Exposing some PKI myths

Myth	*A grain of Truth*	*The new way*	*Examples*
"PKI is difficult and onerous"	Early CAs came years before any actual applications, and tried to offer a one-size-fits-all certificate. The focus had to be on personal EOI: the 100 point check in first generation PKI made sense when we didn't know what certificates were going to be used for. Liability allocation had to be very conservative. But the model was wrong! "For big CAs, there is an implicit assumption that one identity is sufficient for all applications, which contradicts experience" [1].	Digital Certificates are now designed to fit the application, not the other way round. Different certificates are issued for different families of applications. Overseas the trend is to localised "authorisation PKI" rather than "Big CAs". The *relationship* approach [2] allows automatic distribution of certificates to known users within a defined community of interest. Better application design constrains certificates from inappropriate re-use, so no new liability concerns are introduced.	– Gatekeeper "Special purpose" or "Relationship Certificates" [3] – Digital credentials for lawyers, engineers etc. – Known Customer certificates for healthcare professionals[4] – Pan Asia Alliance trade documentation certificates – 60,000,000 Sesam Vitale health cards – 300,000 Taiwan health providers
"Certificates aren't user friendly"	Early PKI suffered from poorly designed user interfaces and clumsy APIs. Certificates had to be manually imported, exported and renewed.	When embedded into applications, especially via smartcards, certificates are no more difficult to use than any normal plastic card. Native support for PKI is improving all the time in commercial software (e.g. Windows 2000, Vista)	– Sweden's BankID (approx 1M users) – CableLabs' digital TV set-top boxes – EMV smart credit cards (>400M) – ICAO e-passports – Skype (>10M users)
"PKI arrangements are complex"	The early simplistic vision was an all purpose global identification system, to allow "stranger-to-stranger" commerce. Without any context, legal arrangements for vanilla certificates are inevitably complex.	Gatekeeper now recognises that "PKI works best when based on existing and trusted business relationships". Relationship certificates can be issued under a user's existing contractual obligations, with little or no new Ts&Cs.	A relationship certificate issued to e.g. a professional represents nothing more and nothing less than the fact that the certificate holder is a member of a body and has a registration number.
"There are better options than PKI"	The *Electronic Transactions Act* is technology neutral and does not mandate PKI. Few banks use it for Internet banking; after early disappointment with PKI, most are now experimenting with two factor authentication (despite the risk of Man in the Middle attack).	**The reality is that no other security technology provides long term transaction authentication. There are plenty of simple access control alternatives, but the AGAF for instance allows only PKI digital signatures for *document* authentication [5]. NIST says that the "only practical solution [to Man in the Middle attack and web fraud] today uses PKI" [6]. So there is no better option than PKI for the sorts of high risk, long life, multi-party transactions typical of the health sector, business banking, trade documentation, property conveyancing, engineering certification and so on.**	

[1] www.asia-pkiforum.org/july_shanghai/2004July/(4)Challenge.ppt
[2] www.lockstep.com.au/library/pki/relationship_certificates
[3] www.gatekeeper.gov.au/__data/assets/pdf_file/52243/Gatekeeper_PKI_Framework.pdf
[4] http://tinyurl.com/qh6tj
[5] www.agimo.gov.au/__data/assets/pdf_file/46796/AGAF_I_Discussion_Paper.pdf
[6] www.asia-pkiforum.org/feb_tokyo/NIST_Burr.pdf