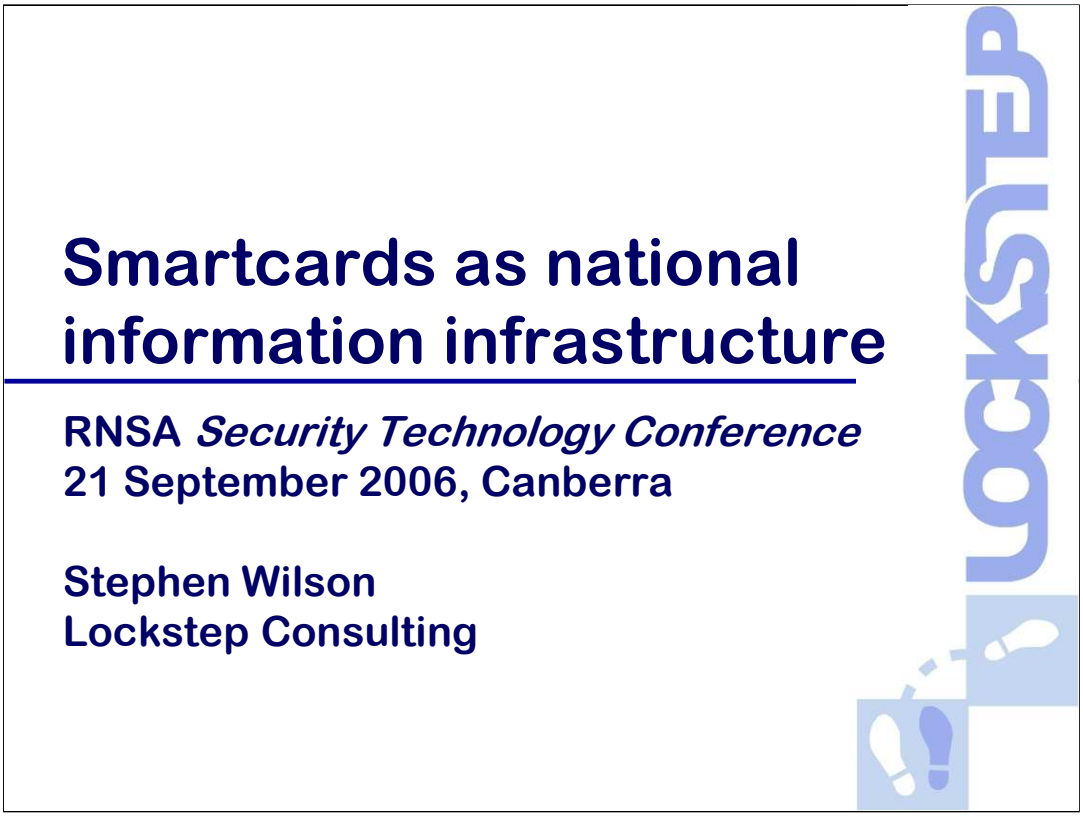


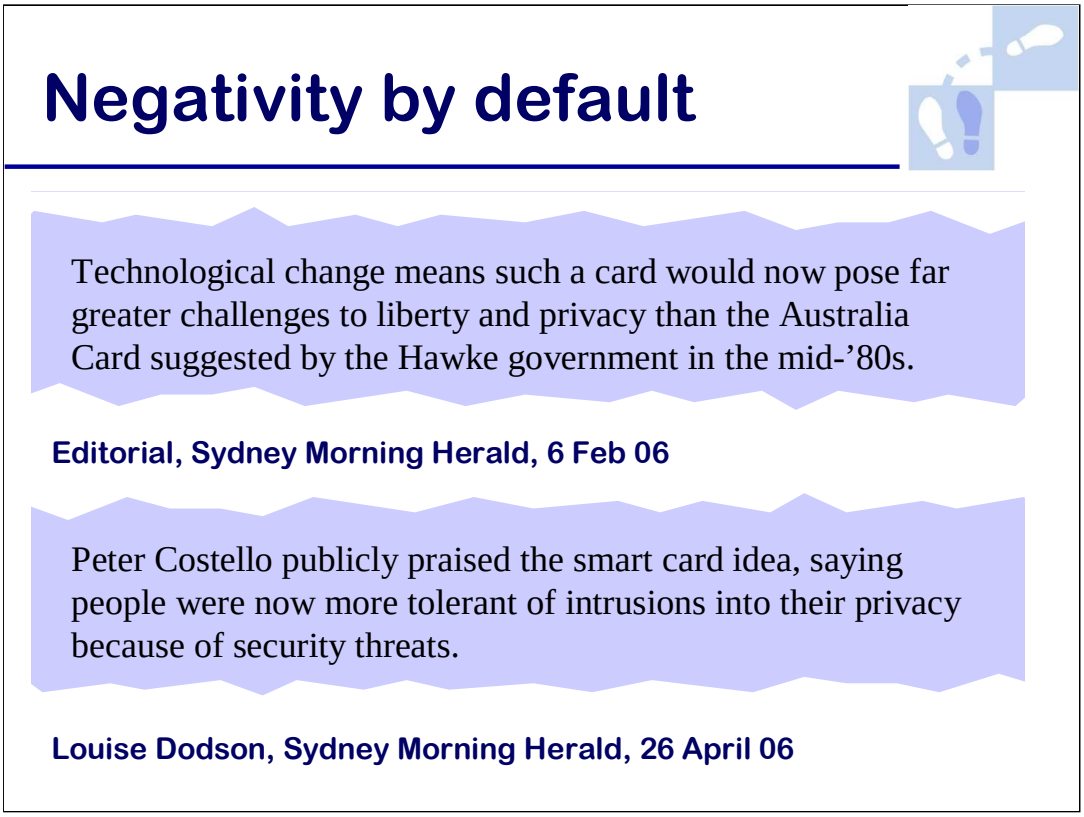
What do I mean when I refer to the possibility of smartcards as infrastructure in Australia?

