A novel application of PKI smartcards to anonymise Health Identifiers

AusCERT 2005 Asia Pacific Information Technology Security Conference, May 2005

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

Abstract

Default thinking about Electronic Health Records (EHRs) and Unique Health Identifiers (UHIDs) has settled on a national numbering scheme, despite the fact that patient privacy can be seriously jeopardised if identifiers ever become linked to individuals' names. A range of generic risk mitigation strategies is envisaged, including strict provider access controls, conservative patient consent provisions, and limiting the amount of personal details recorded for each patient event. Yet none of these measures do anything to control the underlying linkages of identifiers and names, and so a serious gap persists in EHR strategy and architecture. This paper presents a new way to fundamentally anonymise UHIDs through a novel use of public key certificates and smartcards. The design presented here secretes each UHID within an anonymous digital certificate, and links one or more certificates to a smartcard. If an EHR entry is digitally signed via such a certificate, then that entry is directly linked to the UHID, but cannot be linked to the individual's name without having access to the smartcard and the private key it contains. Unique benefits of this approach include strengthened consumer consent controls, efficient off-line identity resolution, reduced reliance on centralised, mission-critical identity servers, seamless support for multiple EHRs, and compatibility with a range of smartcard choices available to consumers in the near future.

1 Introduction and background

Health identifiers are listed by the Commonwealth Department of Health and Aging as amongst the seven most crucial building blocks of the emerging national e-health environment [BLOCKS03, p1]. The complete list (in the Department's own order) is privacy, security, standards activities, architecture, identifiers, provider directories, and change management. Privacy and security are properly given top billing, yet if identifiers are not implemented with care, privacy and security are doomed. Thus, identifiers arguably represent the most important technical issue of all.

Contemporary work on public policy and management of Unique Health Identifiers in Australia can be regarded as having begun in the late 1990s with the National Electronic Health Records Task Force. The task force was composed of noted experts from state and federal health, and worked through extensive public consultation, culminating in 2000 with its report *A Health Information Network for Australia* [NEHRT00]. This work laid the foundations for the project now known as Health*Connect* – "a national health information network supporting electronic health records" [HCBA04, p11].

Amongst many other things, the task force report started the process of outlining the technological and management options for a UHID suitable for controlling health records on a national scale. The report suggested that there were three broad alternatives:

1. options that do not require a universal identifier; e.g. Patient Master Indexes
2. biometric identification, and
3. identifier(s) based on the assignment of a number unique to each individual (which "could be an entirely new one or based on an existing one, such as the Medicare number") [NEHRT00H].

The task force anticipated that the third option would be the most practicable, for a number of non-controversial reasons which need not be reviewed again here. The same conclusion has been confirmed several times since, by the Health*Connect* project team and by independent consultancies, and is now an accepted part of the Health*Connect* Business Architecture. The new

National Electronic Health Transition Authority (NEHTA) has begun detailed work on a national health identifier of some sort [NEHTA05]. In the meantime, over the past four years or so, the Health*Connect* project has moved through requirements, business architecture and technical architecture phases. In 2004, the Commonwealth committed over $100M to the project.

The objectives and properties of a numerical UHID have come to be well understood in the health informatics community.[1] The American Society for Testing and Materials has developed detailed guidelines. A UHID it states must fulfil four main functions:

> "(a) Positive identification of patients when clinical care is rendered, (b) Automated linkage of various computer-based records on the same patient for the creation of lifelong electronic health care files, (c) Provision of a mechanism to support data security for the protection of privileged clinical information … and (d) Use of technology for patient records handling to keep health care operating costs at a minimum" [ASTM03].

The guide lays out 30 detailed criteria to satisfy these functions. In the current context of Health*Connect*, most noteworthy of the ATSM's criteria are the following four:

- *Controllable*: only trusted authorities have access to linkages between encrypted and non-encrypted identifiers
- *Disidentifiable*: possible to create encrypted identifiers with same properties
- *Mappable*: able to create bidirectional linkages between new and existing ids
- *Secure*: can encrypt and decrypt securely.

Note that the issue of encryption of identifiers is revisited below.

