Lockstep Consulting
11 Minnesota Ave
Five Dock NSW 2046
Australia

15 March 2007

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 2

Lockstep is pleased to provide feedback on the management of voluntary medical and emergency information in the Access Card.

Executive summary

Lockstep agrees that there are medico-legal imperatives to safeguard the integrity and authority of medical information held in the Access Card for the express purpose of aiding third party emergency services. While there might appear to be contradictions in granting ownership of information to cardholders while restraining their ability to directly affect that information, we believe that trusted intermediaries can provide satisfactory resolution of many of these issues, as they have in other online service delivery sectors such as banking.

There is obviously a host of management, legal and public policy issues to work through, however Lockstep sees no technological problems in replicating electronically something very much like the Medic Alert system. In fact we propose in this submission a secure, light-touch digital certificate based approach which would simplify the process of loading trusted data, and enhance the privacy and integrity of the system. Using certificates, we can convey the “pedigree” of medical data created by authorised parties without creating an additional special area of the card, or using any special protocol per se for storing authorised data to the card. Instead, pedigree can be embedded in the way the data is packaged before it is stored, simplifying the layout of the chip, and also improving the trustworthiness of data when accessed in offline environments.

About the Lockstep Group

Lockstep Consulting Pty Ltd was established in early 2004 by Stephen Wilson, a leading international authority on identity management and information security. Lockstep Consulting provides independent analysis and advice on security policy and strategy, authentication and privacy. Sister company Lockstep Technologies is developing smartcard and Public Key Infrastructure (PKI) based solutions to enhance privacy and combat web fraud.

Recent Lockstep Consulting clients include the Office of the Privacy Commissioner, the Australian Government Information Management Office, the Australian Divisions of General Practice, and Medicare Australia. Stephen Wilson is active in several policy and advisory bodies including the ALRC Developing Technologies Sub-Committee, the Gatekeeper Policy Committee, and the Asia PKI Forum. He is co-chair of Smartcards and Information Security Australia, and chair-elect of the OASIS PKI Adoption Technical Committee. He was a founding member of the National Electronic Authentication Council 1999-2001, and he sat on the Federal Privacy Commissioner's PKI Reference Group in 2000.

Introduction

In this submission we describe a reasonably detailed vision of how the Access Card could be used to safely manage sensitive data such as – but not limited to – medical and emergency information, with particular reference to the medico-legal considerations of quality and reliability. To support this vision we will address and amplify some of the points in your Discussion Paper 2. By way of background, we will also review some of the pertinent properties of smartcard technology (which to date seem not to have been accounted for in the Access Card's designs) and draw on the Internet banking experience to inform the way personal data might best be managed by intermediaries. Finally we will provide specific comments on most of the Discussion Paper's recommendations.

Review: What do smartcard "resources" involve?

Lockstep has previously submitted to your Taskforce [1] as well as the Senate Finance and Public Administration Committee [2] that the privacy enhancing properties of smartcards seem yet to be fully realised in the plans and designs for the Access Card. When discussing what to do with the "customer controlled area of the card" we submit that it is vital that this resource be understood to be more than mere spare memory.

Unlike magnetic stripe cards (and indeed most other personal authentication technologies) a smartcard can tell what's going around it. It can check what type of terminal device is trying to communicate with it, and refuse to divulge data to any unauthorised systems. This makes well designed smartcards effectively immune to card skimming, and makes lost cards safe against prying or copying. More generally, it equips smartcards with a variety of sophisticated security and privacy safeguards. Smartcards can act as intelligent proxies for their owners, delivering such essential privacy benefits as:

- — decentralising customer reference numbers and identifiers, literally keeping them safe in peoples' wallets, away from databases and call-centres
- — running private off-line security checks inside the chip, to catch such fraud as prescription shopping, without having to aggregate and data-mine all innocent transactions
- — logging users onto secure websites, protecting them against hacker sites

— checking the veracity of e-mails, to protect consumers from phishing and spam (which arguably represent the most serious threats to privacy today).

Smartcards feature embedded microcomputers, incorporating a range of built-in functions and services. Therefore smartcard resources need to be understood to be more than storage space. The customer controlled "area" could include memory protection – so that users can elect who and what has permission to write to or read from their chip – and cryptographic functions to encrypt data, sign transactions and so on.

