

Smartcards as critical national infrastructure

Australian Smartcards Summit
5 June 2007, Sydney

Stephen Wilson
Lockstep Technologies Pty Ltd
www.lockstep.com.au/technologies



For all the smartcard activity in Australia, we're really only just scratching the surface of this technology's potential. There is an immense untapped vein of privacy and safety capabilities in today's smartcard platforms. For instance:

- smartcards decentralise customer identities, literally keeping them safe in peoples' wallets and away from databases and call-centres
- they can run private off-line security checks inside the chip, to catch fraud without having to aggregate and data-mine all innocent transactions
- they can log users onto secure websites, protecting them against bogus cyber crime sites
- they can check the security master codes on signed e-mails, to protect consumers from the scourges of phishing and spam, which arguably represent the most serious threats to privacy today.

So there is a lot more to smartcards than meets the eye, much more than having a little spare memory for consumers to use as a "micro-iPod". But sadly none of these capabilities as yet are on the agenda for smartcard projects in Australia. And so a huge opportunity for our community's privacy and safety online goes begging.

In this presentation, I am going to review the parlous state of security and privacy online, and contrast that with the importance of the information economy. I'm going to characterise the sorts of measures we need to put in place to protect the community in the new economy. It turns out that smartcards offer the only effective national approach.

But we're going to have to do more to make best use of smartcards. We're going to have to treat them as national infrastructure.

The net is critical infrastructure



Broadband “could produce economic benefits of \$12–30 billion p.a. to Australia”

Accenture 2001

Broadband “has the potential to contribute \$300 billion to \$400 billion p.a. to European GDP and \$500 billion to US GDP”

Accenture 2003

“As a result, broadband is fast becoming a key element of critical national infrastructure. In fact, it is argued that broadband will very soon become the ‘next great utility’ after roads, water, electricity and gas.”





Australia’s Broadband Blueprint 2006

It is widely accepted now that high grade network connectivity – that is, the Internet itself – is a new form of critical infrastructure. The government uses appropriate language to liken high speed, high reliability Internet services to roads, rail, power and so on, in respect of its importance to the economy and indeed to contemporary society.

Smartcards as critical national infrastructure

Stephen Wilson, Australian Smartcards Summit 2007

AS/NZS 60265.1:2001 High-voltage switches	
AS/NZS 3000:2000 Electrical installations (Australian/New Zealand Wiring Rules)	
HB 124-2007 Design and Construction of Concrete Masonry Buildings	
AS 2885.1-2000 Solid portable electrical equipment	
AS/NZS 3100:2000 Similarity testing of electrical equipment	
AS/NZS 4801:2000 Low-voltage switchgear and controlgear	
AS 4568.1-2000 Hand-operated electrical equipment	
AS/NZS 4568.2-2000 Hand-operated electrical equipment	
AS 4292.1-2000 Hand-operated electrical equipment	
AS 4292.2-2000 Hand-operated electrical equipment	
AS IEC 60335-1-2001 Safety of household electrical appliances	
AS 2359.6-1995 Powered industrial trucks - Safety code	
AS/NZS 3100:2000 Similarity testing of electrical equipment	
AS/NZS 3100:2000 Similarity testing of electrical equipment	
HB 295.1-2000 Work - Safety	
AS 1271.1-2000 Lifting devices, ladders, ladders, ladders	
AS 3516-2000 Ladders, ladders, ladders	
ACA TS 001-2000 Ladders, ladders, ladders	
AS/NZS 3100:2000 Similarity testing of electrical equipment	
ACA TS 001-2000 Ladders, ladders, ladders	
AS/NZS CISPR 12:2006 Internal combustion engine devices - Radio disturbance	
AS 2805.14.2-2003 Electronic funds transfer - Requirements for interfaces	
AS 2024.1001 High-voltage AC switchgear and control gear	