[1] See for instance the seminal work of the US Department of Health and Human Services *Unique Health Identifier for Individuals* [HHSUHI98] and the up-to-the-minute treatment of privacy in *Curing the Unique Health Identifier: A Reconciliation of New Technology and Privacy Rights* [Netter03].

2 Controlling the linkage of identifier and individual's name

It is clearly important that the linkage between an individual's identity and their identifier(s) be tightly controlled. The linkage must be reliable and 'seamless' in routine clinical usage, yet difficult to establish in all other settings. If unauthorised parties are able to establish the linkage, then large portions (if not the entirety) of a person's EHR may be exposed. Notwithstanding the fact that role-based access controls and other restrictions will apply to them, health record systems will be connected to hundreds of thousands of healthcare workers over periods of many decades, and so from first principles, the risk of unauthorised access must be counted as critical. A sound, multi-layered approach to EHR security demands that *fundamental* restrictions be put on the ability to make linkages, and that consumers be given as much direct control over such linkages as possible.

Australia's National Health Information Management Group (NHIMG) has released a discussion paper on health identifiers. It recommends that agencies managing health information which includes identifiers need to "adopt business rules and technical barriers that restrict the capacity of users to match the UPI to the individual's name." [NHIMG02, p6]. The NHIMG discussion paper mentioned encryption in passing as an example of a technical barrier; no other examples or practical guidance were offered at the time.

Encryption has come to be regarded as the standard means to make it difficult to reconstruct the linkages between a number and the person; as noted above, the ASTM Guide simply takes encryption as a given in UHID security. Yet precious little guidance has yet to be developed on exactly how encryption would be applied. Moreover, in and of itself, encryption is not even a necessary condition let alone a sufficient one, to restrict the linking of an identifier to an individual's name. And beyond encryption, it is difficult to find any other security options. For instance, the Commonwealth's recently released National Health Privacy Code – which one would expect represents the state of the art – only outlines some general business rules, and has nothing at all to say about what could constitute potential *technical* barriers as recommended by [NHIMG02].

A crucial strategic question arises: Why has so little progress been made on robust technical barriers that would genuinely restrict the ability to make linkages between UHIDs and the individuals concerned? Uncertainties on three fronts seem to have conspired to inhibit development of technological solutions to the UHID problem. Firstly, the predominant policy principle of Technology Neutrality has tended to delay the tackling of specific questions about UHID implementations. Secondly, most literature confuses and blurs two logically quite separate roles of the UHID, possibly misleading non-technical policy analysts about the finer points of how identifiers work. And thirdly, while most analysts have anticipated that public key technologies will generally be useful in EHR, PKI at large has been slow to progress, and has yet to contribute much to UHID development. It is instructive to examine these three areas of concern, in order to understand how to break though all of them.

2.1 The need to get technology specific

Most UHID analysis self-consciously avoids getting specific about how the identifier might be conveyed. Technology neutrality is the proper mindset to adopt when framing new e-business regulations; it helps to future proof the law, and to make it more robust in the face of unanticipated combinations of technologies. Subtly different is the effort to remain technologically *generic*, in order to avoid vendor lock-in, and to keep faith with the majority of users by offering them as many options as possible (the classic example being to support both Windows and MacOS/Unix). However, a doctrinaire application of technology neutrality can mean that special powers of new and improved technologies get overlooked, with the result that important but subtle compromises can become entrenched in the architecture.

In EHR literature and standards to date, it is almost universally assumed that UHIDs are simply going to be numbers. As such, little work has been done on standards for UHIDs themselves; after all, what need would there be to standardise a *number*? Detailed design work on UHIDs generally seems to be pushed out of the centralised strategy and standardisation initiatives of EHR, and left for downstream implementation efforts. Such detailed work appears not to be regarded as difficult or even terribly serious. Thus the authoritative HL7 says, rather awkwardly, that "it is desirable to have a 'Unique Identifier' (namely, a unique number) standard for EHR and other purposes, but a 'Unique Identifier standard' is not essential for unique identification" [HL7EHR04, p12].