The pedigree of data held in the chip

We turn now to the issue of ensuring the integrity and accuracy of medical information held in the chip. We agree wholeheartedly with the Taskforce when it is noted on page 13 that "the medico-legal issues are such that there must be authentication and verification of data … This implies limits on the capacity of each cardholder to enter or alter the data in question. It suggests that data entry (and alteration) must be done by approved parties …".

We note that the Taskforce has begun consideration of the potential cost of the requisite administrative layers, the desire to minimise impact on the Office of the Access Card of supporting what would be non-core functions, and the possible involvement of medical practitioners. The Taskforce also appears to be taking a lead from the established Medic Alert system, which includes careful vetting of medical information, approval by medical practitioners, and fees for service. Lockstep agrees that the Medic Alert system is instructive. Lockstep in fact envisages a straightforward way of managing such a scheme electronically, echoing most of the attractive features of Medic Alert, with robust cryptographic mechanisms to embed the necessary data quality, verification and integrity controls into the Access Card. We will describe a model system later in this paper, for discussion purposes.

We can characterise the necessary features of card-based medical information storage thus:

— it must be clear that a qualified and authorised professional and/or entity has vouched for the information

— there must be protections against unauthorised loading, modification and tampering

— the date of creation must be shown

— the information together with its integrity and authenticity checks must be available directly from the smartcard, without going online to backend systems.[1]

In short, critical medical data held in the Access Card must have a self-evident *pedigree*. In the somewhat technical sidebar that follows, we explain how digital certificates issued to a cryptographic smartcard can convey pedigree of data, and prevent those data from being 'claimed' by anyone else, copied from one card to another, or simply made up.

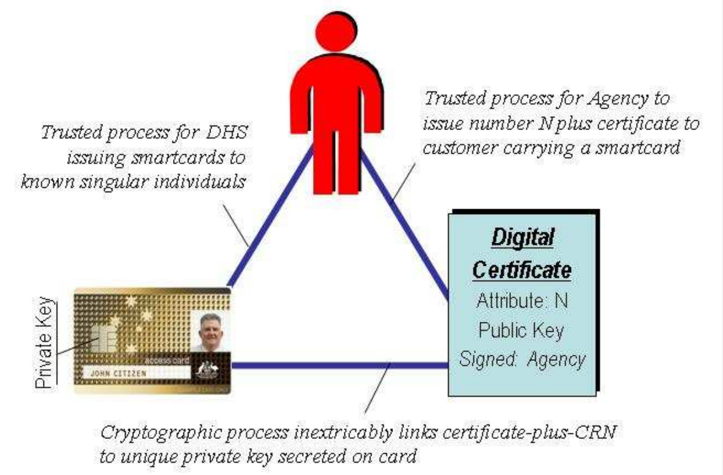
[1] Consider that if it were necessary to go online to check the validity of information in a smartcard, then we might as well refer to online systems for the definitive medical information itself, taking advantage of the superior storage capacity and ability to keep online information up-to-date.

Sidebar: Using digital certificates to convey pedigree

There are ways of issuing personal data to a smartcard that prevent those data from being 'claimed' by anyone else, copied from one card to another, or simply made up. One way to do so is to encapsulate a small amount of data in a digital certificate associated with a private cryptographic key held on the smartcard. Consider an individual named Smith to whom Agency A has issued a unique customer reference number N. If N is saved in ordinary memory in a smartcard or any other portable device, then it has no pedigree; once N is presented by the cardholder in a transaction, it looks like any other number. To better safeguard N in a smartcard, it can be encapsulated in a digital certificate, as follows:

1. generate a fresh private-public key pair in Smith's chip card
2. export the public key
3. create a digital certificate around the public key, with an attribute corresponding to N
4. have the certificate signed by (or on half of) agency A.

The result is a logical triangle that inextricably binds cardholder Smith to their agency number N and a specific Access Card. The certificate signed by A attests to Smith's ownership of both N and a particular key unique to Smith's smartcard. Keys generated inside a smartcard are retained internally, never divulged to outsiders. It is impossible to copy the key to another card, so the triangle cannot be cloned, reproduced or counterfeited.


Trusted process for DHS issuing smartcards to known singular individuals
Trusted process for Agency to issue number N plus certificate to customer carrying a smartcard
Digital Certificate
Attribute: N
Public Key
Signed: Agency
Private Key
JOHN CITIZEN
access card
Cryptographic process inextricably links certificate-plus-CRN to unique private key secreted on card

When Smith wants to present their number in an electronic transaction, instead of simply copying N out of memory (at which point it would lose its pedigree), Smith's software would digitally sign the transaction using the certificate containing N. With standard security software, any third party can then verify that the transaction originated from a genuine Access Card holding the unique key certified by A as matching the number N.

