A new manifesto for smartcards as national information infrastructure

5th Homeland Security Summit – 2006 Security Technology Conference
Canberra, 21 September 2006

Stephen Wilson
Director – Lockstep Consulting Pty Limited
11 Minnesota Ave, Five Dock (Sydney) NSW 2046, AUSTRALIA
swilson@lockstep.com.au

Abstract

The smartcard debate in Australia is beset by misconceptions and tunnel vision. Smartcards are best known as the ideal solution to plastic card fraud, but they also offer unique remedies to the scourges of phishing, pharming, web fraud and spam. A host of novel two factor authentication devices are on the market, yet few of them can stop web fraud. Governments' electronic service delivery ambitions are expanding; profound benefits are rightly anticipated from electronic health records, electronic passports and driver licences, e-voting and online census collection. These programmes carry the most acute needs for privacy and security. If Australians using the Internet fear eavesdropping and identity takeover, then the nation should be introducing properly engineered smartcards as soon as possible and taking a uniform approach to all online identity. The potential benefits of smartcards in safeguarding privacy and security are so strong that they should be viewed as part of the National Information Infrastructure.

Biography

Stephen Wilson is a leading international authority on authentication, trust and public key infrastructure (PKI). He has over twenty years experience in commercial R&D, working in CSIRO, the medical devices sector and information security. He has been awarded three patents for PKI technologies. In 2004 Stephen established Lockstep Consulting, which provides independent research, analysis and advice on PKI and identity management, and undertakes R&D into innovative smartcard solutions for anonymity and mutual authentication. He is an active member of the OASIS PKI Technical Committee, the Asia PKI Forum, the Australian IT Security Forum, and the Gatekeeper Policy Committee.

1. Introduction

What could be meant by the possibility of smartcards as being "infrastructure" in Australia?

Some places invest in substantial physical IT 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. However these are not the sorts of projects that Australia tends to undertake.

Yet we can take a broader, 'softer' view of infrastructure, to encompass know-how and capability, a state of awareness of what a technology can do, and a 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, such as 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 and install readers for their PCs. Over two million smartcard readers have been bought to date by people for "Internet ATM" services offered by most Taiwanese financial institutions, which work using bank-issued smartcards. Uncomplicated readers are commonly available in Taipei for US$10 in convenience stores. This public expectation of service and a widespread, sophisticated understanding of technologies can be viewed as "infrastructure" of a sort that could feasibly be fostered more energetically in Australia.

This paper examines the importance of smartcards in the fight against web fraud, and identifies powerful new possibilities for them to actively enhance privacy. I will argue that smartcards are so important that more should done, urgently, across government and business to bring smartcard capabilities to fruition nationally.

1.1 Public attitudes to smartcards

Smartcards tend to inspire fear. The Sydney Morning Herald editorial writer, commenting in early 2006 on the prospects of a health & welfare smartcard, seemed blithely unaware of even the possibility that smartcards could enhance privacy, when he/she wrote: "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".[1]

Moreover, there is a default view that privacy can (and perhaps should) be traded off in the interests of security. Politicians and even technologists have got into the habit of conceding that some privacy could be

[1] Editorial, Sydney Morning Herald, 6 February 2006, p 10.

given up in the name of better security. A typical remark of this sort was attributed to Australian Treasurer Peter Costello when it was reported that he “publicly praised the smart card idea, saying people were now more tolerant of intrusions into their privacy because of security threats”.[2]

The notion that security and privacy are to some extent opposites runs deep. One recent academic analysis appeals to Maslow’s Hierarchy of Needs, arguing that many aspects of privacy are of a higher order than security. This seems a reasonable proposition, and yet according to Maslow, “if a lower-order need is threatened, the significance of higher-order needs is suspended until the lower-order needs are once again satisfied” (Clark, 2006). One of the deep dilemmas is that privacy is difficult to recover once breached. If we are willing to compromise privacy while we drop down a level to fix security, then it might not be possible to climb back up the pyramid and expect to enjoy privacy once again. So the Maslovian perspective endorses the presumption that we might not be able to have security and privacy at the same time.