Closer to home, the recent Health*Connect* Business Architecture carefully stops short of specifying exactly how identifiers should be managed, ostensibly in order not to limit the project's options too soon, nor to restrict consumer choice. The Business Architecture foreshadows qualified and non-exclusive use of smartcards for conveying UHIDs, but at this none-too-early stage it seems to not regard the smartcard as anything more than a passive memory device, to merely 'store' or 'hold' identifiers ([HCBAreqt04], p15).

Technology neutrality is an important ideal. The HealthConnect architects may well be correct to assume that consumers will find username and password easier to use than more sophisticated authentication mechanisms. And yet the fact is that amongst all authentication options available today, cryptographic smartcards have unique properties and capabilities. The head of Computer Security Technology at the National Institute of Standards and Technology, Bill Burr, recently asserted that, to resist Man In The Middle attacks and account hijacking, the "only practical solution today" uses smartcards or USB keys with public key infrastructure [Burr05].

To make best use of smartcards, we have to move past technology neutral treatments of UHIDs as abstract numbers that might be stored in a variety of ways. This paper articulates a specific way to bind UHIDs to smartcards via anonymous public key certificates. The time has come to be *technology specific* about how UHIDs are held by smartcards, in order that compromises to privacy and security are not cemented into less sophisticated UHID designs.

2.2 Blurring the different roles of a UHID

In Health*Connect*, the one UHID is envisaged to fulfill two logically quite different functions. The latest Business Architecture proposes that the one identifier be used both as an index to key Health*Connect* information such as event summaries, and as a proxy for the user name, akin to an account number, when a consumer

logs on to access their records over the Internet [HCBA04, p63].[2]

Clearly, if a single index is used to key all Health*Connect* contents, and if that index comes to be linked to an individual's name, then one's entire history might subsequently become identifiable. From first principles, a sound technical barrier to mitigate against such linkages being made would be to use *different* mechanisms for logging consumers onto the system and for indexing their records;[3] this point will be expanded on below, in considering the threat of phishing for consumers' Health*Connect* identifying information.

2.3 Practical application of public key technology to EHR privacy and security

For a long time, it has been widely expected that public key technology will be somehow core to EHR security and consumer privacy, yet concrete proposals have proven elusive. The original Health Online report was thick with generic references to – and primers on – Public Key Infrastructure, stating for instance that "it is intended to use public key technology and electronic digital signatures to maintain a highly secure environment for the entire system." [NEHRT00, p29]. In parallel, much academic research has been done on special variants of PKI and key splitting approaches [Chur02], and on privacy enhancing protocols [Bran00]. Yet all proposals to date have been complex. None have yet been standardised, much less realised in off-the-shelf components available to the implementers of EHR systems.

The general stasis in PKI is well known. PKI has been beset by a lack of "killer applications", excessive cost structures [OASIS04], spirited attacks by critics with various agendas [Elli00], and a failure of the imagination on the part of its battle-weary advocates [Wils03]. Against this backdrop, a novel approach to public key certificates, where no personally identifying information is included in the X.509 profile, represents something of a breakthrough.

3 A novel *Anonymous Index Certificate*

What follows is a detailed proposal for how public key certificates and smartcards can be used for holding health identifiers in a secure and private manner. This design appears to be the first to show with precision how to make good use of modern smartcards' public key cryptographic capabilities.[4]

In the current design, each consumer carries a smartcard with the ability to store and operate at least one signature asymmetric key pair. A key pair is generated (ideally on the smartcard), and an anonymous public key certificate created with a special extension populated with a copy of the consumer's UHID. The certificate contains no other information to identify its 'owner'; in particular, there is no name, pseudonym or demographic data. If the consumer has more than one identifier for different EHR datasets, then additional certificates are created, which typically would be tied to the one smartcard.

Under these circumstances, the UHID can be freely used by third parties to access non-identified data from the EHR. There is no direct way to establish the linkage between the UHID and the individual without having access to the smartcard and the private key stored in it.[5] De-

[2] Interestingly, the highly regarded American Society for Testing and Materials' UHID Guide is not exactly clear on the special function of user logon, and in any case, seems to allow for a similar doubling up of functions as we see in Health*Connect*. Recall that the ATSM Guide lists four functions, amongst which are "automated linkage of various computer-based records on the same patient" (i.e. the index) and "provision of a mechanism to support data security" [ASTM03]. The latter might be interpreted to mean a logon.

