

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”



The regulatory landscape



- Technology neutral
Electronic Transactions Act (Cth) 1999
- The Privacy Act(s)
- Focus on “risk management”
- Best practice ISO 17799, 27001
- Anti-Money Laundering (and Basel II)
greater onus to “know your customer”

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**

Perils of Tech Neutrality



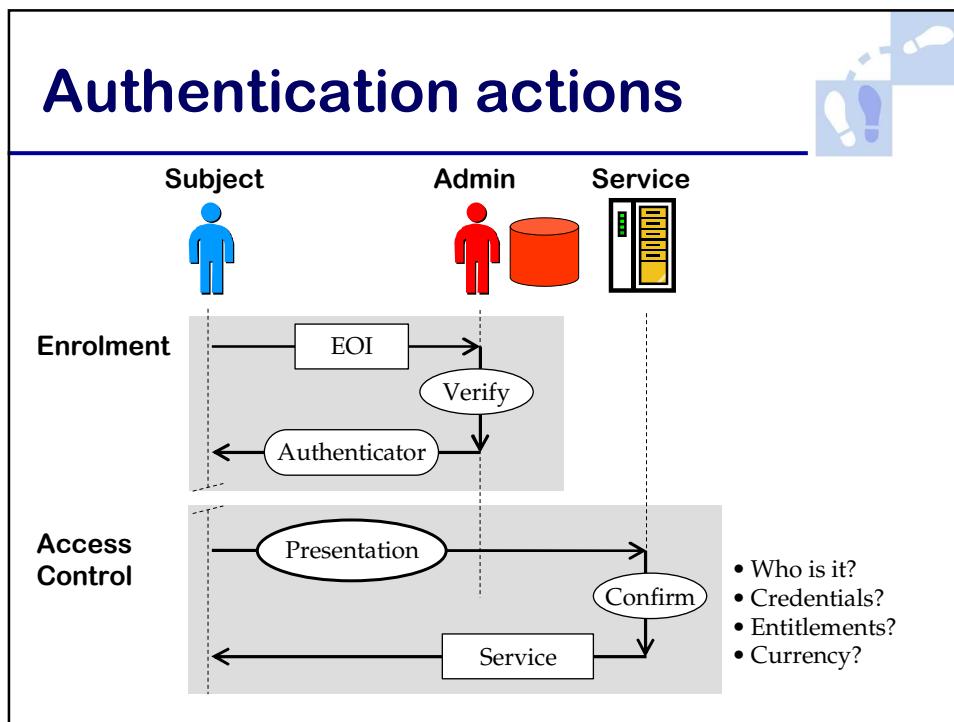
- **Don't slip into technology *indifference***
 - not all technologies are equal
 - users sometimes need guidance
 - risk of non-standard outcomes

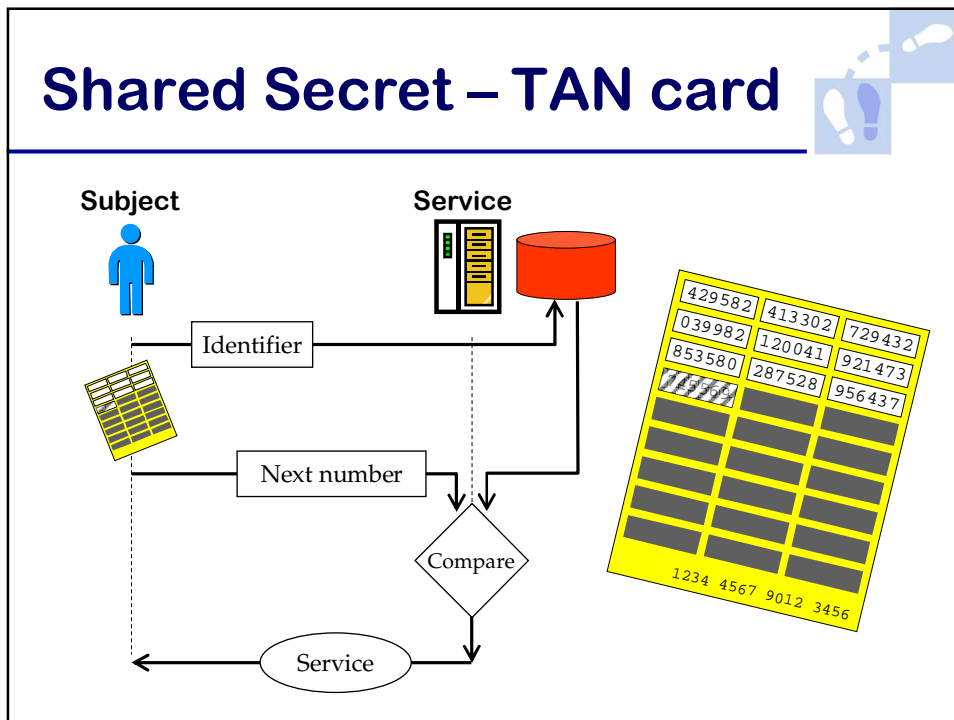
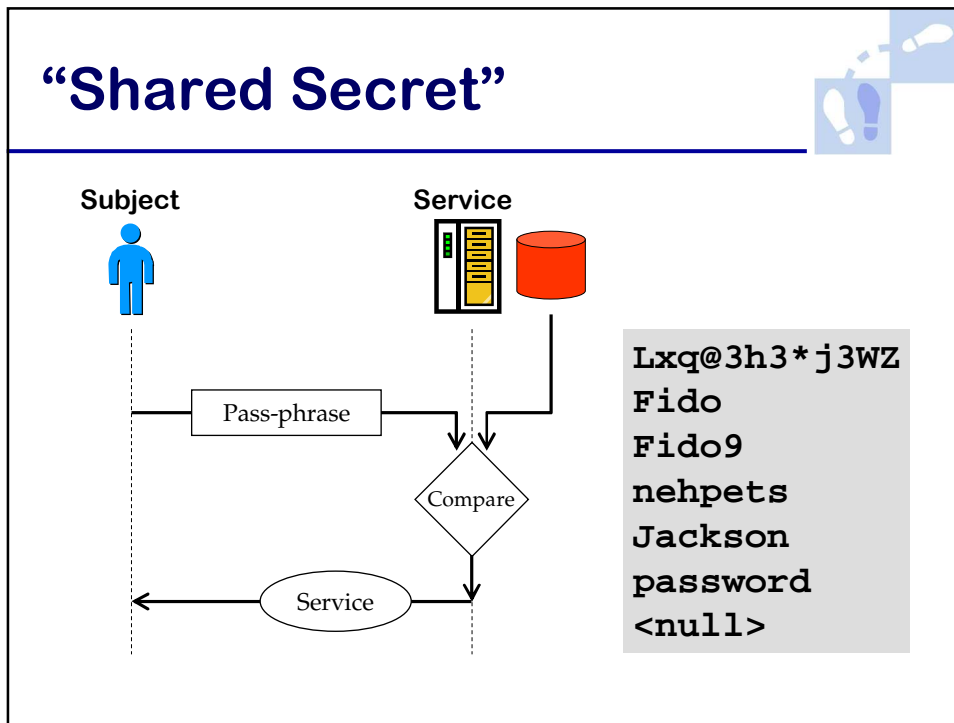
See also