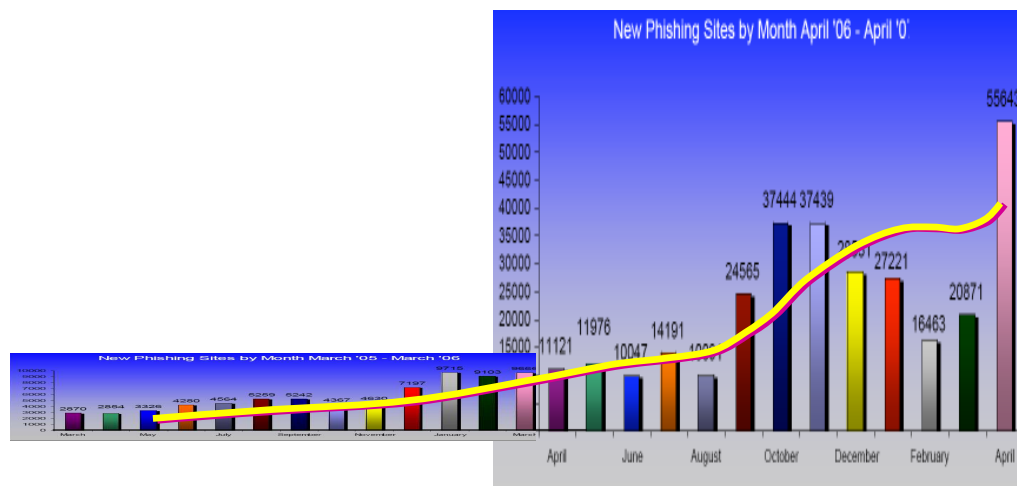


If we accept the Internet as critical to the information economy – or simply, to the economy full-stop – the next question is, do we take online safety as seriously as we do safety around any of the traditional infrastructure? Just look at the efforts we put into safety standards for power, gas, telephony, radio communications and so on.

Now, I certainly don't advocate a heavy handed regulatory approach. But I do suggest that government and business alike need to take a greater interest in the basic rights of consumers to participate safely and confidently in the new online economy. The community as a whole surely deserves a concerted and coordinated approach to their Internet safety.

We look next at the *industrialisation of cyber crime*, to see how seriously compromised online safety and privacy has become. The scale of the problem ought to inspire a systemic national response.

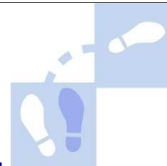
Phishing 2005-07



Phishing trends are reported regularly by the Anti-Phishing Working Group (see www.antiphishing.org). The slide shows two 12 month reporting cycles, drawn to the same vertical scale, culminating in the most recent data for April 2007.

Month by month, phishing goes up and down. It is thought that each major jump in phishing is due to a new breakthrough on the part of organised crime, like access to a big fresh "botnet". The yellow line shows the 6-month rolling average, which is rising inexorably.

Warning signs



“Single factor, replayable authentication is no longer viable to prevent unauthorised access to valued or sensitive online accounts”

Graham Ingram (AusCERT) &
Jeff Carpenter (Carnegie Mellon CERT)
APEC eSecurity Task Group, Singapore, September 2004

“[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

Nearly three years ago – when phishing incidents were only measured in the hundreds per month, rather than tens of thousands – Computer Emergency Response Teams (CERTs) in the US and Australia raised the alarm over “replayable” authentication such as passwords, which can be trapped and re-used by attackers in order to impersonate their owners.

Subsequently, Bruce Schneier and other analysts identified the intrinsic limitations of two factor authentication, recognising that one time passwords and even biometrics, could be replayed just like regular passwords and so defeat the newer transaction security systems. However, the response of businesses to Schneier’s warning was almost universally minimal. The threats were thought to be more or less academic.

Arms race



October 2005: Nordea Bank

Transaction Authorisation Number (TAN) card attacked
www.f-secure.com/weblog/archives/archive-102005.html#00000668

July 2006: Citi Bank

Event based One Time Password (OTP) token attacked
http://blog.washingtonpost.com/securityfix/2006/07/citibank_phish_spoofs_2factor_1.html

April 2007: ABN Amro

Time based OTP token attacked
www.theregister.co.uk/2007/04/19/phishing_evades_two-factor_authentication/

And so began an arms race. Predictably, the simpler two factor authentication systems were the first to fall to attackers – such as the Transaction Authentication Number (TAN) scratchy cards. Electronic sequential (or “event-based”) one time password generators have their users press a button on a key fob rather than scratch a card, but really work on the same principles, and so in mid 2006 Citibank was attacked.

At that time, some security people opined that *time based* OTPs were not so easily replayable because their random passwords roll over every 30 seconds or so. But seriously, how much time does a computer need to rob an online bank? Inevitably, time based OTPs too came to be attacked, with one of the first public reports coming in April of this year.