[3] Better still, diverse identification numbers could be maintained for different sub-sections of Health*Connect*; in particular, it would be good for security and privacy if data moved to HealthConnect from regional or local EHRs retained their original patient master indexes where applicable, without being re-keyed on a single national identifier.

[4] The current proposal differs from other anonymous digital certificate schemes such as that of Zhang and Critchlow [Crit04]. The latter describes a protocol whereby holders of trusted identity certificates can use them to boot-strap secondary anonymous certificates to be used in mobile commerce. In contrast, the current scheme does not concern equipping individuals to assert themselves anonymously in general commerce; rather it aims to allow individuals to be anonymously bound to one or more identifiers used in very specific record systems.

[5] The proposed scheme will work best in a "green field" EHR where new UHIDs are being assigned to

identification processes usually sacrifice precision by relying on aggregation, but in the proposed scheme, fine grained data, even isolated event summaries, can be safely retrieved without the risk of being linked to the individual.

When health event summaries are generated and entered into the EHR, they are digitally signed using the private key from the consumer's smartcard. Event summaries can include the UHID for indexing purposes *but need not include any other identifying information at all.* The digital signature binds the UHID to the rest of the event summary data, and to the Anonymous Index Certificate, which in turn is bound to the private key held on the individual's smartcard (see Figure 1). Therefore, there is a near-absolute[6] assurance that the event summary relates to a certain individual, but the identity of that individual cannot be linked without their smartcard. As Figure 1 shows, health information can be accessed in an non-identified form by legitimate third parties (like researchers, policy analysts and administrators), while the same data can be accessed in its identified form by clinicians who have access to the individual and their smartcard.

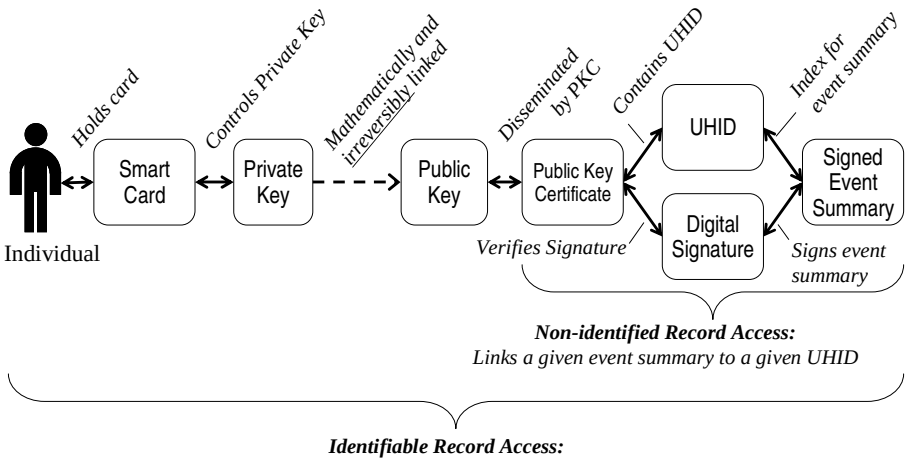

Figure 1: ***Schematic linkages between elements of the Anonymous Index scheme***

3.1 On the Anonymous UHID Certificate profile

On the face of it, the X.509 V3 profile of the Anonymous Index Certificate is not at all unusual. A custom extension may be used to hold the copy of the UHID. The *Issuer Distinguished Name* can be indicative of the EHR scheme, especially in those cases where the scheme in-sources the CA function. The Policy OID should unambiguously identify the particular EHR scheme to which the Anonymous Index Certificate relates.

