

A guide to Authentication for Strategists and Policy Makers

IQPC eGovernment Evolution 2006
27 March 2006, Canberra

Stephen Wilson
Lockstep Consulting Pty Ltd



Overview

- **Introductions & Special Objectives**
- **Context**
- **Foundations**
- **Decision making**
- **Misadventure**
- **New technologies**

What is authentication?



The means by which the recipient of a transaction or message can make an assessment as to whether to accept or reject that transaction.

APEC eSecurity Task Group 1997

Definition is neutral re:

- Technology
- Identity
- “Trust”



Copyright © 2006 Lockstep Consulting Pty Ltd

3

The regulatory landscape

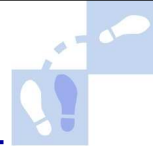


- Technology neutral
Electronic Transactions Act
- The Privacy Act(s)
- Focus on “risk management”
- Best practice ISO 17799
- Anti-Money Laundering

Copyright © 2006 Lockstep Consulting Pty Ltd

4

Technology neutrality



- *No discrimination should be made among the various techniques that may be used to communicate or store information electronically (UNCITRAL)*
- Correct *mindset* when framing law & policy
- Don't build in assumptions that
 - break down too quickly over time
 - break down in unanticipated situations
- Governments (quite properly) like to avoid picking winners

Copyright © 2006 Lockstep Consulting Pty Ltd

5

Tech neutrality gone mad



Results 1 - 10 of about 20,700

Copyright © 2006 Lockstep Consulting Pty Ltd

6

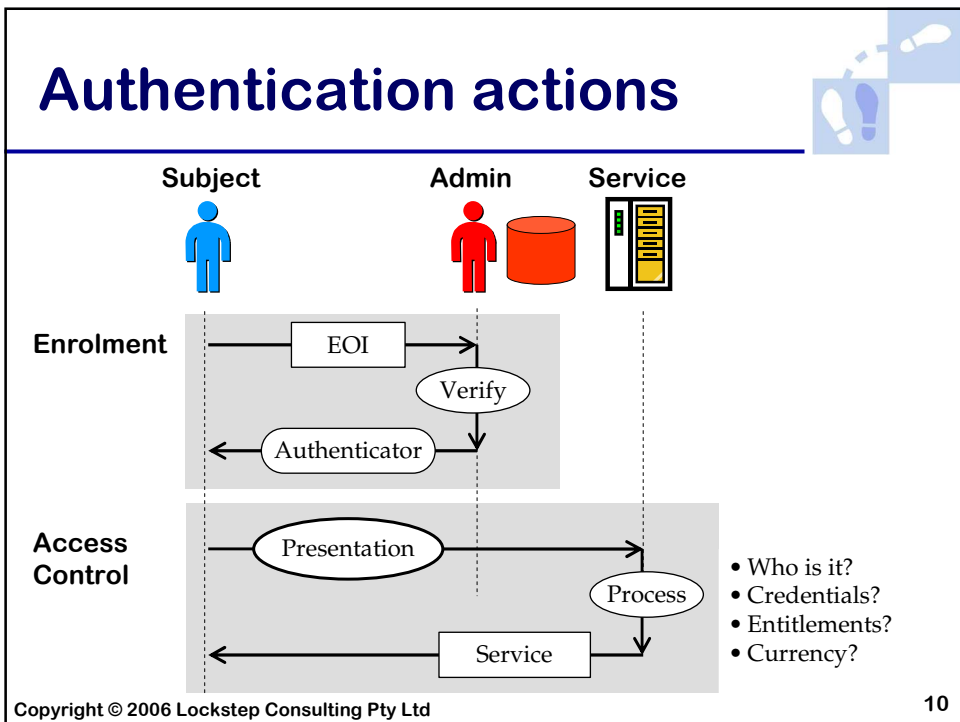
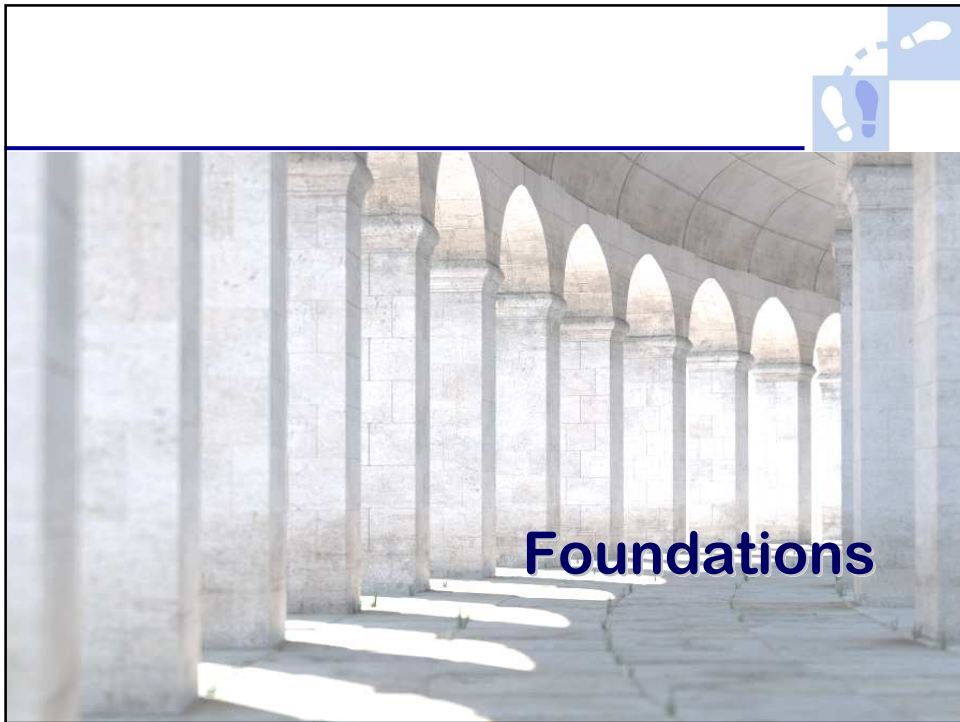
Perils of Tech Neutrality

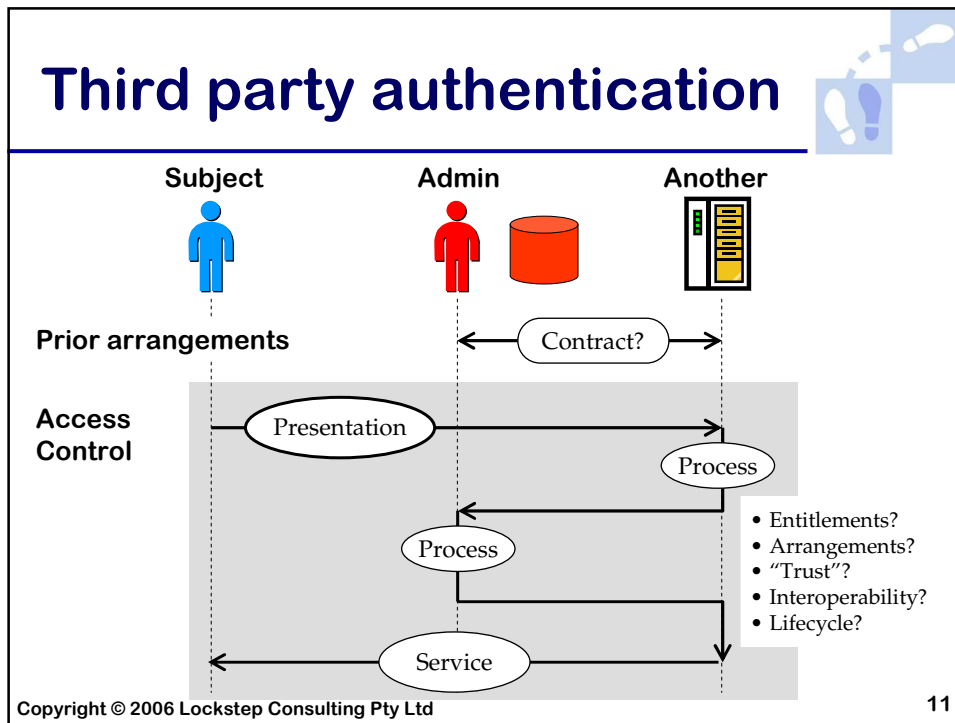


- Technology does matter
 - Not all technologies are equal
 - Users sometimes (!) need guidance
 - Non-standard outcomes
- See also *Technology Neutrality and Secure Electronic Commerce: Rule making in the age of "equivalence"* Michael Baum 1999
http://www.verisign.com/repository/pubs/tech_neutral

