Spreading the cost of smartcards

Banks will find it easier to justify the case for smartcards if they take an all-of-business approach

BY STEPHEN WILSON

Recently I addressed an internal workshop on the EMV chip cards at a bank where my focus was online authentication.

Many commentators are convinced after looking at web fraud trends and two-factor security, that the best way to achieve mutual authentication is through smartcards.

Only smartcards have the ability to actively challenge the veracity of online services, acting as a proxy for the cardholder to protect them against phishing, pharming and web site spoofing.

So my presentation suggested that Internet banking could be transformed if EMV cards were value-added with a simple applet or two and deployed with readers for use over the web.

My session fell a little flat. So I asked my hosts if the material was somehow wrongly pitched. They responded that it all seemed very interesting, but as they were part of the cards group of the bank, it wasn't really relevant to them; they advised me to seek a separate meeting with the Internet banking team.

What's more, the cards group had been tasked with analysing the business case for EMV on their own. That is, the bank's return on investment for EMV had to be worked out on the basis of card fraud alone.

In effect the cards group was not allowed to consider other potential upsides from the rollout of smartcards.

I thought that in this day and age, companies were working across internal boundaries, to adopt an "all-of-business" or holistic perspective. Can it be a good idea to deliberately narrow down the scope of a project's benefits when calculating its ROI? Wouldn't customers and shareholders expect their bank to look at new technologies from all possible angles?

Over the years, it has become possible to access more banking products through a single card, giving customers a uniform experience. Credit cards were first introduced decades ago with "click-clack" machines. With the advent of ATMs and EFTPOS, customers enjoyed vastly increased functionality through the same plastic card.

Now the move to secure Internet banking threatens to disrupt this uniformity and convenience.

Most banking strategists are grappling with the looming problem of the "token necklace", where different banks seem likely to adopt different authenticators – scratch cards, mobile phones, challenge-response calculators, one-time password key fobs, even biometrics.

Rather than push for standardisation at the authenticator level, hugely complex third-party systems are being planned in order to rationalise the token necklace, aiming to make devices interoperable across multiple services.

Let's stop for a minute to consider why there has never been a comparable drive to rationalise our plastic cards.

Plastic card use is so in-grained that we tend to overlook two of its important features.

Card smarts

- **Smartcards are the ideal mutual authentication solution.**
- Conventional two-factor authentication does nothing to prevent Man-in-the-Middle attacks.
- **Smartcards can manage multiple identifiers.**
- Encrypting identifiers and decentralising identity management is the key to interoperation between banking and government smartcards.

Firstly, all cards are used in exactly the same way. Technically we might say they all have the same "user interface". Mistakes are rare and easily forgiven. Credit cards, insurance cards, membership cards and so on are simply keys to different backend schemes. Customers can move from one scheme to another seamlessly, without learning any new behaviour. It is intuitive and reasonable that different schemes tend to have their own keys.

Secondly, there are major advantages in separating the schemes. Different business processes, business rules and backend systems all remain sovereign. It is easier to keep customer data private (and business records confidential). And while "interoperability" is often looked at as some sort of holy grail, we need to remember that it inevitably brings a degree of linking. Change one system and you can find yourself impacting all other systems.

In fact, the wonderful interoperability of ATM and EFTPOS in Australia – achieved through painstaking negotiation of complex standards – is one reason that the introduction of EMV has been relatively difficult here. There is a real fear that interoperability could suffer if any one institution were to switch to EMV before all parties made the necessary system changes in concert.

Returning to the case for smartcards, consistency of the user experience is not a trivial matter. As we've seen, it makes a wallet full of cards entirely manageable. A co-ordinated industry-wide decision to adopt smartcards for Internet banking could avoid not just customer confusion but the cost and complexity of tokens and third-party interoperability schemes.

Only smartcards have the built-in computing power to act as intelligent proxies for their owners. They can "see through" web site spoofing by checking SSL master codes, and avoiding DNS cache poisoning. Thus they offer robust and long term protection of Internet banking customers against phishing, pharming and spam. And they can act as containers for multiple identifiers or digital credentials, to enable secure, segregated and even anonymous transactions with multiple organisations, including government.

If banks can take an all-of-business approach to smartcards – engaging their Internet banking, privacy, compliance and security functions with the cards groups – then they will probably see a stronger ROI. With value-added smartcard functions, it might be possible to start EMV rollout at the card level well ahead of the liability switch and so spread out their infrastructure investment.

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