2. A new manifesto

Perhaps we need a new “manifesto”, to lay the foundations for up-to-date and optimistic technological responses to the challenges of security and privacy. Such a manifesto might include the following four principles.

2.1 There should be no privacy debate

First, we should not even think about having a debate about privacy. Privacy should not be imagined to be readily negotiable. Let us not give it up almost reflexively for fear of security being more important. The public should expect to enjoy privacy and security at the same time.

2.2 We have the right to deal anonymously

Second, we should insist on our rights to deal anonymously. National Privacy Principle No. 8 is in fact all about Anonymity, but sadly it is rarely taken seriously in industry. True anonymity is such a great technical challenge that most people seem to have come to view it as academic and to ignore the practical possibilities altogether.

2.3 We should resist the centralisation of data

Third, we should all resist the ever increasing trend to centralise data storage and management. One of the more obvious and worrying outcomes of data centralisation has been the sale of massed personal information to criminals by corrupt call centre workers.[3] Theft, or accidental leakage of personal information from government agencies, financial institutions and data processing bureaus is regularly reported nowadays. A key question is, Why have we allowed huge stockpiles of our personal details to be aggregated like this by third parties? As identity crime soars, large stores of personal information are increasingly valuable to sophisticated and highly organised attackers.

2.4 The community deserves safe means to access the Internet

And finally, the community deserves some guarantee of safety when people access the Internet. The Australian Government has a laudable goal of moving more and more of its services and transaction traffic online. Australia’s Human Services agencies in particular currently send out hundreds of thousands of pieces of mail every day; the Minister has said “ I would like [Centrelink] to move as much correspondence as possible to email and SMS”.[4] But if it expects citizens to use e-mail, government must surely take active steps to guarantee the safety of the channel in regards to phishing, pharming, spam and website spoofing. The potential for the Human Services Access Card to be applied in this regard has yet to be fully elaborated.

3. A brief review of Authentication technologies

Smartcards compete with other approaches in a rapidly growing marketplace of authentication technologies.

3.1 Two Factor Authentication

Two Factor Authentication protects users against identity theft by making it more difficult to take over their authenticators. The term *Two Factor* refers to verifying someone’s identity online by way of something they *know* (a password) in addition to something they *possess* (a personal device of some sort). A wide variety of Two Factor devices are available with varying degrees of sophistication and cost, including:

— “One Time Password” (OTP) which can be electronically generated on a “fob”, or else provided in advance in the form of a scratchy card or a booklet containing several dozen pseudo-random pass codes to be used in sequence. Some electronic OTPs are “time based” where the key fob is synchronised to the backend server and each pseudo-random number remains valid for only 30 seconds or so before changing over.

[2] Louise Dodson, Sydney Morning Herald, 26 April 06, p1.

[3] See for example the ABC Television Four Corners programme “Your Money and Your Life” broadcast on 15 August 2005; transcript at www.abc.net.au/4corners/content/2005/s1438338.htm (accessed 12 August 2006).

[4] See Minister Hockey’s “Statement of Expectations” for Centrelink, 27 October 2005, at www.humanservices.gov.au/modules/resources/agencies/soe_centrelink.rtf (accessed 12 Aug 2006).

— "Challenge-Response" approaches generally involve the service providing an initial challenge code, and the client being required to calculate a response using a special device. If the calculation proves to be correct then the service can assume that the user is indeed in possession of the right device. Challenge-Response routines can be implemented electronically using a calculator-like device, or through a static form printed with a row-column look up table (sometimes referred to as a matrix card).

— Cryptographic authenticators include smartcards and functionally similar USB keys.

— Text messaging utilises a mobile phone as the second factor. The user trying to access an online service is sent a pseudo-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, representing a response to the problem of end user identity theft or takeover.