Some countries invest in massive national infrastructure. Taipei for example has installed a free wi-fi network across the entire city. And Singapore ran fibre optic network cables past every home.

I accept that these are not the sorts of projects that Australia will undertake. But we can take a broader, 'softer' view of infrastructure, to encompass capability, a state of awareness of what the technology can do, and shared vision for how to apply it.

Across Asia we see many countries developing what we might call societal technology infrastructure. For instance, in Korea it is increasingly commonplace for one's digital credentials to be available and portable across multiple platforms: smartcard, cell phone, PC, PDA and now the set-top box. There is a marketplace there for solutions and capabilities that feed the Korean peoples' expectations for how their credentials can be managed and applied. In Taiwan, smartcards have become so commonplace that people willingly buy readers and install readers. Over 2,000,000 readers have been bought by people for "Internet ATM", which works using their bank issued smartcards. Readers are available for US$10 in convenience stores! This public expectation of service and a widespread, sophisticated understanding of technologies can be viewed as "infrastructure".

This presentation will look at the importance of smartcards in the fight against web fraud and the distinct possibilities for them to actively enhance privacy. I will argue that they are so important that we should all do more, across government and business, to bring smartcard capabilities to fruition across the country.



Let's start by looking at the common perception of smartcards. It is usually negative.

The above editorial from the Sydney Morning Herald presumes, reflexively, that smartcard technology must be bad for privacy.

Moreover, there is a default view that privacy can (and should?) be traded off in the interests of security. Politicians and even technologists have got into the habit of conceding that privacy could be compromised in the name of better security. This is flimsy justification for smartcards; it would be far better if we shared an understanding of how smartcards can actively enhance both privacy and security at the same time.

Perhaps we need a new 'manifesto', to set the scene for modern technological responses to the challenges of security and privacy.

First, we should not even think about having a debate about privacy. Privacy should be a non-negotiable item! Let us not give it up almost automatically for fear of security being more important. The public should expect to achieve privacy and security at the same time.

Second, we should insist on our rights to deal anonymously. Sure enough this is actually one of the National Privacy Principles, but it is rarely taken seriously. True anonymity is such a great technical challenge that most people have come to view it as academic and to ignore the practical possibilities altogether.

Third, we should all resist the ever increasing trend to centralise data management. Last year ABC Four Corners reported on the problem of identity records being sold en masse by corrupt call centre workers. Why have we allowed huge stockpiles of our life's information to be aggregated by third parties like this? Yet the worrying trend continues with central registration databases commonly featuring in new smartcard proposals. As identity fraud becomes an international criminal industry, large stores of personal information are increasingly valuable to sophisticated and highly organised attackers.

And finally, we as a community deserve some guarantee of safety when we access the Internet. The government has a laudable goal of moving more and more of its services and transaction traffic online. The Department of Human Services in particular today sends out 300,000 letters *a day* and will soon start shifting some of these to e-mail. But if it expects citizens to use e-mail, the government must surely guarantee the safety of the channel. It must take active steps to protect consumers against phishing, pharming, spam and website spoofing.

There is a large and growing spectrum of Two Factor Authentication solutions, all of which aim to protect users against identity theft, by making it more difficult to take over their authenticators. Steady progress has been made to address this issue. But a more recent realisation is that identity takeover of the *service provider* – that is, the phenomena of web site spoofing, phishing, pharming and so on – must also be addressed. The later challenge is known as Mutual Authentication, and crucially, it is not the same thing as Two Factor Authentication.

Two Factor devices include:

•**One Time Password** (OTP) which can be electronically generated on a "fob" or provided in advance in the form of a scratchy card or a booklet containing several dozen numbers to be used in sequence. Some electronic OTPs are "time based" where the key fob is synchronised to the backend server and the number generated remains valid for only 30 seconds or so before flipping over to another random code.

•**Challenge Response** involves the service posting a number or a code, and the client being required to calculate a response using a special device. If the calculation is correct then the service can assume that the user is indeed in possession of the right device. Challenge Response can be implemented electronically using a calculator-like device, or in a paper or "matrix" card form printed with a row-column look up table.

•**Cryptographic authenticators** include smartcards and functionally similar USB keys.