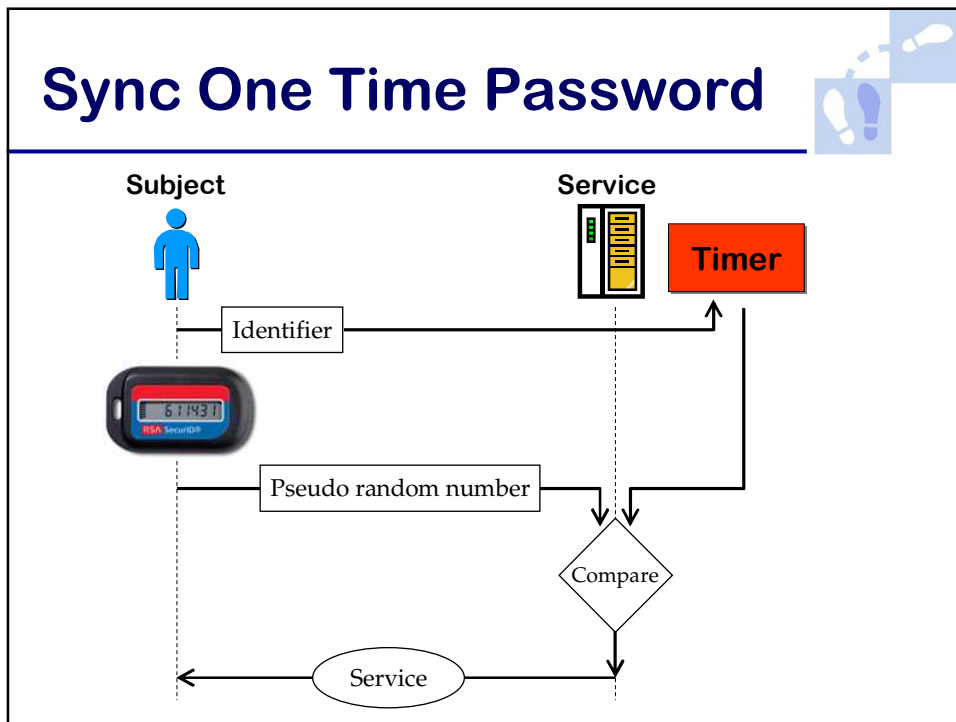
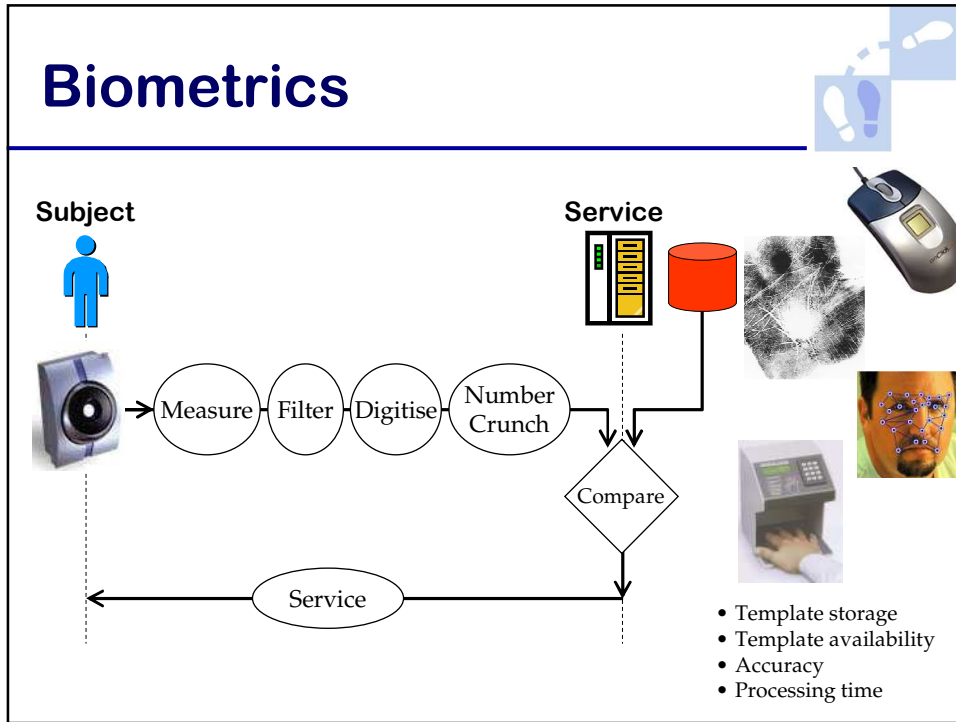
Technology Neutrality and Secure Electronic Commerce: Rule making in the age of "equivalence"