So now in early 2007 we have to understand that the cyber crime arms race has moved on since those statements were made by the CERTs in 2004. **Now the situation is that *two factor, replayable authentication is no longer viable to protect access to valuable online assets.***

Reasonable safety



- **The means to tell good sites from bad**
- **Make e-mail as safe as the post**
- **Protect the pedigree of personal data**
- **Share data on a Need to Know basis**
- **Decentralise as much as possible**

If we are to treat the Internet seriously as critical infrastructure, truly as the backbone of the new economy, we should characterise the sorts of security and privacy provisions that the community should expect if they are to use it safely and with confidence:

- Internet users ought to have the means to discriminate automatically and reliably between fake websites and the real thing. We can no longer take chances when accessing Internet banking and the like. And brand new services of major societal import, such as e-health records and government single sign-on portals, cannot be compromised by flawed authentication mechanisms.
- Given its importance now to business and personal life, e-mail really must be made as safe as the regular post. Consumers ought to be able to open e-mails with some impugny, and they should be much less vulnerable to e-mail borne malware. More robust spam *prevention* should be a higher priority, as opposed to spam filtering and other detection approaches. Digital signature processing ought to be embedded in mail clients to provide true authentication and authorisation of the origin of electronic messages.
- The root cause of so much identity crime is the ease with which personal data can be *replayed*. To prevent replay attack, personal data needs to have "pedigree", so that when account numbers, customer reference numbers, personal identifiers and so on are presented in digital form, receivers can be sure that the numbers are genuine, that they have been presented with the owner's consent in the transaction at hand, and that they have not been stolen and replayed.

Reasonable safety (cont.)



- The means to tell good sites from bad
- Make e-mail as safe as the post
- Protect the pedigree of personal data
- **Share data on a Need to Know basis**
- **Decentralise as much as possible**

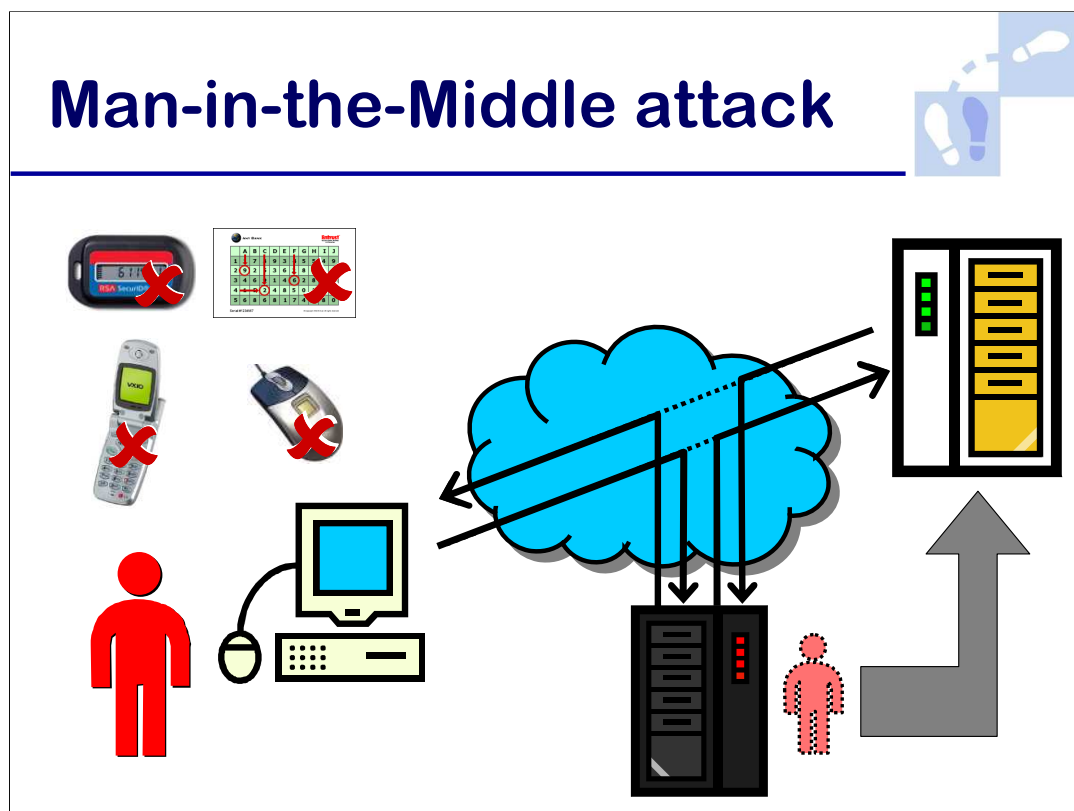
CONTINUED

• If personal digital data can be given a pedigree, then we can restore in day-to-day life one of the cornerstones of security: the "Need to Know" principle. Regrettably, our various personal numbers have so little trustworthiness or value these days that we are forced to supplement them with volumes of otherwise peripheral information to establish our identities. Think of what happens when you phone your bank and the call centre operator begins by asking your account number. They invariably go on to request your full name, your address, date of birth, mother's maiden name, credit limits and so on. The reason they need all this supplementary detail is that your account number on its own is no longer trustworthy. But by feeding more and more personal detail into databases and call centres, to compensate for the fragility of the basic identifiers, we create increasingly rich honey pots of immense value to identity thieves.

