

## fact sheet

### How do I make sure my digital certificates and keys are secure?

---

To ensure the security of online transactions, many companies make use of public key cryptography, which uses digital certificates and a pair of unique 'keys' to identify a business or individual involved in a transaction. (This is the system used by the Australian Tax Office when tax documents are submitted electronically).

Digital certificates and keys provide a strong degree of security for electronic business. However, as with any security device, they can be compromised if not protected properly. When using digital certificates, a major concern is to make sure that only the person or business they identify can access and use them.

For instance, if the key issued to a user is simply stored as part of their email program, anyone with access to their personal computer (PC) will be able to send or tamper with emails. If the machine is connected to the Internet, this might happen even if someone doesn't have physical access to the machine.

A basic method of protecting stored keys is to assign them with a password. When a user wants to sign a message, they enter the password to make the key available. However, a skilled hacker might be still able to read the key from the PC without knowing the password.

A more secure method of protecting a private key or certificate is to lock it into an electronic smart card, which can be accessed on a PC via a smart card reader. A smart card is usually password-protected as well, so that simply having possession of the card does not enable anyone to use it. This is a more costly solution, as it needs a smart card reader added to the PC.

A similar approach uses a hardware 'token' which plugs into the USB (Universal Serial Bus) port which found on most modern PCs. These tokens are compact, and can often fit on a key ring. Because most new PCs have a USB port, they also don't need a separate reader.

#### Terms you should know

**Cryptography** - Converting information into a secret code, using complex mathematical algorithms, so that it can't be read by anyone who does not already understand the code.

**Encryption** - The process of applying cryptography to an email message or document so that it can be safely transmitted over networks such as the Internet.

**Digital certificates** - An electronic file that contains information which uniquely identifies an individual or business when using online services.

**Public and private keys** - For maximum security, digital certificates are used in conjunction with public and private keys. When a message is encrypted, the system uses both a public key (which is freely supplied to anyone who needs to receive information from the sender) and a private key (which is known only to the sender, and ensures that messages from that sender can't be forged by others).