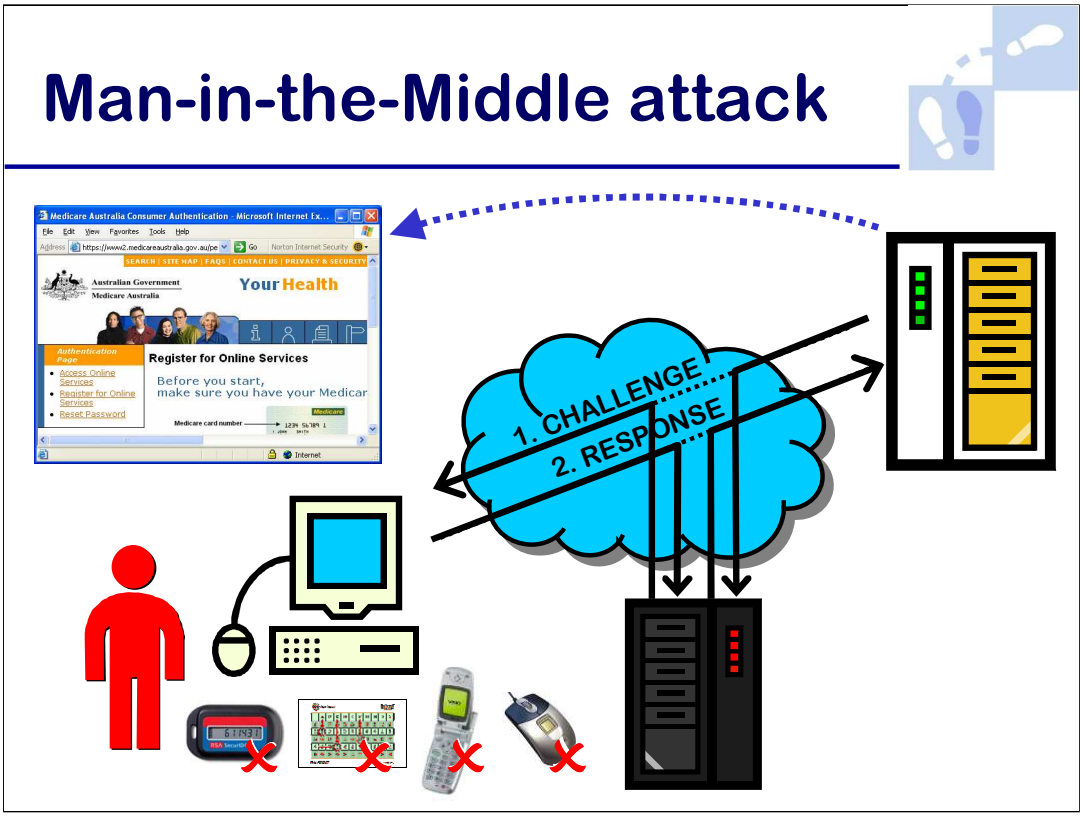
•**Text messaging** utilises a mobile phone as the second factor. The user trying to access the service is sent a random SMS to their pre-registered phone number. They type the text back into their browser, to demonstrate they are in possession of the phone.

•**Biometrics** while sometimes called "Three" Factor (alluding to something you are as opposed to something you have and something you know) are nevertheless in the broad two factor category, as a response to the problem of end user identity theft or takeover.

A year ago, well known cryptographer and security commentator Bruce Schneier raised the alarm over Two Factor Authentication's inability to protect against a raft of threats, typified by the "Man-in-the-Middle" attack. His analysis is cogent, non-technical and readily grasped.

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

However most organisations have been relatively slow to respond. My personal experience was that it was not uncommon for security managers in large businesses to dismiss Schneier's concerns as "academic", and that Man-in-the-Middle attack was unlikely to be perpetrated in anger by cyber-criminals.



The Man-in-the-Middle attack involves a rogue machine interposing itself between the user (client side) machine and the remote (server) end, and intercepting the messaging handshake that establishes a session. By passing authentication messages straight through to the backend, the attacker can impersonate the client, and once a session established, can take over, for example to redirect funds to the attacker's account.

[For an even more convincing attack, it is has become apparent that the SSL certificate path chain that leads to the well-known padlock symbol and also be usurped; refer to the links shown above.]

No conventional Two Factor Authentication device can prevent Man-in-the-Middle attack – including OTP, matrix cards, text messaging and biometrics – because none have the active functionality (or 'smarts') to challenge the veracity of the far end during the early stage of the handshake.

Nordea Bank attacked

3 Oct 2005

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

Several attacks on Two Factor Authentication have been seen.

Best known was the attack on Nordea Bank's One Time Password scratchy pads. The Man-in-the-Middle pharming site closely resembled the real logon screen for Nordea net banking. After the user entered their account name, static password and their one time password, the attacker generated a spoof error message to the effect that there had been a network error, and the user would have to repeat their logon. Since this sort of interruption is not uncommon, most users indeed scratched off another password and tried again. A bogus error message was posted again, and a further password obtained, before the attack machine finally informed the user of a 'fatal error' and closed the session.

Subsequently the attacker was able to replay three consecutive logons for each affected user. Significant funds were stolen from dozens of accounts before the bank became aware of the problem.

