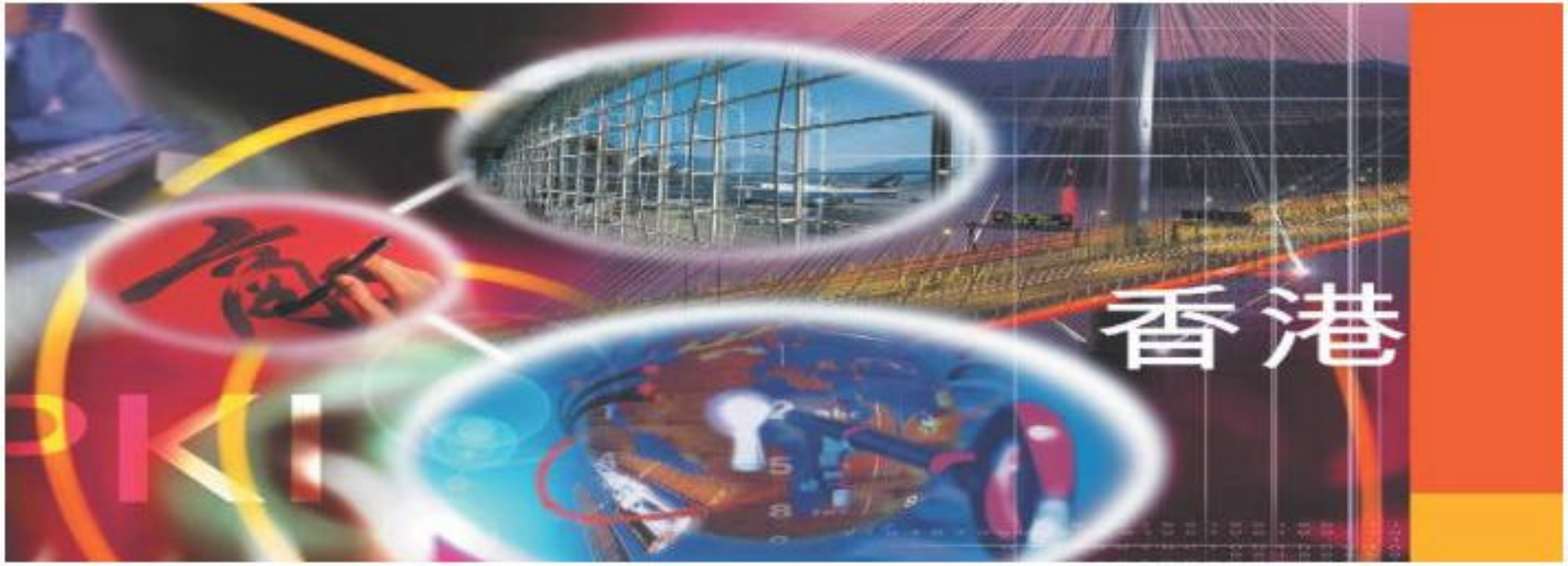
Re-thinking PKI: Electronic Business Card, Not Electronic Passport

Mr. Stephen Wilson

Chief Security Specialist, SecureNet Limited



Re-thinking PKI: Electronic business card, not electronic passport

Hong Kong PKI Forum
September 2003

Stephen Wilson
Chief Security Specialist

Re-thinking PKI

SecureNet

- Trends in embedded PKI
  - the experience of chip-enabled credit cards
- Scheme-based PKI
  - What is the role of government and regulators?
  - Implications for simpler cross-recognition
- Case studies
  - healthcare
  - banking
  - e-government

What do you need to know about PKI?

