Smartcards and PKI at Medicare Australia

AEEMA ICT Forums luncheon
14 February 2006, Sydney

John Brewer, Health eSignature Authority
Stephen Wilson, Lockstep Consulting

LOCKSTEP

Australian Government
Medicare Australia
Health eSignature Authority

Important Disclaimer

HeSA (now Medicare Australia) is not responsible for the Gatekeeper accreditation program. The Department of Finance and Administration (Finance), as the Commonwealth agency responsible for the Gatekeeper accreditation program, accepts no responsibility for any of the material contained in this presentation.

The statements made in this presentation concerning the proposed changes to Gatekeeper and the role of HeSA in the review process do not represent the views of the Commonwealth (or Finance). Finance disclaims any responsibility for them.

HeSA (now Medicare Australia) is a Gatekeeper accredited Extended Services Registration Authority whose accreditation is limited to issuing Individual and Location Certificates for use by entities within the health sector.

All references to other initiatives being undertaken by HeSA are unrelated to the terms of its Gatekeeper accreditation.

Australian Government
Medicare Australia
Health eSignature Authority

Introduction

- History of HeSA
- Current structure & mission
- HeSA in its e-health environment
- The Barwon Health smartcard project
- HeSA and the Gatekeeper reforms

Australian Government
Medicare Australia
Health eSignature Authority

The history of HeSA

- Long time Gatekeeper accredited
- To date 8,000 Individual keys (hard)
- Over 8,000 Location keys (soft)
- Changing usage & business models

  Started out with Individual and Location certs. Demands from the sector and from e-health programs like "HIC online" and "Eclipse" have seen evolution in certificate usage. HeSA is introducing new certificate types and registration processes to continue to meet evolving needs.

Australian Government
Medicare Australia
Health eSignature Authority

HeSA structure & Mission

- Now part of Medicare Australia and the Department of Human Services
- Mission is to facilitate connections across the health & welfare sector
- The core offering is *Managed PKI Services* for health & welfare
- Closely involved with Gatekeeper reform; first deployment of Known Customer certs
- See www.hesa.gov.au

Australian Government
Medicare Australia
Health eSignature Authority

HeSA in its environment

- Big smartcard projects
  - Medicare smartcard
  - Human Services smartcard (to be confirmed)
  - PKI expected to be core to these cards
- Medicare payments being re-engineered
- Meeting the needs of "local" smartcard & PKI projects
- HeSA sees itself as the "wholesale" PKI provider of choice

Australian Government
Medicare Australia
Health eSignature Authority

Barwon Health

- Barwon area health service
  - Geelong hospital
  - 5,500 staff (4,000 FTA)
  - Highly electronic; e.g. HL7 messaging
- Smartcards in the ICU
  - Incarta software developer
  - Sun Ray workstations
- Now: Access control & workflow
  - Barwon Health already invested in Sun Rays
- Soon: Single ID, LAN access, e-health apps
  - bedside notes
  - electronic Discharge Referrals
  - e-Prescribing

Australian Government
Medicare Australia
Health eSignature Authority

PKI smartcard project

- Semi-customised certificates
- Barwon HR acts as RA; HeSA is the CA
- "Known Customer" principles
- Real time issuance & replacement
- Nationally interoperable HeSA PKI
- On-chip key generation
- Locally operated Card Mgt System
- Many e-health applications in the works

HeSA Digital Credentials

- Conceptually straightforward to push out to all Medicare-registered providers
- Certain professionals very well "known" by Medicare Australia
  - doctors
  - pharmacists
  - anyone who bills via C'wealth

