Smartcards

What are Smartcards?

Smartcards are cards that have an embedded integrated circuit or 'chip' in them. They can be used to improve security when accessing information, locations or equipment.

Authentication

Smartcards provide higher levels of security than traditional network access solutions based on username and password. Smartcards do this by allowing traditional single factor authentication methods to be replaced by two factor authentication. Rather than just something you know (e.g. username and password), they enable something you know (e.g. a password) and a second factor, which is something you have (the smartcard).

Some modern smartcards allow for three factors of authentication. Something you know (a password), something you have (the smartcard) and something you are (a biometric).

Flexibility

While they can provide higher levels of security in authentication to a system, they can 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.

Smartcards can be used to access systems facilities or equipment. They can replace traditional physical access control methods, allowing one card to replace multiple 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.

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. They can be used to sign financial transactions and procurements, authorise work etc. In this use case, they can be used to not only ensure that these transactions are not able to be altered, but can also be used for non-repudiation purposes (i.e. they can also to tie the person creating or authorizing the transaction to that transaction).

Confidentiality

Smartcards can also be used to provide confidentiality services. An example is the digital encryption of messages such as emails. The technology means that only the recipient(s) of the message can read the message.

Other Authentication Methods

There are other two factor authentication methods that can be used in place of smartcards such as One Time Passwords (OTP).

OTP solutions have some limitations. One of these limitations is that if the OTP algorithm is compromised (which has happened recently to RSA, one of the largest providers of such tokens) all tokens are compromised as they effectively use the same seed key. Smartcards each have a separate key related to the card and the user, so the compromise of one card does not cause the compromise of all cards.

Many solutions that can use OTP, can also use smartcards (such as the Citrix Remote services solution), but the same cannot be said for OTP. OTP has no ability to provide for physical access control, nor can it be used to assure the integrity of a transaction. OTP is not as versatile as smartcards.

Some examples of those using smartcards in Australia today include:

- Telecommunications companies such as Telstra and Optus that provide mobile phone services use smartcards in the form of a SIM card. Effectively everyone that has a mobile phone in Australia is already using a smart card.
- Many Australian Banks and Credit Unions have started the introducing smartcards in their credit cards.
- Department of Human Services has some identity smartcards that allow network logon.
- Department of Foreign Affairs and Trade use smartcard technologies in the new Australian passport
- Queensland state government is deploying smartcards as the new Queensland Driver's License

Department of Defence has smartcards that allow network logon (logical access), digital signing and physical access to buildings.

Cogito Group is an award-winning 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
www.cogitogroup.net