Symmetric cryptography

Public key cryptography

Hash algorithms

DES, 3DES, RSA, MD5, SHA-1, RC4, AES, ECC

56 bits, 128 bits, 256 bits, 1024 bits, 2048 bits

Key generation, Signature keys & encryption keys

X.500, X.509 v3

CRLs, OCSP

Discrete logarithms, number theory, elliptic curves

…

SecureNet

Compare with Magnetic Stripe Cards

Intrinsic coercivity mHc

Remnant coercivity rHc

Switching Field Distribution

Saturation Magentization

B-H hysteresis loop

Strontium Ferrite (SrFe)

Barium Ferrite (BaFe)

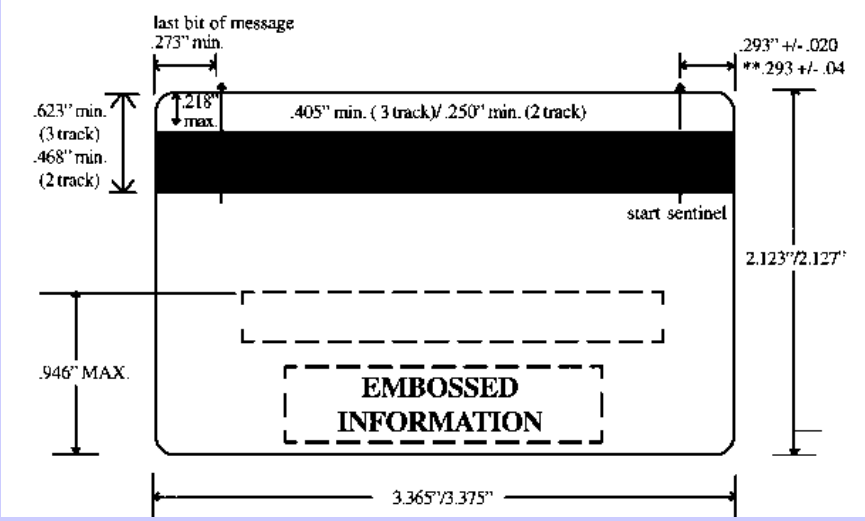