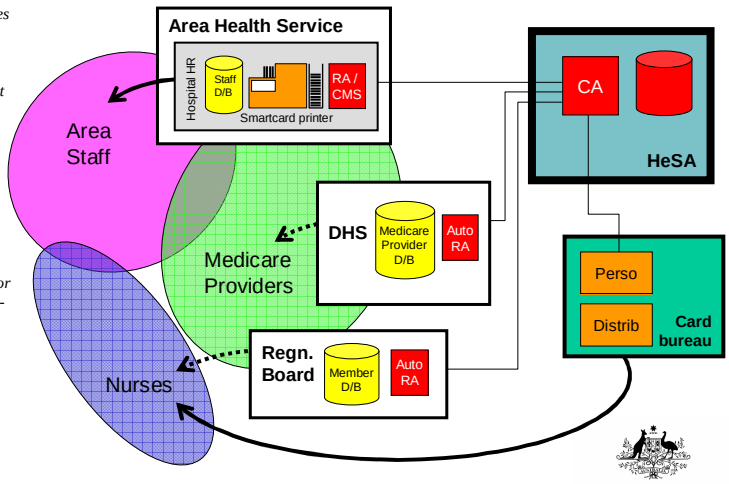
- Push out smartcards (and readers)
- Envisage working with registration boards

Australian Government
Medicare Australia
Health eSignature Authority

HeSA's PKI communities

HeSA sees two high priority types of Known Customer scheme. First, relatively small scale Communities of Interest (e.g. Barwon Health) where we inject customised certs into locally issued cards, predominantly to support local apps. Second, we can arrange to push out smartcards bearing specific digital credentials to healthcare professionals like nurses, GPs, pharmacists etc. For new professionals, their cards would be handed out by their bodies; for existing professionals, bulk mail-out is envisaged.

When communities of interest overlap, and the one person has two or more credentials, we will typically issue multiple certificates (often to the one card). This is simpler and less risky than trying to merge business processes of distinct communities



Australian Government
Medicare Australia
Health eSignature Authority

HeSA and the evolution of Gatekeeper

Australian Government
Medicare Australia
Health eSignature Authority

PKI reform drivers generally

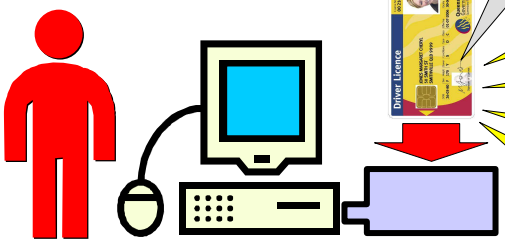
- Cost of Gatekeeper, especially registration
- Fundamental shift to closed/vertical PKI
- "Authorisation" PKI
  - *"For big CAs, there is an implicit assumption that a single cert is all that a user should need. This assumes that one identity is sufficient for all applications, which contradicts experience."* Dr Stephen Kent, Co-chair IETF PKIX WG
- *Known Customer* PKI
  - *"Provide the means to convert a trusted relationship between business and its customers into an electronic credential (digital certificate) to help automate on-line transactions between them"*
- See *Draft Gatekeeper PKI Framework*
  - http://www.agimo.gov.au/infrastructure/gatekeeper

Australian Government
Medicare Australia
Health eSignature Authority

"Modern PKI"

The user's experience of modern PKI is vastly simplified: they insert a smartcard and the system responds with secure services enabled by the type of credential(s) found on the card.

In the past, it was thought that a single general purpose ID certificate issued by e.g. a post office would be useful. Today we deploy different, more focused digital credentials which can support business transactions on their own, without needing to look up back-end credentials data bases.



Post Office
Card holder is:
Stephen Gregory Wilson

Health Insurance Commission
Card holder is:
Dr Stephen Wilson Provider #12345

HealthConnect
Card holder is:
NHID 333 444 555

Electoral Commission
Card holder is:
Voter No. 99999999

Dept of Foreign Affairs & Trade
Card holder is:
Passport Code 43df29a3b99ffc42

Note that the intelligence to look for and seamlessly invoke the right certificates is easily built into the software applications. There is no usability penalty for having multiple credentials or multiple "personae" carried in the smartcard.