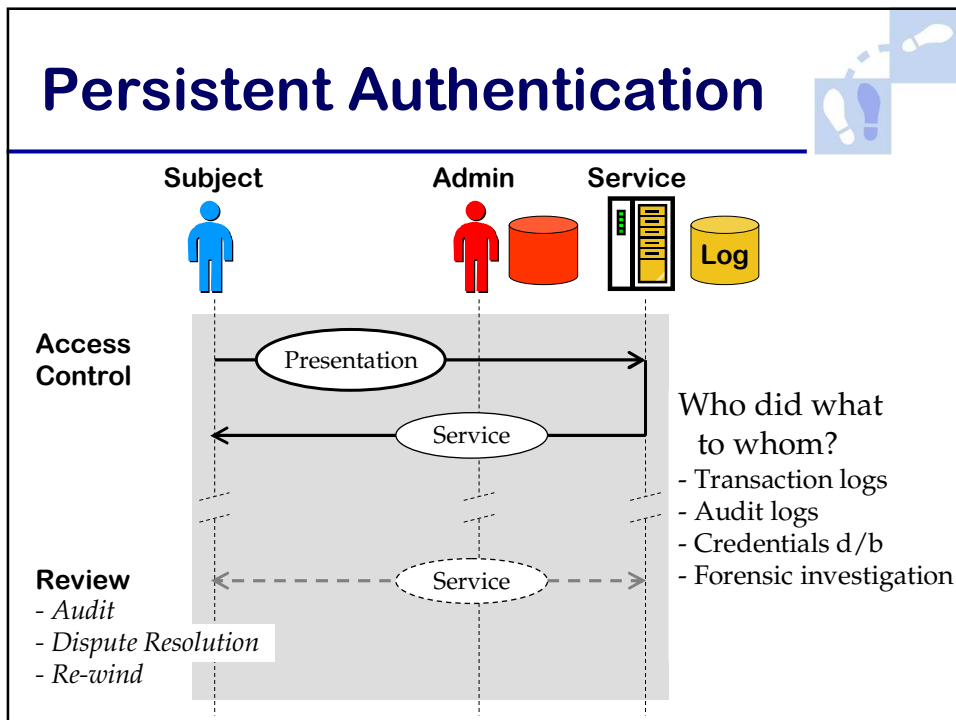
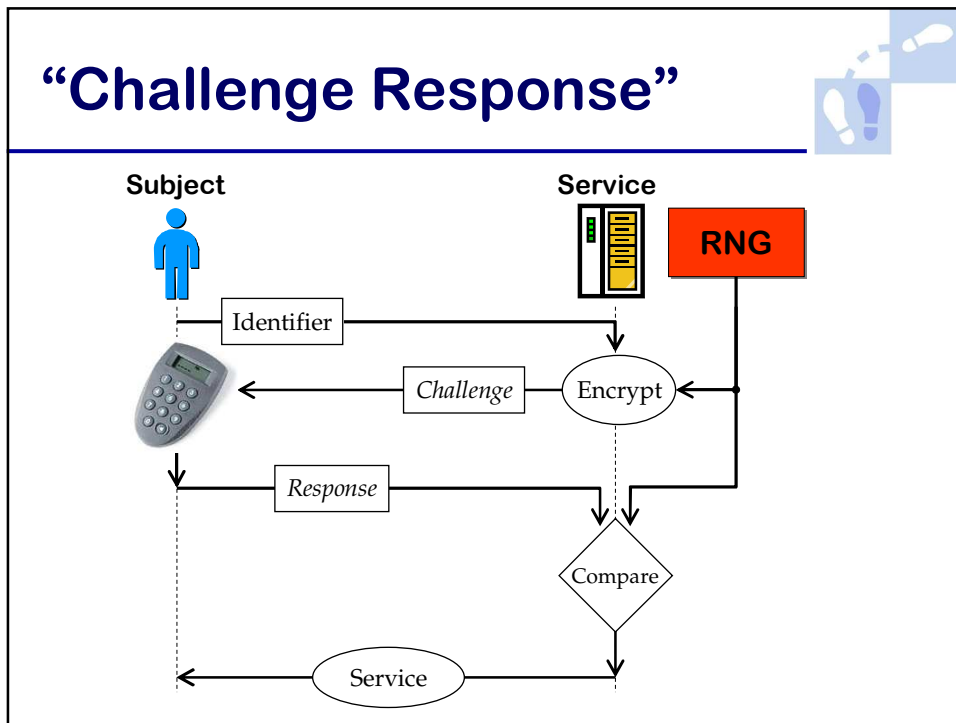
Michael Baum 1999

