Fact Sheet

Cogito Group

Smartcards

What are Smartcards?

Smartcards are cards that have an embedded, integrated circuit or 'chip' in them. They are used to improve security when accessing information, locations, or equipment. Smartcards are often used as a replacement for traditional physical access control methods, allowing one Smartcard to replace numerous keys, cards, and PIN entry systems. Smartcards provide additional assurance when securing digital transactions. Defence has smartcards that allow for network logon, digital signing, and physical access to buildings.

Authentication

Smartcards provide higher levels of security than traditional network access solutions that are based on usernames and passwords. Smartcards do this by allowing traditional single factor authentication methods to be replaced by Multi-Factor Authentication (MFA). Rather than simply providing something you know – your username and password – Smartcards enable a second factor of authentication in something you have – the smartcard. Some modern Smartcards allow for three factors of authentication, adding something you are – biometric data – to the authentication process.

Flexibility

In addition to providing higher levels of security in authentication to a system, Smartcards also provide more flexibility by simplifying sign-on to multiple systems. They do this by allowing a single secured credential within the card to be used by single sign on mechanisms in disconnected solutions.

Digital Security

Smartcards provide additional assurance when securing digital transactions. Smartcards can be used to digitally sign transaction, such as email, to ensure that the content cannot be changed by a third party in transit. This process can be used to sign financial transactions and procurements, authorise work, etc. In this use case, Smartcards can be used to not only ensure that these transactions are not altered, but also for nonrepudiation purposes (i.e. tying the person creating or authorizing the transaction to that transaction).

Confidentiality

Smartcards can also be used to provide confidentiality services such as the digital encryption of messages such as emails. This technology enables messages to only be read by the intended message recipient.

One Time Passwords

Other MFA methods such as One Time Passwords (OTP) can be used in place of smartcards but have significant limitations. If an OTP algorithm is compromised, all OTP are compromised as they use the same seed key. Smartcards each have unique keys related to the card and the user, meaning the compromise of one card does not cause the compromise of all cards in the batch. Many solutions that can use OTP can, however, also use smartcards to improve security such as the Citrix Remote services solution. OTP have no ability to provide physical access control, nor can they be used to assure the integrity of a transaction.

Examples of Smartcard Use

Some examples of those using smartcards today include:

- Telecommunications companies such as Telstra and Optus use smartcards in the form of a SIM card to identify unique phone numbers and users.
- Many Australian Banks and Credit Unions have started the introducing smartcards in their credit cards.
- The Australian Department of Human Services uses smartcards to facilitate logical access to their network.
- The Australian Department of Foreign Affairs and Trade use smartcard technologies in the new Australian passports.
- The Queensland State Government is deploying smartcards as the new Queensland Driver's License.
- The Australian Department of Defence uses smartcards to facilitate physical and logical access to their buildings and network, as well as for digital signing.

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.