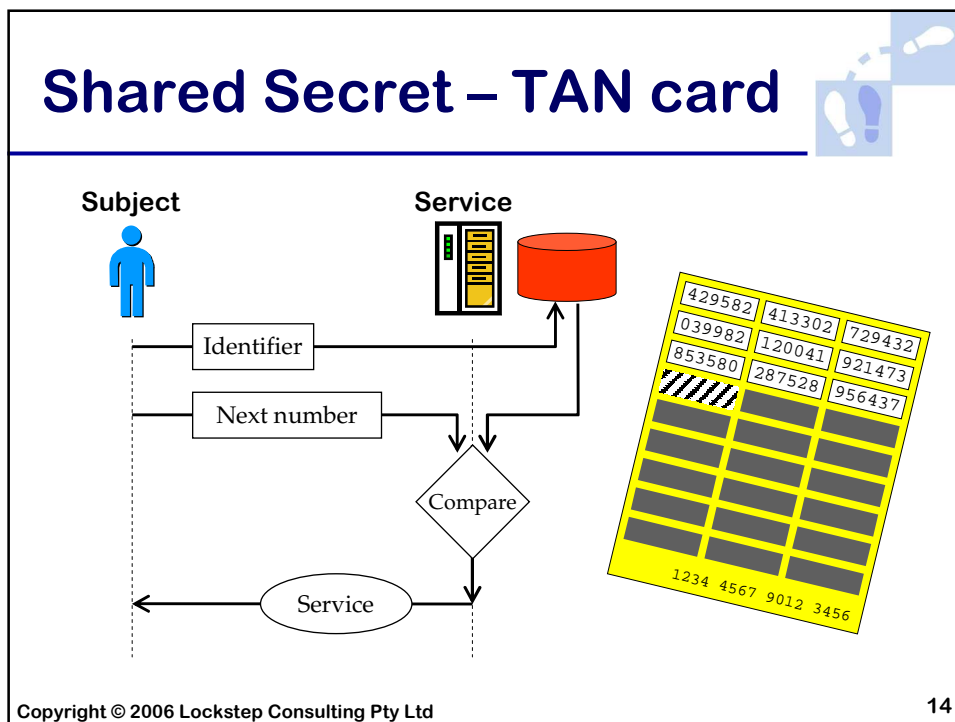
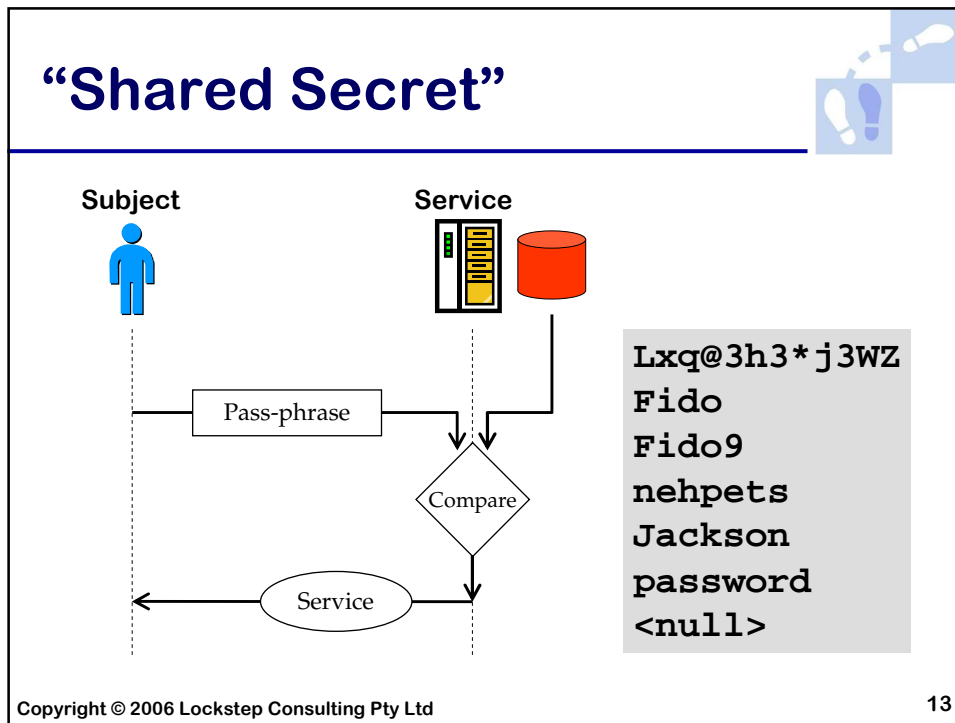
We wouldn't write transport policy without knowing the difference between road and rail. Or without having ever driven a car.

