Lockstep Consulting
11 Minnesota Ave
Five Dock NSW 2046
Australia

25 July 2006

Professor Allan Fels
Access Card Consumer and Privacy Taskforce
PO Box 3959
Manuka ACT 2603

Dear Prof Fels,

Submission on Access Card Discussion Paper Number 1

Many thanks for the opportunity to contribute to your Taskforce's important work on the Access Card.

Executive summary

Overall, Lockstep Consulting is satisfied with the first Taskforce Discussion Paper as a cogent summary of the prima facie issues raised by the Access Card as currently proposed. We agree there are many policy issues to be explored in coming months. These include the sorts of regulatory measures that could prevent the Access Card morphing into a de facto *Australia Card*, the pros and cons of having photographs etched into the surface of the card (including the cost and logistical implications, as well as the likelihood of function creep), and whether the centralised SCRS as currently envisaged presents major avoidable risks, as a "honey pot" for would-be attackers. The paper is a great start along these lines and we commend your team for it.

We would like to draw the attention of the Taskforce to a range of specific matters mostly under the heading "Making the Right Technology Choices". We are concerned that the full spectrum of smartcard capabilities is yet to be articulated, and that the corresponding upside for privacy has yet to be developed. Smartcards differ from magnetic stripe cards in more ways than mere memory size. Their in-built computer processing power, cryptographic functions and ability to work autonomously provide major opportunities for *enhancing* privacy, far beyond the rather obvious point that identity theft needs to be curtailed.

To ensure that the Access Card delivers maximum value to the public and to the government, Lockstep recommends that the following unique capabilities of smartcard technology be more fully factored into the policy formulation and system architecture:

— Mutual Authentication: smartcards should be the clearly preferred means for accessing sensitive services online, to protect consumers against phishing, pharming, web fraud and spam, as well as identity theft.

— De-centralisation of data management: fraudulent card use can generally be better detected by the card itself rather than by data mining all health & welfare transactions, resulting in better consumer privacy protection, less invasion into routine transactions, and better system performance.

— Multiple identifiers: smartcards can store and manage diverse consumer identifiers, to preserve their existing relationships with backend schemes and systems, and thus resist unnecessary data linkages.

— Anonymity: smartcards can encrypt identifiers to protect against eavesdropping, and to "firewall" business conducted in different domains using the one card.

Introduction

Lockstep Consulting was established in early 2004 by Stephen Wilson, a leading international authority on identity management and authentication. Lockstep provides independent advice, analysis and management consulting in security policy and strategy, authentication and privacy. Lockstep also undertakes independent self-funded R&D in smartcards and Public Key Infrastructure (PKI). Current clients include Medicare Australia, the Australian Government Information Management Office (AGIMO), the Australian Divisions of General Practice, and the US-based Organisation for the Advancement of Structured Information Standards (OASIS).

Mr. Wilson is a member of security policy bodies including AGIMO's Gatekeeper Policy Committee, the board of the Australian IT Security Forum, the Asia PKI Forum, and NATA's IT Testing Accreditation Advisory Council. He was a founding member of the National Electronic Authentication Council (NEAC), and he sat on the previous Federal Privacy Commissioner's PKI Reference Group. Lockstep has made detailed public submissions in recent years to privacy related inquiries, including the Senate inquiry into the Privacy Act, DCITA's inquiry into spyware, and the Department of Health and Ageing's development of a National Health Privacy Code.

There should not be a privacy debate!

It is disappointing that privacy discussions are so commonly framed as a "debate", as if privacy were a negotiable commodity. Moreover, there is a pervasive presumption that smartcard technology must necessarily be a threat to privacy. Many politicians and indeed smartcard advocates regrettably legitimise the notion of a compromise with needless remarks along the lines of 'the world has changed since the Australia Card was defeated' or 'people don't mind trading off privacy against security and convenience'. Lockstep contends that privacy need not be traded off against security. Having said that, it is a fact that many of today's security technologies and methodologies are indeed privacy invasive.

Smartcards are a rare exception. Our strong view is that smartcards present such a strong and unique range of privacy safeguards that they should be viewed as critical information infrastructure, for the good of the public. We would therefore like to see a somewhat broader vision developed for the application of the Access Card, while remaining mindful of function creep and the Minister's stated aim of keeping the project focused and contained.

