PKI Adoption Case Study (for the OASIS PKIA TC)

Digital certificates for Australian doctors

PKI Project Title	Healthcare Provider Certificates
Organisation concerned	Health eSignature Authority
Timeframe of implementation	2000-2006
Date went live	2002
Case study author	Stephen Wilson
Contact details	swilson@lockstep.com.au

1. Business background

Please describe the organisation, its business or function, and the broad nature of its transactions and/or online services (one or two paragraphs)

Health eSignature Authority is a specially constituted subsidiary business unit of the Australian federal public health insurer "Medicare Australia" (MCA). MCA is responsible for remunerating primary care providers (typically, family physicians) and most pharmacists under various public health funding programs. Some $20B is disbursed annually.

Increasingly, primary care providers deal with federal government electronically. While funds transfer of insurance payments to doctors is done using conventional (non PKI) banking systems, various statutory reports and claims are submitted with digital signatures (although in the technology-neutral Australian environment there is rarely any mandate for digital signatures to be used). In Australia, a number of localised communications solutions and services have arisen to support secure messaging between medicos. Once a national PKI for doctors reaches critical mass, it is expected that it will be taken up across the board for secure messaging in general.

The uptake of PKI may be about to accelerate in the Australian health sector because, in contrast to previous applications, particular transactions that form part of the latest e-health push are not thought to be possible without PKI and digital signatures. Examples include Shared Electronic Health Record (SEHR) entries and e-prescriptions. The Australian federal Department of Health has had independent security policy advice recommending digital certificates on smartcards for authenticating online prescriptions.

At present perhaps 5-10% of doctors have certificates; "location" certificates are used for business-to-government transactions by 30 or 40% of primary care clinics (TBC).

2. Objectives for the PKI Project

In the context of the business background, please describe the organisation's objectives in implementing PKI. Was the organisation seeking any or all of: better efficiencies, better security, better compliance? Include a description of the target users and their environment (five to ten bullet points).

- Better efficiency by transforming huge volumes of transaction from paper to online
- Long term, fundamental improvements to the availability and timeliness of healthcare information
- Bigger context of e-health is understood to have potential of reducing overall public expenditure on health system by 10% p.a. (representing approx 1% of GDP)
- To enable e-health, it is necessary to convey in the most trustworthy means the professional qualifications and standing of medical providers transacting online

3. System notes

Please summarise relevant technical aspects of the systems and the PKI implementation, such as operating systems, client and server platforms, whether certificate production was insourced or outsourced, the types of key media and so on; ideally, please name the PKI vendors, though we appreciate that this is not always possible (five to ten bullet points).

- Very wide variety of desktop environments;
- Most e-health software solutions are fat client, special purpose applications
- All healthcare provider certificates are on personal hardware tokens (mostly USB crypto-keys; some smartcards)
- PKI is co-sourced: Medicare Australia has end-to-end PKI systems, policies, procedures, all accredited by federal government PKI regulator (Gatekeeper). Baltimore Technologies CA server is hosted by a specialist PKI services provider (Cybertrust).
- Medicare Australia maintains a range of APIs, toolkits etc. licensed to legitimate users and medical software developers at no cost.

Please describe the application that was PKI-enabled, who was responsible for any modifications, including the relative efforts that went into developing new code versus off-the-shelf procurement (one paragraph).

Most applications to date are bespoke government transaction systems, essentially 100% in-house, custom built. Client side gradually migrating from special downloads to integrated functions built into third party medical software products.

4. Business impacts

Describe the impacts the PKI project had on the organisation, both positive and negative; where possible try to quantify the benefits; try to distinguish between immediate impacts and "strategic", long term and/or indirect impacts (two or three paragraphs).

There would be little dispute from any quarter that the Australian federal government PKI for the health sector has yet to make any real impact. Take up in the health sector

has been inhibited by multiple factors, especially the relatively high impost involved in obtaining certificates (including passport-level proof of identity checking) and an absence of compelling applications with which to use the system's certificates.

Business impact is set to improve however with major initiatives with respect to both of the foregoing problems. New registration modes have been developed (and endorsed by the Government's PKI policy office) where existing holders of official medical credentials may be automatically registered for and provided with digital certificates, dramatically streamlining deployment. Further, a new wave of modern e-health applications is upon us, connecting multiple parties in legally complex risky transactions such as e-prescriptions and shared electronic health records. These sorts of applications create far stronger demand for robust digital certificates than foregoing relatively simple applications such as online lodgement of B2G (doctor-to-government) Medicare claims.

5. Next steps and suggested improvements

What if any are the organisation's next steps in PKI? What would you do differently if you were starting all over again? What suggestions would you offer to others implementing PKI? (one or two paragraphs)

- Foster better integration of PKI primitives into commercial software
- Better awareness needed of practical implementation issues
- Better awareness needed of how to embed dig sig into user interfaces
- Certificate renewal needs to be better automated.

6. Your suggestions to the PKI industry

Based on your experience, what would you like to see done in the PKI industry to facilitate adoption? (three to eight bullet points).

- Have CAs work more closely with application developers and vendors to bring out the full value of certificates
- Work collaboratively on nuts & bolts issues like automatic certificate renewal, and better distribution of root keys
- Better choice of applications in which to integrate digital signatures, so that there are fewer disappointments to do with over engineering, or excess complexity.