We shall see later (see e.g. slide 13) that smartcard technology allows personal identifiers to be individually protected and controlled by their owners, so identifiers are only released to parties who need them, and only released with the minimal personal data needed for each transaction.

• In general, we should be doing much more to resist the trend to centralise personal data. Customers should be able to establish their bona fides with service providers and their entitlements to particular transactions, without transmitting so much extraneous personal information, which inevitably gets aggregated.

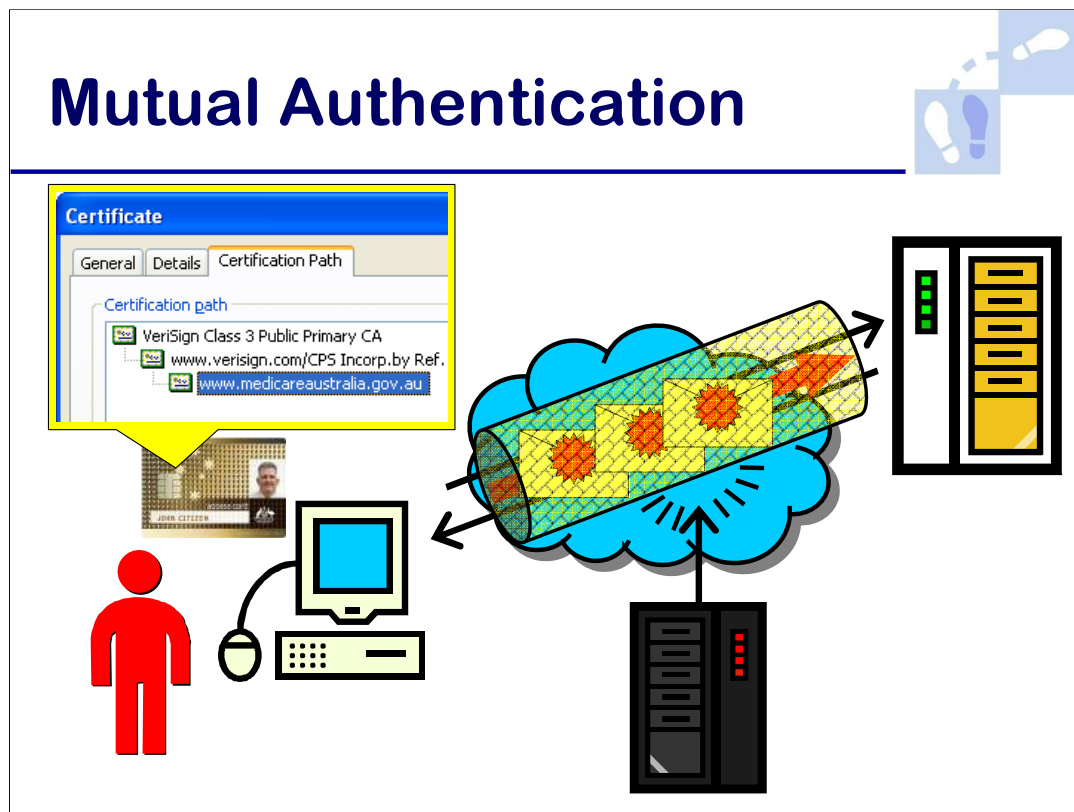
We will now review the basic vulnerabilities of most personal security devices, and look at how smartcards alone provide the sorts of large scale online protective mechanisms needed to restore safety to the Internet.



It's easy to see how most two-factor authentication methods are vulnerable to Man-in-the-Middle attack, whether they be random password generators, lookup tables, text messaging or even biometrics. Put simply, these technologies do nothing to prevent Internet users from 'knocking on the wrong door', because they are not smart enough to know the difference between a bogus website and the real thing .

In a Man-in-the-Middle attack, a bogus website mimicking the genuine article intercepts authentication messages exchanged by the customer and the service provider, both of whom remain oblivious to the interloper. It doesn't matter what these messages are, nor how they are created; the attacker's server simply passes them back and forth until the user authentication is done. From that point on, the Man-in-the-Middle can cut off the user and instead issue its own fraudulent requests to the provider's server, such as funds transfers to the fraudster's account.

Unlike phishing spam, which mostly depend on unwitting users making some sort of mistake, a Man-in-the-Middle pharming attack can have a 100 per cent hit rate. Until the illicit server is detected, all connections from all customers can be hijacked.



