Fact Sheet

Cogito Group

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. Digital credentials 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.

What Are Their Uses and Capabilities?

Digital credentials are now being integrated with many traditional, paper documents to increase their capability and strengthen the anti-fraud qualities of the documentation. For example, both the new Australian Passport and Queensland drivers' licence implement digital credentials. This allows real time checking of credentials and the information associated with those credentials from a central database. The new Queensland drivers licence allows information to be checked, such as whether the licence has been reported as lost or stolen, and if the driver has had their licence suspended, by simply waving the licence over a card reader.

What Are the Risks and Issues?

Traditionally, a user presents a username and password to enter an electronic system, however there are several problems with this solution. Firstly, the traditional authentication model of usernames and passwords requires a single user to 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 these traditional electronic authentication methods also introduces a single point of vulnerability for all users. That is, if the authentication database is compromised, the attacker has access to every user's account on that system. Federation, based on the username password model, increases this vulnerability across multiple systems.

Digital Credentials

Fact Sheet

What Are Their Uses and Capabilities?

The new Australian passport has an embedded chip, currently only used as an anti-fraud device, but could be changed in the future to allow the passport to expand its 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 solutions, with further use of digital credentials for other forms of electronic transactions such as email and the signing of electronic forms.

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

- Ability to be used for logical access.
- 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.

About Cogito Group

Cogito Group is an award-winning, Australian owned and operated ICT company, specialising in authentication, cloud security, identity management and data protection. Cogito Group protect the authentication methods used to access information through the use of Identity and other security technologies. Cogito Group protect data not only from unauthorised access and disclosure, but also from being altered by an unauthorised third party or a trusted insider with malicious intent. This assists in the detection and prevention of fraud or other malicious activities by third parties or trusted insiders.