Note that N doesn't have to be a customer number; it could be any personal data, including a biometric template or a package of medical information. Note also that Lockstep Technologies has developed a variation on this method, marketed as "Stepwise", in which the digital certificate is itself anonymous, which thereby enables transactions created using the smartcard to be de-identified and yet retain the indelible linkage to the agency number. See www.lockstep.com.au/technologies.

The likely importance of intermediaries in administering medical information

We note and agree with the Taskforce's emphasis on the need to ensure the quality of medical information, and in particular the suggestion on page 13 that there be "limits on the capacity of each cardholder to enter or alter the data in question". This may strike some as contradicting the axiom that users will 'own' and 'control' anything stored in their own of the chip, but as we shall discuss in another sidebar below, we can take guidance from the field of Internet banking as to balancing ownership and quality control.

We take these considerations as implying that *intermediaries* should play a crucial role in managing consumer controlled Access Card resources and interfacing consumers to those resources. We would like to reinforce this argument by bringing to the Taskforce's attention some additional factors that would limit the utility of medical information held on the Access Card unless intermediate software and services come into play:

— It is not yet clear whether medical and emergency information would in the main be read by humans or by machines. We guess that in the early stages, humans like paramedics and ER personnel will be the most common users, but over time, with more sophisticated medical software systems, it seems likely that machines will read and process data from the chip.[2] To ensure machine readability, data on the chip would have to be specially formatted and prepared before loading.

— The use of a standardised medical vocabulary (e.g. SNOMED) for describing existing conditions, contraindications, prescriptions and so on is essential, especially in the case of machines reading the data. This means that data cannot be prepared using a conventional editor (such as Notepad or Word) but instead must be composed using special software with access to known good versions of the vocabulary.

— It might also be the case that interoperability with external health information systems dictates the use of standardised metadata and transport protocols (e.g. HL7).

— The smartcard's limited available memory must be managed carefully, so as not to be unexpectedly exhausted, especially by overloading with relatively unimportant data. Some ranking scheme will be needed to prioritise different types of medical information vying for inclusion in the chip. Such a ranking must obviously be determined by medical experts and would have to be enforced in a special purpose software interface through which all information would pass before being loaded.

[2] In principle machine readability could be especially useful if future Access Cards features a contactless interface, so that the presence of a card on a patient's person and the availability of medical information could all be determined automatically. Mutual authentication between the card and the peripheral would control the risk of unauthorised eavesdropping.

Sidebar: What can Internet banking tell us about consumer control of their card data?

It is axiomatic that the consumer will 'own' and 'control' any data they elect to have stored in their area of the Access Card. But on the face of it, there are tensions between such ownership and the evident need for some restriction on how the card is used, at least for crucial medical data. Further, because the available smartcard resource tends to be thought of as little more than memory with no obvious compelling application, the debate has been largely uninspiring. When I appeared before the Senate FPA Committee on March 2, I remarked:

It has to be said that our deliberations in this area are hampered somewhat by the public's fairly unsophisticated understanding of what [the individual's area] can do. It is all too easy to think about this as a "micro iPod", and people quite rightly say that is a silly approach, because we are all awash with USB sticks that have literally hundreds of thousands of times greater capacity. So, we have to think more precisely about what a handful of memory would do, and we need to think in terms of protecting access to it. That is, not just read access, but it is important that consumers can control who writes to that as well. You do not want have your memory soaked up by an application that thinks that it would be a good idea to put all of your bank account details in there or what have you. There have to be some technical gates that affect what gets written to it and [read] out. It has occurred to me recently that this is a little bit like internet banking insofar as our view of our money on the internet goes through a number of stages.

Internet banking involves a complicated chain of command and control – some technological, some regulatory, some contractual – whereby the contents of a bank account are rendered before one's eyes on a browser. The user experience is one of owning the money displayed on the screen (and of course that is the customer's legal position as well). Yet it is not really money that they have any direct control over – it is ones and zeros, manipulated with the help of a multitude of intermediaries, from the bank's mainframe with its probable old COBOL programs, through a web server, one or more ISPs, and the browser. Typically several of these intermediaries are outsourced. Almost all of the software involved is written by third parties; much of the software is general purpose and entirely unrelated to the field of banking. Yet there is a raft of controls, standards and legal mechanisms that protect consumers and serve to underpin the compelling illusion that they are in direct control of money over the Internet.