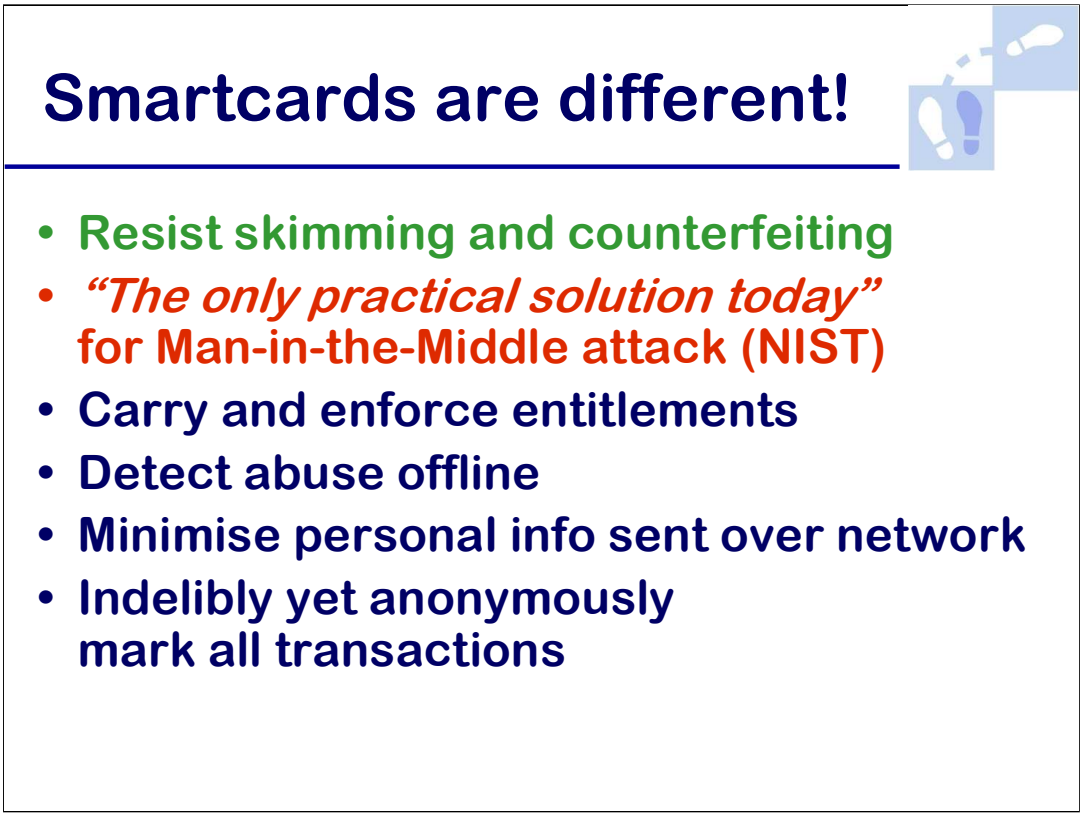
Citibank attacked

10 July 2006

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

Worse was to come. An electronic One Time Password system was attacked in July 2006. This attack was first spotted by a security research firm in the wild, hosted on a Russian based hacker site. The bank was alerted promptly and the site shut down before much if any damage was done. But the lesson is sobering: event based OTP is badly broken. And there is no reason to feel more confident in time-based OTP, since the attacks are automated and can replay stolen one time passwords within seconds while they remain valid.

The necessary response to these types of attack is proper Mutual Authentication (which can of course also embody two factors). The issue is so acute that even the mainstream media is now covering it. The ABC Radio *PM* program of 25 July 2006 reported on the Citibank attack, and moreover, took time to explain Mutual Authentication in plain English. See http://www.abc.net.au/pm/content/2006/s1696632.htm.



The importance of smartcards has shifted over the past few years.

In the late 1990s the value of smartcards was seen largely in terms of multi-functionality. Some spectacular products were launched especially in Asia featuring EMV credit card with integrated telephone calling card, post office digital certificates, and stored value. None of these seem to have succeeded, perhaps for the simple reason that marketing and managing so many functions, each vying for brand attention, proved so difficult. Multiple product functionality is not seen as so important anymore (although as we shall see, multiple embedded functionality is more important than ever).

Another longstanding benefit for smartcards of course is their resistance to skimming and counterfeiting. This is still vital, but there are many more advantages today.

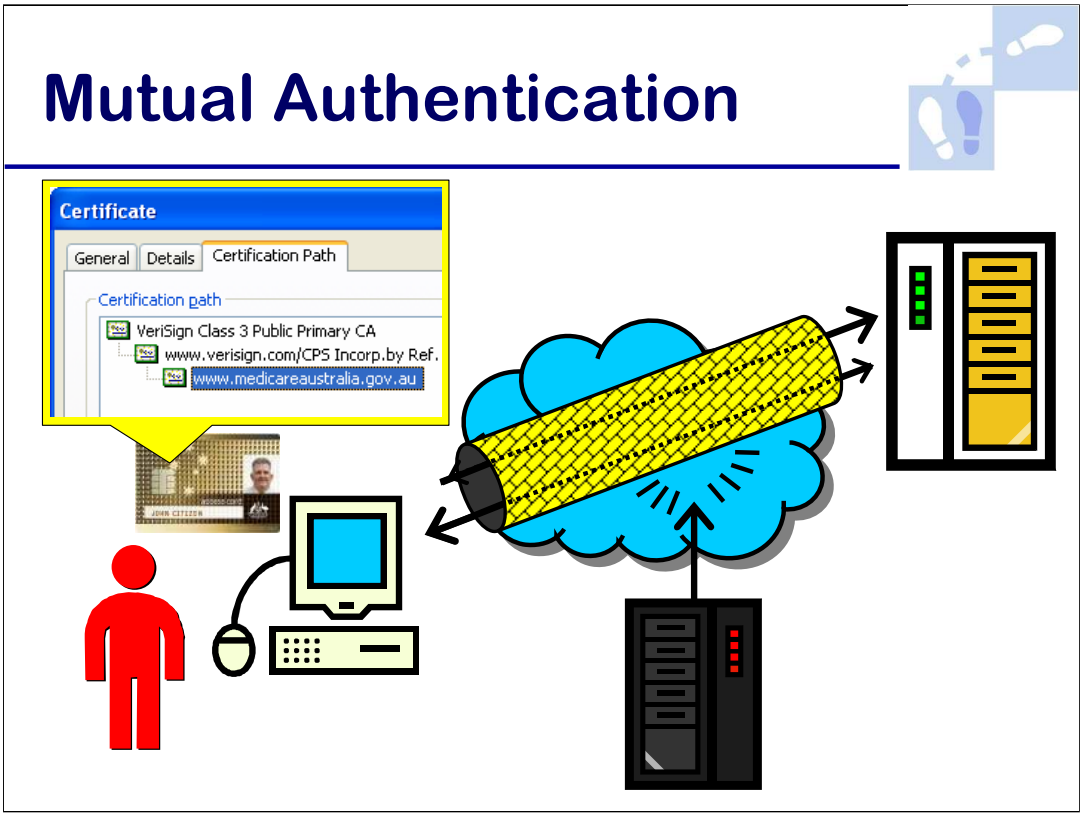
The EMV smart credit/debit program is driven by more than skimming. A major issue in Europe is the cost to merchants of EFTPOS card validation, because telephone calls are timed. Merchant terminals usually dial up no more than once a day, and so are vulnerable to stolen card fraud. But smartcards can monitor their own usage patterns, checking daily transactions against preset limits. Thus a stolen smart credit card can see for itself if it is being abused, and flag the fact to the terminal. This power to check and enforce entitlements offline could be critical to enhancing privacy while expanding the use of health & welfare cards (some applications along these lines are outlined later in this paper).

