The momentum for mobile

Digital signatures make m-commerce a convenient reality

BY STEPHEN WILSON

At the Banktech conference in July, Westpac's CIO for consumer financial services Patrick Eltridge confirmed that the bank sees wireless PKI as a "game changing technology". WPKI looks like being central to the rapid expansion of mobile phone banking into full-blown financial services.

So is WPKI just another spin on this controversial technology? Or will it reinvigorate PKI to deliver its full potential after all?

The mobile phone is clearly an attractive channel for delivering at least some banking services. In Australia mobile phone penetration is so high that we can take for granted that most customers have a phone. And innovative marketing methods using simple text messaging are being developed with increasing frequency (although SMS spam may yet become a curse!)

Building on consumers' familiarity with text messaging is the idea of transacting over the phone. With multi-media interfaces and broadband connectivity to the Internet now commonplace, one view is that there is nothing you can do over a web browser that you can't also do on a mobile handset.

Certainly there are no technical barriers, with WPKI available as an option through most 2.5G SIM cards. But human factors – that is, plain old usability – do come into play.

So in planning and architecting mobile banking applications, we need a keen eye for practicality and value. With this in mind, there are a number of exciting scenarios where WPKI security can deliver great gains in timeliness, efficiency and productivity.

WPKI, like any PKI implementation, delivers its greatest benefits for transactions that demand the customer's signature.

To date, the vast majority of Internet banking has been based on the same business rules as telephone banking. No signature is required, but there are tight constraints on what is possible, and the customer only ever deals with a single counterparty – the bank itself.

In such a hub-and-spoke system, the customer signs an upfront contract (on paper!), and uses a simple mechanism such as a password to authorise a small set of pre-arranged operations, for example, funds transfers.

In contrast, more complex transactions for financial services products such as loans, insurance, conveyancing and superannuation cannot be shoe horned into this tightly controlled context. In particular, these transactions traditionally require a handwritten signature to indicate that the customer understands and agrees to their commitments and obligations.

> **Substantial down payments could be originated safely from a mobile phone**

The strength of PKI lies in digital signatures. Subtler than the tired idea of "non-repudiation", a digital signature ties the individual's digital certificate to the transaction. In turn, the certificate can contain any useful authority information used to substantiate the transaction.

One of the more important developments in digital certificates is the move to include more application-specific types of authority information in addition to – or instead of – the individual's name. So, for example, a digital certificate containing the customer's account number will irrevocably "burn" that number into the transaction every time they sign something using that certificate. The trustworthiness of a digitally certified account number means we could remove extraneous personal information from routine transactions, and help restore customer privacy.

The beauty of PKI is that the customer's digital signature, certificate and embedded account number can be readily checked down the track. The state of a transaction is thus frozen in time; it remains verifiable long into the future, even if the customer changes banks.

These properties are what make digital signatures uniquely suited to multi-party and long-lived transactions such as trade documentation, electronic conveyancing and superannuation administration. Most security analysts agree that going paperless for these sorts of dealings requires PKI.

The mobile phone interface may be best suited to narrow "slivers" of transactions, where the customer has some background and wishes to act on particular events. Certain transactions such as home loans and personal lending can bring the customer into periods of closer real time interaction with their bank. During these periods, the mobile phone could become enormously convenient.

With WPKI secured transactions, a customer could deal with their bank instantaneously in situations such as car sales or property auctions. In remote locations, substantial down payments could be originated safely from a mobile phone using a digital signature. Well-authenticated m-commerce could also bring together institutions and new customers shopping around for finance, car insurance or travel insurance.

We're all familiar with the numerous pieces of ad hoc paperwork – contract variations, declarations, consents to release records and so on – generated during any big deal, for example, re-financing. The delays that mount up when these pieces of paper cannot be signed and delivered straight away are not just frustrating; they can become deal breakers. But they could all be digitally signed immediately on a WPKI mobile phone, no matter where the customer is at the time.

Surely I'm only just scratching the surface here. With brokers, financial advisers and personal bankers all increasingly mobile, the combination of digital credentials and WPKI can enable even greater efficiency in banking product delivery. So we should expect digital signatures to make the mobile phone an invaluable tool not only for retail customers but also for business banking.

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.

swilson@lockstep.com.au