How modern PKI is used

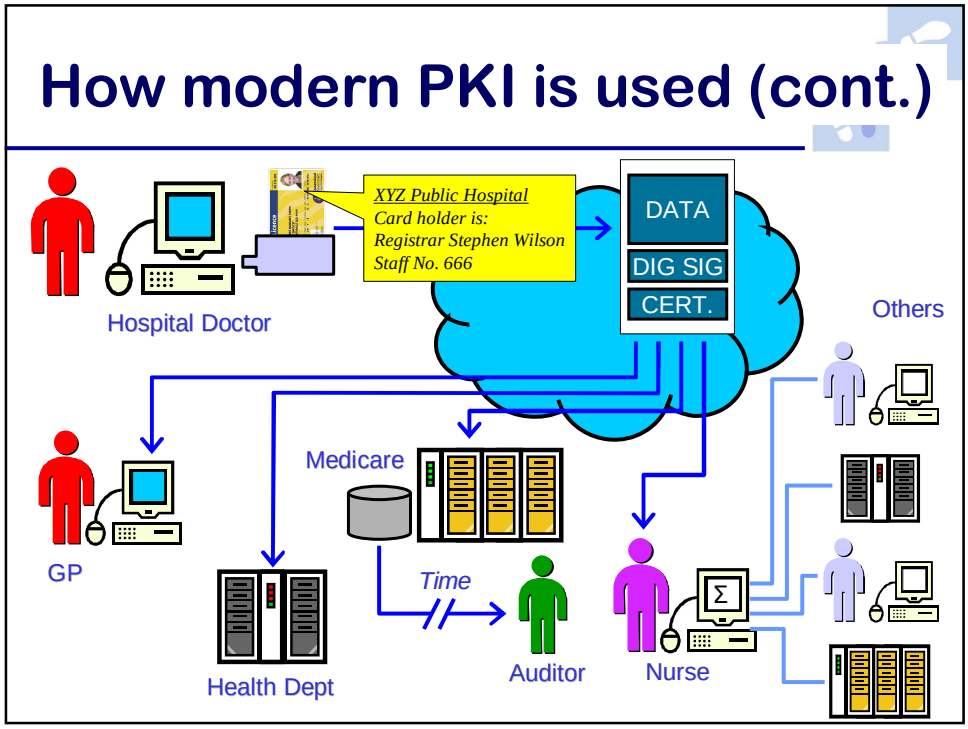
The following slide illustrates why PKI so important in complex information management environments like healthcare. PKI isn't just about access control; crucially, it allows for transactions to carry the authority information of the originator, bound to the transaction by digital signatures, and forever after instantly verifiable without needing to defer to historical data about the originator's authority and credentials.

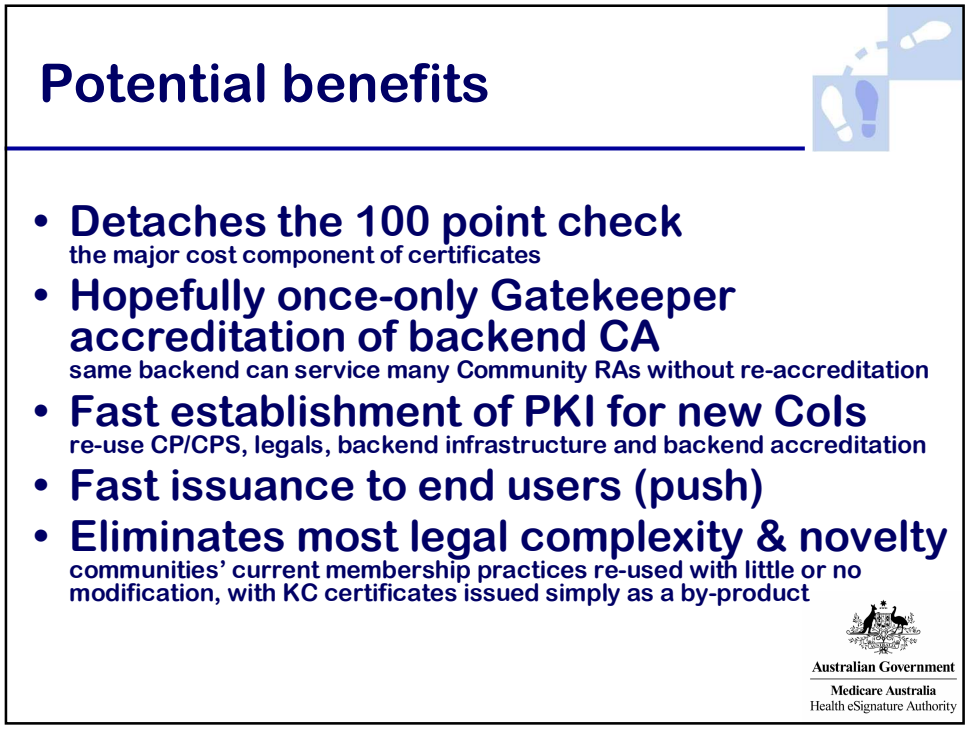
In the following, a health event summary (such as a discharge referral) is created by a hospital doctor, who has been issued a digital credential by their hospital (note that hospital doctors are typically not "known" as such by the Commonwealth, because they are not yet part of the Medicare Australia payments system, and so their credentials usually need to be issued locally). The event summary may need to be sent to – and processed straight through – by a large number of "Relying Parties", over arbitrarily long periods of time. These may include other healthcare professional involved in the patient's care, the Health Department, and Medicare. Data will often be accessed down the track by auditors. Data will also be processed and added to by professionals, and sent on again to others.