Smartcards are much more than capacious magnetic stripe cards

The power of smartcards as *privacy enhancing technologies* (PETs) goes far beyond the aphorism that security is necessary for privacy. Even the entirely reasonable observation that "there's no worse privacy breach than for someone to pretend to be you"[1] only scratches the surface. It is true that smartcards are one of the most effective means for preventing identity theft, for they can be effectively impossible to skim or counterfeit. But more subtle – yet more powerful – is the smartcard's capacity to actively safeguard people online, by managing multiple identifiers, encrypting identifiers, and applying anti-fraud logic at the client side of transactions (and even offline) so as to reduce the need for centralised logging and data mining. We will explore these abilities in more detail below.

With appropriate programming of their embedded microcomputers, smartcards can act as *intelligent proxies for their owners*, in various ways. For one thing, a smartcard can autonomously monitor the way in which it is being used, and apply security rules to detect and prevent abuse, without needing to connect to backend systems. In the EMV scheme for instance, smartcards tally daily activity and when a pre-set limit is reached, they can block all subsequent transactions, or flag the irregularity to the merchant terminal.

Lockstep has researched this sort of capability further, to develop anti-fraud concepts for health & welfare smartcards; see [1] and [2]. If card abuse can be detected and managed at the client side, then we can reduce the transmission and centralisation of activity data, and cut the unnecessary exposure of the vast majority of 'innocent' health & welfare transactions to data mining.

Another way in which smartcards can act as proxies for their owners and protect them from harm is in remote authentication. The task of knowing to whom or to what one is connecting online is becoming ever more fraught. Phishing, pharming and spam are all manifestations of the same basic problem, namely the challenge of accurate online authentication. The cyber-crime arms race has come a long way in thirteen years since it became received wisdom that "on the Internet, nobody knows you're a dog".[2] As the US Federal Financial Institutions Examination Council (FFIEC) explained last year, "one reason phishing attacks are successful is that unsuspecting customers cannot determine they are being directed to

[1] Paul Chadwick, Victorian Privacy Commissioner, speaking on SBS Television "I Spy", 15 March 2005; http://news.sbs.com.au/insight/trans.php?transid=935.

[2] "On the Internet, nobody knows you're a dog" by Peter Steiner, New Yorker, 5 July 1993.

spoofed Web sites during the collection stage of an attack" [3]. Today, sophisticated "Man-in-the-Middle" attacks mean that no web site is safe. In particular, the well known SSL padlock is more or less broken; its appearance at the bottom of the browser screen no longer guarantees that a site is genuine. Awareness in Australia of Man-in-the-Middle risks is mounting rapidly; even as I was writing this letter, ABC Radio's "PM" reported on the issue.[3]

In the next section we expand on the issue of remote – and in particular, *mutual* – authentication and explain how smartcards have a vital role to play in protecting users online.

Mutual authentication

"Mutual authentication" is set to become a benchmark for all serious e-business. Put simply, Internet users need the ability to verify the identity of an online service *before* that service verifies them. Security discussion around the Access Card to date has been dominated by the aim of mitigating the risks of lost, stolen and counterfeit cards. But equally important in the online environment is to ensure the authenticity of service providers like DHS itself and potentially other agencies and institutions. For as we have seen, the general inability of users today to be sure of the identity of sites they are visiting lies at the heart of the problems of phishing, pharming and much web fraud.

Two Factor Authentication is a widespread response to identity theft, involving something a user possesses in order to grant them access to an online service, in addition to something they know (namely their password). The principle of Two Factor Authentication is beyond reproach, for it makes identity theft far harder to perpetrate unnoticed. But most Two Factor devices today address only half of the problem. As respected cryptographer and commentator Bruce Schneier has written, one time password key fobs, challenge-response devices, mobile phone text messaging, "matrix" cards, transaction authorisation scratchy cards and even biometrics, are vulnerable to Man-in-the-Middle attack [4]. These risks are not theoretical (as was first thought by banking security strategists); successful attacks have now been recorded against Two Factor Authentication systems at Nordea Bank[4] in Finland and Citibank[5] amongst others.

Smartcards however are different. The US National Institute of Standards and Technologies (NIST) has declared that to resist Man-in-the-Middle attacks, "the only practical solution today" uses PKI-enabled smartcards [5]. Indeed, this fact is one of the drivers behind the planned migration for US government workers to use the Personal Identity Verification (PIV) smartcard for remote logon. The FFIEC too has noted that "digital certificate authentication is generally considered one of the stronger authentication technologies, and mutual authentication provides a defence against phishing and similar attacks."