This experience might help us think more progressively and creatively about how Access Card holders may still own and control data that will almost certainly be loaded onto their card not by them directly but by intermediaries working on their behalf.

A model for managing medical and emergency information in the Access Card

Lockstep certainly supports the basic proposal that small packages of important medical information be held on the Access Card, at the consumer's discretion, for use in emergency and similar situations. For various reasons that seem to be widely endorsed, detailed medical records ought not to be held in smartcards. Instead the card should carry (1) small amounts of data that need to be accessible offline, and (2) secure keys for safely accessing more comprehensive records and generally more sophisticated systems online.

We have made the case above that digital certificates are an ideal means for encapsulating packages of personal data, including emergency medical data and identifiers, so as to convey their pedigree and integrity. Importantly, all the basic standards, building blocks and services needed to implement digital certificates in the Access Card have already been specified in the tender documents to date. We will now build on the certificate idea to show how medical information can be managed comprehensively, in ways that echo the trusted Medic Alert approach. We understand that the cornerstone of the Medic Alert is a form completed by the patient's doctor – who must be a registered medical professional – and signed by both the doctor and the patient.

In our suggested model, standard clinical software packages as commonly used in general practice would be enabled to interface with Access Cards, as well as Medicare Australia's HeSA[3] professional smartcards. A new screen would be added to the software for the task of creating what we will call here an "Emergency Health Record" (Record) and loading it to the Access Card, as follows:

1. The Record would comprise data of the type defined as "absolutely necessary", known by the doctor about their patient. The software screen would likely provide pull down menus of common options, such as allergies, to help construct the Record. Other data such as current medications might be imported automatically from the patient database. Once assembled, the doctor and the patient would together review the Record, discuss the implications of loading it to the Access Card, and reach an informed agreement.

2. After the contents of the Record have been accepted, the actual data that will comprise the Record as stored in the chip would be formatted by software, to comply where appropriate with accepted standards (such as SNOMED, HL7 etc. as agreed).

3. To securely bind the Record to the patient smartcard, the application would create a special digital certificate, where the Record is included as a custom attribute. The certificate would be generated thus:
   i. the application requests the Access Card to generate a fresh public-private key pair (an action which would likely require the patient to enter their PIN)
   ii. the public key is exported from the Access Card to the application
   iii. a certificate is generated, including the patient's public key and the Record data[4]
   iv. the certificate is signed by the doctor's HeSA private key or some other key[5]
   v. the certificate is loaded to the Access Card.

[3] Health eSignature Authority; see www.hesa.gov.au.

[4] The detailed design of this special certificate profile could include other administrative information, such as the issue date and a nominal expiry date (which could help relying parties judge the currency of the Record. A unique X.509 Policy Object Identifier would also "brand" the certificate indicating that it had been issued to an Access Card under the terms and conditions of the formalised "Emergency Health Record" scheme.

[5] Standard HeSA practitioner certificates are probably not configured to allow the signing of certificates, but straightforward modifications could be made to the HeSA smartcard to enable the emergency health record scheme as described. Alternatively, a new type of private key could be deployed on the doctor's smartcard, dedicated to the scheme and issued under what might well be largely commercial terms & conditions.

As a result, anyone retrieving such an Emergency Health Record from an Access Card can be assured that the Record:

— was created (and signed) by an authorised medical doctor

— was created with the cardholder's consent

— had been carried on a genuine Access Card

— cannot have been tampered with after being signed by the doctor

— has not been copied from another card, or otherwise made up.

The integrity and authenticity of emergency health information sealed within a digital certificate can be verified offline.[6] Note also that the use of digital certificates to encapsulate medical data and convey its pedigree removes the need to reserve particular areas of card memory with special write properties.

Feedback on the Taskforce's Recommendations

We will now provide feedback on the Taskforce's recommendations.

Regarding the Taskforce's Recommended Scheme

> *The customer controlled area of the access card should contain a two-tiered system of emergency and health information:*
>
> - *in the first tier, which should be accessible to anyone with an approved reader, there should be listed only that data which is absolutely necessary to facilitate the provision of emergency health treatment in a crisis situation;*
> - *in the second tier, which should be PIN protected (and thus accessible only with the express consent of the cardholder) other medical and health data could be listed*

— Lockstep remains undecided whether it is advisable to have sensitive medical information so freely viewable as is implied by the recommendation. We agree that a PIN override style mechanism is likely to be too complex, but there may be ways of using application-to-card mutual authentication to gate access to authorised users.

