Using a Public Key Registry for Improved Trust and Scalability in National E-Health Systems

Vicky Liu, Science and Engineering Faculty, Queensland University of Technology, Brisbane, Queensland, Australia

William Caelli, Science and Engineering Faculty, Queensland University of Technology, Brisbane, Queensland, Australia

Yu-Nien Maggie Chen, Graduate School of Asia and Pacific Studies, Waseda University, Tokyo, Japan

ABSTRACT

An increasing number of countries are faced with an aging population increasingly needing healthcare services. For any e-health information system, the need for increased trust by such clients with potentially little knowledge of any security scheme involved is paramount. In addition notable scalability of any system has become a critical aspect of system design, development and ongoing management. Meanwhile cryptographic systems provide the security provisions needed for confidentiality, authentication, integrity and non-repudiation. Cryptographic key management, however, must be secure, yet efficient and effective in developing an attitude of trust in system users. Digital certificate-based Public Key Infrastructure has long been the technology of choice or availability for information security/assurance; however, there appears to be a notable lack of successful implementations and deployments globally. Moreover, recent issues with associated Certificate Authority security have damaged trust in these schemes. This paper proposes the adoption of a centralised public key registry structure, a non-certificate based scheme, for large scale e-health information systems. The proposed structure removes complex certificate management, revocation and a complex certificate validation structure while maintaining overall system security. Moreover, the registry concept may be easier for both healthcare professionals and patients to understand and trust.

Keywords: E-Health Security, E-Health Security Solutions, Non-Certificate-Based Cryptosystem, Public Key Registry, Trust In E-Health Systems

INTRODUCTION


- Population ageing is unprecedented, without parallel in human history —and the twenty-first century will witness even more rapid ageing than did the century just past.
- Population ageing is pervasive, a global phenomenon affecting every man, woman and child—but countries are at very different stages of the process, and the pace of change differs greatly. Countries that started the process later will have less time to adjust.

DOI: 10.4018/ijehmc.2013100105
Population ageing is enduring: we will not return to the young populations that our ancestors knew.

Population ageing has profound implications for many facets of human life.

This report has profound implications for the development and operation of e-health systems worldwide particularly in those countries most affected, such as Japan, Australia and others. It has been argued that e-health information systems have the potential to markedly improve service delivery in this area and numerous countries have such systems in some stage of development, including Singapore, Australia, Canada, the United States of America, the United Kingdom and the Netherlands. Interestingly, these countries have been seen as being particularly exposed to the problems of an aging population as report by the United Nations. The concern, then, given that an aging population is seen as requiring more and better, and often more advanced, healthcare services, e-health information systems will play a vital role in providing new levels of efficiency in this area.

Overall information security/assurance plays a vital role in the acceptance of any system. In turn, any assurance system must be both understandable to its users while being capable of providing notable levels of expansion capacity and overall performance and efficiency. In this regard, legislative and regulatory actions have taken place in some countries to attempt to improve such trust. This includes the United States’ Health Insurance Portability and Accountability Act (HIPAA), enacted in 1996 to spur the development and usage of these systems to improve the deliverability of healthcare services as well as to potentially decrease overall costs in the healthcare sector. HIPAA required appropriate levels of cyber-security services to be incorporated.

Cryptography has been the method of choice for the creation of security services in most on-line information systems, including those in the banking and finance sector in particular. Indeed cryptographic technologies play a vital role in the provision of the confidentiality, integrity, authentication, non-repudiation and like services needed to create such trust in any information system. Their role in e-health systems cannot be underestimated when aspects of confidentiality, and resulting privacy concerns, take on added dimensions. However, the cryptographic keys used, for both public and private key cryptographic schemes, must be secure requiring that keys be safely generated, distributed, managed, used and deleted when no longer required. In particular, keys used for digital signature purposes require particular security services, for instance extended lifetime for the purposes of safe and secure archiving of patient records. The cryptographic sub-systems must, however, besides being themselves particularly secure since other information security services depend upon them, be efficient, scalable and easily understood and managed. This obligation largely resides with the e-health system provider and manager who must recognise that cryptographic key management is a critical aspect of overall systems security and protection in an e-health environment.

To achieve these goals, Australia’s National Authentication Service for Health (NASH) scheme adopted a digital certificate oriented Public Key Infrastructure (PKI) to be a critical security architecture for Australia’s proposed national e-health services (Australian Department of Health and Ageing, 2011). However, there are well understood problems with such a structure if it is proposed to be used in very large scale information systems with major requirements for scalability and overall system performance. In addition, public key certificate system complexity, particularly in regard to certificate creation, deployment and management, as well concerns for certificate timeliness and revocation have been of note (Adams & Lloyd, 2002). These concerns cannot be largely ignored in relation to e-health systems deployment at a national level and led to the research undertaken by the authors. Any such system adopted must be relatively easy to understand, particularly by system administrators and managers as well as by users, both e-health professionals and their clients alike. Without that understanding and confidence in the underlying cryptographic and associated hardware/software sub-systems
Perceived Organizational Environment and Performance Reliability in the Case of Hospital Nurses
[www.igi-global.com/chapter/perceived-organizational-environment-performance-reliability/36523?camid=4v1a](www.igi-global.com/chapter/perceived-organizational-environment-performance-reliability/36523?camid=4v1a)

Spatial Heart Simulation and Analysis Using Unified Neural Network
[www.igi-global.com/chapter/spatial-heart-simulation-analysis-using/13072?camid=4v1a](www.igi-global.com/chapter/spatial-heart-simulation-analysis-using/13072?camid=4v1a)