While all of these approaches provide a measure of protection against end user identity theft, a more recent realisation is that identity takeover of the *service provider* – that is, website 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, as we shall see.

3.2 Attacks on Two Factor Authentication

A little over a year ago, cryptographer and security commentator Bruce Schneier raised the alarm over two factor authentication's inherent inability to protect against a raft of threats, typified by the "Man-in-the-Middle" attack (as explained in section 3.4 below) warning that "two-factor authentication won't work for remote authentication over the Internet" (Schneier, 2005). Schneier's analysis is cogent, non-technical and readily grasped. However most organisations have been relatively slow to respond. My personal experience as a security professional was that security managers in large businesses tended to dismiss Schneier's concerns as "academic". A typical position was that the Man-in-the-Middle attack was thought to be only theoretical, and that in any event, businesses have mechanisms for detecting a run of suspicious transactions and shutting down the channel.

Just a few months after Schneier's warnings, the first successful assaults on two factor authentication were seen. Best known was the attack on Nordea Bank's One Time Password scratchy pads.[5] A 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. Another bogus error message was posted, 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.

Worse was to come. The electronic One Time Password system of Citibank was attacked in July 2006.[6] This attack was first spotted in the wild by a security research firm, hosted on a Russia-based hacker site. The bank was alerted promptly and the site was shut down before much if any damage was done. But the lesson is sobering: event based OTP really is vulnerable. And there is no reason to feel more confident in time-based OTP, since these attacks are automated and can replay stolen one time passwords within the few seconds that they remain valid.

The necessary response to these vulnerabilities is proper mutual authentication (which can of course also embody two factors). The issue has become 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.[7]

3.3 Mutual Authentication

One of the peak finance sector regulators in the US, the Federal Financial Institutions Examination Council (FFIEC), in late 2005 started advocating stronger remote authentication. The FFIEC has called for the introduction of two factor authentication, and separately, pointed out the need for mutual authentication too: "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

[5] See also news at http://www.f-secure.com/weblog/archives/archive-102005.html#00000668 and analysis at www.schneier.com/blog/archives/2005/10/scandinavian_at_1.html (accessed 15 July 2006).

[6] See http://blog.washingtonpost.com/securityfix/2006/07/citibank_phish_spoofs_2factor_1.html (accessed 15 July 2006).

[7] See www.abc.net.au/pm/content/2006/s1696632.htm (access 10 August 2006).

considered one of the stronger authentication technologies, and mutual authentication provides a defence against phishing and similar attacks" (FFIEC, 2005).

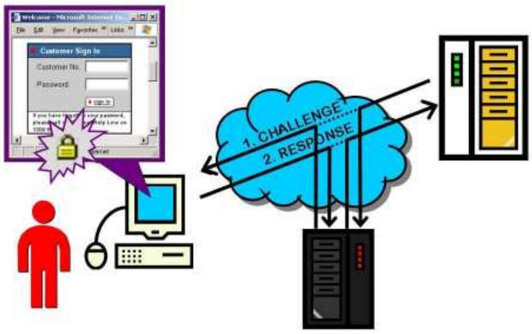
The United States has already taken a policy position on mutual authentication. The US National Institute of Standards and Technology has published binding guidelines that stratify electronic transactions according to risk level, and characterise in detail the type of security services that are needed to support each level. "Level three" and "level four" (the highest classifications) require "cryptographic strength mechanisms that protect the primary authentication token (secret key, private key or onetime password) against compromise by the protocol threats including: eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks" (NIST, 2004). The head of cryptography at NIST has emphasised the special capabilities of smartcards and similar devices, starting that in respect of Man-in-the-Middle attacks, "the only practical solution today uses PKI [on hard tokens]" (Burr, 2005a). So, while the new US Federal Government Personal Identity Verification (PIV) smartcard was driven by counter-terrorism concerns, there is evidently a strong move to utilise the PIV PKI-enabled smartcard for remote mutual authentication as well (Burr, 2005b).

