Fact Sheet

Cogito Group

Card Management Systems

What is a Card Management System?

Card Management Systems (CMS) manage the lifecycle of Smartcards. Smartcards are credit card sized cards, with a chip that can be used to provide logical network access to computer systems, physical access to facilities and to secure and authenticate digital transactions. CMS manage such cards from the production stage, through the card's useful life, and manages their retirement from use. They do this with a high level of auditing and security.

What are the Benefits?

In a medium to large-sized organisation it becomes extremely difficult to manage credentials (such as cards) by traditional methods such as a stock management system or an excel spreadsheet. These methods also don't address security and auditing requirements that usually come with large-scale deployments of smartcards. CMS manage smartcard deployments in a secure and auditable manner, allowing an organisation to:

- Issue cards.
- Personalise cards with authentication capability.
- Manage cards post-issuance from a central location.

What are They Used For?

CMS can personalise cards to meet certain organisational requirements. This can be accomplished in several ways:

- Inserting secure credentials onto cards.
- Printing cards.
- Additional Identity Management capabilities such as:
  - Evidence of Identity (EOI) and personal information capture.
  - Biometric capture.
  - Logical Access Control System (LACS).
  - Physical Access Control System (PACS).
  - Instantiate and manage card applets (small, on-card applications).
  - Other forms of credential management such as mobile-device credential management, OTP and soft-token management.

CMS and CAMS

Smartcards can optionally be issued with pre-installed applets. A Card Application Management System (CAMS) manages these card applets, whereas the CMS manages the cards. Some CMS vendors are now introducing CAMS functionality into their CMS's.

Examples of Use Today

There are several large examples of card deployments today. One of the largest is the US Department of Defence, which has issued millions of Smartcards. While this is the largest deployment within a single agency, the US Federal Government would be considered the largest body to implement cards. This is because in 2004, they issued a mandate (HSPD-12) which indicated that all Federal agencies would be required to improve the quality of their forms of identification. The outcome of this is that all Federal agencies are now required to have a Smartcard solution.

In Australia, the largest deployment of cards is also associated with a Federal Department. Centrelink, now a part of the Department of Human Services, has issued approximately 30,000 Smartcards, providing logical and physical access to their facilities.

Other government departments, such as the Department of Defence, have also implemented widespread Smartcard solutions. Other organisations to implement this technology include the UK National Health Service, Lockheed Martin, Boeing, G & D, Booz Allen Hamilton, Nissan and the World Bank.

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.