Smarter than your average card

Smartcards are set to be the next big thing in secure, convenient Internet banking

BY STEPHEN WILSON

Awareness of the limitations of conventional two-factor authentication continues to build. ABN Amro's time-based one-time password (OTP) tokens are the latest in a long line to be attacked. Moreover, other industry analysts are voicing the same general conclusions that I've already discussed in *Online Banking Review:* to combat man-in-the-middle attacks will take an active authentication technology, like smartcards.

The highly regarded Australian Computer Emergency Response team (AusCERT) looked at this issue in its submission to ASIC on the EFT Code of Conduct. AusCERT recommended that "one relatively simple and currently effective method of preventing fraudulent and unauthorised transfers … is to digitally sign each transaction" using a device other than the user's computer, which might be infected and unreliable. EMV Chip and PIN cards have this functionality.

According to AusCERT:

[The EMV smartcard] differs markedly from most other two-factor authentication mechanisms currently in use in Australia. The unique advantage of the mechanism is that it has the ability to still protect the integrity of transactions undertaken even in the event that the account user's computer is compromised with malware.

The same consideration is driving the US Government to use their new FIPS 201 smart ID badges for employee remote logon.

So what is the latest with smartcards in the Australian Government? Over and above the Department of Human Services' huge Access Card project, other arms of government have been laying the foundations for broader and more effective use of smartcard technologies. The Australian Government Information Management Office (AGIMO) has released the first two parts of its Australian Government Smartcard Framework, and has taken public comment on the latest draft parts concerned with standards and implementation guidelines. This initiative is tightly integrated with the overarching e-government strategy.

A big part of AGIMO's vision for smartcards is interoperability, and there are strong signs throughout the framework that sharing infrastructure with the private sector is a high priority. The implications for the financial services industry are important, while it continues to face barriers to the take-up of this technology.

The Government's framework aims to facilitate the re-use of multi-function smartcards across multiple domains, including the private sector, to help reduce costs and re-work. The framework says:

"Any smartcards issued by government represent a significant investment in resources. It is desirable that the maximum potential for re-use across the broader economy be facilitated wherever possible taking account of user needs and privacy protection."

It will be a real breakthrough when Internet banking is done using the good old card!

The vision is progressive. For instance, the framework anticipates that "a bank-issued smart credit card might also furnish … personalised access to government services and multiple individual digital certificates." In the context of multi-programming and re-use, privacy and project risk management are of the utmost concern to all stakeholders. The framework, therefore, sets out a number of detailed principles by which cardholder privacy will be safeguarded, and the business interests of a smartcard's original issuer protected.

The rollout of smartcards by government will do much to foster take-up across the board. For one thing, it will get more consumers familiar with what is really just a new take on conventional plastic cards.

For decades now we've used plastic cards across all walks of life. Countless card-based services all work the same way. Almost unconsciously you select the right card from your purse or wallet, pop it into a slot, usually enter a PIN, and services are delivered. At this level, ATMs, eftpos, over-the-counter claiming for Medicare and health insurance, airline check-in, many loyalty programs, and building access control systems all work in an identical fashion.

It will be a real breakthrough when Internet banking is done using the good old card!

Another benefit of government-issued smartcards, if properly managed with respect to privacy and user awareness, would be the standardising of new ways for consumers to conduct their affairs safely online. As AusCERT says, smartcards are truly distinct from all other personal security technologies. They can involve their owner in each transaction to combat identity theft, even if their computer has been affected by Trojans or keyboard sniffers.

It's true that consumers probably don't yet know enough about smartcard technology, and so they remain vulnerable to fear, uncertainty and doubt. But it's not hard to understand at a practical level. In fact, the average consumer's knowledge of SIM cards is a good starting point – SIMs are, after all, a type of smartcard.

Like SIMs, smartcards are smart – they can tell what's going on around them. They can detect if they've been plugged into uncertified equipment, in an attempt, for instance, to skim their contents. They can enforce PIN entry for a range of operations, such as updates of sensitive data, or execution of certain applications. And they can digitally sign pieces of data like payment instructions or electronic documents, to prevent tampering and replay attack.

The Australian Government Smartcard Framework should be compulsory reading for anyone involved in online authentication, no matter what their sector. The government's ICT infrastructure policies and its stated goals for responsive e-government open the way for a range of exciting cooperative programs with business.

Stephen Wilson is a leading international authority on identity management and information security. He founded the Lockstep Group in 2004 to provide independent security advice, and to develop new smartcard solutions for web security and privacy. Lockstep consulted to AGIMO on the Australian Government Smartcard Framework.

swilson@lockstep.com.au.

1. See Phishing attack evades ABN Amro's two-factor authentication at www.out-law.com/page-7967. 2. See EFT Code Review Submission to ASIC, AusCERT www.auscert.org.au/render.html?it=7536. 3. The Framework is available at www.agimo.gov.au/infrastructure/smart_cards. And the e-government strategy is at www.agimo.gov.au/government/e-government_strategy. 4. See Framework Part A "Overview and Principles", page a14. 5. See Framework Part B "Smartcard handbook", page b10.