Longitudinal Redundancy Check Character

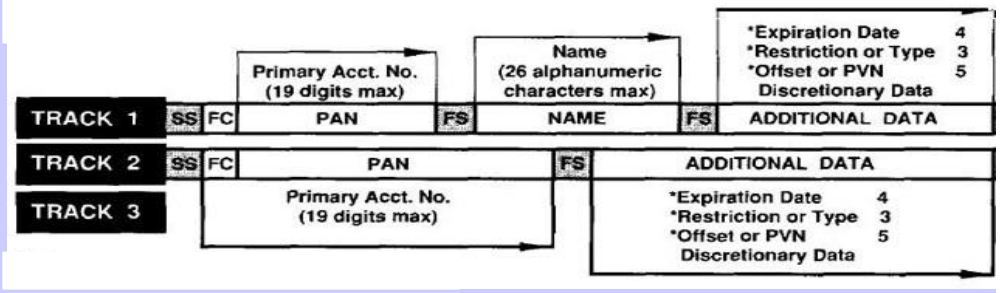
Archival stability

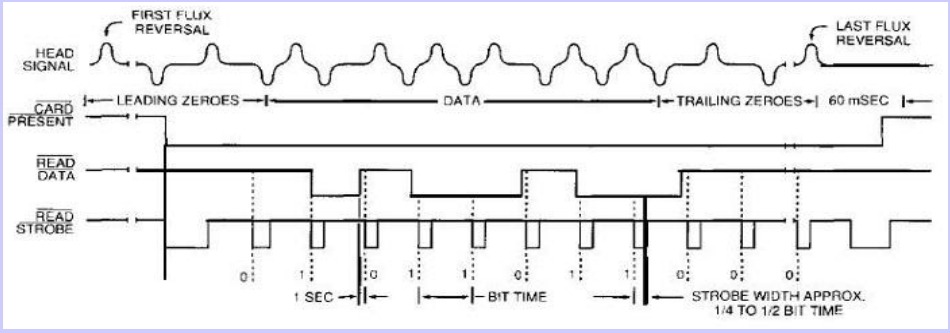
ISO 7811 ISO 7813

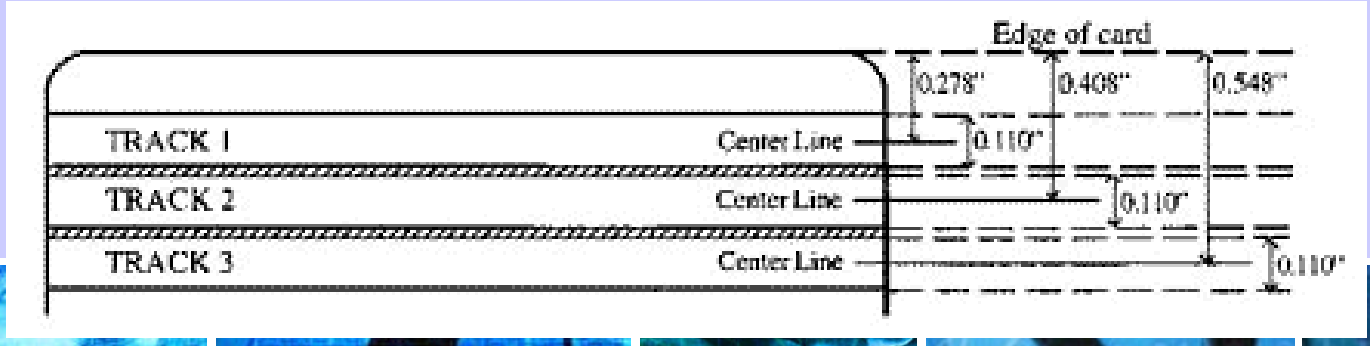
Mag stripe cards: complex standards

SecureNet



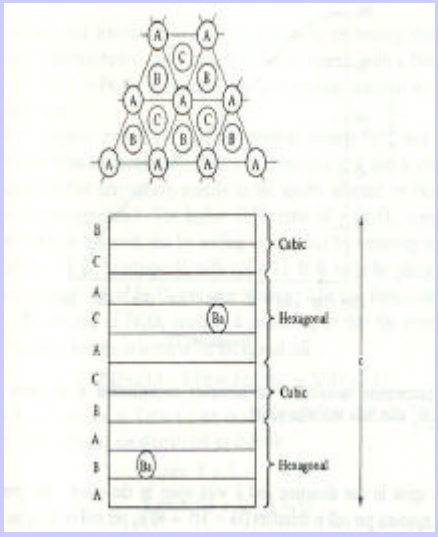