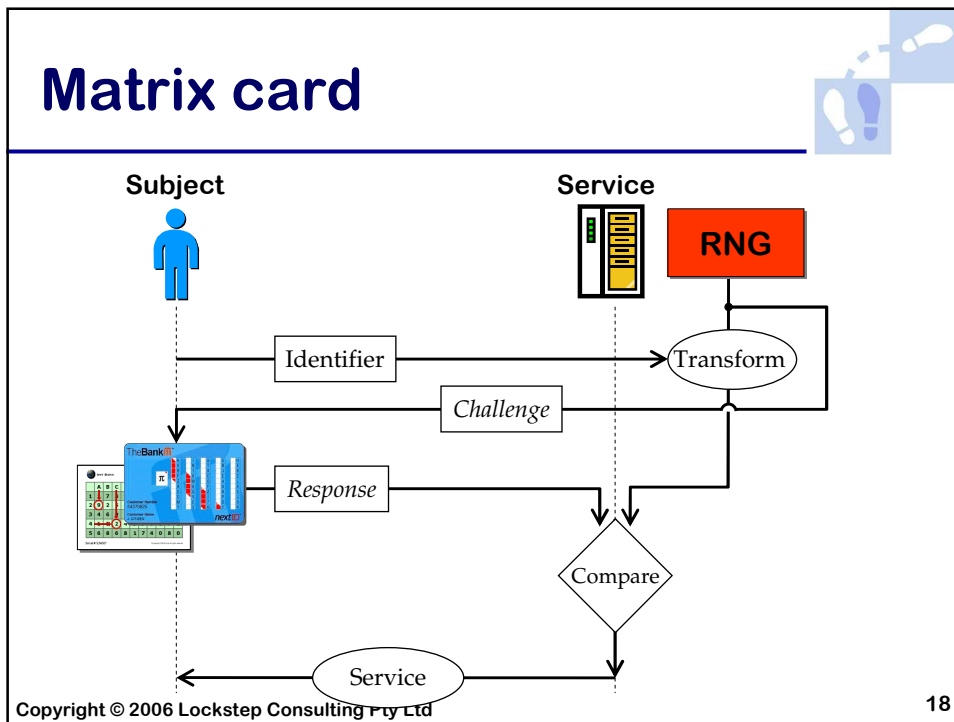
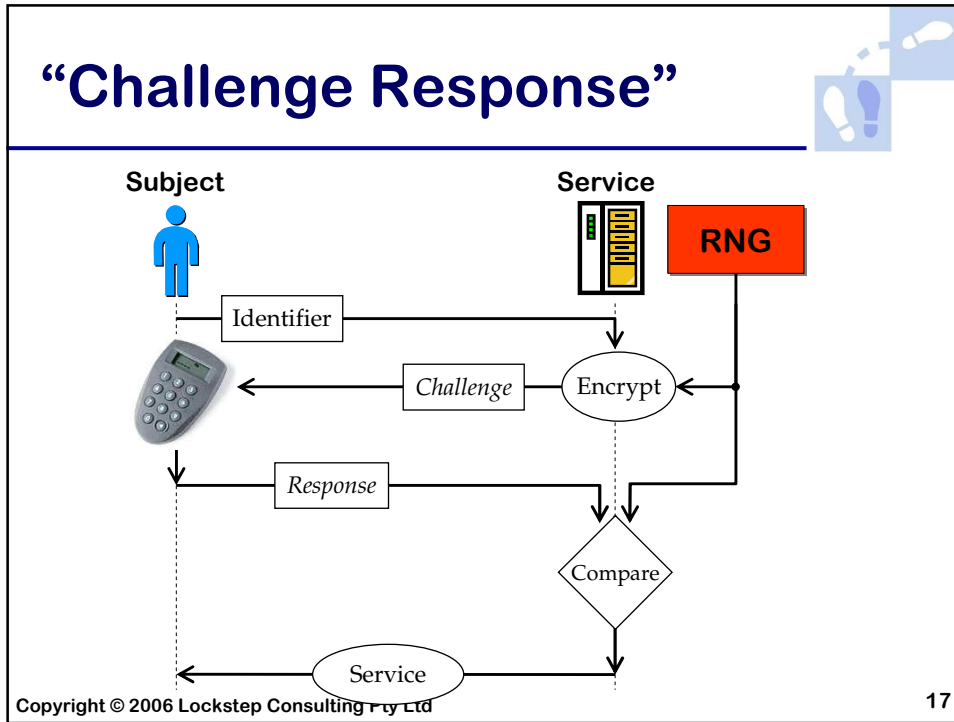


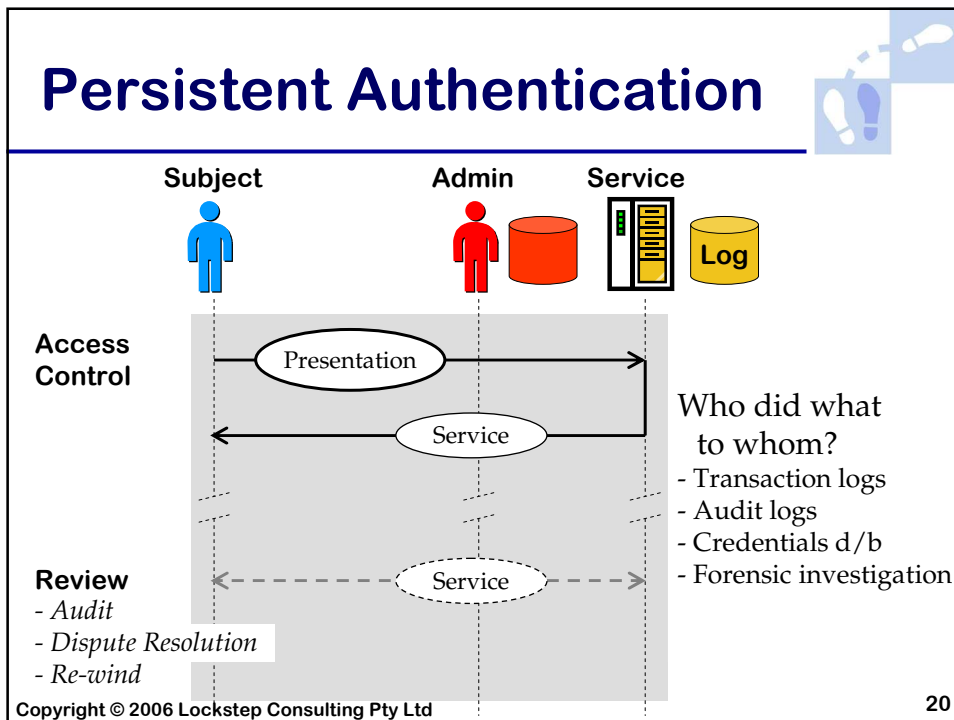
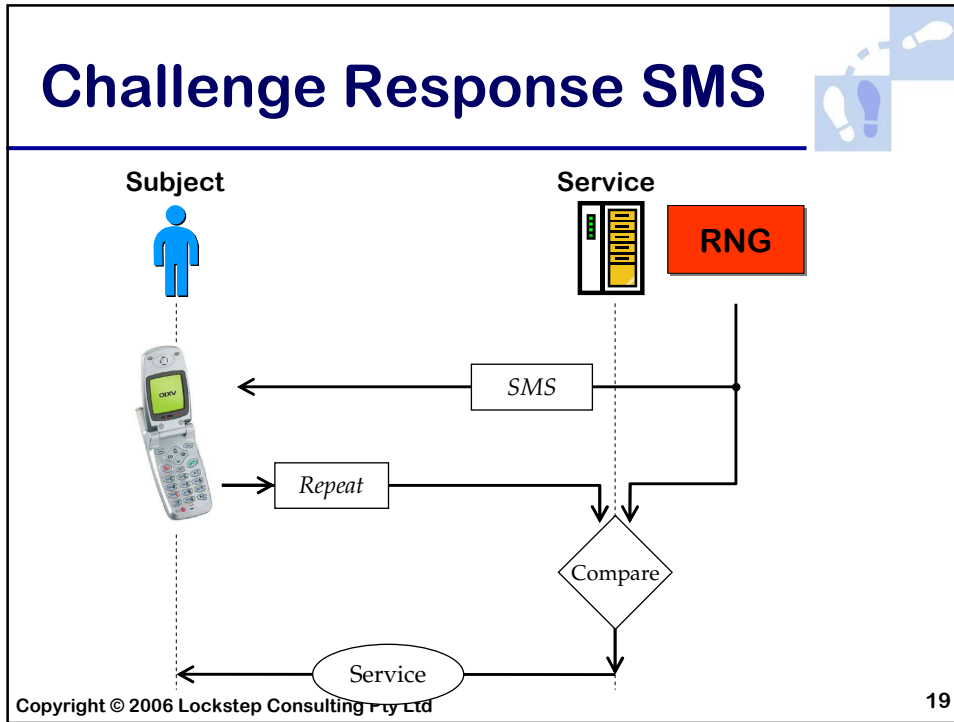