3.4 The Man in the Middle attack

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 network session (Fig 1). By passing authentication messages straight through to the backend, the attacker can impersonate the client, and once a session is established, can take over, for example to redirect funds to the attacker's account.

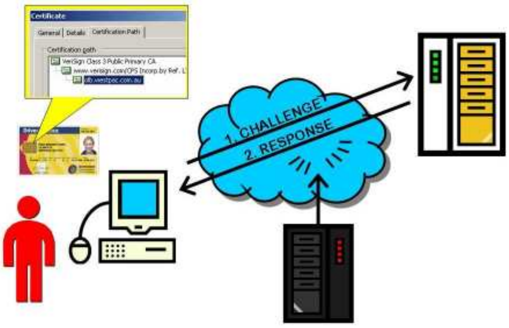
For an even more convincing attack, it is has become apparent that the Secure Sockets Layer (SSL) protocol, which is signaled by the well-known padlock symbol on a web browser, can also be usurped by an attacker. There is a vulnerability where any SSL server certificate that chains back to a root key held in the browser can be blindly accepted by web browsers.[8] The fundamental problem is that root certificates held in a PC's memory can be tampered with or substituted.

Figure 1: Man-in-the-Middle attack



No conventional two factor authentication device– be it One Time Passwords (Burr, 2005b), matrix cards, text messaging or biometrics (Burr, 2005b) – can prevent Man-in-the-Middle attack because none have the active functionality to challenge the veracity of the far end during the early stage of the handshake. 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 (Fig 2). Note carefully therefore that the directions of the challenge-response arrows are reversed compared with Figure 1.

Figure 2: Mutual Authentication to thwart the Man-in-the-Middle



One important way that smartcards can implement mutual authentication is to use them to hold tamper proof copies of the digital certificates which underpin 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.

3.5 A complete picture of smartcard benefits

The headline benefits of smartcards tend to be thought of as greater storage capacity compared with magnetic stripe cards, and a resistance to skimming and cloning. These are certainly compelling features, but there is much more to smartcards, as summarised below.

[8] See www.theregister.co.uk/content/4/26924.html and www.theregister.co.uk/content/4/26620.html.

3.5.1 Protection against skimming, counterfeiting

Smartcards can be made, for all practical purposes, resistant to those forms of card fraud that involve replicating card holder data. Rather than holding all data in freely readable magnetic memory, a smartcard stores and actively manages data using an on-chip operating system.

3.5.2 Vastly greater storage capacity

Smartcards today can commonly hold several tens of Kbytes of data, which is of the order of one hundred times the capacity of a magnetic stripe card.

3.5.3 On-chip processing

More important than sheer memory capacity is that smartcards are literally "smart", in that they have their own programmable computers. They can regulate their own functions according to the environment they find themselves in; for instance, some functions can be withheld unless a particular kind of smartcard reader is detected, such as one with a tamper resistant PIN pad.

3.5.4 Security

Smartcards offer intrinsically greater security for stored data than most other portable media. The embedded computer system can protect data with tiered access controls comparable to a conventional PC's file management system. Dedicated smartcard operating systems (COSs) have typically been designed from the bottom up with more robust inherent protection mechanisms than conventional computers.

3.5.5 Mutual Authentication

See section 3.3.

3.5.6 Multiple Identifiers

Modern identity management principles, as exemplified by the Laws of Identity (Cameron, 2005) hold that individuals can and should conduct their affairs under a number of separable identities or identifiers. Smartcards can be configured to act as flexible 'containers' for multiple identifiers; benefits include de-centralisation of identifier resolution, lower cost and improved performance in offline environments, and reduced need for intrusive data mining and the aggregation of 'innocent' transaction information.

