Anonymity & Pseudonymity in eResearch via smartcards and Public Key Infrastructure

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

The fastest way to get somewhere is to be there already
Paramahansa Yogananda

And the best way to de-identify is to never identify in the first place

INTRODUCTION

Much healthcare and social science research requires that study subjects remain anonymous or pseudonymous. Tensions arise between privacy, authenticity and integrity. Without compromising confidentiality, reported data must correspond to real subjects, and must resist corruption. eResearch is conducted in an increasingly stringent regulatory environment, with legislated privacy requirements, and raised confidentiality expectations.

"*Stepwise*" is a Privacy Enhancing Technology (PET) that de-identifies study subjects and ensures the integrity of their pseudonymns or IDs. *Stepwise* secretes IDs within anonymous digital certificates and smartcards (or like devices) issued to each subject. The solution leverages public key infrastructure services that are increasingly widespread in the tertiary sector, and can be deployed using a wide range of authentication form factors.

THEORY

Orthodox PKI entails identity checks and the issuing of general purpose digital "passports". Yet the same digital certificate technology can be used to create a secure notarisation of any attribute of the user. *Stepwise* uses digital certificates to bind a subject's study ID to a private key contained in a chip, such as a USB key or smartcard.

The subject's ID is subsequently bound to data records by way of a digital signature. When the data record is received and the signature verified, the receiver is assured that the ID is legitimate and that it has been used with consent. By enhancing the "pedigree" of personal IDs, *Stepwise* allows all demographic information to be dispensed with, dramatically improving de-identification and privacy.

BENEFITS

- 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.

WORKED EXAMPLE: CLINICAL TRIAL CONFIDENTIALITY

Smartcards (or alternatively, USB keys) carry *Stepwise* IDs and are used at follow up visits to secure data records.

Study set-up: Equip investigators with protocol, subject information packs, data collection software, treatments, and investigator smartcard and reader.

Subject enrolment: explain study, provide information pack, obtain consent, personalise smartcard online, load Stepwise ID (automatically), issue card

Follow-up: Data collated; all personally identifiable information stripped from the record; record digitally signed twice, by investigator's card and subject's *Stepwise* ID card.

TECHNICAL NOTES – PKI

The *Stepwise* certificate is generated by a conventional Certification Authority (CA) server, available as a managed service in the emerging tertiary sector PKI. The certificate request is generated by a registration (RA) module integrated in the study administration system, and signed using the investigator smartcard.

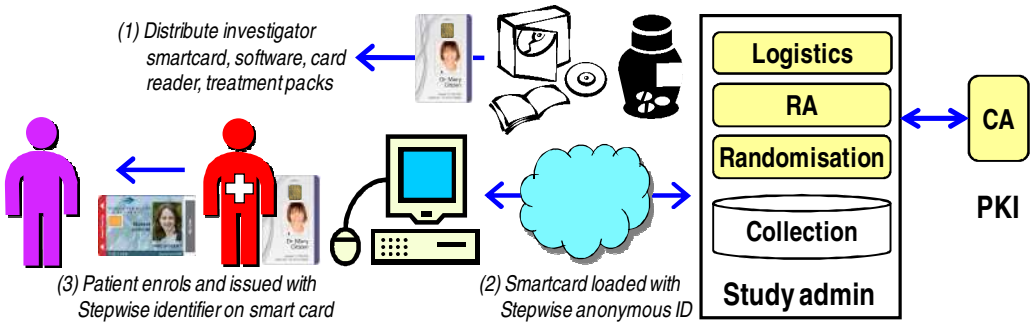

Figure 1: Issuing study subjects with Stepwise-protected IDs

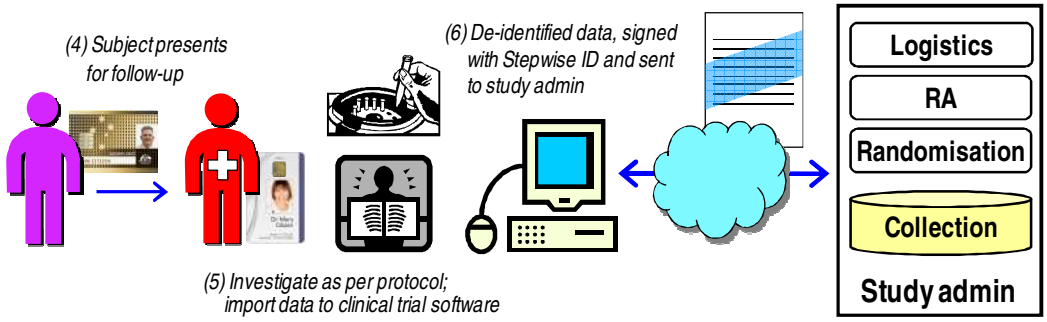

Figure 2: Using Stepwise-protected IDs at follow-up visits

OTHER APPLICATIONS

- apomediation
- anonymous online social networking, onliune counselling
- anonymous voting in student elections and the like [2]
- confidential personal e-health records.

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.