Put trust in your pocket: CSIRO's trust extension device

February 19 2008

Image credit – CSIRO

CSIRO has developed a prototype portable device that will allow people to do business across the internet on any computer in a trusted manner.

Known as a Trust Extension Device (TED), the TED consists of software loaded onto a portable device, such as a USB memory stick or a mobile phone. It is able to minimise the risk associated with performing transactions in untrusted and unknown computing environments.

"The problem is that trust is currently tied to specific, well-known computing environments," says CSIRO ICT Centre's, Dr John Zic.

"TED makes that trust portable, opening the way for secure transactions to be undertaken anywhere, even in an internet café."

The concept behind TED is that an enterprise issues a trusted customer with a portable device containing a small operating system, as well as a set of applications and encrypted data.

This device creates its own environment on an untrusted computer and, before it runs an application, it establishes trust with the remote enterprise server. Both ends must prove their identities to each other and that the computing environments are as expected.

Once the parties prove to each other they are trustworthy, the TED accesses the remote server and the transaction takes place.

Focus groups run by the Centre for Networking Technologies for the Information Economy, funded by Australian Government, suggested developing a device to facilitate trusted transactions and provide authorised people with access to confidential and private information.

For instance, banks could use a technology like TED to provide authorised customers and employees with access to financial data, or conduct financial transactions over the internet.

"The idea is that the person or organisation issuing the device runs their own computing environment and applications within the TED," says Dr Zic.

"Wherever you go, whichever machine you run on, you and the issuer can be confident both parties are known to each other, cannot engage in any malicious acts, and that the transactions are trusted."

Source: CSIRO