— We note that the Taskforce seems to presume some form of special authorisation when it refers to "approved" readers in this context. We agree with this general thrust. It may be that more work is needed to define how readers would be approved and controlled.

— We believe it may be useful to generalise these considerations beyond emergency medical information. There are probably many applications for the consumer controlled area where authorised service providers would use some of the memory, and where access by others is restricted somehow. Emergency medical data management is intuitively appealing, but many other uses could be just as meritorious. Examples

[6] It is unlikely that this type of certificate would ever be revoked and so we won't ever need to check a Certificate Revocation List or online certificate status.

include longitudinal electronic health records, health insurance, superannuation, state government services, and the host of paperwork addressed by the Commonwealth from time to time under the heading "GP red tape".

Regarding Recommendation 1

> *That the Taskforce's preferred two-tier model be considered as a standard should the inclusion of voluntary emergency and health information be available to the individual for inclusion on their access card chip.*

We feel we have to reserve judgement on the two-tiered model at this time. It may be useful to do further work on access control mechanisms, to explore whether top priority emergency information really needs to be effectively in the public domain. And it may be helpful to generalise the problem space beyond emergency medical information, to foster a consistent approach to all potentially sensitive applications for the cardholder controlled area.

Regarding Recommendation 2:

> *That consultations be undertaken with the relevant medical and emergency service authorities to draw up an agreed definition of what should be regarded as "absolutely necessary" medical data to be included in the first tier of the proposed model.*

Lockstep agrees that such consultations should occur.

However we suggest that technology consultations be undertaken in parallel with the same degree of urgency, to better define the mechanisms for access control, quality control, maintenance and so on required to safeguard the medical data and ensure its pedigree. The medical software industry at some level should be part of these deliberations if, as Lockstep suggests, doctors' software should be modified to mediate the creation and loading of voluntary data to the Access Card.

Regarding Recommendation 3:

> *That no voluntary medical information be entered into any part of the access card without verification of the accuracy of that information by an approved medical or other practitioner.*

Lockstep agrees entirely with this recommendation. We hope that the worked example provided above provides some useful leads as to the feasibility of implementing a practical scheme, in which individuals remain closely involved with how their Access Card is used, and yet cede the ability to directly manipulate the medical data as stored in the chip.

Regarding Recommendation 4:

> *That the medico-legal issues arising from persons acting in good faith on the medical data contained in an access card be addressed and clarified in future legislation related to the operation of the access card chip.*

Lockstep agrees entirely with this recommendation.

Regarding Recommendation 5:

> *The Australian Government, in its information campaign, restate its policy that the Access Card will not be used to store electronic health records or link to existing electronic health records.*

Lockstep disagrees strongly with this recommendation.

There are sound arguments in favour of smartcards for protecting health identifiers, and safeguarding access by consumers to their own electronic health records [1][4]. We agree by and large that medical records themselves ought not to be saved on smartcards, but we are strongly of the view that the safest way to access electronic health records is via identifiers held on smartcards. In fact we're disappointed that the previous Minister's call for the Access Card to act as "a set of keys that would open a number of doors to a range of government services" [5] was never taken up. We see the Access Card as a unique opportunity to put into the hands of every citizen the ideal means for safely accessing their own e-health resources and indeed all other government online services. While DHS has been understandably keen to rein in the scope of the project, there are potential advantages to the Access Card if it embraces carefully selected external applications, for improving the utility of the smartcard will enhance the community's acceptance of it and their take-up rate.

Crucially, the current separation of the Access Card and NEHTA's work on health identifiers is arbitrary. The Discussion Paper at page 9 states that "the Australian Government has *concluded* that the Access Card program is not related to work being undertaken by NEHTA as this would represent a significant departure from the stated purposes of the access card" (emphasis added). In fact, the previous Human Services Minister long emphasised the importance of the Access Card as infrastructure suitable for a wide range of applications[7] and so there is no *conclusion* as such for the government to draw that NEHTA's work is unrelated.