•Mutual Authentication, as we shall see below, is a unique attribute of smartcards, and is becoming an acute need in the online environment.

•Smartcards can handle multiple identifiers seamlessly, and automatically invoke the right one in the context of what the cardholder is trying to do.

•Combining the abilities to check entitlements offline and to manage multiple identifiers, smartcards can radically decentralise identity management, reducing dependencies on mission critical directories, eliminating honey pots, improving system-wide resilience, and cutting back the trafficking of sensitive personal information.

•And the built-in cryptographic processors of modern smartcards can mask or encrypt identifiers, so that transactions cannot be linked or reverse engineered. An example of this also is detailed later.



In general terms, proper Mutual Authentication involves the client checking the identity of the server before the server checks the client (by which time it can be too late for the user to avoid being connected to a fraudulent site). So note carefully that the directions of the arrows above have been reversed compared with the previous slide.

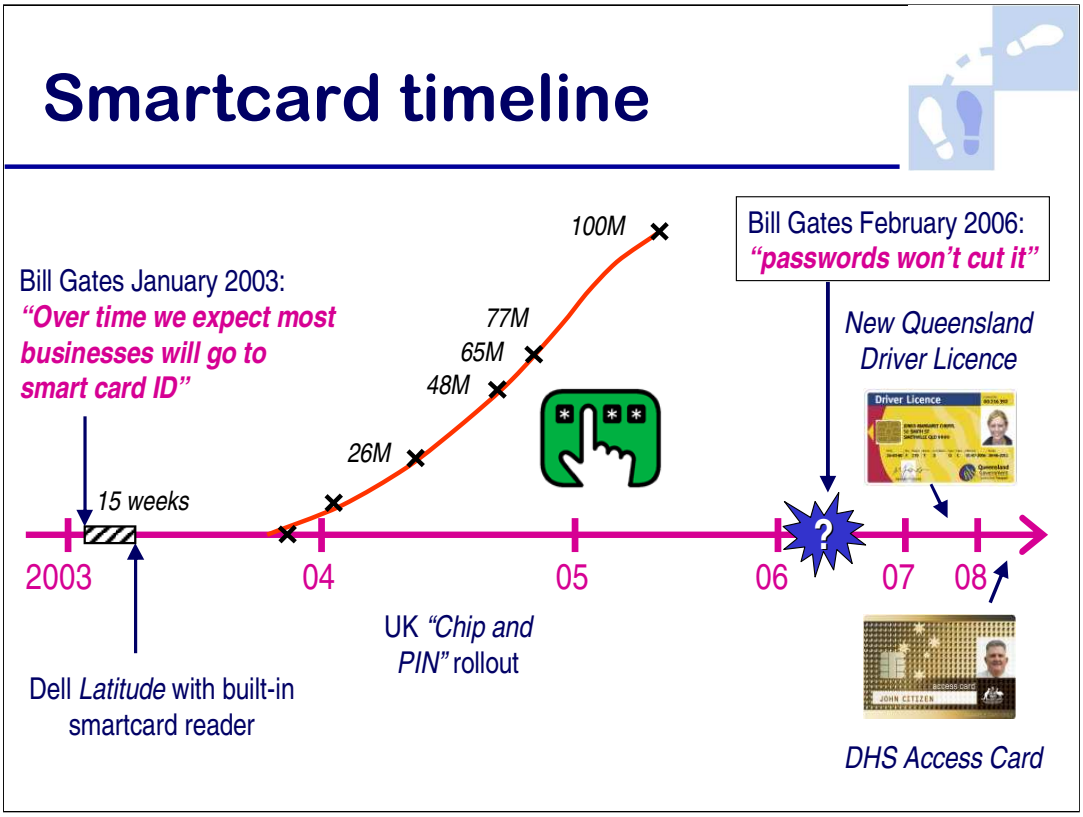
One important way that smartcards can implement Mutual Authentication is to use them to hold tamper proof copies of the certificates underpinning SSL. We usually think of a smartcard as holding the private keys of the cardholder, but here we extend the card to also hold one or more *public* keys belonging to the *issuer*. SSL has a certain vulnerability where any SSL server certificate that chains back to a root key held in the browser can be blindly accepted by web browsers.

See http://www.theregister.co.uk/2002/09/03/ms_outlook_digital_sigs_easily

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

The fundamental problem is that root certificates held in a PC's memory can be tampered with or substituted.

On the other hand, a smartcard issued for instance by a bank, can hold the particular root key used by the bank to anchor its SSL certificate. For added security, the smartcard could hold the entire certificate chain, to prevent injection of fraudulent certificates.