3.5.7 Self-monitoring to detect fraud

EMV[9] smart credit and debit cards can be programmed to tally daily spending. In the event that a transaction cap is breached, the card can respond intelligently, by blocking the next transaction, or more subtly, by flagging the fact to the merchant who might handle the situation in a variety of ways. Similar offline monitoring could detect and manage fraud in the health & welfare sector; see 5.1 and 5.2.

3.5.8 De-identification and anonymity

Finally, modern smartcards usually feature a built-in cryptographic co-processor which can be used to encrypt or mask identifiers. In certain circumstances, such as electronic health records, robust anonymity appears to be possible (Wilson, 2005).

4. Recent smartcard market developments

Smartcards continue to suffer from a widespread assumption that their time has not yet come. It is instructive to review the rollout of some major programs overseas, and strategic policy developments in the IT industry, most notably at Microsoft, for they will drive the development of essential commercial infrastructure, such as integrated smartcard readers, software toolkits and emerging applications.

In early 2003, Bill Gates issued one of his occasional "executive e-mails" where he espoused the virtue of smartcards for authentication. He said that "over time we expect that most businesses will go to smartcard ID" (Gates, 2003). The effect on the PC and laptop industry was almost instantaneous; within 15 weeks Dell introduced its first computer 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, credit and debit card security became an urgent issue in Britain, where fraud had reached GBP 400 million p.a., about 50% of which was predicted to be saved through the introduction of smartcards (Haddad, 2005). 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. British domestic credit and debit card usage has transitioned rapidly to smartcards; fraud is reported to be down by 30% already.[10]

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

[9] EMV stands for Europay-MasterCard-Visa, the original founds of this standards setting consortium for smart credit card technology. See www.emvco.com.

[10] See www.chipandpin.co.uk/reflib/chipandpin_10oct05.pdf (accessed 10 July 2006).

In Australia the two largest and most prominent smartcard proposals are the New Queensland Driver Licence (NQDL)[11] and the proposed new Department of Human Services Access Card.[12] Both of these from time to time have been cautiously touted as providing keys to online services, but neither project has yet to commit itself to supporting remote authentication. If we had a broader shared vision of smartcards as infrastructure, then the NQDL and the Access Card could both be viewed as important resources for the whole community, becoming over time the preferred means for individuals to interact with government online. Within the timelines for the rollout of both of these programmes (that is, 2008 onwards) the new smartcard-aware Windows Vista operating system will penetrate the market, and it seems inevitable that smartcard support will become commonplace at the application level and in the standard commercial PC build. This means potential impediments to the widespread use of smartcards at home will be steadily falling, and the widespread use of smartcards for remote access will become practicable.

5. New proposals to combat fraud using smartcards

Note that in the rest of this paper, a depiction of the Department of Human Services Access Card is used for illustration. There are no commitments from the Access Card project to use their card for this type of purpose, and no implication should be inferred from this paper that the proposals presented here are endorsed by government.

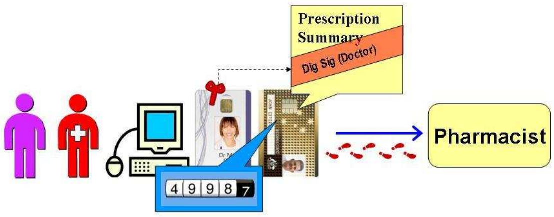
Smartcards can autonomously enforce all sorts of entitlements rules and "reasonableness tests", not just financial ones. In health & welfare, where connectivity is notoriously variable, it can be prohibitively expensive or outright impossible to connect to backend data-bases for real time fraud monitoring. Furthermore, monitoring every single transaction to weed out a tiny minority of fraud cases jeopardises the privacy and security of the vast majority of 'innocent' users. The first two of the following proposals show how smartcards could be utilised in place of transaction data aggregation and mining, in order to combat two important forms of fraud.