[3] http://www.abc.net.au/pm/content/2006/s1696632.htm

[4] http://www.theregister.co.uk/2005/10/12/outlaw_phishing

[5] http://www.finextra.com/fullstory.asp?id=15570

To properly verify the identity of another computer over the Internet requires the examination of complex security codes, in minute detail, to thwart today's more subtle attacks. This task is essentially beyond human users, but it can be automated on their behalf by smartcards. A smartcard can be pre-configured with tamper resistant copies of the unique security codes of its issuer, and can subsequently check those codes each and every time the card holder attempts to connect to associated services online.

"Making the Right Technology Choices"

Lockstep suggests that the greater potential of the Access Card to protect consumers could be brought out under the heading in your Discussion Paper, "Making the Right Technology Choices". Not only must the right technologies be selected, but decisions must be made in the policy formulation, requirements analysis and architecture stages of the project that fully realise their privacy enhancing benefits. These benefits include the following:

— ***Mutual authentication***. Smartcards should be the clearly preferred means for accessing sensitive services online, to protect consumers against phishing, pharming and web fraud. The Access Card could be vastly more useful to the community if it became, over time, the universal key for accessing government and related services over the Internet. The Department of Human Services has the laudable goal of transitioning an increasing proportion of consumers to web-based service delivery, but surely it is incumbent on government to safeguard consumers against the possibility of spoofed health and welfare sites, spam e-mail and so on.

— ***Multiplying identifiers.*** All things being equal, it is better for privacy if consumers can conduct their affairs independently across multiple service providers. Different identifiers should be reserved for different systems (and of course National Privacy Principle 7 expressly forbids the re-use of government-issued identifiers for other purposes[6]). Smartcards can act as "containers" for holding and managing a consumer's set of identifiers, in order to protect them, streamline and automate their use, and above all, to help resist the trend to otherwise rationalise identifiers.

An important objective of the Access Card is to streamline those instances where a consumer has multiple entitlements. Yet it is not clear from the documentation released to date exactly how this will take place. In our view, it is to be hoped that individuals who today have multiple DHS agency identifiers will continue to have multiple identifiers, with little or no change in the way respective backend systems deal with them. The most elegant and most secure way to accomplish this could be to store a person's various identifiers in their Access Card. Yet sections 6.1.4 to 6.1.8 of the KPMG Report [6] concerning the information to be stored in the chip appear to rule this out.[7]

[6] http://www.privacy.gov.au/publications/npps01.html#g

[7] What's more, KPMG in passing seems to play down the importance of different identities in different backend systems when it states on page 5 that "fundamentally all of the cards contain the same information, i.e. name, some form of registration identifier and a person's entitlement to different services." On the contrary, registration

Furthermore, the Access Card is a superb opportunity to better manage other identifiers, especially in the health sector. It could be made available to qualified third party services, such as Commonwealth and state health departments, for carrying their respective identifiers. The need to safeguard electronic health record users against pharming and web fraud is so acute that in our view, NeHTA's planned Individual Health Identifier should be joined to the Access Card. If the smartcard is architected as a container that can be 'topped up' with approved third party identifiers, then the attendant project management risks for the Access Card are close to zero.

— ***Decentralisation of personal data management***. The online health & welfare environment brings increasing pressure for centralised management of personal information, with consequential risks to privacy. Already, banking details for certain social security recipients are held on government databases. To combat fraud, data on doctor visits, prescribing behaviours, medical testing and so on looks like being compiled and mined. And as we have seen, the KPMG report leaves open the possibility that people with multiple entitlements could have their various agency identifiers linked on the SCRS.

  An alternative philosophy is to decentralise data management using the smartcard. Most of the fixed personal data needed in routine encounters with human services systems, such as banking details and diverse identifiers, can be secreted within the chip, access-controlled, and retrieved when needed. Furthermore, transactions can be tracked locally within the smartcard memory, with fraudulent patterns detected at the client side, eliminating the need to transmit routine activity information to central repositories for surveillance. Finally, on those occasions when a consumer needs to access two entitlements systems at once, it is far better that their identifiers be linked on the client side with the aid of their smartcard (as opposed to centrally in the SCRS for instance), not least because the need to present the card manifests concrete cardholder consent.

— ***Anonymity***. Not only can smartcards hold multiple identifiers, they can use their in-built cryptographic processors to encrypt or mask those identifiers, enhancing privacy even further. Lockstep has published academic peer-reviewed research elaborating how genuine anonymity for health records systems can be achieved using standard digital certificate functions; see [7]. Provided a suitable smartcard platform is selected – most contemporary banking and government services card products are suitable – the anonymity function would not impact the Access Card project cost or scope.

numbers for different cards are *fundamentally not the same thing at all*, for they each represent a separate relationship. The processes by which one person might come to have multiple government service relationships ought not to be treated as being amenable to combination or rationalisation, for that would open the way for almost automatic linkages between backend systems.