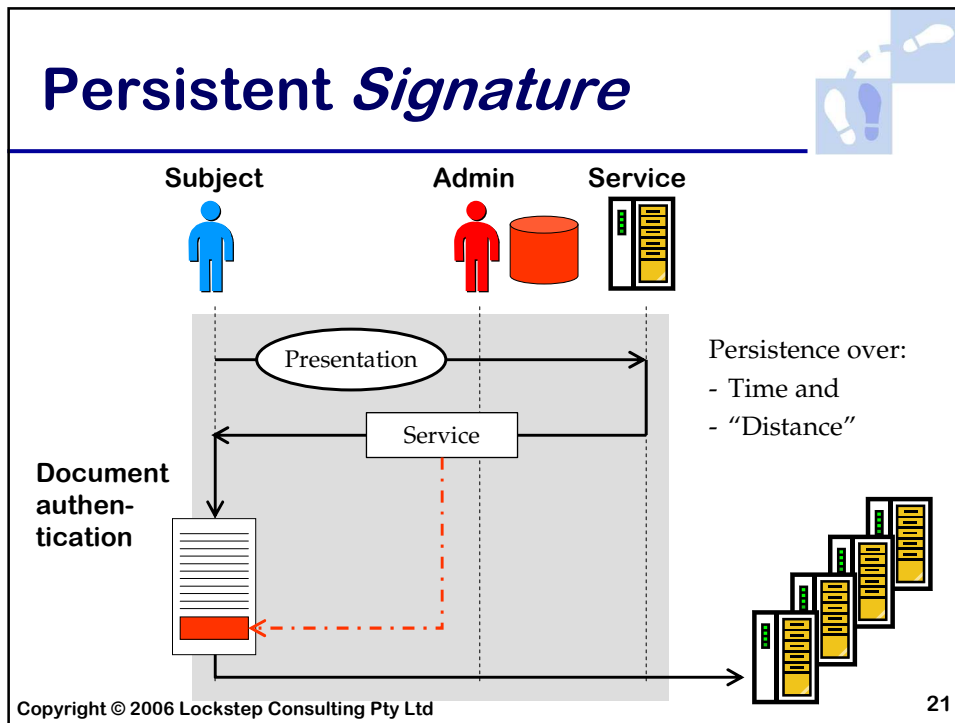


- ## Access control options
- Shared secret
 - Shared secret – TAN card
 - Biometrics
 - Synchronous One Time Passwords
 - Challenge-Response tokens
 - Matrix card
 - SMS
- Copyright © 2006 Lockstep Consulting Pty Ltd 12









Electronic signatures

- “Electronic Signature” not defined in ETA
- UNCITRAL:
 - Electronic signature means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory’s approval of the information contained in the data message

Copyright © 2006 Lockstep Consulting Pty Ltd 22

Our ETA on e-signatures



10 Signature

Requirement for signature

(1) If, under a law of the Commonwealth, the signature of a person is required, that requirement is taken to have been met in relation to an electronic communication if:

- (a) in all **cases—a method is used to identify the person and to indicate the person's approval** of the information communicated; and
- (b) in all **cases—having regard to all the relevant circumstances at the time the method was used, the method was as reliable as was appropriate for the purposes** for which the information was communicated; and

Enhanced e-signatures

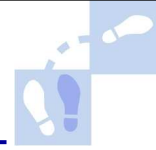


UNCITRAL:

Enhanced electronic signature means an electronic signature in respect of which it can be shown, through the use of a security procedure, that the signature:

- (i) is **unique to the signature holder** for the purpose for which it is used;
- (ii) was created and affixed to the data message by the signature holder or using a means **under the sole control of the signature holder**;
- (iii) was created and is linked to the data message to which it relates in a manner which provides **reliable assurance as to the integrity of the message**

Digital signature

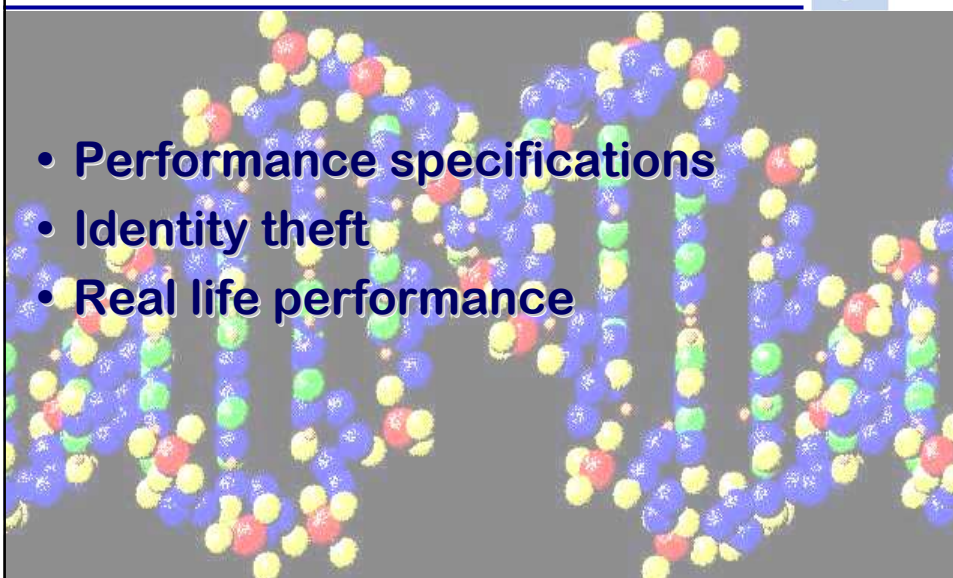


- An electronic signature based specifically on *public key cryptography*
- Uses a “key” unique to the user
- Key should be difficult to copy or steal
- Signature unique to the data too
 - i.e. provides *integrity* assurance

More on biometrics



- Performance specifications
- Identity theft
- Real life performance



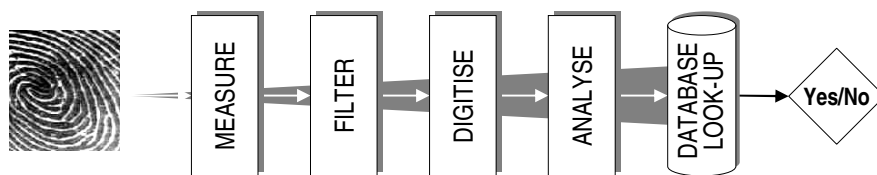
Biometrics specifications

- **False Accept Rate (FAR)**
 - False Positives
 - False Match
 - Error Type 2
- **False Reject Rate (FRR)**
 - False Negatives
 - Error Type 1
- **Failure to Enrol**
- **Equal Error Rate?**
 - Interesting benchmark ...
 - ... *but you might prefer one error over the other*

Copyright © 2006 Lockstep Consulting Pty Ltd

27

Sources of error



*Dirt, sensor damage
Angle / pressure / volume
Injury, ageing
Environmental noise*

*Sensor error
Sensor-to-sensor
variation*

*Filtering
Modeling assumptions*

Copyright © 2006 Lockstep Consulting Pty Ltd

28

FAR-FRR tradeoff

Highly *specific* system

Highly *sensitive* system

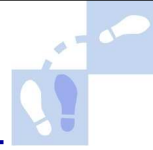
Copyright © 2006 Lockstep Consulting Pty Ltd 29

Gummi Bear Attack

- Gelatin fakes produced from live fingers
- *as well as from latent prints*
- 11 fingerprint readers susceptible to gummy fakes 67-100% of the time

Matsumoto et al *Impact of Artificial Gummy Fingers on Fingerprint Systems*
Proceedings of SPIE Vol. 46772002

Biometrics performance



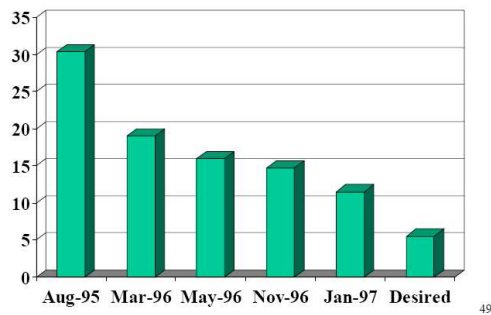
| | Test | FRR | FAR |
|-------------|-----------|--------|------|
| Fingerprint | FVC 2004 | 2% | 2% |
| Face | FVRT 2002 | 1-% | 1% |
| Voice | NIST 2000 | 10-20% | 2-5% |