http://www.verisign.com/repository/pubs/tech_neutral









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

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

Biometrics

- Performance specifications
- Identity theft
- Real life performance

Sources of error

```

    graph LR
      A[MEASURE] --> B[FILTER]
      B --> C[ANALYSE]
      C --> D[DATABASE LOOK-UP]
      D --> E{Yes/No}
  
```

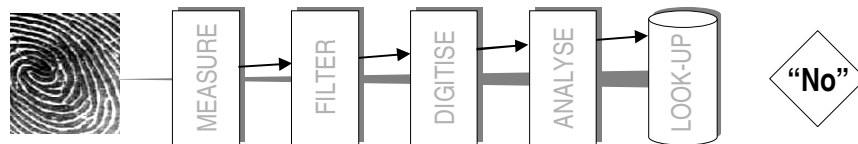
*Dirt, sensor damage
Angle / pressure / volume
Injury, ageing
Environmental noise*

*Sensor error
Sensor-to-sensor
variation*

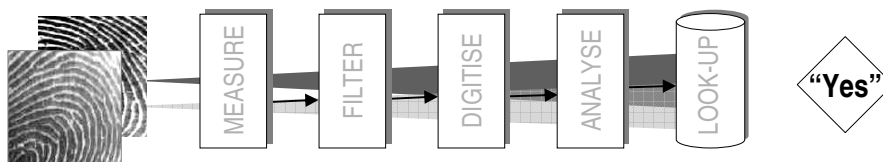
*Filtering
Modeling assumptions*

FAR-FRR tradeoff

Highly *specific* system: False Reject

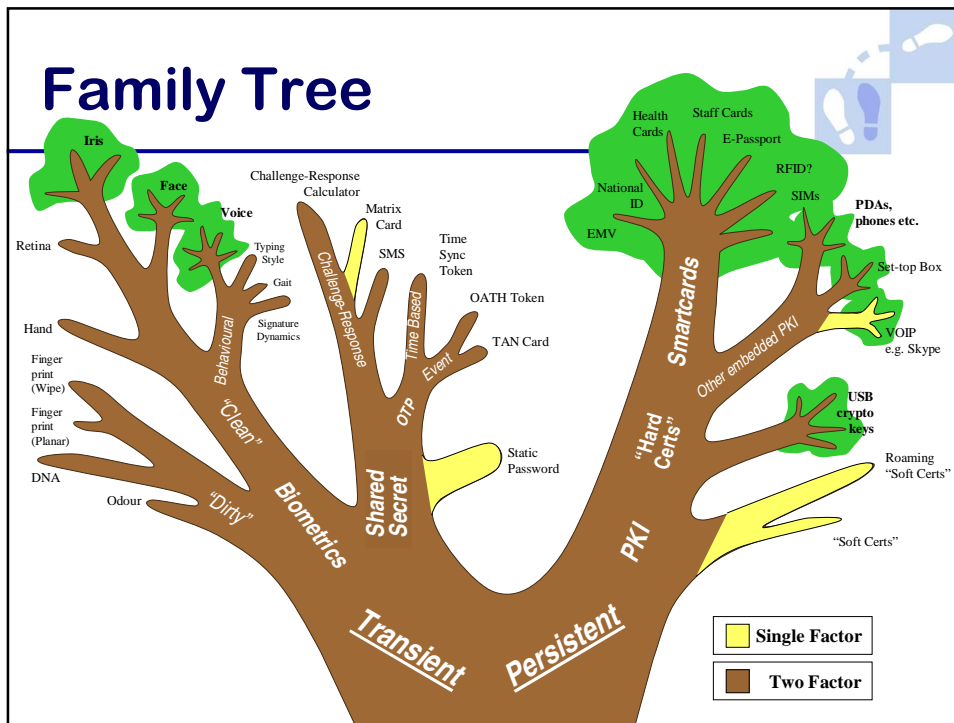


Highly *sensitive* system: False Reject



Biometric odds & ends

- Strategy in event of compromise?
 - Check Fail to Enroll rates
 - Insist on liveness detection
 - Expect to fine tune thresholds
-
- <http://www.heise.de/ct/english/02/11/114/>
 - <http://www.seweb.uci.edu/faculty/cole>
 - <http://cryptome.org/gummy.htm>



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?