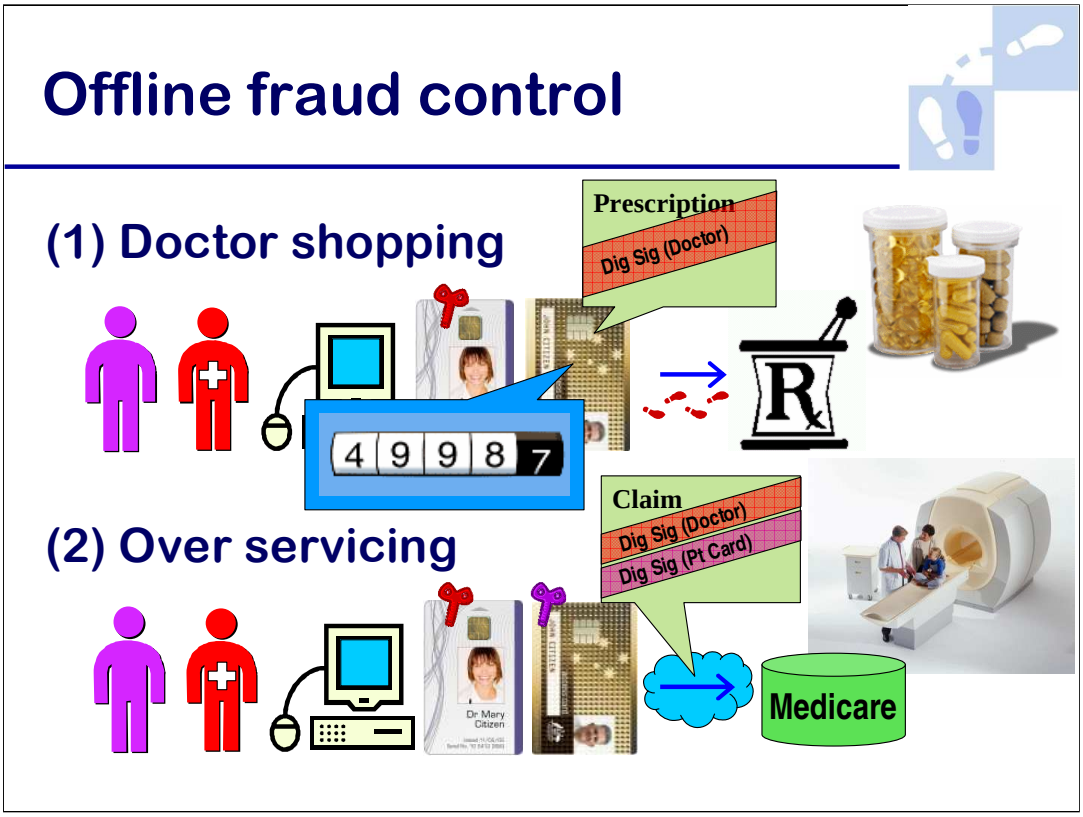


Here are some of the more significant milestones in the recent history of smartcard deployment. In early 2003, Bill Gates sent around one of his occasional "executive e-mails" where he espoused the virtue of smartcards for authentication. The effect on the PC and laptop industry was almost instantaneous; within 15 weeks Dell introduced its first machine with a built-in smartcard reader. Several others followed, spurred by the likelihood that smartcard applications would soon follow given Microsoft's support for the technology in its operating system.

Around the same time, EMV became an urgent issue in Britain. In one of the most impressive rollouts anywhere in the world, over 100 million smartcards were issued under the "Chip and PIN" program in 18 months to early 2005.

In early 2006, Bill Gates made a keynote speech on security at the RSA Conference in San Francisco, and went further in his promotion of smartcards. We can expect another spike in smartcard interest from the PC industry; indeed, a new Acer notebook already features an integrated reader.

In Australia two of the best known proposals are the New Queensland Driver Licence (NQDL), and the Department of Human Services Access Card. Both of these from time to time have been cautiously touted as providing keys to online services, but neither project has yet to elaborate how this would be done in practice. Within a broader smartcards-as-infrastructure vision, the NQDL and the Access Card could both be viewed as important resources for the whole community, and they would be promoted as the preferred means for individuals to interact with government online. Within the timelines for their rollout – 2008 onwards – the new smartcard-aware Windows operating system will penetrate the market, and it seems inevitable that smartcard support will become commonplace at the application level and in the PC standard build. This means potential impediments to the widespread use of smartcards at home will be steadily falling.



To extend our vision of smartcards as infrastructure, let's look at innovative ways to tackle fraud.

Note that we use the Department of Human Services Access Card here purely for illustration. There are no commitments from the Access Card project to use their card for this type of purpose.

Smartcards can autonomously enforce all sorts of entitlements rules and "reasonableness tests", not just financial ones. It is often prohibitively expensive or outright impossible to connect to backend data-bases for real time fraud monitoring in health & welfare. Furthermore, monitoring every single transaction 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 Medicare fraud.