FVC = International Fingerprint Verification Competition
 RFRT = Facial Recognition Vendor Test
 NIST = National Institute of Standards and Technology

Disney World



Disney Access Time Improvement



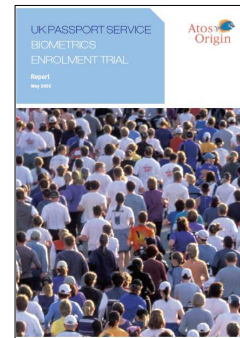
Reference:
*Biometric Authentication Technologies:
 Hype Meets the Test Results*
 Jim Wayman
 San Jose State University, 2002

UK Passport Office Trial



>10,000 subjects (incl. 750 disabled)

| | Time (abled) | Time (disabled) | Accuracy |
|--------|--------------|-----------------|----------|
| Face | 39 sec | 63 sec | 69% |
| Iris | 58 sec | 78 sec | 96% |
| Finger | 73 sec | 80 sec | 81% |



May 2005

Copyright © 2006 Lockstep Consulting Pty Ltd

33

Biometric odds & ends

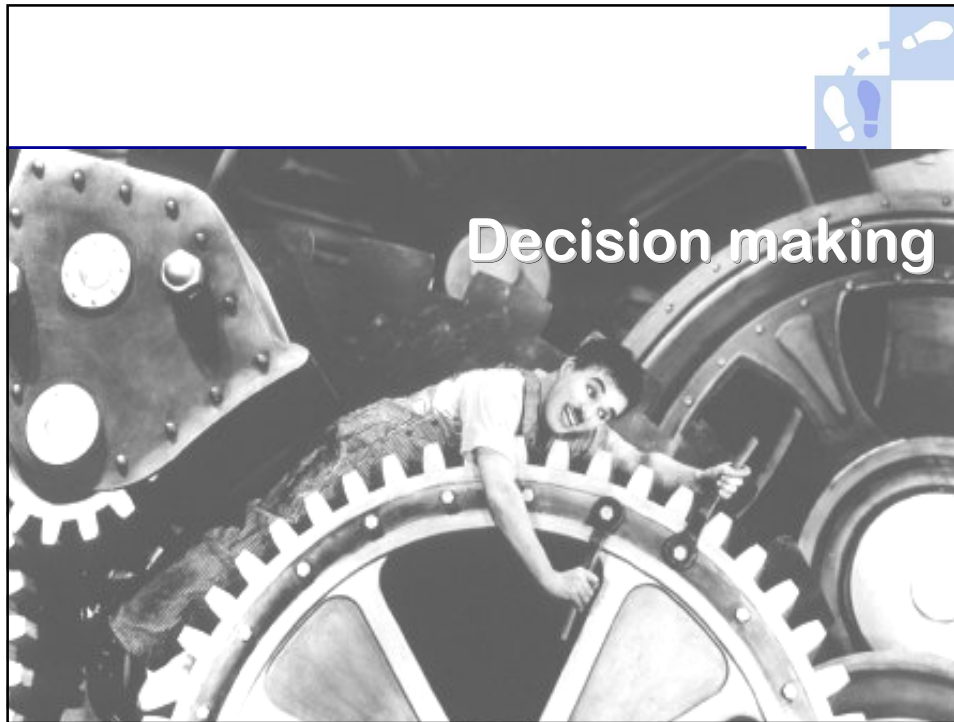


- Strategy in event of compromise?
- Check Fail to Enroll rates
- Insist on liveness detection
- Expect to re-program thresholds

- <http://www.heise.de/ct/english/02/11/114/>
- <http://www.seweb.uci.edu/faculty/cole>
- <http://cryptome.org/gummy.htm>

Copyright © 2006 Lockstep Consulting Pty Ltd

34



How to rate authenticators?

- **Linear ranking?**
 - Low-Medium-High
 - Good-Better-Best
 - Bronze-Silver-Gold

How to rate authenticators?



- Do we select cars by one criterion?
- e.g. Horsepower
 - Or fuel economy
 - Or comfort
 - Or reliability ...
- Getting from A to B ...
 - on suburban street
 - on race track
 - on dirt track
 - on the Pacific Highway

Authentication Risks



1. Counterfeiting
 - Can the authenticator be copied?
 - Are the technology and the manufacturing process sound?
2. Impersonation
 - Is the enrolment process sound?
 - Are liabilities clear?
3. Loss of control
 - Is loss of authenticator obvious?
 - How easy is it to look after?

Auth. Risk Management (1)

Anti-Counterfeiting

- Technological features (algorithms, secret keys, security printing etc)
- Physical security of manufacturing
- Procedural & Personnel controls
- “Chain of Trust”

Auth. Risk Management (2)

Anti-Impersonation

- Evidence of Identity (EOI)
100 point checks (?)
- Identity document verification (DVS)
- *Negative Identification* at enrolment time
(biometrics?)
- *Known Your Customer*
i.e. decentralise enrolment

Auth. Risk Management (3)

Control identity theft

- **Make loss of control more difficult**
 - Two Factor Authentication
 - Consider familiarity of device
 - Biometrics cannot be “lost” (really?)
- **Make loss of control more evident**
 - Passwords (and biometrics) are not self evident
- **Ensure lost authenticators can be revoked**
- **Help desk issues**

Copyright © 2006 Lockstep Consulting Pty Ltd

41

Authenticator attributes

1. **Physically Two Factor**
 - to ward off theft, and make it evident
2. **Mutual Authentication**
 - to resist spoofing, phishing etc
 - to resist Man In The Middle attack
3. **Familiar**
4. **Revocable**
5. **Reliable**
6. **Persistent (depending on the app)**

Copyright © 2006 Lockstep Consulting Pty Ltd

42

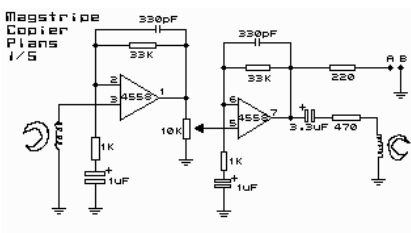
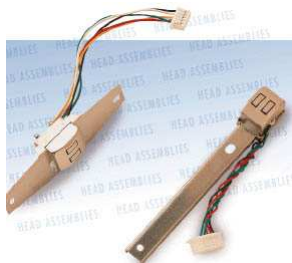
Mapping attributes

| | No. Factors | Mutual Auth? | Revocable? | Persistent? | Familiarity (of 5) | Reliability (of 5) |
|---------------|-------------|--------------|------------|-------------|--------------------|--------------------|
| Shared Secret | 1 | X | ✓ | X | ***** | ***** |
| Biometric | 2 | X | X | X | * | ** |
| Matrix Card | 1 | X | ✓ | X | * | ***** |
| SMS | 2 | X | ✓ | X | ***** | *** |
| OTP etc. | 2 | X | ✓ | X | * | ***** |
| PKI smartcard | 2 | ✓ | ✓ | ✓ | ***** | ***** |