In one variation of the design, the contents of the *Subject Distinguished Name* and *Subject Common Name* fields are set to some value that is the same for all subjects in this scheme. I would caution that while this appears not to technically breach any of the X.509 standards (e.g. [RFC2459]), it does deviate from the orthodox interpretation of X.509 certificates as binding a public key to a *unique* DN. It is conceivable that this departure might create conflicts of some sort in real-world X.509 software implementations. An alternate design has the UHID inserted into the *Subject Distinguished Name* field. More work is needed in this area, including a more exhaustive search of the standards, and interoperability testing.

It is worth highlighting my philosophical position on this point, which is that the meaning of a public key certificate can be powerfully abstracted more broadly than representing conventional "identity". If it turns out that having non-unique (and indeed trivial) *Subject Distinguished Names* does in fact break some aspect of X.509, then perhaps a fresh recommendation should be put to the IETF (see *Other research directions* below). It is beyond the scope of the current paper to debate this point

all individuals. In legacy EHRs, where identifiers have been circulating 'in the wild', it is possible that sufficient information has already been released from the system for linkages between UHIDs and individuals' names to be made.

[6] To the level of confidence provided by public key cryptography.

further, but I would suggest that this position is in part what makes the Anonymous Index Certificate novel.

3.2 The Anonymous Index Certificate in action

As described, the Anonymous Index Certificate is a standard X.509 public key certificate; together with the associated private key, it can be readily processed by any PKI-ready application software via standard APIs. The basic operation of the certificate is as follows. During each clinical encounter, the individual's UHID is retrieved by application software from the smartcard; where more than one UHID is present on the smartcard, software can select the appropriate certificate by examining, for example, the *Issuer Distinguished Name* or the Policy OID. Subsequently, central EHR data may be retrieved by keying on the UHID. When the clinician chooses to create an event summary and lodge it with the EHR, software invokes standard digital signature functions within the smartcard.

From the point of view of those accessing a central EHR, the scheme sets up two different domains. The first domain is for those concerned with the clinical care of the card holder; here, EHR data is identifiable. The second domain is for authorized third parties with legitimate interests in non-identified EHR data. See Figure 2, which for illustrative purposes only draws on elements of the Health*Connect* Technical Architecture [HCSA03] such as "*Health Record System*" (*HRS*) and *Event Summary*. Figure 2 also illustrates interoperation with multiple EHR systems.