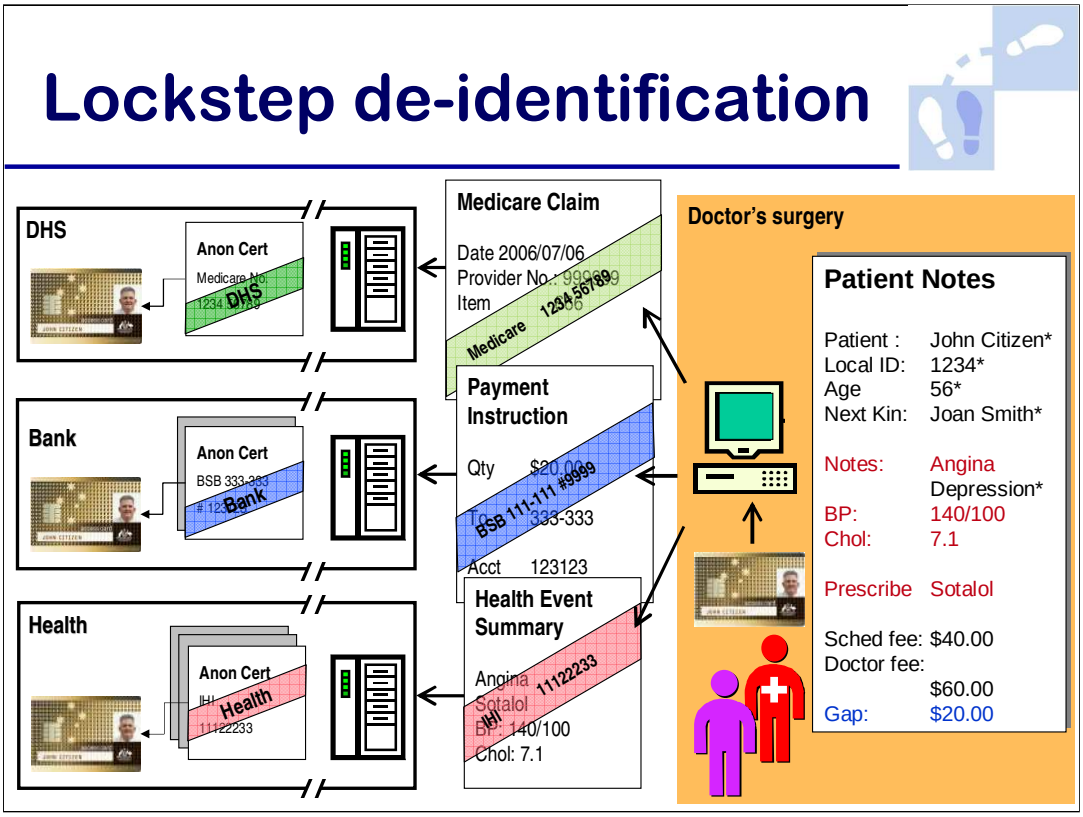
1. Doctor shopping, where a patient sees a number of different providers in quick succession to obtain drugs or some other benefit, can be detected by the card without transmitting sensitive data over the network, by checking e.g. the time between doctor visits, or the number of scripts written in a period.

Today's health system is vulnerable to doctor shopping primarily because at the time that a prescription is written or medication dispensed, clinical and pharmacy systems are not online to backend systems that might police usage and detect abuse. But smartcards can monitor usage autonomously and enforce rules offline.

In the diagram, 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 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. An attempt by the card holder to obtain additional prescriptions could be detected simply by checking the smartcard for details of pending scripts or the recent prescribing history.

2. Over-servicing, or fraudulent claiming by providers for item numbers not actually delivered. A related problem is the counterfeiting of claims by administrative clerical staff with illegitimate funds being obtained from the government and channelled to personal bank accounts.

The diagram shows an un-forgeable, indelible virtual stamp – *Dig Sig(Pt Card)* – created using an embedded key specific to the patient card, and attached to the 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.



Finally, Lockstep has developed a concept solution for de-identifying diverse transactions created using a smartcard. Again we use the Access Card purely for illustration.

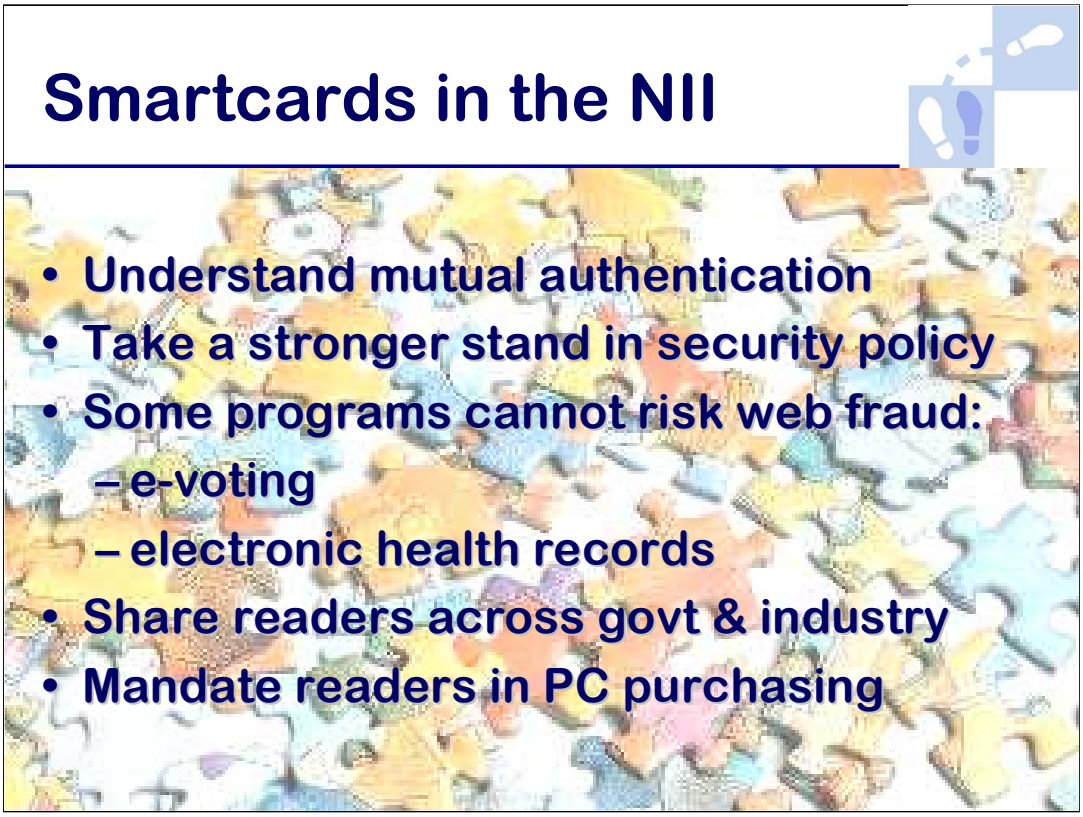
The Lockstep approach secretes identifiers within anonymous digital certificates issued to the smartcard. Transactions signed using such a certificate have the identifier indelibly bound to them, without any other identifying information.

