Is PKI Finally on the Cards?

With mutual authentication looming large, the time is ripe for institutions to take a fresh look at both smartcards and PKI.

BY STEPHEN WILSON

While the public key infrastructure industry has had its difficulties, the unique value of public key authentication in securing paperless transactions is now widely acknowledged.

The early rosy vision of a single, all-purpose identity infrastructure has given way to a more sophisticated landscape of *multiple* PKIs, used not so much for managing identity per se, but rather more complex relationships, affiliations, credentials and so on. In this issue, we are going to show how PKI implemented with smartcards is emerging as a critical infrastructure.

The return on investment in smartcard technologies can be far greater than commonly realised when we apply them to both offline and online channels. It is well known that smartcards are practically immune to skimming and counterfeiting. However, their in-built computing power enables them to detect fraud and abuse offline, apply strong indelible authentication on a per transaction basis, and decentralise identity management. Further, smartcards are the only practical option for mutual authentication, so critical to eliminate phishing and web fraud. With governments increasingly committing to smartcards for secure service delivery, the business opportunities for financial institutions – as issuers, processors and infrastructure providers – are multiplying almost daily.

Under the covers, PKI is core to all modern smartcards. The near universal experience of successful PKIs is that they suit "closed" or "bounded" populations of users. This strikes some critics as a limitation of PKI, but the truth is we should never have expected a single identity management regime to prevail. Not only would a single general purpose top-down PKI prove unwieldy and expensive, it wouldn't even be terribly useful.

For it turns out that real e-business is conducted on the basis of credentials and relationships, and not personal identity. The distinct PKIs we see around the globe – in customs and trade documentation, healthcare, enterprise messaging, gaming, embedded applications and so on – therefore map on to real world groupings. Different PKIs are customised to suit different communities of interest, conducting specific types of transactions. It is a fact of life that business occurs in defined communities, bounded by membership arrangements, contracts, professional qualifications, and/or regulations.

PKI smartcard programs

- **Johnson & Johnson USB keys for staff (100,000+ users)**
- **Hong Kong SMARTICS ID card (6 million users)**
- **Taiwan National Health Insurance smartcard (22 million users)**
- **US Personal Identity Verification (15 million users by end of this year)**
- **EMV smart credit/debit cards worldwide (350 million+ users)**

The truly unique thing about PKI is the way it binds not just user's names but also their *authority information* to the transactions they digitally sign. The digital certificates that are issued in an orthodox PKI convey the holders' names and cryptographic codes, binding them together. A digital certificate traditionally represents an assertion by the certificate issuer that the holder is who they say they are.

But a far more powerful construct is emerging: the *Relationship Certificate*. Here the issuer asserts not just the identity of the holder but also the relationship between them. If the issuer is an authoritative credentialing body, then that relationship can be definitive proof of the certificate holder's standing in a business community.

With Relationship Certificates, your digital signature doesn't just bind your identity to what you sign – it binds your business credentials as well. Digital signatures last for years and years, and they survive intact being copied or forwarded any number of times. So when we need to prove "who did what to whom and when", in high risk, long lived and multi-party environments, PKI provides the most robust security model. PKI is not for every application, but it is uniquely suited to complex settings like electronic conveyancing, superannuation administration, trade documentation, government reporting, and healthcare.

Public key technology depends on cryptographic codes and physical security which have proved awkward to implement in conventional software. A critical recent development has been to embed and automate these mechanisms in smartcards (and similar tokens, and even mobile phones). Embedded PKI then becomes just as easy to use as conventional magnetic stripe cards – but hugely more powerful.

No other authentication technology binds credentials directly to transactions; all alternatives to PKI require additional infrastructure in order to verify the status and currency of credentials, especially as transactions age. In cases where transaction records must remain available over long periods of time, the effort of archiving credentials databases and audit logs, or of forensic investigation when historical records must be reconstructed, introduces enormous costs.

PKI enabled smartcards are emerging as a compelling combination. While we usually think of smartcards as being immune to skimming and counterfeiting, their full power is based on their in-built computers. Smartcards can carry and enforce cardholder entitlements offline, and can detect a wide range of abuses, without needing to connect to backend systems. In the EMV system for instance, the cards themselves keep track of and enforce daily transaction totals. Decentralising security greatly minimises the personal information transmitted over open networks, thus preserving privacy, simplifying system design, improving performance, and reducing compliance costs.

With mutual authentication looming large, and customers increasingly agitating for convergent means for dealing with their banks and other services, the time is ripe for institutions to take a fresh look at both smartcards and PKI.

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