For their part, NEHTA has long maintained a technology neutral position in respect of health identifiers and this policy position has artificially distanced NEHTA from the Access Card. In a recently newspaper interview, NEHTA chief Ian Reinecke said in respect of storage media for identifiers that "We're not positing a token. The identifier could be attached to a range of things. … Oh, we'd be happy to use cards as tokens if that option were available but there are other tokens, such as USB devices, and other forms of authentication. We're agnostic on that" [6]. Yet there are signs that technology neutrality has reached its use-by date in e-health policy. In 2006 the Department of Health and Ageing, based on independent analysis and advice it commissioned, concluded that "Although [there is] a range of technologies that may be used for e-signatures, at the current point in time, PKI is the preferred e-signature solution for prescribing and dispensing" [8]. Already overseas health smartcards (in France and Germany) are being upgraded to be digital signature capable, in order to support electronic prescribing. Lockstep has elsewhere proposed a

[7] For example, Joe Hockey once said "The infrastructure we rollout is a railway line. It's a railway line that over many years is going to provide the opportunity for different types of rolling stock to go along and service consumers better" [7].

number of exciting new applications using embedded digital certificates in health smartcards, to dramatically enhance consumer privacy [9][10][11].

We would therefore urge the government, at the very least, to not shut the door on the Access Card being applied to a range of more general health related applications. We submit to the Taskforce that in contrast to Recommendation 5, government policy should allow for – and in our view actually encourage – the Access Card to be used to link to existing electronic health records (with robust technological, administrative and regulatory safeguards of course).

Regarding Recommendations 6, 7 & 8:

> *[Concerning consensual flagging of organ donor status, optional advanced directives and other non-commonwealth records, and engagement of the Office of the Privacy Commissioner.]*

Lockstep agrees with these recommendations.

Regarding Recommendation 9:

> *Once decisions about the inclusion of medical and health data have been made, the Australian Government must consider the question of whether such a scheme should be administered in the public sector or by some private sector operator chosen in an open tender process.*

Lockstep agrees with this recommendation.

We submit to the Taskforce that there may be special benefits in allowing the private sector to drive and operate certain health related services using the privacy and security resources that should be available in the consumer controlled area of the card. While consumer privacy must always be strenuously protected against the trespasses of unchecked commercial interests, there are clear advantages in fostering a degree of business involvement. This may include contestability, innovation, enhanced consumer choice, speed of deployment of new services, and revenue returns to government. We believe that the various elements described in this letter – light-touch digital certificates, carefully controlled intermediaries, and the suggested processes for managing critical information in the card – might be extended and combined to support a contestable but ordered marketplace of value-adding Access Card applications and services.

Sincerely,

Stephen Wilson
Managing Director

By e-mail.

Sources and Further Reading

[1] Lockstep Consulting Submission on Access Card Discussion Paper No. 1, 25 July 2006; www.accesscard.gov.au/discussion/1C6_lockstep.pdf

[2] Lockstep Consulting Submission to Senate FPA Committee Inquiry into Human Services (Enhanced Service Delivery) Bill 2007, 28 February 2007; www.aph.gov.au/senate/committee/fapa_ctte/access_card/submissions/sub45.pdf

[3] Proof Committee Hansard – Senate Standing Committee on Finance nnd Public Administration, 2 March 2007 Reference: Human Services (Enhanced Service Delivery) Bill 2007; www.aph.gov.au/hansard/senate/commttee/S10026.pdf

[4] Lockstep Consulting Submission to Senate Legal and Constitutional Committee Inquiry into the Privacy Act, 25 February 2005; www.aph.gov.au/senate/committee/legcon_ctte/privacy/submissions/sub11.pdf

[5] "Future Directions for the Access Card; Your Card – Your Security", Joe Hockey, Minister for Human Services, National Press Club Speech, Canberra, 8 November 2006; www.humanservices.gov.au/modules/resources/media_centre/2006/061108_address_to_the_national_press_club.pdf

[6] "Doing the numbers on e-health", Karen Dearne The Australian, 30 January 2007; australianit.news.com.au/articles/0,7204,21124569%5E24172%5E%5Enbv%5E24169,00.html

[7] Address to the Committee for the Economic Development of Australia, Joe Hockey, Minister for Human Services, Sydney, 24 July 2006; www.humanservices.gov.au/modules/resources/media_centre/2006/060724_address_to_committee_for_the_economic_development_of_australia.pdf

[8] "Electronic Signatures for Prescribing and Dispensing" SMS Management and Technology for the Department of Health and Ageing eHealth Branch, 15 June 2006; available at www.msia.com.au/esig_prescript_document.pdf

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

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

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