Other specific comments on the Taskforce paper

There are some technical errors in the paper which we recommend be corrected in future work.

- *Digital Signatures*. The term "digital signature" is used in several places to mean an image of the card holder's handwritten signature; a better term would be "digitised autograph" or "digitised signature". The term "digital signature" has a quite different meaning in e-security and, moreover, in Australian Government agencies implementing PKI, such as Centrelink and Medicare Australia. Specifically, it means a machine-generated electronic signature created using an asymmetric private key (they have special advantages in respect of longevity, delegation and their ability to convey attributes as well as identity). Digital signatures are a vitally important security technology which for a range of reasons, some of which are canvassed in this letter, ought to be implemented in the Access Card chip.

- *Algorithms*. The term "algorithm" is mis-used. An algorithm is not the reduced numerical dataset derived by biometric analysis of a photograph; rather, it is the method for doing the reduction. The proper term for the reduced biometric dataset is usually "template".

- *Negative Identification*. At the end of page 30, mention is made of the business objective of being able to detect duplicate registrations for Access Cards. The paper says that if only templates rather than photographs were stored in the SCRS, then "the system would no longer be able to detect duplicate registrations". This is probably not correct. An effective facial biometric should produce a unique template for each new face, and reliably generate a matching template whenever the same face is presented again. This means that storing templates and comparing each new registrant's template against the enrolled database ought to be equally good at detecting duplicates.

Recommendations

1. **Encourage the use of the Access Card for mutual authentication, to protect online users of DHS services against phishing, pharming, website spoofing and spam**. If it is desirable for a greater proportion of qualified health & welfare services to be provided over the Internet, them it is incumbent on government to protect their online channel. Conventional Two Factor Authentication has been comprehensively exposed as vulnerable. Smartcards however are widely acknowledged to represent the state of the art in mutual authentication, and the stated objectives of the Access Card could usefully be expanded in this regard.

2. **Ensure that the Access Card architecture will support the addition of extra identifiers by qualified third party services, especially in the health sector.** Lockstep appreciates that Access Card project managers will prefer not to expand

their scope beyond the immediate objectives of DHS. Yet we should weigh the community's strong interest in proper protection of their privacy and security as they deal increasingly with government online. If the Access Card is suitably specified in terms of cryptographic capacity and memory size, then there is not much more that the project would have to do to support third party identifiers. The project risk should be close to zero.

3. **Consider whether or not instances of multiple DHS agency identifiers could be best managed on the Access Card** (rather than at the SCRS as would otherwise seem to be the case).

4. **Include in the mix of anti-fraud measures the automatic detection of misuse by the smartcard itself**, so as to decentralise fraud control and reduce the aggregation of 'innocent' transaction data. Positive measures to combat provider fraud can be implemented using smartcards, which might also help redress the perception that smartcards tend to target citizen misbehaviour indiscriminately.

In conclusion, I hope this input is of value to the Taskforce. And I would be happy to discuss these matters further, if you have any questions.

Sincerely,

Stephen Wilson
Managing Director

By e-mail.

Sources and Further Reading

[1] "Smartcards and healthcare provider fraud" *Lockstep Babysteps* No. 6, 2006; available at www.lockstep.com.au/library/babysteps

[2] "Smartcards and Doctor Shopping" *Lockstep Babysteps* No. 7, 2006; available at www.lockstep.com.au/library/babysteps

[3] "Authentication in an Internet Banking Environment", Federal Financial Institutions Examination Council, 2005; http://www.ffiec.gov/press/pr101205.htm

[4] "The Failure of Two-Factor Authentication", Bruce Schneier, *Crypto-Gram*, March 2005; www.schneier.com/crypto-gram-0503.html#2

[5] "Electronic Authentication in the US Federal Government", Bill Burr, Manager Security Technology, NIST, 2005 http://asia-pkiforum.org/feb_tokyo/NIST_Burr.pdf

[6] "Health and Social Services Smart Card Initiative Volume 1: Business Case Public Extract", KPMG, 2006; http://www.humanservices.gov.au/modules/resources/access_card/kpmg_access_card_business_case.pdf

[7] "A novel application of PKI smartcards to anonymise Health Identifiers", Stephen Wilson , *AusCERT2005* Refereed R&D Stream, 2005; http://www.isi.qut.edu.au/events/conferences/auscert2005/proceedings/wilson05novel.pdf

[8] "A fresh look at smartcards" *Lockstep Babysteps* No. 2, 2006; available at www.lockstep.com.au/library/babysteps.