In all cases, the original bona fides of the hospital doctor must remain verifiable, despite the "separation" in time and space between her and subsequent Relying Parties.

Only PKI has the ability to bind the originator's credentials and authority information directly to the transaction, resist tampering, and preserve that information binding over arbitrarily long periods of time. Conventionally we may use audit logs to work out who did what to whom when we need to "rewind" electronic transactions, and in simple closed systems like Internet banking, audit logs suffice. But in more complex environments, where logs are not guaranteed over long periods of time, PKI is the only viable way to preserve transaction authority.

Australian Government
Medicare Australia
Health eSignature Authority


How modern PKI is used (cont.)
XYZ Public Hospital
Card holder is:
Registrar Stephen Wilson
Staff No. 666
DATA
DIG SIG
CERT.
Hospital Doctor
Others
Medicare
GP
Time
Health Dept
Auditor
Nurse


Potential benefits
• Detaches the 100 point check
the major cost component of certificates
• Hopefully once-only Gatekeeper accreditation of backend CA
same backend can service many Community RAs without re-accreditation
• Fast establishment of PKI for new CoIs
re-use CP/CPS, legals, backend infrastructure and backend accreditation
• Fast issuance to end users (push)
• Eliminates most legal complexity & novelty
communities' current membership practices re-used with little or no modification, with KC certificates issued simply as a by-product
Australian Government
Medicare Australia
Health eSignature Authority

Smartcard drivers

- **Anti skimming**
  The initial driver in many smartcard programs was the elimination of skimming & counterfeiting; smartcards cannot be cloned or counterfeited
- **Off-line fraud control**
  Just as important in EMV is the ability of the card to enforce business rules (e.g. daily transaction limits) and to respond intelligently when rules are broken
- **Sophisticated identity management**
  Smartcards can hold multiple credentials/identifiers, selectively control access to each of them, and serve them up to applications selectively
- ***Entitlements* management**
  Cardholder entitlements can be programmed into the card; eligibility can be checked by the card, without sending personal info across the network
- **Multi-applications**
  E.g. ticketing & tolling, loyalty, e-purse; multi-application capability used to be seen as the major "value add" but it does tend to complicate the business case and implementation by tying too many projects and business processes together
- **Mutual authentication**
  This is set to become the more important value add. Smartcards are uniquely able to protect against Man In The Middle and other forms of web fraud, and so could supersede regular two factor authentication.

Australian Government
Medicare Australia
Health eSignature Authority

Mutual authentication

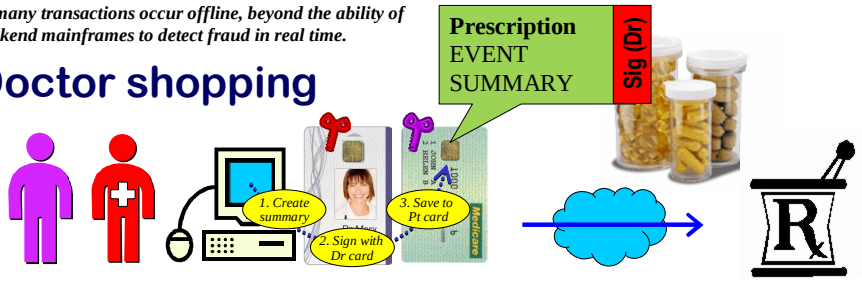
- The business requirement is for a client or user to be able to positively verify the identity of a server *before* the server identifies the user and opens a session. Otherwise, users are still vulnerable to visiting a spoofed website (pharming).
- The US Government *Personal Identity Verification* (PIV) FIPS 201 is driven by a Homeland Security Presidential Directive (HSPD-12).
- PIV stratifies authentication levels (a little like the Australian Government Authentication Framework).
- **PIV level 4 mandates that remote authentication *"must resist eavesdroppers [and] must resist man-in-the-middle attacks".***
- **NIST says that the *"only practical solution today uses PKI [on hard tokens]"*; i.e. smartcards.**
  [Reference: Bill Burr, Manager Security technology, US NIST http://asia-pkiforum.org/feb_tokyo/NIST_Burr.pdf]
- Thanks to their built-in computer, smartcards are uniquely able to actively check the identity of the server before opening a session