The only systemic defence against Man-in-the-Middle attack is *Mutual Authentication*. Not only must the service provider know for sure which customer it's talking to, the customer has to be able to verify the identity of the provider. Alone among two-factor identity solutions on the market today, smartcard technology has the ability to perform true mutual authentication. For instance, smartcards can safeguard copies of the service provider's SSL "master codes". This ensures that each SSL session is properly encrypted from each end, and resistant to hijacking. Further, each and every transaction sent from the customer can be digitally signed using the tamper-resistant smartcard, creating in effect an inviolable tunnel between them and the service provider.

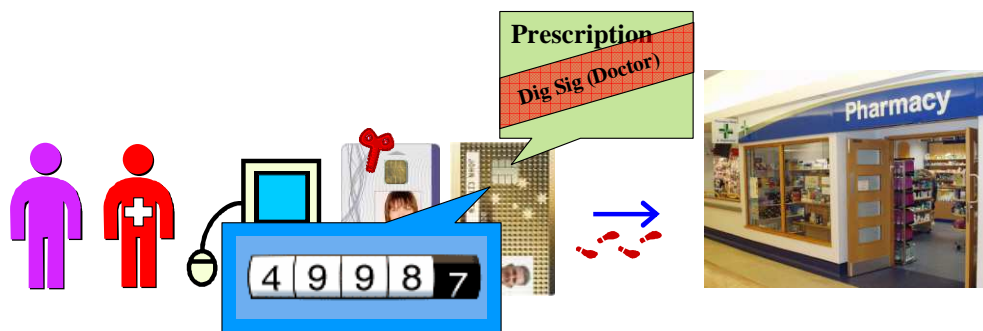
It is easy therefore to appreciate why Bill Burr, the head of cryptography at the US National Institute of Standards and Technology has said that **PKI-enabled smartcards provide "the only practical solution today" to eavesdropping and account hijacking** [Ref: Asia PKI Forum 2005, http://asia-pkiforum.org/feb_tokyo/NIST_Burr.pdf].

NB: The image of the proposed Health & Welfare Access Card is used here for illustration only.

Decentralise fraud control



Detect prescription shopping



While fraud control is a major justification for deploying smartcards, orthodox business cases tend to focus on counterfeiting and identity takeover. Yet there are many more possibilities; the technology is especially powerful in offline environments where points of service are not connected to central mainframe computers. One of the key strengths of smartcards is their ability to monitor transactions and to apply business rules for themselves. In the health sector, it is often impractical or prohibitively expensive to connect to backend databases for real time fraud detection. Furthermore, centralised monitoring of every single transaction in order to weed out a tiny minority of fraud cases jeopardises the privacy and security of the vast majority of law abiding users.

Smartcards can directly address two major forms of social security fraud:

1. Prescription shopping, where a patient sees a number of different providers in quick succession to obtain drugs or some other benefit (see this slide)
2. Fraudulent claiming by providers for reimbursable items not actually delivered, or the counterfeiting of claims by administrative clerical staff (see next slide).

In the example shown here, when a doctor prescribes a drug, certain details are written to the patient's smartcard, in an event summary digitally signed with the doctor's professional smartcard. For each new prescribing event, the doctor's local software (or that of the pharmacist) is then able to check the recent history, and generate an alert if the entitlements seem to have been breached. For instance, the smartcard can keep track of how many scripts have been written in a given period of time. If the patient has special entitlements, to prescription narcotics for instance, then more specific rules could be coded into their card. An attempt by the card holder (or a thief) to obtain additional prescriptions is detected simply by checking the smartcard for details of pending scripts or the recent prescribing history. Ideally pharmacy systems would 'close the loop' by updating the card with dispensing details.

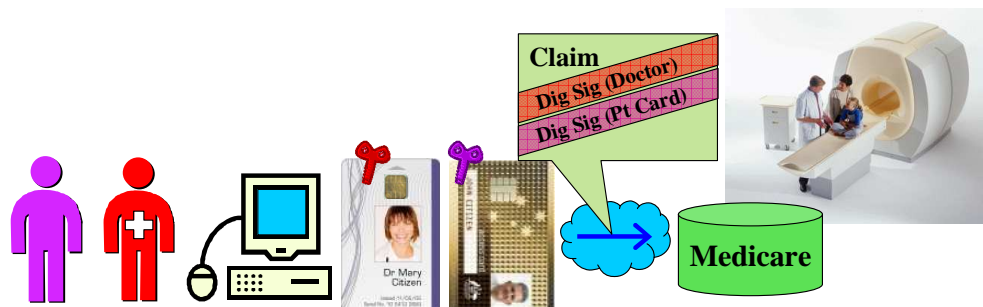
See also "Babystep No. 6" at www.lockstep.com.au/library/babysteps.

