information from the documents) to establish their identity when setting up an account and then subsequently providing the account username and password each time they interact with the service to 'prove' that the person interacting with the service is the same person who originally created the account.

This is problematic in several ways:

- People are asked to provide copies of their sensitive documents to many different organisations with little information about how their information will be used. It is difficult to determine whether the service asking for me to upload my drivers license is a legitimate and trustworthy organisation or someone who is impersonating a legitimate service. The more we normalise the process of providing copies of sensitive personal documents the worse this problem becomes.
- Many different organisations are all trying to do the same thing: determine identity attributes of the people who are interacting with their services and not all of them are well equiped to do this.

A well regulated national system could address these problems by providing a way for organisations to verify identity attributes in a consistent, trustworthy way so that:

- people no longer need to provide their sensitive information to multiple different organisations, and
- those organisations don't need to be responsible for establishing people's identity and securely handling the sensitive information.

The goal of an economy wide system to facilitate organisations verifying information about the people interacting with their services worthwhile. If implemented well the result could be that people have:

- greater privacy,
- more trust in the services they interact with, and
- more protection against people stealing their personal information.

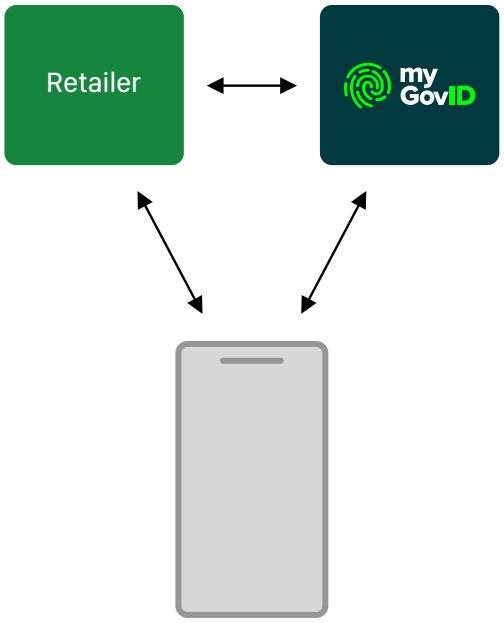
A missed opportunity

However, the legislation in its current form is too focussed on a Digital ID based on signing in and fails to recognise better alternatives such as verifiable credentials.

Systems based on signing in and those based on verifiable credentials are both seeking to solve the same problem. Consider the example of a retailer that sells groceries and alcohol. Their problem is that they only want to sell alcohol to people over a certain age so they need a way to verify the age of the person who is using their app.

An approach based on signing in

In the approach considered by the proposed Digital ID legislation a customer would need to establish an account with an approved identity provider (such as myGov ID) and then sign in to the retailer's app using their myGov ID. As part of this sign in process the retailer would receive some claims about the person's identity.



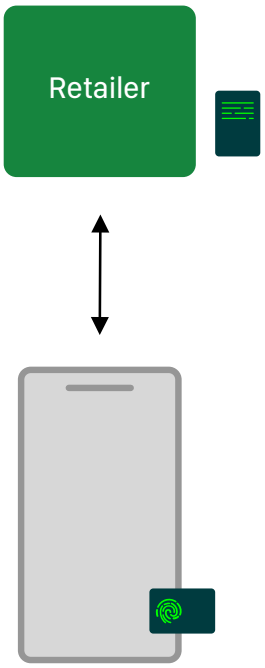
This approach starts with a person launching the retailer's app and choosing some things they'd like to buy.

1. When they're ready to make the purchase the app asks them to sign in.
2. The app directs them to myGovID where they sign in with their existing myGovID account and then they're redirected back to the app with an authentication token issued by myGov that contains claims about their identity (including their name and potentially date of birth).
3. The app presents the authentication token to the retailer who can verify that it is valid and extract the claims about the person's identity.

4. **The retailer would receive the person's name and date of birth** and could then determine whether or not to allow the purchase of alcohol.
5. **myGov ID would receive meta-data about the sign-in** including the details of which myGov ID account was signing in to which retailer's app.

An approach based on Verifiable Credentials

In an alternative approach based on verifiable credentials the person using the retailer's app wouldn't necessarily need an account at all. They would store a Government issued identity document in a secure digital wallet on their phone and present information from this identity document to the retailer's app.



This approach also starts with a person launching the retailer's app and choosing some things they'd like to buy.

1. When they're ready to make their purchase the app asks them verify that they're old enough to purchase alcohol.
2. The app asks the operating system to prompt the user for permission to access information from their verified identity document. If the user agrees then the operating system provides the app with information that they're over the age of 18. This information is cryptographically signed by the trusted authority.
3. The app sends the signed information to the retailer's service who can then verify that it was signed by the trusted authority (using the authority's public cryptographic information that they'd previously obtained).
4. **The retailer would not receive the person's name or date of birth** but would only receive information **that the person is over the age of 18**.
5. **The trusted authority would not be involved in the individual interaction at all** so would **not receive any information about which person presented their information to which retailer**.

Recommendations

The establishment of an economy-wide trusted system to facilitate organisations verifying information about the people interacting with their services is worthwhile and could have considerable benefits to people's privacy and their confidence to interact with services online.

The current proposed legislation is too narrowly focussed on a model that requires people to sign in and fails to consider alternative ways for organisations to verify attributes about a person without actually needing to know their identity.

The widespread adoption of any Digital ID will be influenced not only by the legislation but also by how well the technology is implemented on the devices people use every day. For example, Apple have a Verify With Wallet API[1] that offers a simple way for people to present apps with verified information in a way that is very similar to Apple Pay. If 'showing your Digital ID' was as simple as making a payment with Apple Pay then many more people will adopt it.

Whilst legislation can be amended in the future, the need to change legislation can be seen as a barrier that can prevent future improvements to systems. In its current form the proposed legislation would not support the use of verifiable credentials or APIs like Apple's Verify With Wallet and I fear we'd be stuck with a system that is both more difficult to use and less private.

Consider whether the proposed legislation could be changed before it is introduced to accommodate different ways for organisations to verify information about the people who are interacting with their services.

Consider a pilot of the use of verifiable credentials in one jurisdiction to inform the future design of the national system. A small jurisdiction like the ACT might be a good place to try out something like Apple's Verify With Wallet.

Thank you for the opportunity to provide feedback on the proposed legislation.

Regards,

Jake MacMullin
Managing Director
Stripy Sock Pty Ltd

[1] https://developer.apple.com/wallet/get-started-with-verify-with-wallet/