Access all areas

There is far more to smartcards than memory capacity and resistance to skimming

BY STEPHEN WILSON

The rapid development of a new Health and Welfare Access Card has continued to accelerate through the new year period.

As discussed in recent editions of *Online Banking Review*, this federally funded program of the Department of Human Services promises to issue in excess of 16 million multi-function smartcards starting in 2008.

Major tenders have been called for the issuance and management of the cards, and for the systems integration of complex back-end systems. An exposure draft of the associated Access Card legislation was released in December for public comment.

The implications for the banking sector are still emerging, piece by piece.

Strategically, the Access Card will serve to raise peoples' general awareness of the technology of smartcards. Certain applications may involve the use of simple smartcard readers in the home or office environment (the previous Minister for Human Services Joe Hockey deliberately flagged the potential usefulness of a "$25 reader attached to the home computer" to gain access to expanded government services.

If open interface standards are selected by the Access Card architects, and provided that business takes proper care with privacy compliance, then we should see an environment that stimulates innovative third-party applications being developed and deployed to add value to the Access Card.

The government has announced that a portion of the Access Card chip will be made available to consumers and the private sector. For a 64K chip, it appears that around 20 kilobytes of memory will be allocated to individuals. For larger chips, say 128K, there is no reason why this figure wouldn't rise to 80 kilobytes or more.

This scale of smartcard real estate should represent a significant opportunity for financial sector product development (and a corresponding revenue raising opportunity for government). The memory allocation might seem small by modern mass storage standards, but when it comes bundled with intelligent access controls, mutual authentication, key management and digital signature functions, smartcard real estate becomes a powerful package, as we shall see below.

The cost of smartcard readers, which to be fair must include installation and support overheads, will continue to fall as penetration grows. Already, a smartcard plus simple USB reader costs about the same as a one-time password generator – and yet they provide vastly greater security and value-added functionality. And because the one smartcard reader can support multiple applications, the cost can be more readily shared between public and private sector programs where synergies exist. For instance, the health insurance sector could facilitate the bringing together of patient-centred wellness programs and online data management tools, accessed safely via the smartcard.

The effective cost of smartcard readers will eventually be pushed all the way down to zero, as they become built in to standard PCs and laptops. Smartcard security is being promoted as a central feature of the new Windows Vista operating system. Bill Gates explained in a recent speech that: "Another weak link is in authentication. Today, we're using password systems, and password systems simply won't cut it … So we need to move to multifactor authentication. A lot of that will be a smartcard-type approach … It's a significant change and that needs to be built into [Windows] itself."

As regular *OBR* readers will appreciate, there is far more to smartcards than memory capacity and resistance to skimming. By bearing their special properties in mind, we can start to see some of the possibilities for integrating the new Access Card infrastructure into financial services.

Online Mutual Authentication

Only smartcards have the autonomy and built-in logic to challenge the identity of web servers when establishing Internet connections and so safeguard against Man-in-the-Middle attack. So smartcards can uniquely act as intelligent proxies for their owners making them the ideal logon device for Internet banking.

An Access Card could, at its holder's discretion, be topped up at a branch with the security codes of a bank and thus "activated" for Internet banking. When a smartcard is used as the key to access a website, it becomes impossible for the user to be misdirected to any site other than that configured in the chip.

Digital Credentials

Smartcards can hold and manage multiple digital credentials – such as bank account numbers, policy numbers, customer identifiers and so on – within secure memory "slots". However, credentials must be safeguarded against counterfeiting, cloning, or simply being made up. So storing them as numbers in spare slots is not enough. A better solution is to notarise credentials inside digital certificates linked to unique keys held on the cardholder's chip.

Anonymity

Lockstep research and development has shown that by using anonymous digital certificates to hold personal credentials, it is possible to de-identify certain transactions, such as payment instructions, entitlement checks, insurance claims, online voting and so on.

Online Evidence of Identity is a crucial requirement if totally electronic account origination is to ever be possible. If an identity credential is presented online by a customer, it is essential for the receiver to know the data is genuine, current, and is being sourced from a trusted medium like a smartcard. Notarising such data inside digital certificates issued to the smartcard is an approach unequalled for its security and privacy, providing a unique digital pedigree for a customer's transactions.

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