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. **Renewable**
5. **Reliable**
6. **Persistent (depending on the app)**

Mapping attributes



	No. Factors	Mutual Auth?	Renewable?	Persistent?	Familiarity	Reliability
Shared Secret	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	*****	?
Biometric	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	*	***
Matrix Card	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	*	****
SMS	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	****	***
OTP etc.	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	*	****
PKI smartcard	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	****	*****

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

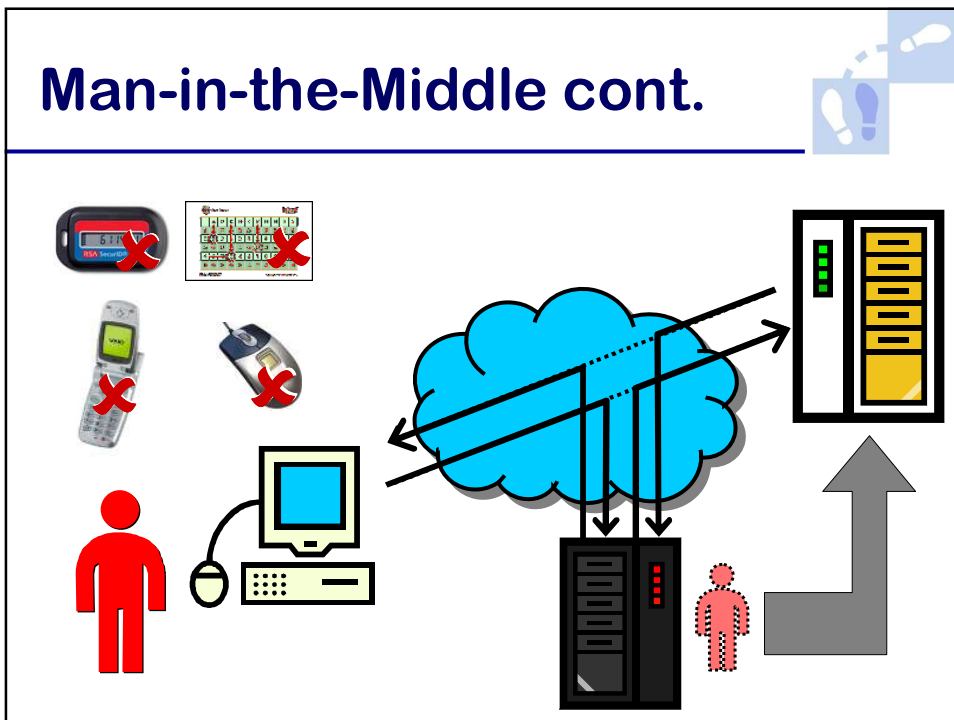
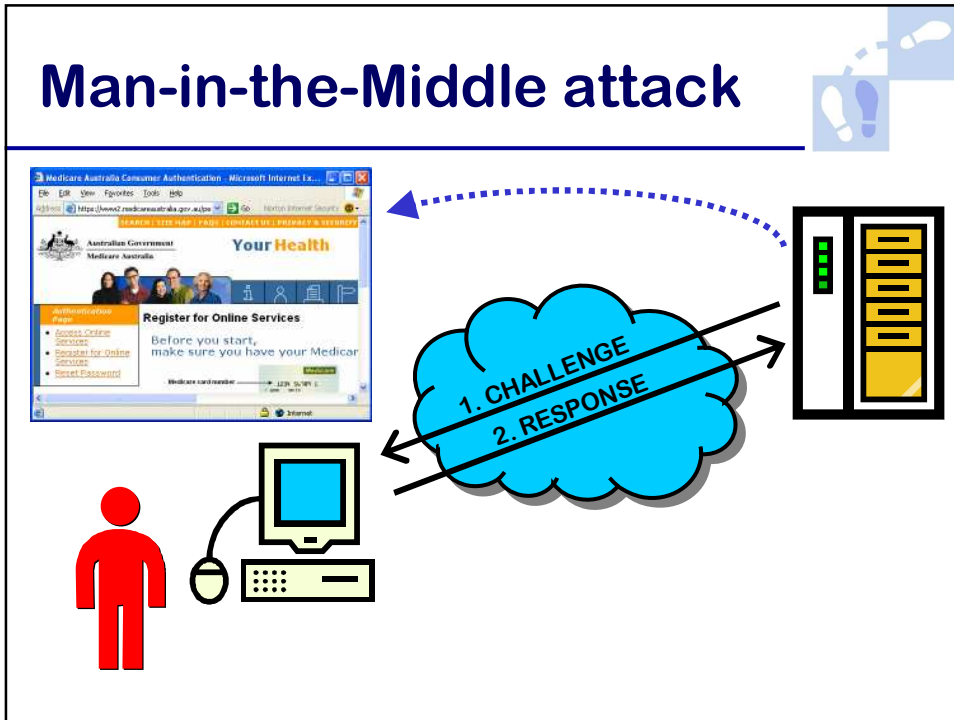
- 2 factors: “hard token”
- Must resist eavesdroppers
- Must resist man-in-the-middle attacks

“Only practical solution today uses PKI”