5.1 *Doctor shopping*

"Doctor shopping" is when a patient sees a number of different providers in quick succession to obtain prescription drugs or some other benefit. 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 computers are not online to backend systems that might police usage and detect abuse. Such abuse is relatively easy to detect from transaction patterns but only at audit-time, weeks or months after the event. Real time detection by data mining carries significant privacy risks, not to mention performance challenges. However, just as EMV smartcards working offline can tell when daily spending limits are breached, a health & welfare smartcard could detect abuse autonomously and without transmitting sensitive data over the network.

A schematic proposal is shown in Figure 3. When a doctor prescribes a drug, certain details (if not the entire script) would be written to the patient's smartcard, and digitally signed with the doctor's professional smartcard.[13] The smartcard would automatically count some pre-defined parameter such as the number of scripts written in a certain period of time. 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 cardholder's entitlements seem to have been breached.

Figure 3: Using a smartcard to mitigate doctor shopping



5.2 *Provider fraud*

Another serious problem is over-servicing for financial gain, or fraudulent claiming by providers for services not actually delivered. A related issue is the outright counterfeiting of health insurance claims by administrative clerical staff with illegitimate funds being channelled to personal bank accounts.

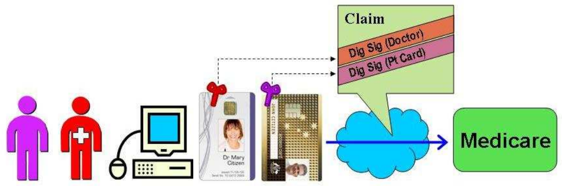
Figure 4 shows one way to combat counterfeiting and over-servicing, wherein an unforgeable, indelible "seal" – Dig Sig(Pt Card) – is created using an embedded key specific to the patient card, and attached to the claim. For a claim to be legitimate, it would have to feature both the digital signature of the doctor, and the seal 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.

[11] See www.transport.qld.gov.au/new_driver_licence (accessed 16 August 2006).

[12] See www.humanservices.gov.au/access/index.htm (accessed 10 July 2006).

[13] Medical professional smartcards are in widespread use in countries including Taiwan, France and Australia; see for example www.hesa.gov.au.

Figure 4: Using a smartcard to mitigate provider fraud



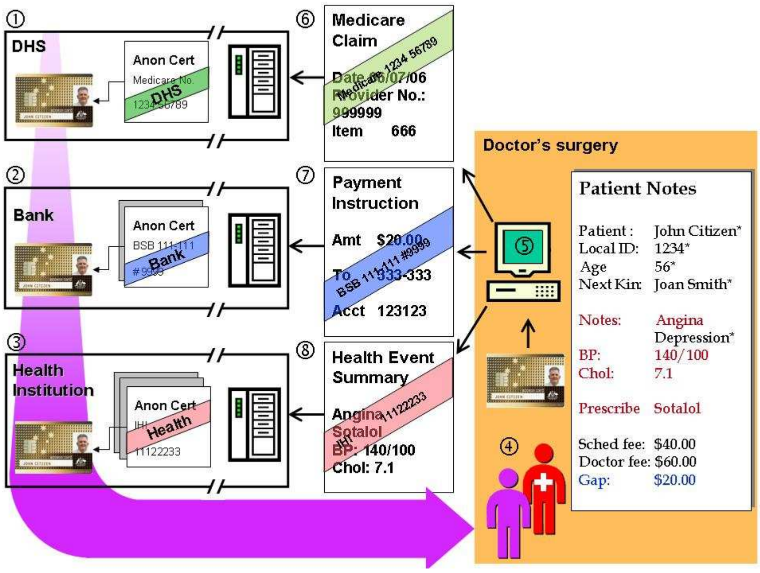
5.3 Transaction de-identification

Finally, Lockstep has developed a concept solution for de-identifying diverse transactions created using a smartcard. 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 (Wilson, 2005).