Copyright © 2006 Lockstep Consulting Pty Ltd 43



Identity theft by skimming



Copied from Hack-Tip 8.9/10
Copyright © 2006 Lockstep Consulting Pty Ltd

```

PUBLIC READ_MAG1
EXTERN MDI_SEF (XDATA) ;buffer
EXTERN XP (BIT) ;present
EXTERN M1_CLK (BIT) ;clk bit

M1_SS EQU 5 ;start sentinel
M1_ES EQU 1FH ;end sentinel
SEG CODE
READ_1 PROC
CALL MAG

L?RM1:
MAG_SAM

L?MS1:
L?MS2:

L?MS3:

INC R1 ;sample counter
CJNE R1,IM,L?MS1
L?MS4: MOV A,R1 ;final counter
    
```



Id theft by key logging

| TimeStamp | Window |
|-------------------------|---|
| Thu 05/16/02 @ 01:26 AM | XML File Detail - Microsoft Internet Explorer |
| Thu 05/16/02 @ 01:26 AM | Enter Network Password |
| Thu 05/16/02 @ 01:26 AM | slow.txt - Notepad |
| Thu 05/16/02 @ 01:26 AM | Welcome to MSN.com - Microsoft Internet Explorer |
| Thu 05/16/02 @ 01:25 AM | RealNow Control Panel - Microsoft Internet Explorer |
| Thu 05/16/02 @ 01:25 AM | No page to display - Microsoft Internet Explorer |
| Thu 05/16/02 @ 01:19 AM | ispn.is done |
| Thu 05/16/02 @ 01:16 AM | ispn.is done |
| Thu 05/16/02 @ 01:16 AM | ispn.is done |
| Thu 05/16/02 @ 01:16 AM | ispn.is don |
| Thu 05/16/02 @ 01:16 AM | ispn.is do |
| Thu 05/16/02 @ 01:16 AM | ispn.is d |
| Thu 05/16/02 @ 01:16 AM | ispn.is |
| Thu 05/16/02 @ 01:16 AM | ispn.is |
| Thu 05/16/02 @ 01:16 AM | ispn.is |
| Thu 05/16/02 @ 01:16 AM | ispn.l |
| Thu 05/16/02 @ 01:16 AM | ispn2 |
| Thu 05/16/02 @ 01:16 AM | ispn |
| Thu 05/16/02 @ 01:16 AM | is |
| Thu 05/16/02 @ 01:16 AM | i |

Copy

Phishing lowlights



May 04: (Gartner) 57 million affected in US
3% provide personal info; **19% click through**

Sep 04: *“Non-lending losses increased [through 2004] with higher levels of phishing and cheque fraud”*
A Big Four bank, Financial Results FY04

May 05: IBM reports phishing up 226% in 6 months

Jun 05: *“ASIC issues alert as ‘phishing’ reports double”*

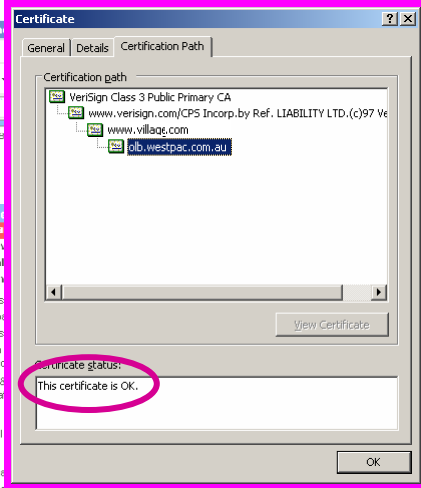
http://news.com.com/2100-7349_3-5234155.html
<http://biz.yahoo.com/bw/050630/305291.html?.v%3D1>
http://www.antiphishing.org/APWG_Phishing_Activity_Report_April_2005.pdf

Trusted websites?



Copyright © 2006 Lockstep Consulting Pty Ltd

The padlock is broken!



The screenshot shows a Windows Certificate dialog box with the 'General' tab selected. The 'Certification path' section lists the following hierarchy: VeriSign Class 3 Public Primary CA, www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign, www.village.com, and job.westpac.com.au. Below the path, the 'Certificate status:' field displays 'This certificate is OK.' The dialog box is overlaid on a web browser window showing a banking site. A red padlock icon in the browser's address bar is circled in red, indicating a security warning. To the right of the dialog box, the text 'The SSL Path Validation flaw' is displayed. Below this text, two URLs are listed: <http://www.theregister.co.uk/content/4/26924.html> and <http://www.theregister.co.uk/content/4/26620.html/>. The page number '49' is in the bottom right corner.

The SSL Path Validation flaw

<http://www.theregister.co.uk/content/4/26924.html>

<http://www.theregister.co.uk/content/4/26620.html/>

Copyright © 2006 Lockstep Consulting Pty Ltd 49

Cautions

The Failure of Two-Factor Authentication

“[Regular] Two-factor authentication won't work for remote authentication over the Internet”

Bruce Schneier Crypto-Gram

March 2005

www.schneier.com/crypto-gram-0503.html#2

US Govt raises the bar



NIST Special Publication 800-63 v1.0.1

Level 4 remote authentication

- 2 factors: “hard token”
- Must resist eavesdroppers
- Must resist man-in-the-middle attacks

“Only practical solution today uses PKI”

Bill Burr, Manager Security technology, NIST

February 2005

http://asia-pkiforum.org/feb_tokyo/NIST_Burr.pdf

Copyright © 2006 Lockstep Consulting Pty Ltd

51

Victoria raises the bar



Inquiry into Fraud and E-Commerce, Drugs and Crime Prevention Committee, 2004

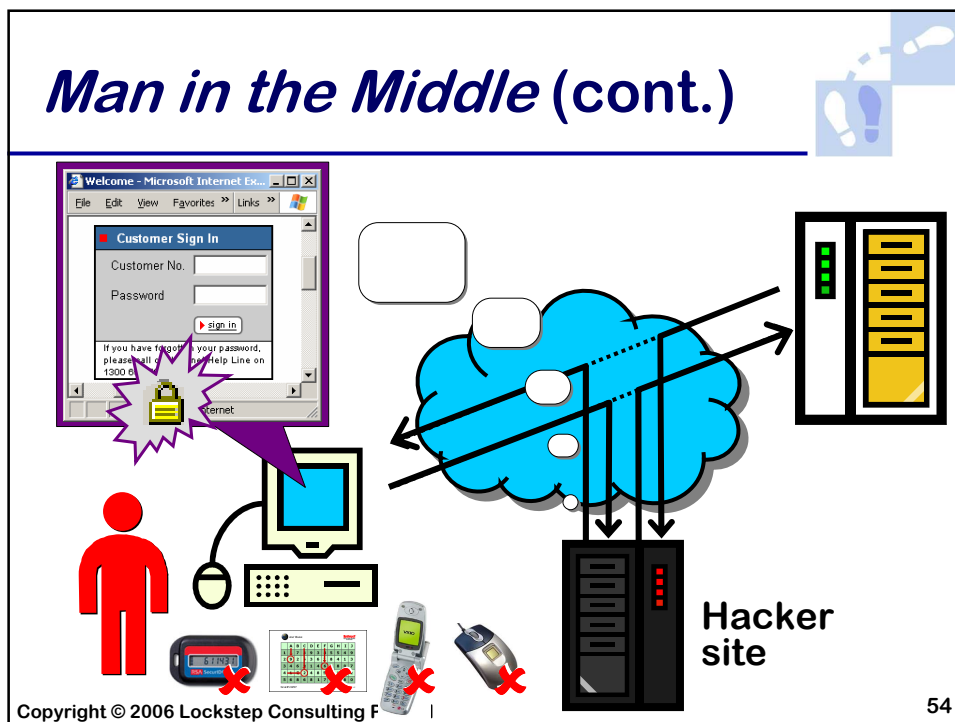
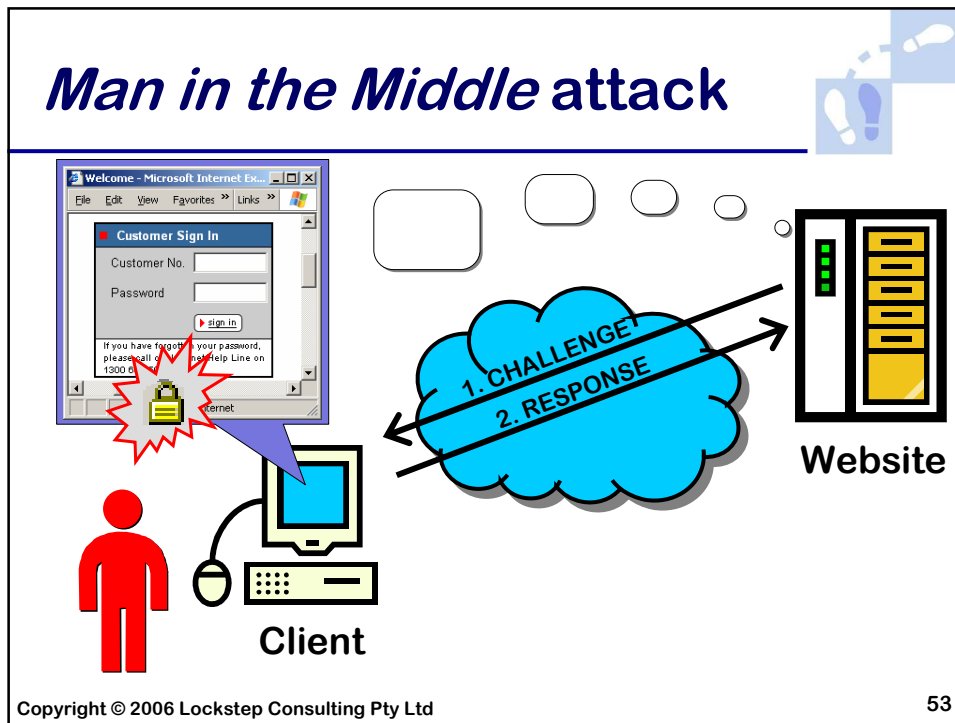
“The Victorian government should support the early roll-out of EMV standard computer-chip plastic cards for use in electronic transactions”