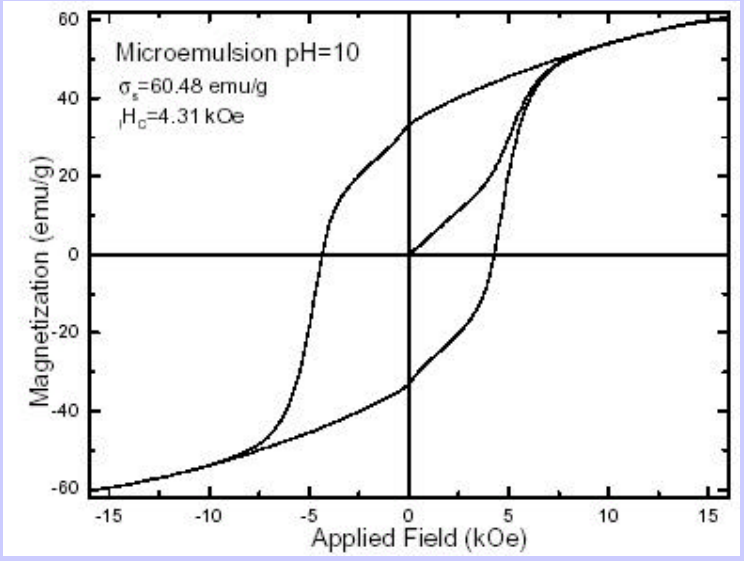


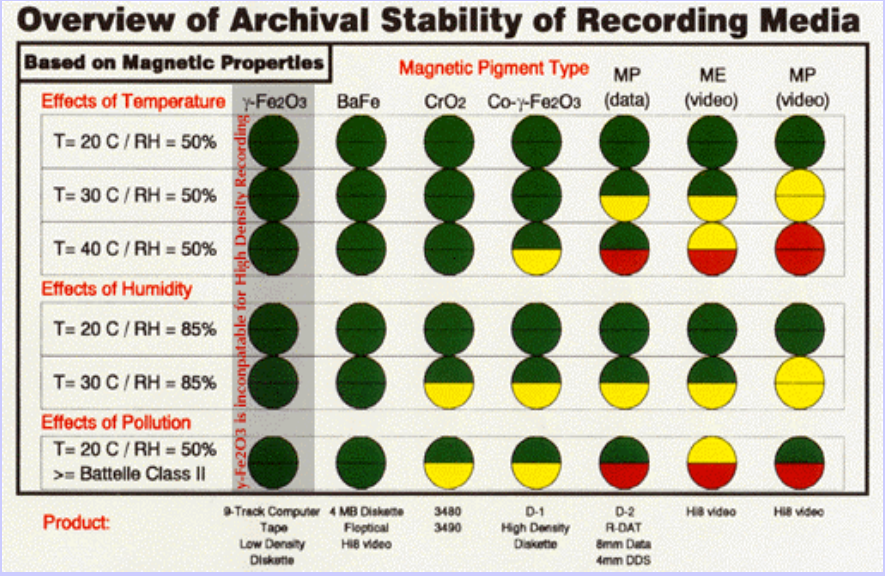


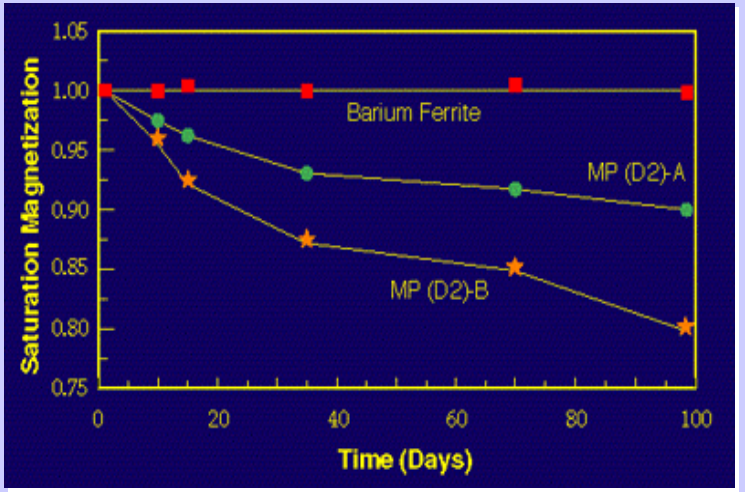
Mag stripe cards: complex technology

SecureNet





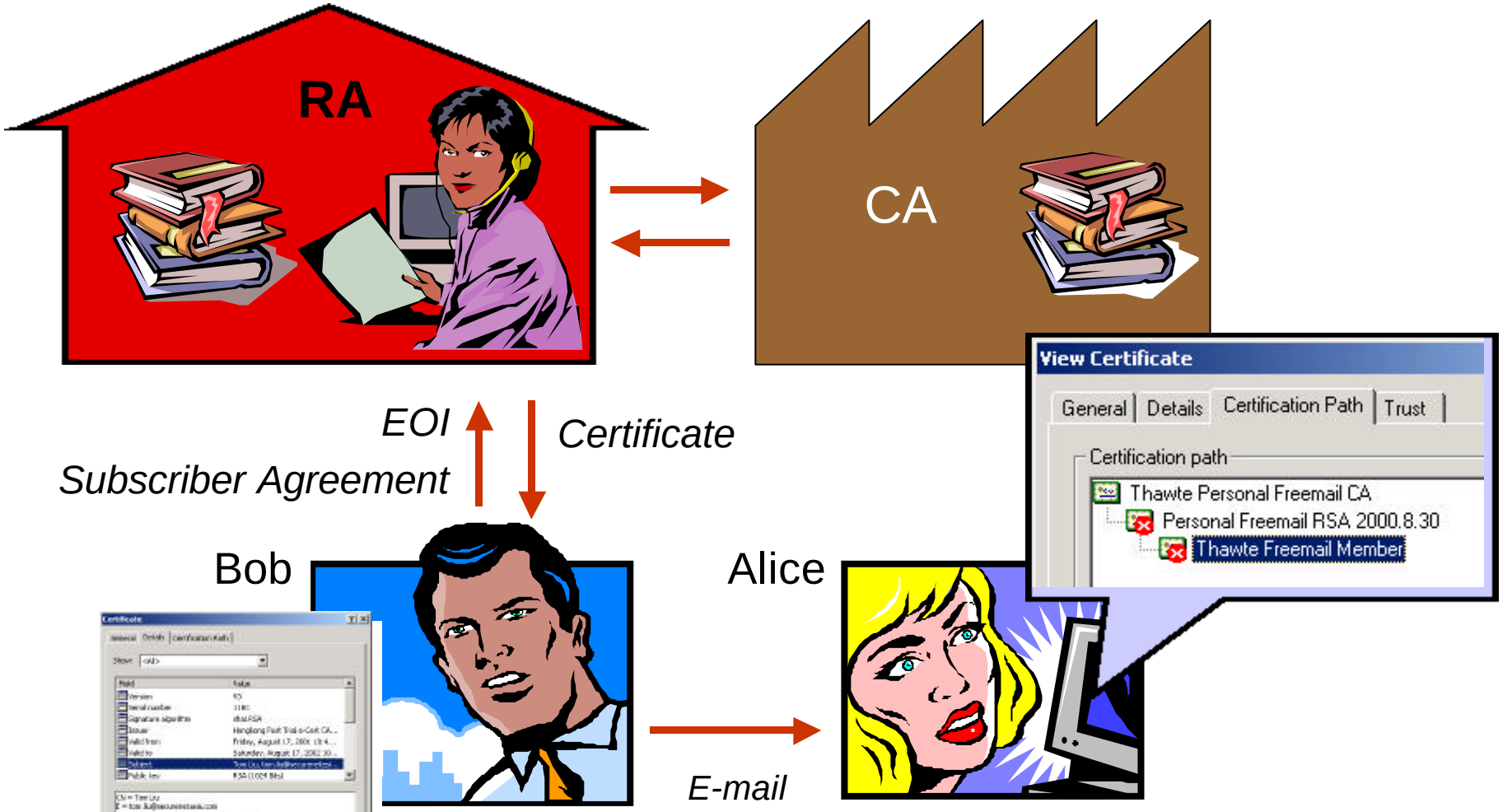




So what do you *really* need to know?

