Extended Abstract: Anonymity & Pseudonymity in eResearch via smartcards and Public Key Infrastructure

Stephen Wilson
Lockstep Technologies Pty Ltd, Sydney, Australia, swilson@lockstep.com.au

INTRODUCTION

A great deal of research in healthcare and the social sciences requires that study subjects remain anonymous (or pseudonymous). Tensions arise between privacy, authenticity and integrity: without compromising confidentiality, there must be assurances that reported data truly corresponds to real subjects, and that data has not been corrupted either accidentally of deliberately. Further, eResearch is conducted in an increasingly stringent regulatory environment, with legislated privacy requirements, and raised confidentiality expectations especially in the USA with strict FDA and health record privacy rules.

Lockstep Technologies R&D into PKI-based identity and access management has led to an anonymous records system called "*Stepwise*" which can be applied to ensure anonymity or pseudonymity of research subjects. The proposed solution is especially applicable when study data is collected and managed electronically throughout its lifecycle. *Stepwise* securely encapsulates identifiers within anonymous digital certificates issued to a subject's smartcard or similar device. *Stepwise* isolates each identifier, removes all extraneous personal detail and linkages, and ensures that when any identifier is presented online, we can be confident that it is legitimate and that was used with consent.

This presentation details how *Stepwise* can be applied to ensure anonymity or pseudonymity of study subjects in the exemplar of a clinical trial. The solution leverages increasingly widespread public key infrastructure services in the tertiary sector, and can be deployed using a wide range of authentication devices including smartcards and USB keys.

BACKGROUND: LOCKSTEP TECHNOLOGIES' *STEPWISE*

Stepwise seals an identifier within an anonymous digital certificate issued to a subject's smartcard or similar cryptographic key media. *Stepwise* strips the identifier of all extraneous personal detail, and ensures that when the identifier is presented online, all concerned are assured that it is legitimate and that it has been used with consent. *Stepwise* prevents an identifier from being stolen and abused without permission, modified, detached and re-attached to a different record, or counterfeited. By enhancing the "pedigree" of personal IDs, *Stepwise* allows all demographic information to be dispensed with, dramatically improving de-identification and privacy. The benefits of *Stepwise* include:

- Identifiers cannot be cloned, counterfeited, or illicitly copied
- every transaction bears a tamper-proof (digitally signed) pedigree, proving it originated from an authentic personal authentication device carrying a bona fide identifier, and used with the consent of the subject
- because all data records are digitally signed and de-identified, the integrity and traceability of data, and the confidentiality and privacy of patients are all greatly enhanced.

More detail of the *Stepwise* technology is available at [1].[1]

WORKED EXAMPLE: USING *STEPWISE* TO IMPROVE CLINICAL TRIAL CONFIDENTIALITY

Huge amounts of highly sensitive data are gathered routinely (and increasingly, electronically) during clinical trials. De-identification and anonymity are critical; not only is patient confidentiality paramount, but assignments to treatment and control arms in double-blind trials must remain secret.

We propose using smartcards (or similar cryptographic key media) and *Stepwise* digitally certified identifiers to manage the data from clinical trial subjects, so as to protect patient confidentiality, and de-identify all reported data. The proposal introduces smartcard issuance and an additional layer of standard PKI-based security to existing clinical data management software.

Figure 1 illustrates the enrolment stage of the proposed identity & access management solution; Figure 2 shows the smartcard and ID in action during follow-up. The setup of a clinical trial generally involves equipping investigators with data collection software and, in the case of drug trials, treatment packs. With the *Stepwise* solution, each investigator will also be issued with their own unique smartcard, and a smartcard reader. At enrolment, each study subject will be issued with their own smartcard, to carry their *Stepwise*-protected ID.

In more technical detail, the *Stepwise* certificate is generated by a conventional Certification Authority (CA) server, which could be available as a managed service in the emerging tertiary sector PKI. The certificate request is generated by a registration (RA) module at the study administration system, triggered by a secure order originating from the investigator and secured using their smartcard.

[1] Technical details will be elaborated in the poster.