Recommendation 18, p179

www.parliament.vic.gov.au/dcpc/Reports/DCPC_FraudElectronicCommerce_05-01-2004.pdf

Copyright © 2006 Lockstep Consulting Pty Ltd

52



Mutual authentication

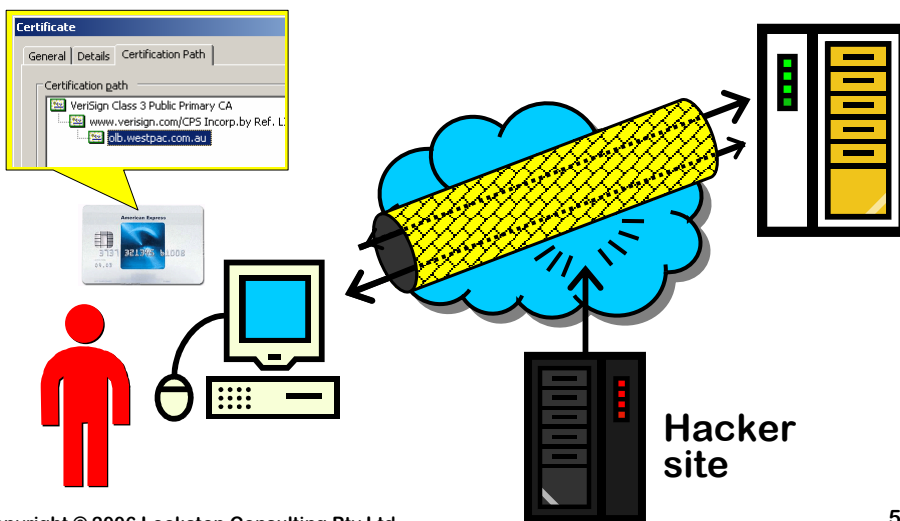


Not the same as Two Factor!

“One reason phishing attacks are successful is that unsuspecting customers cannot determine they are being directed to spoofed Web sites during the collection stage of an attack. ... Digital certificate authentication is generally considered one of the stronger authentication technologies, and mutual authentication provides a defence against phishing and similar attacks.”

US Federal Financial Institutions Examination Council; www.ffiec.gov/press/pr101205.htm

Mutual authentication



Federation



Liberty Alliance



Federated Identity:

“Allows users to link identity information between accounts without centrally storing personal information”

“In practice, this means that users can be authenticated by one company or web site and be recognized and delivered personalised content and services in other locations without having to re-authenticate, or sign on with a separate username and password”

www.projectliberty.org

Standards and tools



- Liberty Alliance
- Shibboleth
- SAML
 - Security Assertions Markup Language
- IIA, Australia Post, eID, Eidentity

Issues



- Drivers licences and video stores
 - Boot strapping vs. live federation
- How difficult is de-federation?
 - What if schemes' rules are different?
- Is it always useful to split identity and authorisation?
 - Or do we have *real*/multiple identities?

PKI



PKI's traditional advert



- **Confidentiality**
 - But this is *symmetric* crypto function
- **Authentication**
 - *Authorisation* usually more important
- **Integrity**
 - Many alternatives to PKI
- **“Non-repudiation”**
 - A myth! Does not require PKI

PKI's fundamental benefits

1. Tamper resistant, long lived evidence of “who did what to whom”
2. Digital certificates can bind *authority information* as well as (or instead of) identity e.g. credentials, licences, affiliations
3. 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 |
|-----------------------|--------------------------------------|---|
| <i>Meaning</i> | “e passport” | e business card |
| <i>Intended use</i> | General purpose e-commerce | Specific B2B apps |
| <i>Communities</i> | One: the public | Many (industry sectors, professions, schemes ...) |
| <i>Implementation</i> | Single one-size-fits-all certificate | Multiple certificates, increasingly embedded) |
| <i>Registration</i> | Strict face-to-face ID proofing | Automatic via existing member databases |

Understanding evolves (2)

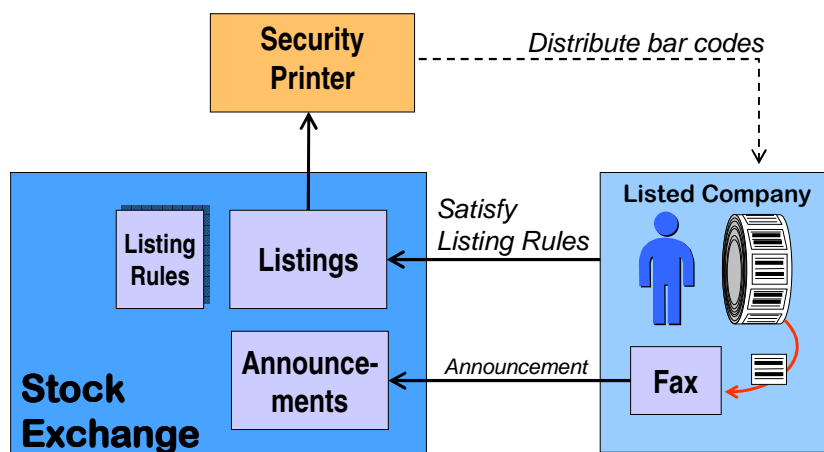


Dr. Stephen Kent (co-chair IETF PKIX WG)