Australian Government
Medicare Australia
Health eSignature Authority

Offline fraud control (1)

The health system is vulnerable to fraud largely because so many transactions occur offline, beyond the ability of backend mainframes to detect fraud in real time.

Doctor shopping



Patient smartcards can be used to combat doctor shopping, by using the intelligence of the card itself to enforce "business rules". We assume in the model shown here that when a doctor prescribes a drug, certain details of that prescribing event are stored to the card, in an Event Summary digitally signed with the doctor's HeSA card. The entire prescription might be lodged somewhere else for various reasons, which in detail do not concern us here.

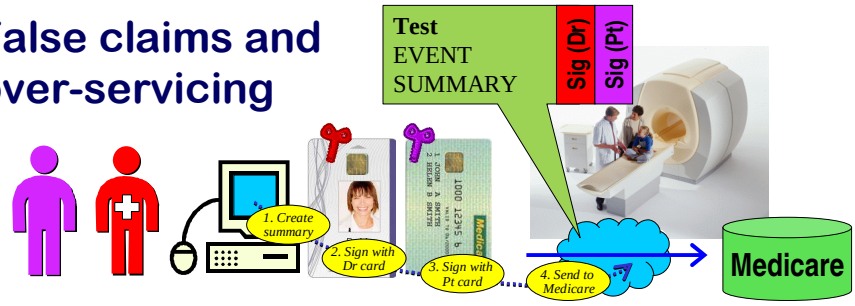
The important thing is that the card is able to apply certain tests to the prescribing event and alert the doctor if rules seem to have been broken. For instance, ***the smartcard can keep track of how many scripts have been written in a period of time.*** *If a patient has special entitlements, for example to be prescribed schedule 8 medications, more specific rules could be coded into their smartcard. Ideally pharmacy systems would 'close the loop' by accessing the smartcard and updating pertinent details about the dispensing event.*

Note too the ***privacy benefits of enforcing rules in the card****, because sensitive personal data is not sent over the net.*

Australian Government
Medicare Australia
Health eSignature Authority

Offline fraud control (2)

False claims and over-servicing



The spectrum of provider fraud includes doctors claiming for services not delivered – or for services delivered at a different time, as in the MRI rebate scam – as well as receptionists or even internal government staff creating false claims. These types of fraud could all be mitigated if the ***patient smartcard were used to "stamp" the claim with an un-forgeable, indelible audit mark that ties the claim to an actual event.*** *A claim could not be generated without collusion at least with the patient, and over-servicing would be readily detected if the same patient card was seen in multiple claims.*

Technically, these audit marks would be digital signatures created using a special private key unique to the patient card. However, these marks would not use any personal private key, nor would they reveal any personal information about the patient (unless fraud is detected and an investigation initiated).

Australian Government
Medicare Australia
Health eSignature Authority

Summary

- *Known Customer* streamlines digital credentials to professionals and more
- Flexible; low cost; user friendly
- Meshes with Gatekeeper reforms
- PKI resurgent worldwide; now core to most multi-application smartcards
- *Mutual Authentication* via smartcards looming as a major issue
- HeSA positioned as wholesale provider of choice for Human Services credentials

Australian Government
Medicare Australia
Health eSignature Authority

Discussion

John Brewer
john.brewer@medicareaustralia.gov.au

Stephen Wilson
swilson@lockstep.com.au

Australian Government
Medicare Australia
Health eSignature Authority