As shown in Figure 5, a smartcard when first issued could come with one's Medicare number already installed in an anonymous certificate (step 1), 'sealed' by the issuer, namely the Department of Human Service (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 issued by a bank and by a health institution respectively (steps 2 and 3).

During a routine visit to the doctor (step 4), the doctor's system creates a set of local Patient Notes, containing such information as a local record ID, next of kin, 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.

Figure 5: De-identifying transactions using anonymous credentials on a smartcard



At the conclusion of the visit, the doctor asks the patient if they would like a number of transactions to be launched on their behalf (step 5). Handing over their smartcard, the patient consents to having a Medicare claim (step 6), a payment instruction (7) and a health event summary (8) 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" extending from the card back through to the issued credentials. Yet none of these transactions are linked to each other, and none can be reverse identified without having access to the patient's smartcard. Note that none of the data marked with an asterisk in the patients 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.

6. Conclusion

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 government-to-citizen and business-to-consumer e-business to smartcard authentication, being the only robust, long term solution to phishing, pharming, web spoofing and spam. Most Internet transactions could come to be supported by a national smartcard infrastructure, comprising interoperable smartcard readers, operating systems, software toolkits, and common practices for managing smartcard based identifiers.

If we take an infrastructure view of smartcards, then a number of critical projects could usefully be joined up. For example, the new Human Services Access Card could be made available as a carrier for health identifiers, enabling true anonymity of electronic health record entries. And the banks' EMV rollout could be joined to their own Internet banking services, superseding the Two Factor authentication tokens that have already proved vulnerable to Man-in-the-Middle attack.

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

References

Burr, W. 2005a Electronic Authentication in the U.S. Federal Government, *Asia PKI Forum Conference* Tokyo 24 Feb 2005: p22, at http://asia-pkiforum.org/feb_tokyo/NIST_Burr.pdf (accessed 10 July 2006).

Burr, W. 2005b NIST SP 800-63 Electronic Authentication Guideline and Biometrics, *Workshop on Biometrics and E-Authentication Over Open Networks* Gaithersburg, Maryland 30 March: p10, 15 & 18, at http://csrc.nist.gov/pki/BioandEAuth/Presentations/Wednesday,%20March%2030/Burr.pdf (accessed 15 August 2006).

Cameron, K. 2005 The Laws of Identity, Microsoft Corporation at http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf (accessed 8 August 2006).

Clarke, R. 2006 What's 'Privacy'? at www.anu.edu.au/people/Roger.Clarke/DV/Privacy.html (accessed 15 August 2006).

FFIEC (Federal Financial Institutions Examination Council), 2005 Authentication in an Internet Banking Environment, 12 October 2005, at www.ffiec.gov/pdf/authentication_guidance.pdf (accessed 12 August 2006).

Gates, W. 2003 Security in a Connected World, Microsoft, at www.microsoft.com/mscorp/execmail/2003/01-23security.asp (accessed 10 July 2006).

Gates, W. 2006 Microsoft's Security Vision and Strategy, *RSA Conference 2006* San Francisco, 14 Feb 2006, at www.microsoft.com/billgates/speeches/2006/02-14RSA06.asp (accessed 10 July 2006).

Haddad, A. 2005 *A New Way to Pay: Creating Competitive Advantage Through the EMV Smart Card Standard* London: Gower.

NIST (National Institute of Standards and Technology), 2004 Electronic Authentication Guideline, Special Publication 800-63 v1.0.1: pp vii-viii.

Schneier, B. 2005 The Failure of Two-Factor Authentication, *Cryptogram* 15 March 2005, at www.schneier.com/crypto-gram-0503.html#2 (accessed 15 July 2006)

Wilson, S. G. 2005 A novel application of PKI smartcards to anonymise Health Identifiers *AusCERT 2005 Asia Pacific Information Technology Security Conference*, May 2005, at www.isi.qut.edu.au/events/conferences/auscert2005/proceedings/wilson05novel.pdf (accessed 10 July 2006).