Relationship Certificates for *Known Customers*

A new PKI paradigm

Asia PKI Forum 5th International Symposium
Beijing, 5 November 2005
Stephen Wilson

New ways to build PKI

Introduction of Japan PKI Forum's New Project "Next Generation Electronic Authentication"
APKIF Interoperability WG Beijing 3 Nov 2005

"This project is characterized by making 'trusted organization' perform the user registration procedure and authentication instead of a service provider in order to protect a user's personal information, and by realizing whole optimization."

And so we see that many PKI designers today are thinking about new ways to build PKI, with a shift away from generic identity service providers towards trusted and authoritative organisations.

PKI's traditional "advert"

The traditional advertised benefits of PKI are not truly unique!

- Confidentiality
  - This is *symmetric* crypto function and is not directly provided by PKI
- Authentication
  - *Authorisation* usually more important than authentication; we do not need to artificially separate authorisation and authentication; sometimes they can be performed at once
- Integrity
  - There any alternative ways to ensure integrity, not just PKI
- "Non-repudiation"
  - A myth! "Non repudiation" is not black-and-white; the real business problem is the expense and difficulty of proving "who did what to whom". Non PKI technologies provide plenty of non-repudiation especially in private applications like net banking, where PKI has been rare in the US, Australia and Europe

PKI's fundamental benefits

- Tamper resistant evidence of "who did what to whom" in e-business, easily verified by any party, at any time in future
- Digital certificates can convey *authority information* as well as (or instead of) identity e.g. credentials, licences, affiliations
- PKI smartcards are *"the only practical solution [to eavesdropping & account hijacking] today"*

  Bill Burr (NIST) Asia PKI Forum, Tokyo, Feb 2005
  http://asia-pkiforum.org/feb_tokyo/NIST_Burr.pdf

Understanding evolves (1)

	Old PKI	New PKI
Meaning	"e passport"	e business card
Intended use	General purpose e-commerce	Specific B2B apps
Communities	One: the public	Many (industry sectors, professions, schemes …)
Implementation	Single one-size-fits-all certificate	Multiple certificates, increasingly embedded)
Registration	Strict face-to-face ID proofing	Automatic via exiting member databases

Understanding evolves (2)

Dr. Stephen Kent (co-chair IETF PKIX WG)

"For big CAs, there is an implicit assumption that a single cert. is all that a user should need. This assumes that one identity is sufficient for all applications, which contradicts experience."

Asia PKI Forum, Taipei, September 2005

Australian Govt Review

"Cost identified by [Australian Parliamentary Committee] as a major factor in the low take-up of Gatekeeper. The major cost component is the registration process required to verify the identity of the applicant."

See www.gatekeeper.gov.au

PKI best practices

"As everybody knows", most successful PKIs today serve closed user groups.
In the following best practice examples, identity is not as important as relationships

- **US Patent & Trademark Office**
  10% of filing online X $200 saved = $6M p.a
- **Pan Asia Alliance**
- **Health eSignature Authority**
- **Land Victoria** Online real estate buy/sell
- **UK Chip & PIN** EMV smartcards
- **CableLabs** embedded PKI in set-top boxes
- **US FIPS-201** employee smartcards

"Identity crisis"

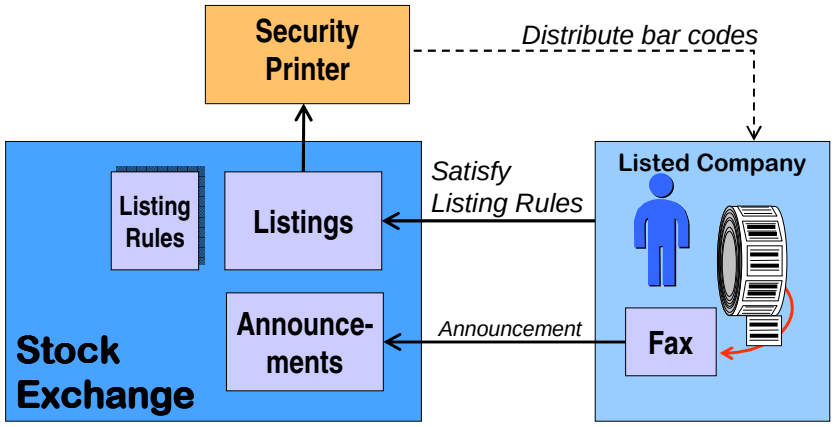
- "Stranger-to-Stranger" business is hard (and very rare in real world)
- "Trust" doesn't come easy (and should not be a deliverable of a CA)
- We don't usually do business based on identity alone
- Need authorisation plus authentication
- Credentials matter more than identity in B2B and B2G e-business