Note that we're not advocating that doctors' software necessarily be programmed to refuse prescriptions under these circumstances, only that the overall system be better designed to detect abuse in a decentralised manner, that protects the privacy of all innocent transactions.

Expand fraud control



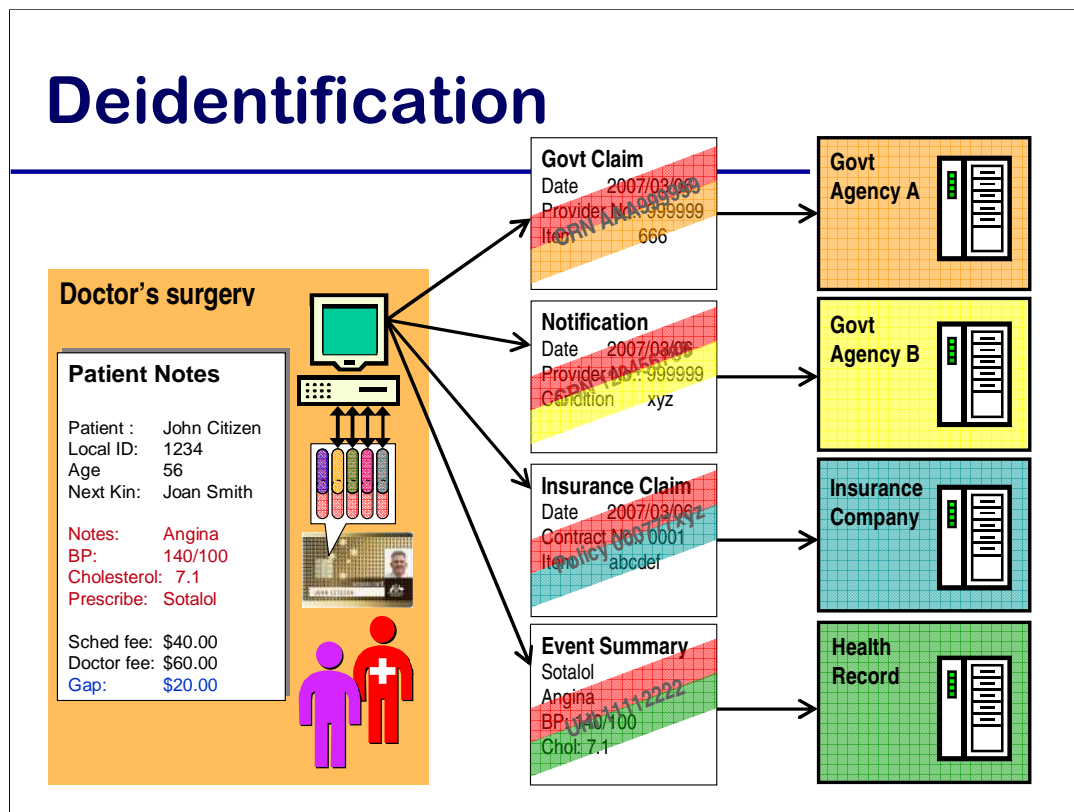
Detect over servicing



We should in fact expand the horizons for fraud control. Smartcards can be used to combat not just fraud perpetrated by individuals but also by corrupt service providers and clerical staff. Recall the case some years ago when a number of radiologists who had already spent money on their expensive MRI scanners tried to access a new federal government rebate for high tech imaging by falsifying the dates on several dozen Medicare claims. Patient smartcards could be used to prevent forgery of or tampering with claims in this manner.

In this slide we see how an un-forgable, indelible digital stamp – *Dig Sig(Pt Card)* – is created using an embedded key specific to the patient card, and attached to a Medicare claim. For a claim to be legitimate, it would have to feature both the digital signature of the doctor ordering the item, and the stamp corresponding to the patient. Counterfeit claims could not be created without collusion with the patient and access to their particular smartcard. Over-servicing would be readily detected if the same patient card was seen to be associated with multiple claims.

See also “Babystep No. 7” at www.lockstep.com.au/library/babysteps.

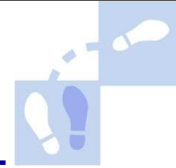


Finally, Lockstep's own R&D has led to new ways to dramatically enhance privacy and security using smartcards to de-identify sensitive transactions. Anonymous digital certificates issued by respective service providers can be used to encapsulate diverse personal identifiers, customer reference numbers and so on. In the scenario shown here, a cardholder issued with such anonymous identifiers visits a doctor. During the course of the visit, a typical set of clinical notes is created, subsets of which can be extracted to populate various transactions, such as government claims for rebates, notifications of important conditions, insurance claims, and electronic health record entries.