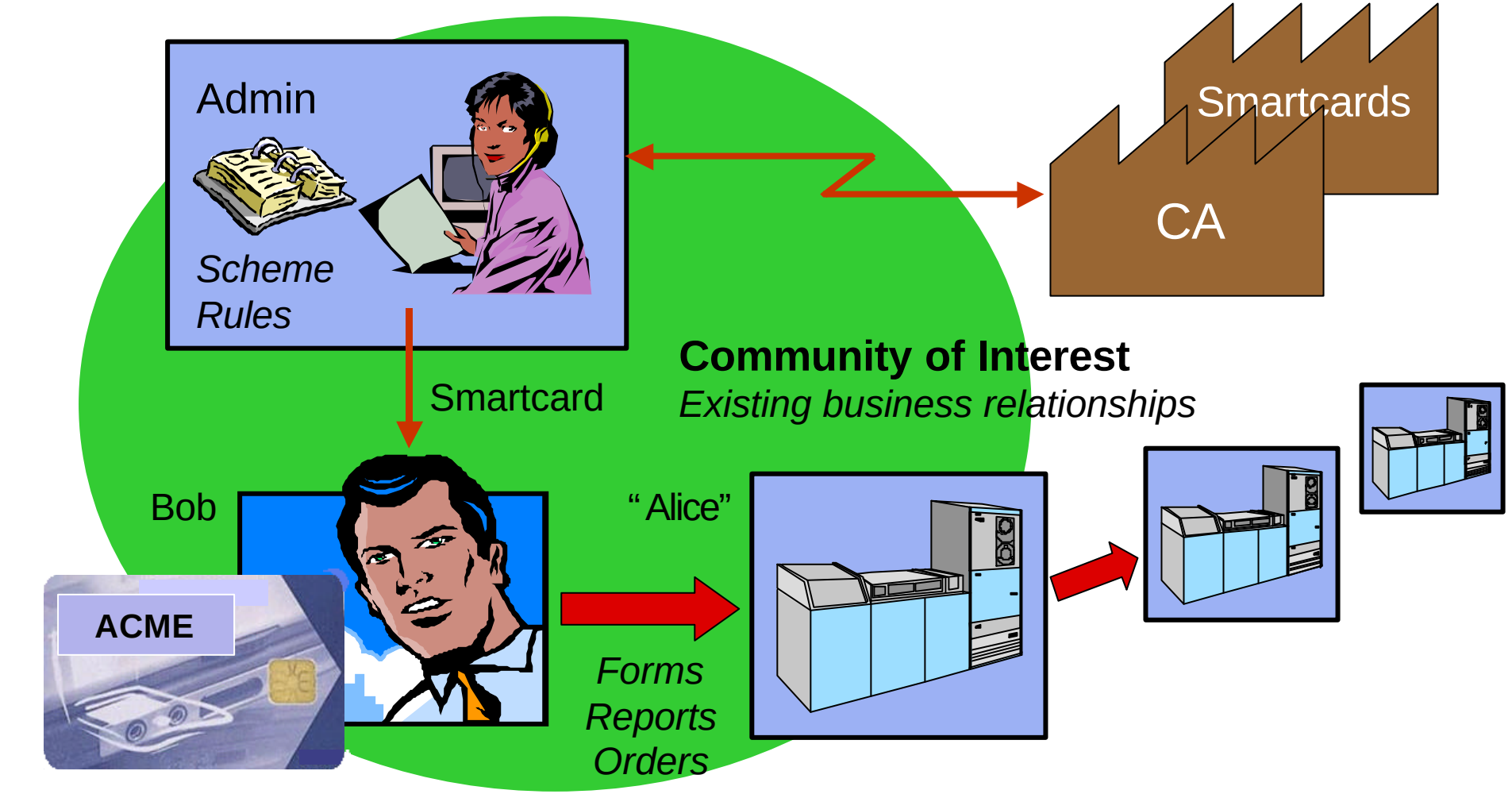
First generation PKI

SecureNet



Contemporary PKI

SecureNet



The technical benefits of digital signatures

SecureNet

- Machine readable
- Preserve integrity and authenticity
  - over long periods of time, and
  - over many copies of the message
- Better quality electronic evidence

The business benefits of digital signatures

SecureNet

- Totally paperless transactions
- Fully electronic completion of contracts
- Easy to rewind transactions
- Reduced cost of IT forensics
- Reduced cost of dispute resolution

Good PKI applications

SecureNet

- **Where a signature is required**
- Reasonable transaction volume (for good ROI)
- Automated / straight through processing
- Multiple receivers; multiple copies
- High risk of dispute or legal challenge

- *Forms, not simple e-mails*
- *Not "stranger-to-stranger" e-business*

Best practice PKI applications

SecureNet

Health eSignature Authority

identrus

United States Patent and Trademark Office

THE NEW TAX SYSTEM

Australian Taxation Office

“Scheme-based” PKI

SecureNet

- Parties already have a business relationship
  - Doctors, lawyers, accountants, other professionals
  - Licence holders (stock brokers, taxi drivers …)
  - Credit card holders
  - Employees, agents …
- Liability determined by existing terms & conditions
- Automatically register user for smartcards
- Use smartcards in special purpose applications

