# Digital Credentials

Cogito Digital Credentials

## What are Digital Credentials?

Digital credentials are the digital equivalent of a person's signature on a piece of paper. They can also act as a digital version of identity documents issued by trusted parties such as government organisations. They are used to establish a person's privileges, characteristics and identity in the electronic world and can be used to interact with that electronic world.

Physical identity credentials are coming under increasing pressure from counterfeiting and other fraudulent use. They also cannot be used easily by electronic devices such as a mobile phones and personal computers. Digital credentials resolve some of these issues.

> *"Physical identity credentials are coming under increasing pressure from counterfeiting and other fraudulent use. Digital credentials resolve some of these issues."*

> *"The Australian department of defence is now rolling out a card to a selected group of users."*

> *"Federation based on the username password model increases this vulnerability across multiple systems."*

## What are their uses and capabilities

Digital credentials are now being integrated with many of the traditional paper documents to increase their capabilities and to strengthen the anti-fraud qualities of the documentation. An example is the new Australian Passport and the new Queensland drivers' licence, both of which implement digital credentials. This allows the real time checking of the credential and the information associated with that credential with a central database. In the example of the Drivers licence, it allows information to be checked such as if the licence has been reported as lost or stolen and if the driver has had his/her licence suspended, just by waving the licence over a card reader.

## What are the risks and issues?

Traditionally, a user has entered a username and password to enter an electronic system. There are several problems with this solution. Firstly, the traditional authentication model of username and password means a single user must have multiple accounts on disparate systems. Federation can assist here but relies on the trust between organisations and can increase the chance of compromise. The use of traditional electronic authentication methods (such as username password) also introduces a single point of vulnerability for all users. That is, if the authentication database is compromised, the attacker has every user that can access the system. Federation based on the username password model increases this vulnerability across multiple systems.

## What are their uses and capabilities?

The new Australian passport has an embedded chip, which is currently only used as an anti-fraud device, this could be changed in the future to allow the passport to expand it's capabilities.

Centrelink (now part of DHS), have implemented digital credentials for logical access to their network (computer logon). This could be expanded to their physical access solution with further use of digital credentials for other forms of electronic transactions (such as email and signing of electronic forms).

The Australian Department of Defence is now rolling out a card to a selected group of users with the following capabilities:

- Ability to be used for logical access (allows computer logon)
- Ability to be used for physical access to sites and facilities (supporting backwards compatibility with the current solution door and barrier solution, but it is working towards a more secure physical access solution)
- Electronic signature of email
- Electronic signature of forms
- Electronic signature of financial transactions
- Electronic signature of approvals
- Access to web site portals
- Access to web-based systems