Bill Burr, Manager Security technology, NIST

February 2005

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



Successful attacks



Oct 2005 Nordea Bank

– TAN Card

www.f-secure.com/weblog/archives/archive-102005.html#00000668

July 2006 Citibank

– Event based OTP Card

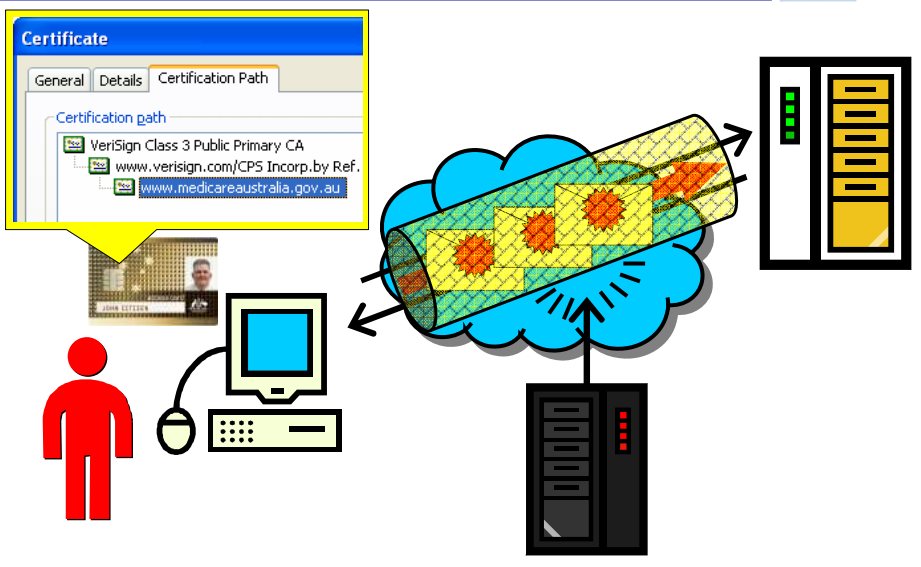
http://blog.washingtonpost.com/securityfix/2006/07/citibank_phish_spoofs_2factor_1.html

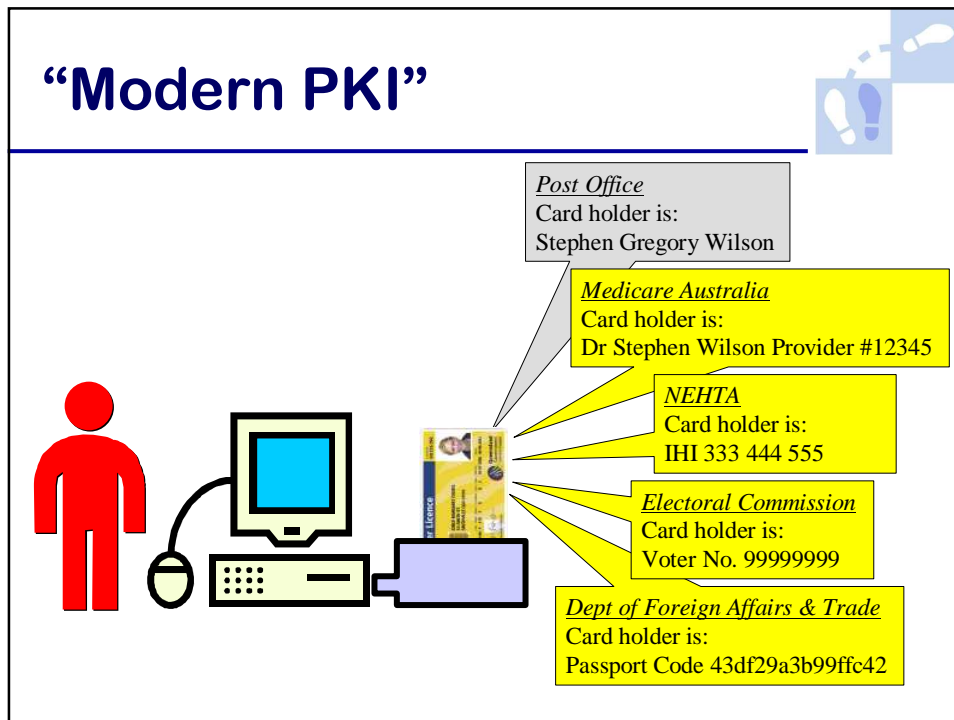
April 2007 ABN AMRO

– Time synchronised OTP Card

http://www.theregister.co.uk/2007/04/19/phishing_evades_two-factor_authentication/