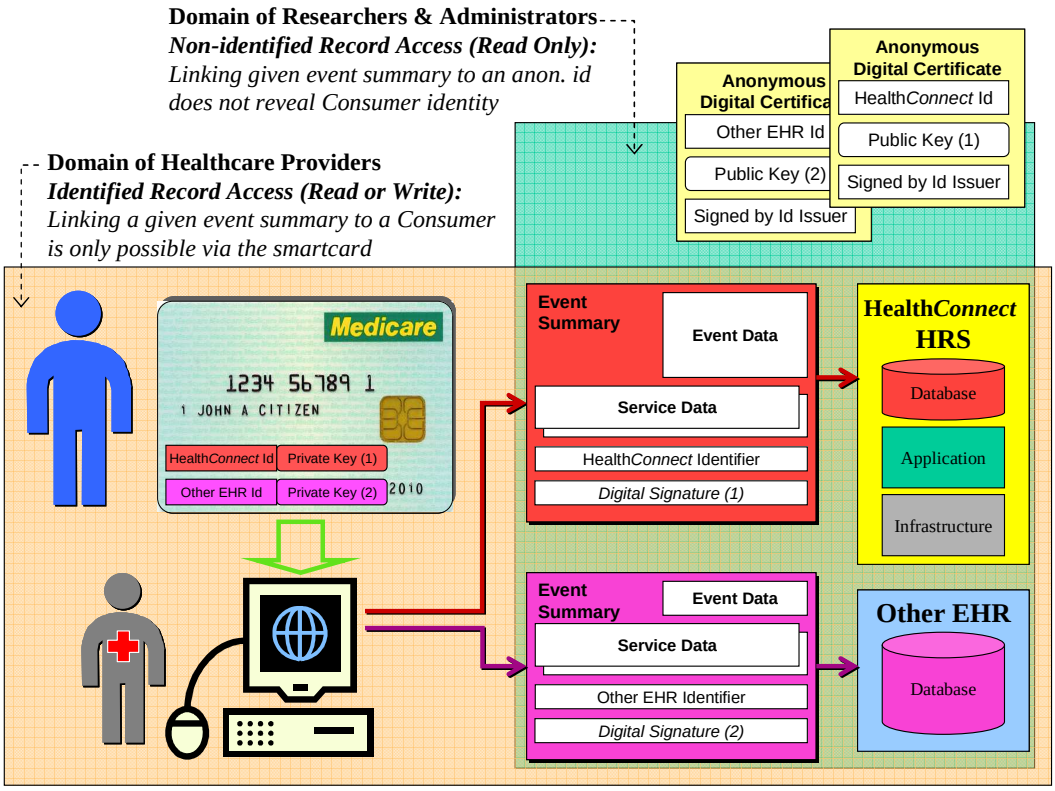

Figure 2: ***Anonymous Index Certificates in action with multiple EHRs***

A range of flexible smartcard lifecycle and work flow options are available, including:

- Anonymous Index Certificates could be pre-loaded onto Medicare smartcards at personalisation time (for opt-in EHRs, the private key and certificate would not be activated until the card holder gives consent)
- Anonymous Index Certificates could be loaded individually onto Medicare smartcards any time later, using a kiosk at a doctor's office or at some other EHR access location (equally, given proper physical security measures such as a secure smartcard reader, a doctor's regular workstation could run RA software to support the loading of certificates onto patients' smartcards)
- Similarly, additional EHR system identifiers could be loaded onto a person's Medicare card at any time
- Anonymous Index Certificates could just as well be loaded onto other types of compatible smartcards, such as the planned New Queensland Driver License, or the EMV credit/debit smartcards soon to be rolled out by financial institutions.

4 Benefits of the Anonymous Index Certificate

The design described has the following benefits in electronic health records:

- Enables secure, anonymous health records, with high levels of trust and safety
- enables secure, seamless, de-identified linkages across multiple EHR systems
- provides consumers with clear and tangible consent mechanisms, and explicit control over linkages between disparate EHRs
- defines a clear information system boundary across which no personal identity information is transmitted
- simplifies de-identification of research or administrative data because event summaries are not identified in the first place
- greatly enhances the security, privacy and trustworthiness of new smartcards which can otherwise be controversial when applied to EHR, making it more attractive for consumers to opt-in to EHR systems
- greatly reduces the exposure of identity linkages by obviating the need for a central directory in routine clinical encounters
- moves the task of identity resolution across multiple EHRs offline onto the card
- allows ready detection of multiple registrations or repeat enrolments
- standards based, with low incremental cost over and above the smartcard itself.

4.1 On the importance of separating consumer logon and EHR index

While usability and accessibility issues undoubtedly remain, I would argue that smartcard technologies should be more seriously considered for securing consumer access to EHRs over the Internet. As discussed above, re-using the UHID for consumer logon represents from first principles a significant security compromise. To provide a concrete example, phishing for EHR details may become a problem once large numbers of consumers have Internet access to their records. It is likely that unscrupulous healthcare entrepreneurs, as well as outright criminals, will seek to lure consumers into divulging their identifiers, under false pretexts such as the promise of free health assessments if their UHID is handed over.

Two factor authentication is the norm for access control in cases of information deemed to be of high risk or high value. However, most EHR planners to date have felt the need to offer consumers the option of simple username and password access; see e.g. [HCBA04, p62]. This is understandable naturally, since user convenience is perhaps the major determinant of the success of any complex new IT system, and smartcard readers have yet to penetrate into domestic computing to any appreciable degree.[7]

[7] Penetration is rather different in Taiwan. There, all bank cards have been switched to chip technology, all citizens have a national health smartcard, and 800,000 people have availed themselves of a government-issued "Citizen Digital Certificate" IC card. The Taiwanese government sells smartcard readers over the Internet for about US$15 each; see http://reader.buyloud.net/ShopStyle/card/default.asp.