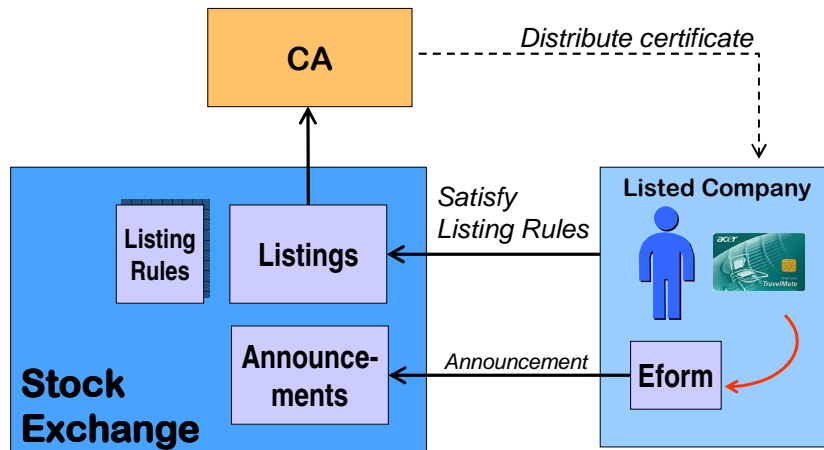
“For big CAs, there is an implicit assumption that a single cert. is all that a user should need. This assumes that one identity is sufficient for all applications, which contradicts experience.”

Asia PKI Forum, Taipei, September 2005

Analogy: CAs as security printers



Analogy: CAs as security printers (2)



Copyright © 2006 Lockstep Consulting Pty Ltd

67

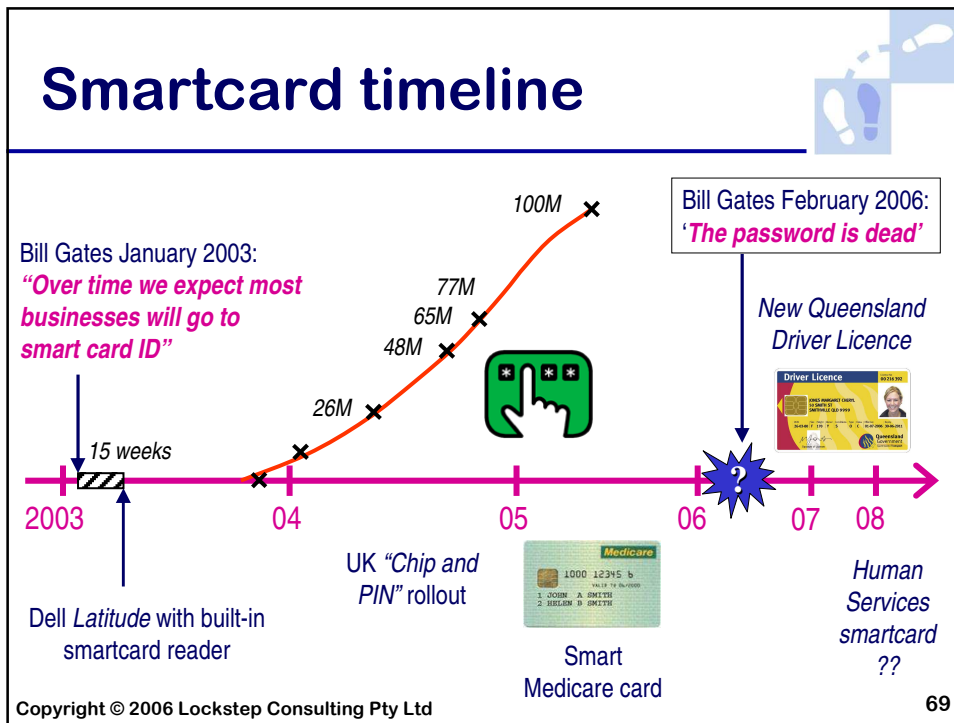
PKI best practices

- **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



Copyright © 2006 Lockstep Consulting Pty Ltd

68



Bill Gates RSA 14/2/2006

"Another weak link is in authentication. Today, we're using password systems, and password systems simply won't cut it ...

And so we need to move to multifactor authentication. A lot of that will be a smart-card-type approach ... It's a significant change and that needs to be built into [Windows] itself."

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

Copyright © 2006 Lockstep Consulting Pty Ltd 70


Smartcards globally

| | |
|--------------------|--|
| Australia: | ½ M ANZ <i>First</i> cards |
| Japan: | 1 M residence cards |
| Hong Kong: | 4 M SMARTICS (6M target) |
| USA: | 4 M staff id cards in DoD (14 M PIV cards end CY06) 18 M Visa & Amex smartcards |
| Taiwan: | 22 M health smartcards |
| UK: | 110 M chip & PIN cards |
| EMV global: | 329 M (up 25% in 6m to June 05) |

Copyright © 2006 Lockstep Consulting Pty Ltd 71

Offline fraud control


(1) Doctor shopping



**Prescription
EVENT
SUMMARY**

Sig (Dr)

(2) Over servicing



**Test
EVENT
SUMMARY**

**Sig (Dr)
Sig (Pt Card)**

Medicare

Copyright © 2006 Lockstep Consulting Pty Ltd 72

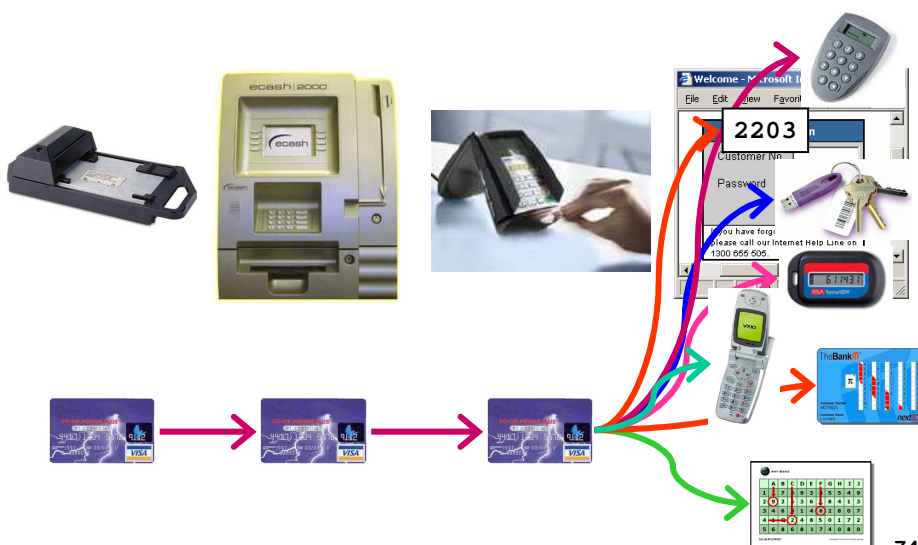
Benefits of smartcards

- can carry and enforce card holder entitlements
- can detect abuse offline
- minimise personal info transmitted over network (preserving privacy and improving performance)
- can indelibly yet anonymously mark all transactions, to mitigate fraud without compromising privacy
- provide the “*the only practical solution [to eavesdropping and account hijacking] today*”
- resist skimming and counterfeiting.

Copyright © 2006 Lockstep Consulting Pty Ltd

73

Authentication diverges ...



Copyright © 2006 Lockstep Consulting Pty Ltd

74

... or converges!



Copyright © 2006 Lockstep Consulting Pty Ltd

75

Further reading

- www.lockstep.com.au/library
- www.pkiforum.org/resources
- piv.nist.gov
- www.antiphishing.org

Copyright © 2006 Lockstep Consulting Pty Ltd

76

Discussion



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

Copyright © 2006 Lockstep Consulting Pty Ltd