Each claim or transaction is digitally signed using the identifier relevant to the context of the transaction. For example, the claim sent to Agency A is bound via an anonymous certificate to the encapsulated customer number AAA999999, plus the name of the issuer, Agency A, indicated by the orange seal. Separately, the event summary lodged with an electronic health record is bound via a different certificate to the encapsulated unique health identifier 11112222, plus the name of its issuer indicated by the green seal. Note that each transaction carries the bare minimum personal data. Furthermore, each recipient can be assured that their de-identified transaction originated from a genuine smartcard, used with the cardholder's consent. That is, each encapsulated identifier has a robust digital pedigree.

See also www.lockstep.com.au/technologies.

Smartcards are different!



They know what's going on around them

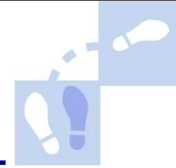
- Resist skimming and counterfeiting
- *“The only practical solution today” for Man-in-the-Middle attack (NIST)*
- Intelligent proxy for the user:
 - Carry and enforce entitlements
 - Detect abuse offline
 - Minimise personal info sent over network
 - De-identify sensitive transactions

In summary, smartcards are unique and truly distinct from all other personal security technologies. Simply put, smartcards are *smart*; they can tell what's going on around them. And so their potential for protecting users online goes far beyond the usual point (shown in green) that they are resistant to card skimming.

It is essential that policy makers, strategists and regulators understand that:

- Smartcards offer the only practical solution to Man-in-the-Middle attack (according to the head of cryptography at the US National Institute of Standards and Technologies; see slide 10 notes).
- Smartcards can act as intelligent proxies for their users, to convey a large array of entitlements, decentralise fraud detection, reduce the volume of extraneous personal data sent across the networks, and de-identify sensitive transactions, such as e-health record entries and in future, electronic voting.

What are we afraid of?



Technological change means such a card would now pose far greater challenges to liberty and privacy than the Australia Card suggested by the Hawke government in the mid-'80s.

Editorial Sydney Morning Herald 6 Feb 06

Peter Costello publicly praised the smart card idea, saying people were now more tolerant of intrusions into their privacy because of security threats.

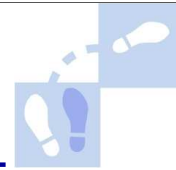
Louise Dodson, Sydney Morning Herald 26 April 06

Smartcards continue to suffer from widespread mistrust. Take for instance the unguarded comments of the Sydney Morning Herald editorial writer who seemed entirely unaware of even the *possibility* that smartcard technology might render today's cards safer than the Australia Card proposition; the form of words reveals an attitude that technological advances are *necessarily* threatening to privacy.

Furthermore, there is a regrettably common presumption that perhaps privacy *ought* to be traded off in the interests of better security, post 9-11. Policy makers, politicians and even technologists these days often accept – and indeed frequently promote – the idea that privacy and security are somehow mutually exclusive.

But as we have seen, smartcard technologies can dramatically enhance security and privacy at the same time. If these possibilities were better understood, the details debated and allowed to inform policy development, I suggest that smartcard technologies would gain far better (perhaps even unanimous) support across the community, in contrast to today's unnecessarily polarised responses to proposals like the DHS Access card.

Compare with SIMs



- **SIM lock**
 - Mutual authentication between SIM and handset
 - i.e. PIN is not the only layer of security
- **Save to SIM**
 - The mobile operator can't see your contact numbers
 - Personal data in an Access Card could be just as safe

Many anxieties about smartcards are genuinely held but are often unfounded. Interestingly, the operation of SIM cards (which are of course a type of smartcard) seems not to raise comparable concerns. Let us consider two particular issues.