Mutual Authentication





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”*

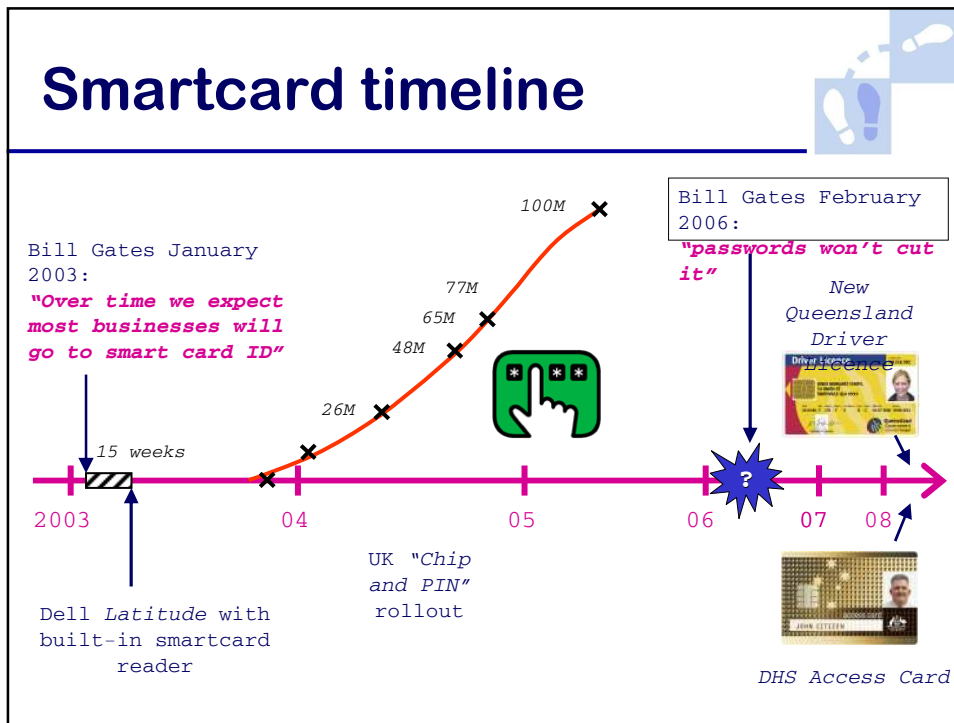
Bill Burr (NIST) Asia PKI Forum, Tokyo, Feb 2005
http://asia-pkiforum.org/feb_tokyo/NIST_Burr.pdf

Understanding evolves

	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

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 
- **Skype** 



Smartcard landscape scan

Australia:	1 M ANZ <i>First</i> cards cf. 12M Credit cards in Australia
Hong Kong:	5 M SMARTICS (6M target)
USA:	4 M staff id cards in DoD 40 M PIV cards 2007-10 estimate 18 M Visa & Amex smartcards
Taiwan:	22 M health cards ?? M All mag stripe bank cards replaced Currently transitioning to EMV
France:	40 M Sesame Vitale health cards Phase 2 brings PKI, e-signatures
Germany	80 M Gesundheitskarte
UK:	110 M Chip & PIN EMV cards
EMV global:	410 M (approx 40% CAG 2005/06)

Decentralise fraud control

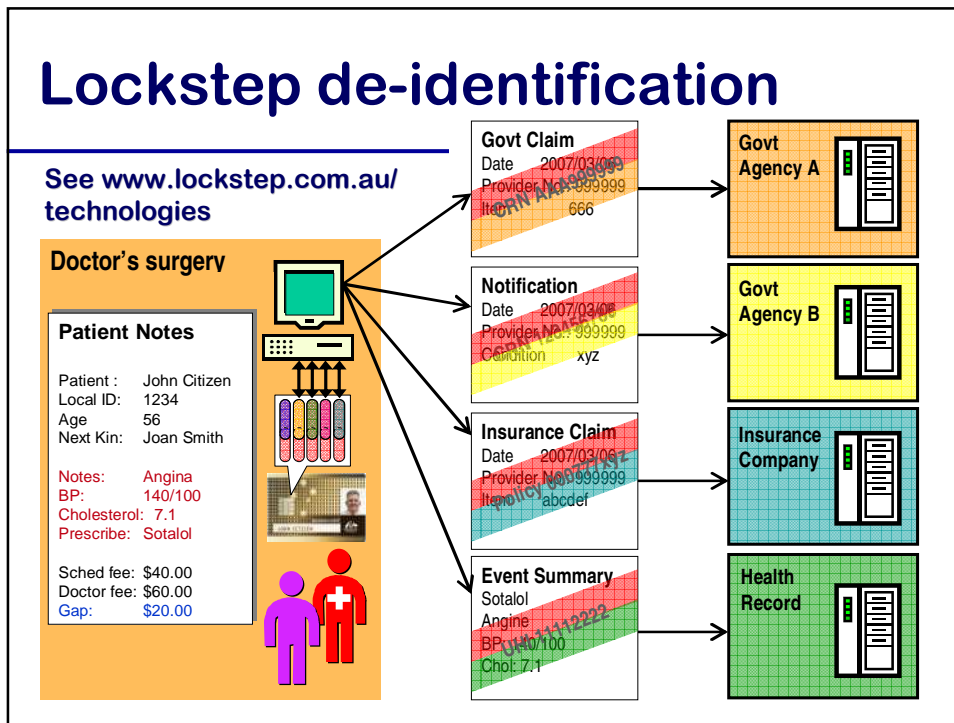
Detect prescription shopping

The diagram illustrates the process of detecting prescription shopping. On the left, a purple person icon and a red person icon with a white cross are shown. Next to them is a computer monitor and keyboard. A red key is positioned above a blue box containing the number '49987'. A speech bubble points to the keyboard area, containing the text 'Prescription Dig Sig (Doctor)'. A blue arrow points from the keyboard area towards a photograph of a pharmacy building on the right. A red footprint trail leads from the keyboard area towards the pharmacy.

