The importance of PKI in health & welfare

While PKI has had its difficulties (as have many new information technologies) its unique ability to secure paperless transactions is now widely acknowledged, especially in the complex, high risk, long lived and multi-party applications characteristic of the health & welfare sector.

What are PKI Digital Signatures?

A Digital Signature is an electronic seal that uniquely identifies (1) the originator, (2) a set of attributes contained in their Digital Certificate, and (3) the issuer of the Certificate, and binds all that "authority information" to a document or transaction.

Old PKI and new PKI

The term "PKI" has many connotations. Basically, a PKI is a coordinated system of technologies, services and policies for managing Digital Certificates. An early vision for PKI was to create an all-purpose, one-size-fits-all digital identity regime. This model of course proved unwieldy, intrusive and expensive. Moreover, the security needs of e-business turn out to be more about credentials, memberships and relationships than personal identity. Therefore the overwhelming trend worldwide is towards vertical, "closed" or application-specific PKIs (plural!). Different PKIs today customise their Certificates to mean different things, to suit their own applications.

Public key technology depends on cryptographic codes which are not user friendly in conventional software. A critical development has been to embed and automate these codes in smartcards and similar personal tokens. Embedded PKI is just as easy to use as conventional magnetic stripe cards – but hugely more powerful because Digital Signatures bind complex authority information to every document or transaction.

Healthcare documents and transactions must:

- bear the professional credentials or licence particulars of their originators
- resist counterfeiting and tampering
- maintain their data integrity over long periods of time (often many years)
- be verifiable offline, as processing occurs in a wide range of settings, many without continuous network connectivity to government
- remain auditable long after the originator's credentials may have changed
- be able to be copied to many other parties – other providers, agencies, insurers and so on – with no loss of data fidelity and no dilution of the proof of the sender's bona fides.

Digital Certificates issued by authoritative credentialing bodies indelibly bind the bona fides of their owners to the transactions they create. Digital Certificates remain readily verifiable offline for years into the future. 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.

Smartcards with embedded PKI:

- can carry and enforce card holder entitlements offline, and can detect a wide range of abuses, without needing to connect to backend systems
- greatly minimise the amount of personal information that needs to be transmitted over open networks, thus preserving privacy, simplifying system design, improving performance, and reducing compliance costs
- can indelibly yet anonymously seal transactions with data unique to the card holder, to mitigate fraud, but without compromising privacy
- according to NIST provide the "*the only practical solution [to eavesdropping and account hijacking]*"[1]
- resist skimming and counterfeiting.

Embedded PKI is a mature technology:

- half a billion of "EMV" credit & debit smartcards issued worldwide have embedded Digital Certificates
- hundreds of millions of health & welfare smartcards in France, Germany, Italy, Belgium and Taiwan have embedded certificates
- all new national ID cards – such as those of Hong Kong, Malaysia Belgium, Estonia, Libya, Saudi Arabia, Sweden and Thailand – can carry one or more embedded certificates[2]
- Bill Gates, addressing the 2006 RSA Security conference heralded the end of passwords and the migration to smartcards for authentication across the Microsoft platform.[3]

[1] www.asia-pkiforum.org/feb_tokyo/NIST_Burr.pdf.

[2] ID cards are cited only as a sign of the maturity of the technology, and not to take any position for or against the controversial topic of national identity.

[3] www.microsoft.com/billgates/speeches/2006/02-14RSA06.asp.