"Relationship Certificates"

Compared with identity certificates, relationship certificates are:

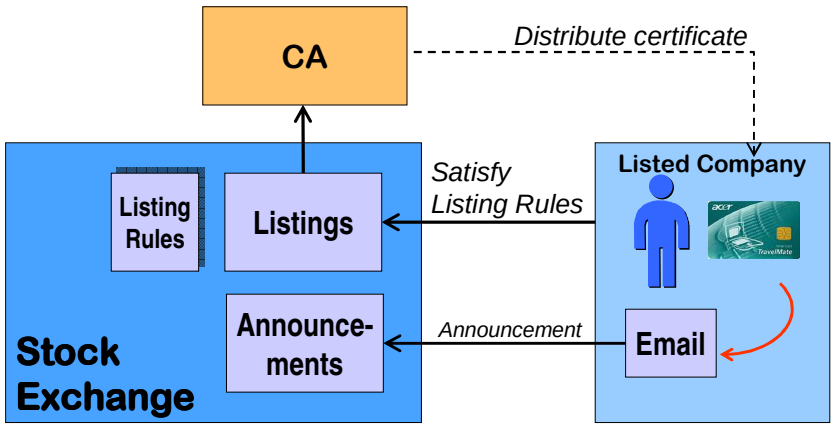
- a different type of affirmation:
  - they show that the Subject has a particular type of relationship with the RA
  - *not* that the Subject has been identified to any particular external standard
- and more closely tied to intended application
  - they should not be used outside the "community of interest"

Analogy: CAs as *security printers*



To transmit confidential company announcements to a Stock Exchange, listed companies in some countries use special bar codes to authenticate faxes. The barcodes are manufactured on behalf of the Stock Exchange by a specialist security printer. The printer has no interest in the content of their printing, and have no liability in the event of misuse of the barcodes. Security printing businesses must have physical, personnel, technology and process security on a par with Certification Authorities.

Analogy: CAs as *security printers* (2)



A better secure communications method for company announcements is digitally signed e-mail. In principle, an easy upgrade of the barcode method is to manufacture special purpose digital certificates (on smartcards). Traditional PKI would involve face-to-face identity proofing of the subject, but if the listed company and its representatives have met Listing Rules, then it is not necessary to impose additional identity processes if the certificates are only to be used in the closed application. Following the security printer metaphor, the CA has no liability in this case for misuse of the certificates. ***See also www.lockstep.com.au/library/pki/the_security_printer_model_fo***

Characteristics

Relationship Certificates:

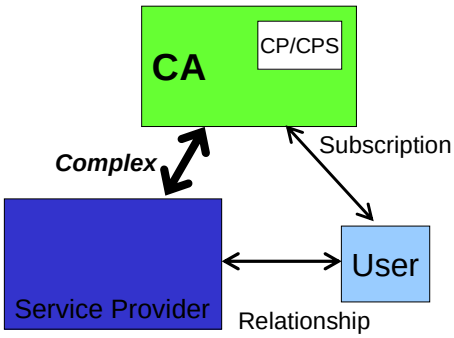
- should be issued by RAs inside trusted organisations or communities of interest
- must have unique Policy OIDs which map to the intended application
- are technologically the same as X.509 identity certificates
- require no new infrastructure and no new software (unlike "Attribute Certificates")
- are user friendly if embedded and automated by application software