Internet banking has similarly been wedded to simple password security; until very recently, user convenience was considered more important than improving perceived security. This is all about to change, driven by the acknowledged threats of phishing and identity theft. The Australian Prudential Regulation Authority responded in mid 2004 to the escalating levels of identity fraud by urging stronger Internet authentication.[8] More recently, the Australian Bankers Association foreshadowed the introduction of a standard approach to two factor security before the end of this year [SMHABA05]. In 12 months or so, it is probable that all major financial institutions in Australia will offer at least the option of two factor authentication for Internet banking. It would be unfortunate for public policy in EHR security to lag behind the banking sector. The public would probably expect EHR custodians to take at least as much care with their electronic health records as do the banks with their money.

5 Conclusions

5.1 Comprehensive privacy protections in EHR

It is important to emphasise that the use of anonymity solutions to protect UHIDs 'in the wild' is only one part of a successful privacy strategy. As mentioned previously, the NHIMG recommends the adoption of both business rules and technical barriers to help prevent unauthorised linkages from being made [NHIMG02, p6]. It is well known of course that the identity of individuals in an EHR may be reconstructed from other data, especially where the overall data set is small and the individual concerned is somehow unusual [VicDHS]. The main benefit of using anonymous digital certificates to convey UHIDs is to make it safer for UHIDs to be used by third parties without violating patient privacy, but it is no guarantee that linkages cannot be made by other means. Nor can anonymous UHIDs prevent linkages being inadvertently revealed through lax EHR business rules or system design.

5.2 e-Voting and other applications

The Anonymous Index Certificate should lend itself to other applications, especially once general purpose smartcards become widespread amongst the public. For e-voting, a single use Anonymous Index Certificate could be issued to all participating individuals, and loaded onto their smartcard via a kiosk or through a web portal. In this case, the anonymous identifier would likely be a serial number used to prevent repeat ballots being cast. On polling day, each electronic ballot would be digitally signed using the smartcard. This approach would ensure integrity of the individual ballots, complete anonymity, and yet easy auditability. Online census forms could be secured similarly, by another single use anonymous certificate.

Electronic passports too might find a use for this approach. Special purpose identifiers could be assigned to individuals, with the true linkages being recorded on a highly secure restricted database. These identifiers could be then bound into anonymous certificates, and loaded onto e-passports to help monitor passenger movements. Only once a suspicious pattern was detected would it be necessary to reverse the relevant identity from the restricted database. It would not be necessary for identity linkages on the vast majority of innocent travelers to be made across all information systems. A balance might thus be struck between privacy and the modern need for international law enforcement to monitor fine grain travel patterns.

5.3 Other research directions

In addition to exploring new applications as mentioned above, further technical R&D would be worthwhile around the possibility that the Anonymous Index Certificate is 'pushing the envelope' of orthodox X.509 "identity" certificates. If the approach of populating certificates with a constant *Subject Distinguished Name* does turn out to conflict with X.509 norms, then there may be cause to propose a new work item to the IETF to enable this novel usage. Further, as mentioned in the notes on certificate profile above, interoperability testing is almost certainly needed given the possibility of a clash with existing software implementations, regardless of technical standards compliance.

[8] "APRA strongly recommends that all [institutions] offering services over the Internet … implement strong authentication and control mechanisms to provide reliable safeguards against identity theft" [APRA04]. APRA does not take a firm position on two factor authentication specifically, but tellingly, in the same document it chooses to highlight that "a number of banks have recently announced their intention to introduce two-factor authentication as a means of overcoming some of the recent threats".

6 References

[APRA04] *Emerging Threats To Internet Banking* (Memo to all APRA regulated Authorised Deposit-Taking Institutions) Australian Prudential Regulation Authority 26 August 2004; http://www.apra.gov.au/ADI/loader.cfm?url=/commonspot/security/ getfile.cfm&PageID=7589.

[ASTM03] *Standard Guide for Properties of a Universal Healthcare Identifier (UHID)* American Society for Testing and Materials, ATSM E1714, 2003.

[Blocks03] *Progress Report: E-health building blocks* Commonwealth Department of Health and Aging, April 2003; http://www.healthconnect.gov.au/pdf/v2-8.pdf.