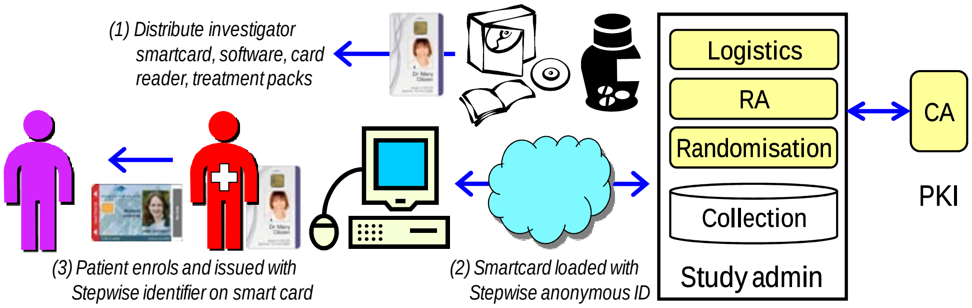
(1) Distribute investigator smartcard, software, card reader, treatment packs
Logistics
RA
Randomisation
Collection
Study admin
CA
PKI
(3) Patient enrols and issued with Stepwise identifier on smart card
(2) Smartcard loaded with Stepwise anonymous ID

Figure 1: Issuing study subjects with Stepwise-protected IDs

At follow-up visits, the subject presents their smartcard and their ID is retrieved by the software and validated through the *Stepwise* capsule. Test results and other reportable data are collated as usual, and then digitally signed using the *Stepwise* capsule and the subject smartcard. All other personal information can be stripped from the record before signing, de-identifying it and enhancing patient confidentiality.

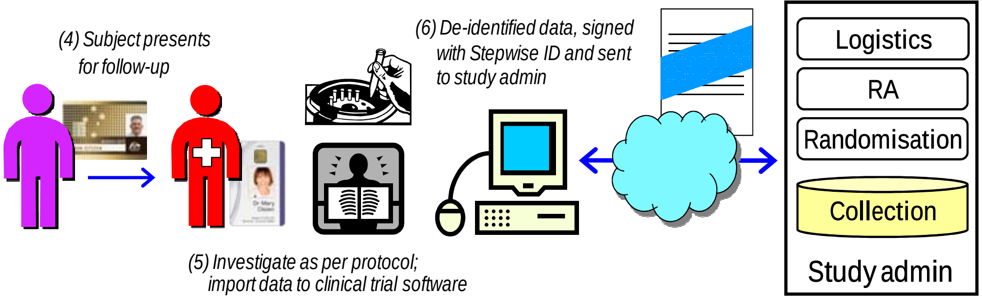
(4) Subject presents for follow-up
(6) De-identified data, signed with Stepwise ID and sent to study admin
Logistics
RA
Randomisation
Collection
Study admin
(5) Investigate as per protocol; import data to clinical trial software

Figure 2: Using Stepwise-protected IDs at follow-up visits

Stepwise is an entirely standards-based approach. It uses conventional multi-function cryptographic smartcards and digital certificate services. As such, Stepwise is fully compatible with such PKI schemes as the tertiary sector's Australian Access Federation (AAF).

BENEFITS

Using *Stepwise* to de-identify social science and healthcare study subjects will deliver several benefits to eResearchers (and their subjects) including:

- fundamentally enhanced confidentiality
- better confidence on the part of subjects
- better privacy compliance
- better study data integrity, and
- better resistance to fraud and/or data errors.

OTHER APPLICATIONS

In the tertiary education sector smartcards are becoming more widespread for student identification, and PKI services are available through programs like the AAF. Multi-function smartcards with native public key security functions lend themselves to many other *Stepwise*-enabled applications, including:

- anonymous voting in student elections and the like [2]
- confidential personal e-health records
- de-identified participation in online social networking and role playing games.

ACKNOWLEDGEMENTS

Stepwise demonstrator applications were developed with the assistance of an AusIndustry Commercialising Emerging Technologies (COMET) grant.

REFERENCES

1. Wilson, S. *A novel application of PKI smartcards to anonymise Health Identifiers* AusCERT2005 Security Conference Academic Refereed Stream, Gold Coast, May 2005.
2. Wilson, S. *An easily validated security model for e-voting based on anonymous public key certificates*, AusCERT2008 Security Conference Academic Refereed Stream, Gold Coast, May 2008.