The smartcard when first issued could come with one's Medicare number already installed in an anonymous certificate, 'sealed' by DHS. At any future time, and at the card holder's discretion, the card can be topped up with banking details and health identifiers, each sealed in their own anonymous certificates by a bank and by a health authority respectively.

During a routine visit to the doctor, the doctor's computer system creates a local record, containing such information as clinical signs and test results, prescribed drugs, the Medicare code for the type of service delivered, the scheduled fee (to be reimbursed by Medicare), and whatever additional gap fee the doctor will charge the patient for the appointment.

At the conclusion of the visit, the doctor asks the patient if they'd like a number of transactions to be launched on their behalf. Handing over their smartcard, the patient consents to having a Medicare claim, a payment instruction and a health event summary each created, sealed and sent out for processing. Each of these transactions is composed of a minimum set of data required for its context, and is sealed using the associated certificate and private key on the smartcard. Each transaction can be processed straight-through by its respective organisation, on the basis of the "chain of trust" from the card back through to the issued credentials. Note that none of the data coloured black in the local patient notes (much of which is extremely sensitive) is transmitted outside the doctor's environment.

All manner of additional transactions could be managed in a similar fashion. For example, private health insurance transactions could use anonymous certificates bearing the cardholder's respective insurance account numbers.



In conclusion, it is time that we expanded our view of smartcards, to see them as literally the keys to on-line safety. With several major national scale smartcard projects in their formative stages, we have a unique opportunity to switch over all G2C and B2C e-business to smartcard authentication, being the only robust, long term solution to phishing, pharming, web spoofing and spam.

If we take an infrastructure view of smartcards, then a number of critical projects could usefully be joined up. For example, the new Access Card ought to be made available to health authorities as a carrier for health record identifiers. And the banks' EMV rollout should be joined to their own Internet banking services.

Some programs, such as e-voting and electronic health records, are so critical that we suggest they should not be contemplated at all without the security – especially the mutual authentication – of smartcards.

There is a natural concern on the part of national smartcard projects that cards have been difficult enough to implement and that expanding the project scope in these early days may best be avoided. Yet all big smartcard projects are suffering public image problems, especially where they appear to threaten card holder privacy. If the Access Card, New Queensland Driver License and similar programs were to embrace a broader vision for smartcards – including mutual authentication, multiple identifiers, and de-identification – then they might well attract wider community support.

Further reading

A novel application of PKI smartcards to anonymise Health Identifiers
AusCERT academic stream 2005
www.lockstep.com.au/library/ehealth/a_novel_application_of_pki_sm

Smartcards and Healthcare Provider Fraud
and
Smartcards and Doctor Shopping
www.lockstep.com.au/library/babysteps

In closing, let's draw some inspiration from international experiences.

With the world increasingly shifting to smartcards, we should envisage a marketplace of innovative new products and services to grow up around the underlying infrastructure. And indeed smartcards are being applied in many exciting new ways.

1. The problem of smartcard readers is commonplace, and connecting smartcards to personal computers is still a challenge. But in some places, EMV smartcards are being used for remote authentication without needing to connect them directly, by adapting the smartcard for challenge-response two factor authentication. A special sleeve-like reader features a key pad for entering the challenge code; the reader interfaces to a cryptographic applet in the card which performs the challenge-response transformation and returns the result which is displayed by the reader. This solution is not perfect for online authentication, as it remains vulnerable to Man-in-the-Middle attack, but it does form a useful stepping stone to eventual full blown client side authentication, and it avoids doubling up the EMV smartcard with additional tokens.
2. Set-top cable TV boxes typically use a smartcard for subscriber management. Australian Foxtel users will be familiar with this. In the UK, set-top boxes for some time have featured a spare slot, and with the advent of Chip and PIN, the spare slots are coming into their own. At least one bank has teamed with a cable TV operator to offer online shopping, with authentication and payments effected through an EMV card inserted into the second slot.
3. In Taiwan, demand for smartcard readers has driven innovative low cost products, such as the "EZmini" reader. With no cable, this model is a little larger than a familiar USB 'thumb drive' and in effect acts as an adaptor to join the card to the PC. Over half a million EZminis have been sold in Taipei.
4. Blackberry has responded to the US Government's PIV program by developing a smartcard reader that hangs on a lanyard, holding the person's PIV card like a regular ID badge carrier, and interfaces with the PDA over Bluetooth.

Discussion

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