[Bran00] *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy* Stefan Brands, MIT Press, 2000.

[Burr05] *Electronic Authentication in the U.S. Federal Government* Bill Burr, National Institute of Standards and Technology, Asia PKI Forum Conference, Tokyo, February 2005; available at http://asia-pkiforum.org/feb_tokyo/NIST_Burr.pdf.

[Chur02] *The use of probabilistic record linkage, public key cryptography and trusted third parties to improve the protection of personal privacy and confidentiality in disease registers and tissue banks* Tim Churches, in Proceedings of the Symposium on Health Data Linkage, published by the Commonwealth Department of Health and Ageing, 2003.

[Crit04] *Security enhanced accountable anonymous PKI certificates for mobile e-commerce* Critchlow & Zhang, Computer Networks 45, pp 483–503, 2004.

[Elli00] *Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure* Carl Ellison and Bruce Schneier, Computer Security Journal, v 16, n 1, 2000, pp. 1-7; available at http://www.schneier.com/paper-pki.pdf.

[HCBA04] *HealthConnect Business Architecture V 1.9* Commonwealth Department of Health and Aging, November 2004 http://www.healthconnect.gov.au/pdf/BArc1-9.pdf.

[HCBAreqt04] *HealthConnect Business Architecture Version 1.9 Specification of HealthConnect Business Requirements* Commonwealth Department of Health and Aging, November 2004 http://www.healthconnect.gov.au/pdf/BAV1-9g%20Attach.pdf.

[HCSA03] *HealthConnect Systems Architecture V 0.9* Commonwealth Department of Health and Aging, July 2003; available at http://www.healthconnect.gov.au/archive.htm.

[HHSUPI98] *Unique Health Identifier for Individuals: A White Paper* US Department of Health and Human Services, July 1998; http://ncvhs.hhs.gov/noiwp1.htm.

[HL7EHR04] *HL7 EHR System Functional Model: A White Paper* Health Level Seven Inc., 2004; available from http://www.hl7.org/ehr/downloads/index.asp.

[NEHRT00] *A Health Information Network for Australia*, Report to Health Ministers by the National Electronic Health Records Taskforce, July 2000; http://www.healthconnect.gov.au/pdf/ehr_rep.pdf.

[NEHRT00H] *Health Identifiers: Options In An Electronic World* Appendix H of the Report to Health Ministers by the National Electronic Health Records Taskforce, July 2000; http://www.healthconnect.gov.au/pdf/ehr_rep.pdf.

[NEHTA05] National E-Health Transition Authority Work Program (accessed January 2005 at http://www.ahic.org.au/nehta/index.html#wp).

[Netter03] *Curing the Unique Health Identifier: A Reconciliation of New Technology and Privacy Rights* Wendy Netter, American Bar Association Jurimetrics, Volume 43 pp 165-186, 2000.

[NHIMG02] *Issues for the use of unique patient identifiers in statistical collections* National Health Information Management Group, October 2002; http://www.aihw.gov.au/publications/hwi/iuupisc02/iuupisc02.pdf.

[NHPC03] *Proposed National Health Privacy Code* The National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, August 2003; http://www7.health.gov.au/pubs/pdf/code.pdf.

[OASIS04] *PKI Action Plan* OASIS Public Key Infrastructure Technical Committee, February 2004; http://www.oasis-open.org/committees/pki/pkiactionplan.pdf.

[RFC2459] *Internet X.509 Public Key Infrastructure Certificate and CRL Profile* IETF Request For Comment RFC 2459, Housely, Ford, Polk & Solo, January 1999; ftp://ftp.rfc-editor.org/in-notes/rfc2459.txt.

[SMHABA05] *Online bankers face double layer of security* Sydney Morning Herald, 9 March 2005.

[VicDHS] *De-identifying Information* Victorian Department of Human Services; http://www.dhs.vic.gov.au/privacy/downloads/pdfdocs/deidentifying_info.pdf.

[Wils03] *PKI without tears* Stephen Wilson Voice & Data Magazine, November 2003; available at http://www.voiceanddata.com.au/vd/newsletter/nov_2003/default.asp.