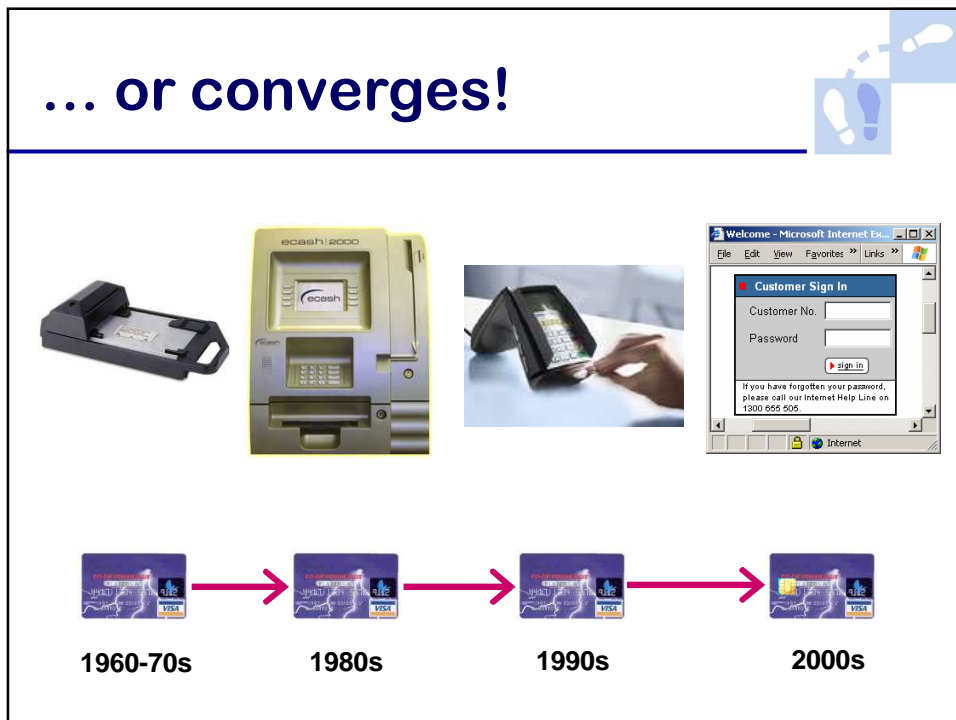
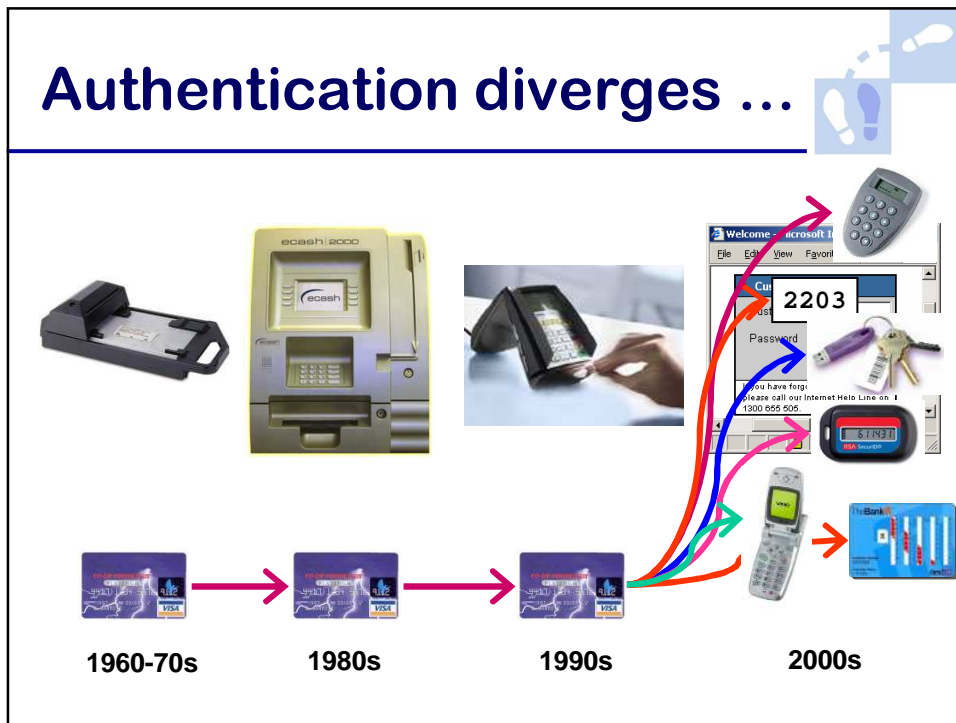
Expand fraud control

Detect over servicing

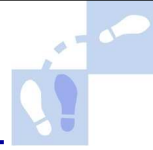
The diagram illustrates the process of detecting over servicing. On the left, a purple person icon and a red person icon with a white cross are shown. Next to them is a computer monitor and keyboard. A red key and a purple key are positioned above a photograph of a Medicare card. A speech bubble points to the Medicare card area, containing the text 'Claim Dig Sig (Doctor) Dig Sig (Pt Card)'. A blue cloud with an arrow points from the Medicare card area towards a green cylinder labeled 'Medicare' on the right. A photograph of a medical scan machine is also shown on the right.



- ## Benefits of smartcards
- 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.



Further reading



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



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

LOCKSTEP

