Banking on the Access Card

Built-in 'smarts' could see the Government's planned Access Card become a useful tool for customer identification

BY STEPHEN WILSON

The Federal Government's Access Card is really taking shape. Major tenders are expected within weeks for the provision of over 16 million smartcards, associated new enrolment services, kiosks, and backend systems. And greater clarity is emerging around the government's vision, through several recent keynote speeches by Human Services Minister Joe Hockey.

One day soon we could literally be banking on the Access Card. There are clear signs that a portion of the new platform will be made available for personal and business use. The implications for banking are deep and multi-facetted.

Minister Hockey has said the Access Card could become a "gold standard" as evidence of identity, as a result of its fresh enrolment process. Presentation of a valid Access Card will represent strong evidence that the cardholder has passed a rigorous identity test.

An immediate challenge is to resist the slide towards a de facto national identity card. If presentation of the Access Card was to become routinely necessary for a wide range of services, then there is a risk that the totality of one's personal business becomes traceable and vulnerable to those who would exploit detailed knowledge of your daily activities.

The first line of defence against such abuses is that new Access Card legislation will forbid non-government businesses demanding that it be presented as a form of ID.

Nothing will prevent consumers voluntarily presenting the Access card as an adjunct form of identification when opening a new bank account. So the real fear remains that the Access Card may go the same way as drivers licences in Australia, or the Social Security Number in the USA, growing over time into a near-universal identity system, where people are inadvertently penalised if they cannot provide their card.

The saving grace of the Access Card should be its built-in smarts. There are good signs that a sophisticated multi-function smartcard platform will be specified for the project. Further, end users and service providers are expected to be able to utilise the platform for their own purposes, with the minimum of government involvement. This should pave the way for each Access Card to become a powerful proxy for its owner.

As Man-in-the-Middle attacks against one time password devices mount, it is becoming ever more clear that only active devices like smartcards can provide genuine mutual authentication needed for safe Internet banking. But if banks wish to leverage and share public infrastructure like the new Access Card, they will need to implement careful privacy measures that segregate business and government applications. And they will need to minimise the electronic trails that are left behind as a smartcard is used across diverse services (while retaining just the right level of auditability to manage their compliance and customer service obligations).

Sharing the infrastructure

- **Converge towards smartcards as the ideal access mechanism for all online services**
- Share the same smartcard readers for banking and government services at home
- **Appreciate that smartcard "real estate" is more then mere memory**
- Use embedded PKI to prove the pedigree of identifiers and transactions.

There is the encouraging news that one third of the capacity of the Access Card chip is to be made available to consumers and the private sector. But what good is 20-odd kilobytes of read/write memory?

Public debate and most lay peoples' general awareness centres on a smartcard's potential "free read" memory. It is commonly imagined that one's medical history and allergies, or contact details for next-of-kin could be stored there, accessible to emergency doctors and the like.

However, there is more to smartcard resources than mere memory. The more sophisticated card platforms – like "Global Platform", EMV and the new US Government staff ID standard FIPS 201 – include built-in card management functions which oversee precisely how memory gets accessed. Different areas of memory can be protected in different ways. For instance, a PIN can be required to read or write to defined segments. Some segments can be configured to be un-readable except by expressly authorised applications or terminal equipment. So it is not necessarily the case that any attacker with a reader can simply scan the contents of your smartcard.

With these memory management functions in mind, we can plan far more powerful uses for the spare capacity of an Access Card. Perhaps the most crucial applications will manage personal identifiers for third -party services like financial institutions.

If individuals are to carry bank account, policy numbers and so on in private segments of their smartcards, it is critical that the integrity of this data be guaranteed. There must be trusted, inviolable processes for writing identifiers into the chip and for safeguarding them over time. And when the numbers are put into action – by being retrieved from a smartcard and "quoted" in a transaction – it is crucial that relying parties are confident that the identifiers have come from a genuine Access Card.

The embedded PKI functions built into modern smartcards meet these requirements in ways that are still coming to the fore. One or more credentials can be electronically notarised by loading them inside digital certificates issued by banks and other trusted institutions, and bound to cryptographic keys generated within the card's chip. All transactions created using an Access Card could thus bear a unique digital pedigree, indelibly sealed with a notarised identifier, proving the bona fides of the smartcard and the legitimacy of the card holder's credentials.

Stephen Wilson is a leading international authority on identity management and information security. In early 2004, Stephen established Lockstep Consulting to provide independent security advice and to develop new smartcard solutions to identity theft.

swilson@lockstep.com.au