Regulatory implications

SecureNet

- Different PKIs for different business applications
- Do not expect digital certificates to be equivalent!
- “Cross certification” is not an important business objective
- Cross recognition of electronic business cards is better
- Assessment of PKI providers by commercial auditors
- Regulate via Mutual Recognition Arrangements
- Australian Government Gatekeeper scheme moving to:
  - outsource some assessment to IT auditors
  - joint governance with standards accreditation bodies
  - Cross recognise Identrus

From e-passport …

SecureNet

	Early PKI c.1998
Metaphor	Electronic passport
Meaning	Personal identity
Intended use	General purpose transactions
Communities of Interest	General public

… to e-business card

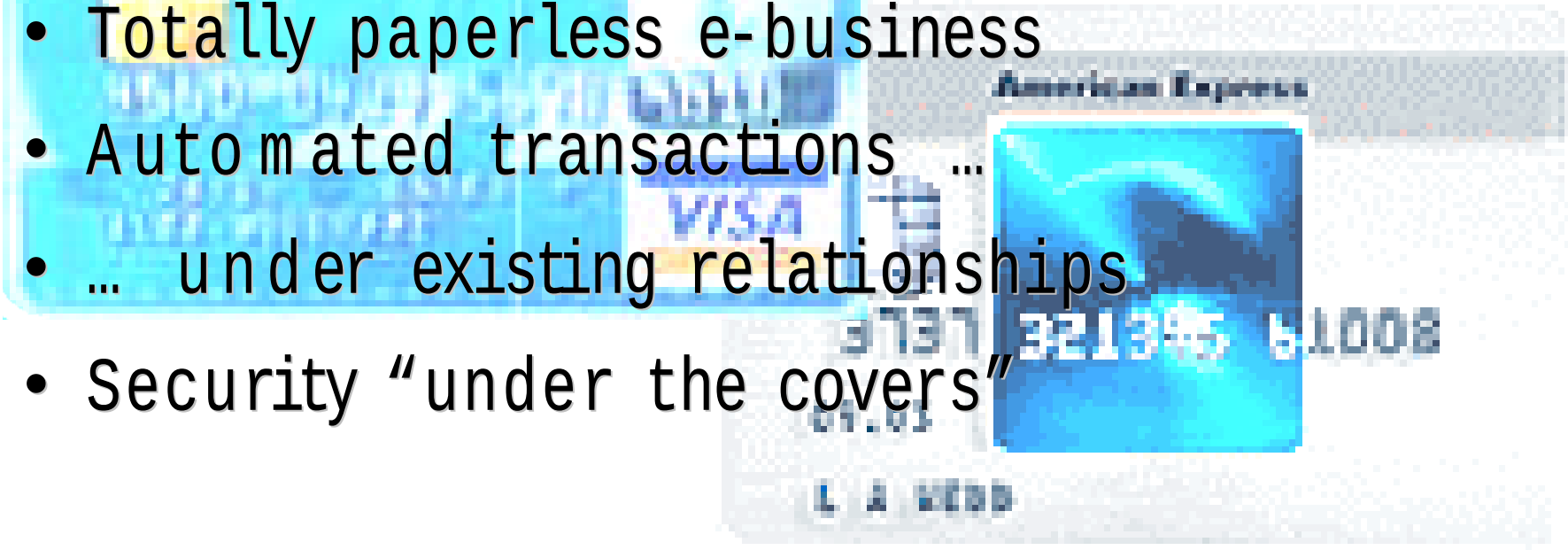
SecureNet

	Early PKI c.1998	Modern PKI c. 2003
Metaphor	Electronic passport	Electronic business card
Meaning	Personal identity	Qualifications
Intended use	General purpose non-descript (email) amongst strangers	Specific transactions between parties with existing relationship
Communities of Interest	General public	Professionals, business licence holders etc.

Contemporary PKI delivers the benefits

SecureNet

- User experience as per any plastic card
- Totally paperless e-business
- Automated transactions …
- … under existing relationships
- Security “under the covers”



Questions?

Stephen Wilson
Chief Security Specialist
swilson@securenet.com.au

www.securenet.com.au

www.securenet.com.au