Examples – Australia

- Hospitals to issue smartcards to medical staff with embedded certificates "printed" by Health eSignature Authority www.hesa.gov.au
- Law Society plans to issue "Digital Credentials" to licensed lawyers
- Commonwealth Project Gatekeeper new "PKI Framework" to introduce Relationship Certificates for Known Customers www.gatekeeper.gov.au

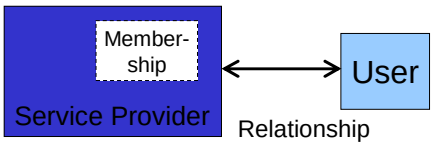
ID vs Relationship: "Trust"

Third Party Identity Certs



Traditional PKI requires users to enter into subscription arrangements with CAs, regardless of their relationship with a service provider. The CA and the service provider usually have no prior relationship, leading to enormous complexity.

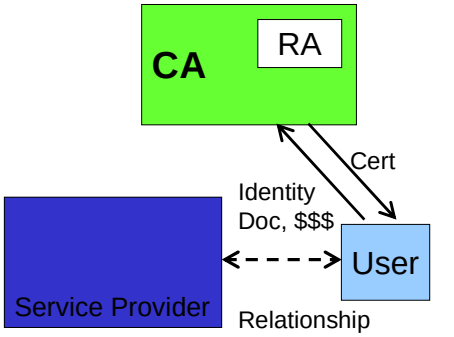
Relationship Certificates



New PKI, based on relationship certificates, recognises the primacy of the trust relationship between service provider and user. No CA can introduce "trust" per se.

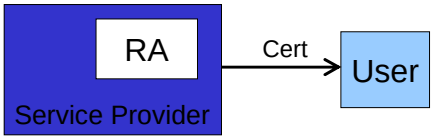
ID vs Relationship: RA

Third Party Identity Certs



Certificates are traditionally issued after the User presents detailed (and inconvenient) identity documentation, plus a fee. Prior relationship with the service provider is likely to be ignored entirely.

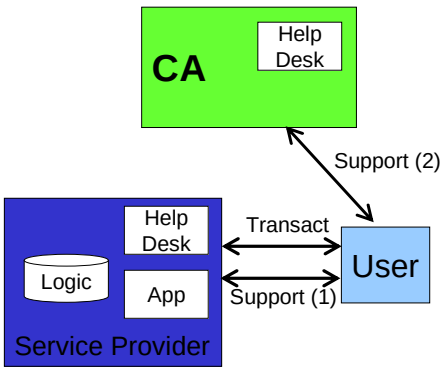
Relationship Certificates



If a service provider with a standing relationship with the user sets up a local RA, then relationship certificates can be issued automatically. Not shown is an outsourced CA acting as a 'security printer' simply minting certificates on order from the RA.

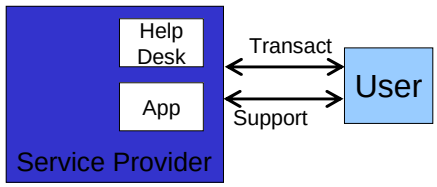
ID vs Relationship: In use

Third Party Identity Certs



When used in transactions with a service provider, general purpose identity certificates require complex business logic to determine rights & entitlements. Two support relationships are also entailed, one with the application provider and another with the CA.

Relationship Certificates



Relationship certificates can embody all necessary rights & entitlements information directly, greatly simplifying the business logic at the application provider. And only one support relationship is needed.

Strategic implications

- Employ large volume, wholesale CAs
- Need only small number of CAs
- Need large numbers of RAs!
- Cross recognise at app / RA level
- Review the value of Bridge CAs?
- Sovereignty of Root CAs not critical
- Makes PKI easy!

Further reading

Presentation available at www.lockstep.com.au

"Relationship Certificates"
www.lockstep.com.au/library/pki/relationship_certificates

"The Security Printer model for CA Operations"
www.lockstep.com.au/library/pki/the_security_printer_model_fo

Stephen Wilson
Lockstep Consulting
swilson@lockstep.com.au
0414 488 851