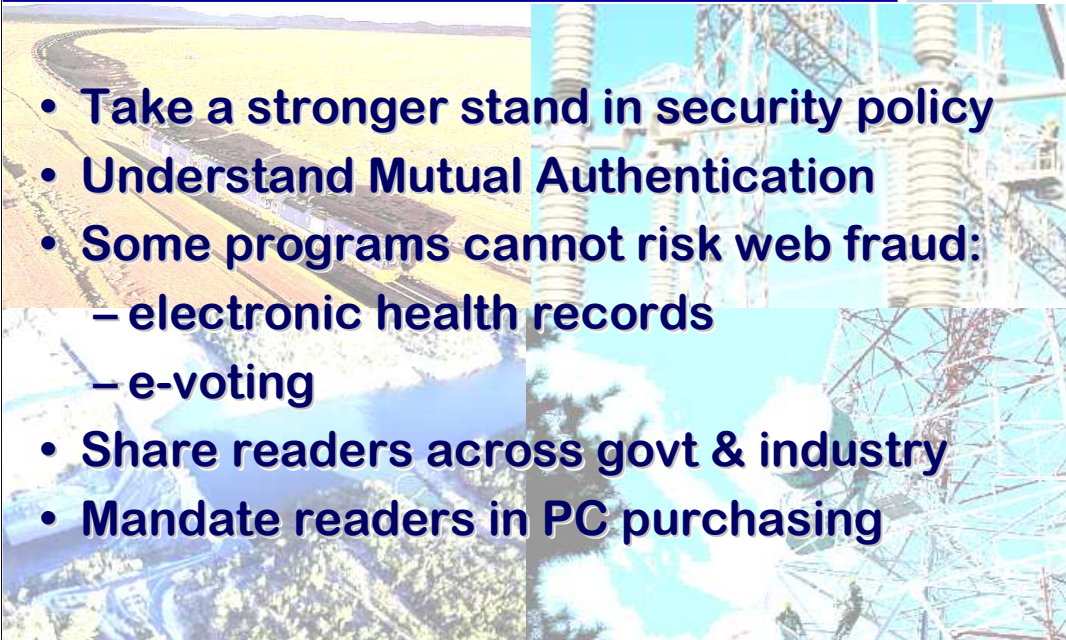
Firstly, people tend to worry that data stored in a smartcard – especially in consumer-controlled sections of memory – can be readily accessed, classically by a low cost “Dick Smith” reader. Yet this is not so with well designed multi-layered access control. The most important point missing from most non-technical accounts of smartcard security is that the chip can tell what sort of reader and backend application it is communicating with. That is, smartcards and readers engage in Mutual Authentication. So even if a smartcard is mislaid *together with its PIN*, it is not necessarily the case that any old reader will be able to gain access to all memory.

To better appreciate mutual authentication between smartcard and reader, lay people can refer back to the well known “SIM lock” feature of mobile phones, which prevents certain SIM cards from operating when moved from one handset to another. SIM lock is an example of mutual authentication, whereby the chip has the ability to ‘test’ its surroundings and behave accordingly.

Secondly, there are fears that the more personal information is stored on a smartcard, the greater the opportunity for surveillance of cardholder activity and/or unauthorised linkages being made between their different transactions. However, data held on a smartcard is not automatically accessible to third parties. Again, this is a property that most people apparently take for granted in their SIMs, when it comes to storing contact numbers. We save phone numbers to our SIMs without giving a moment's thought to the theoretical possibility that carriers might be able to access them without our knowing it.

So we should be able to use smartcard memory with similar levels of confidence and trust as we do SIM cards.

Smart infrastructure policy



- Take a stronger stand in security policy
- Understand Mutual Authentication
- Some programs cannot risk web fraud:
 - electronic health records
 - e-voting
- Share readers across govt & industry
- Mandate readers in PC purchasing

Smartcards, with their ability to tell what's going on around them and thereby act as proxies for their users to protect them from cyber crime, are unique amongst all personal security technologies. The widespread deployment of smartcards is the only robust, long term approach to safeguard Internet users against phishing, pharming, spam and other forms of identity theft; smartcards could prove to be central to protecting the information economy itself.

We need to treat as critical infrastructure the community-wide ability to use smartcards routinely in Internet transactions. It will take time to achieve widespread adoption but governments and businesses could start right away to work together as follows:

- Security policy in the Australian private and public sectors – as typified by e.g. the Australian Government Authentication Framework, and Internet banking security guidelines – has been historically light touch, with regulators and policy bodies assiduously avoiding technology mandates. **I suggest that such technology agnosticism has reached its “Use By Date” and that it is time for minimum standards to be laid down in the interests of consumer safety.**
- In particular, when planning security requirements for Internet transactions, more attention is needed to true Mutual Authentication, to ward off Man-in-the-Middle attack, which has proven effective against all two factor authentication solutions in Internet banking.
- Certain imminent online programs simply cannot be contemplated without an uncompromising stance on user privacy and safety. Electronic health records, online voting and the like are expected to have profound impact over time. Surely we cannot afford to risk Man-in-the-Middle attacks on these programs.
- Government and industry could do more to share the cost (including support) of smartcard readers. In places like Taiwan, smartcard readers are commonplace. Over two million readers have been purchased by regular users there, at convenience stores and the government's own G2C portal.
- And one of the best ways to promote particular new technologies is to incorporate them into standard government procurement. For some years, the US Dept of Defence (as well as some NSW Area Health Services) has mandated smartcard readers in every new personal computer system purchased.