PKI state of play

Argus Forum
Canberra 7 May 2004

Stephen Wilson
Lockstep Consulting

Some of PKI's baggage

- The passport metaphor

Likening digital certificates to passports has created inflated expectations and vast complexity. They should not have been imagined to be all-purpose identifiers.

- The e-mail exemplar

Vendors like to illustrate PKI in action using e-mail. They often show Alice studying the certificate of stranger Bob to work out who he is. But killer apps involve machine processing in high volume, NOT occasional manual use for stranger-to-stranger comms.

- "Digital Signature"

Digital signatures are truly NOTHING like handwriting.

- Evidence of Identity (EOI)

Preoccupation with personal evidence of identity, dating from early days when we thought there were national security implications in PKI, have created one of the greatest barriers to entry: the uncalled-for 100 point check.

- CP/CPS

PKI was originally (mis) conceived as being a solution for general purpose stranger-to-stranger dealings, with no reference to the context of the application. The only way to test the fitness for purpose was to wade through a CPS.

- Non repudiation

PKI vendors typically act as though digital signatures have a monopoly on "non-repudiation". In reality, it can be very difficult to speciously deny taking part in a non-PKI secured transaction like Internet banking. And nothing stops somebody repudiating a PKI based transaction if for instance they lost control of their private key.

Some missing pieces

- Context of the transaction
  - simplify liability
  - seamlessly allow multiple credentials
  - rationalise registration and EOI
- Automate & embed dig sig functions
- Automate registration
- Smartcards, readers, OS support

Is PGP a viable alternative?

- Doesn’t scale well
- But can be congruent with local relationships between providers
- Penetration and support are problematic
- Hard to ensure uniform registration
- Better to leverage authoritative credentialing processes?

Is biometrics disruptive?

- Hype belies fundamental limitations
  - No persistent signature
  - No ability to revoke lost identifier
- Huge uncertainties at large scales
- Acute security/convenience tradeoffs

Conclusion: new PKI vision

- *Business card* a far better metaphor than passport
- Instantiate *relationships* not personal identity
- Overlay certificate registration on existing membership arrangements
- Leverage “mutual recognition arrangements”
- Don’t impose 100 pt EOI rules from outside
- Keep eye on credit card developments, as they will drive embedded PKI rollout
- Public Private Partnerships?
- Horses for courses: PGP alongside PKI in cards carrying multiple private keys