Public Key Infrastructures in eHealth

By

Dr Salah Mandil, Principal Consultant, E-Health & E-Strategy, WISeKey SA

Jérôme Darbellay, Services & Alliance Relations Manager, WISeKey SA

Introduction

This paper emphasises the significance of providing security in any form of health and healthcare transactions over networks, Intranets, Extranets and particularly the Internet. It highlights Public Key Infrastructure (or PKI) as the security technology, and discusses how PKI would secure the various types of transactions in the health sector, between Individuals (such as patients, doctors, specialists, pharmacists, health professionals) and between institutions (such as hospitals, clinics, radiology services, laboratories, pharmacies, ...). The paper ends by briefly citing the options for choosing a PKI solution for eHealth.

Networking & Telecommunications in Health

The ***provision of Health Care*** requires, and generates, a wide variety of data and information, which need to be collected, processed, distributed, accessed and used – securely and respectful of strict ethical and legislative rules. This is particularly vital for the Clinical and Managerial information. Other types of information are the Epidemiological, Literature and Knowledge.

The ***sources*** of these types of data and information are within and outside the Health Care infra-structure and located at varying distances from their respective users. In practice, users require and generate a mix of these types of information and at differing stages of their respective functions, e.g. a physician may consult a knowledge base, whilst examining a patient and would make a relevant entry onto the patient's record, which may be used for billing purposes.

The ***Health Care encounters and transactions*** are multi-faceted. They occur, for example, between a patient and a physician; between two physicians; between a physician and an expert consultant; a patient and a health institution such as a test laboratory, a pharmacy or a rehabilitation centre. And, such encounters may occur in one's own community, in another part of the country or abroad. All such encounters require data and information prior to the actual start of the encounter, and generate the same during the encounter or soon thereafter. Such data and information could be in *differing volumes*, at *differing times* and in *differing forms* such as voice, numbers, text, graphics and static or dynamic images, and are often a judicious mix of these.

The ***sources and repositories*** of such data and information could spread over differing locations and would take differing forms, for example, complete patients records; hand-written prescriptions; reports by a physician, a consultant or a laboratory.

Traditionally, all such encounters were face to face, and the spoken and the written word were the main modes of communications and medical record-keeping, whilst transport was mainly by road, rail or air, public and private services. As the telephone services network grew, it became the communication network of the health professionals and institutions, nationally and internationally, until the advent and growth of modern tools of ***Health Telematics***.

The uses of technology in the clinical/medical aspects of the Health Care services steadily grew and included ***instrumentation and equipment***, particularly *sensing and measuring* equipment, laboratory services, *static and dynamic imaging*. With the growth of the uses of such technologies and of the variety and sophistication of these, it was inevitable that many of such technological services became separated from the mainstream Health Care institutions - separated in distance and more significantly in management. So, the communications between such technology-based services and the mainstream Health Care services became an important consideration in the efficacy and economy of such services.

The popular use of ***Information and Communications Technologies*** by the health sector, started over 25-years ago with simple electronic messaging (E-mail) carrying purely alpha-numeric notes and reports. Just as voice communications was the main motive for the installation of telephones in physician's cabinets and Health Care institutions, E-mail was the main initial justification for the installation of modern telecommunication links. And, as E-mail services grew, so did the demands on their performance and geographic coverage: more locations at more speed and with more bandwidth to cater for the growing attachments to the E-mail messages. The past ten years have witnessed an exponential growth in the uses of E-mail in the health sector, within and between countries, even in the poorest countries, ***particularly over the INTERNET***. For example, ***e-Transactions*** are taking over those functions that do not really require face-to-face encounters, such as preparing and sending prescriptions and reports, fixing appointments and scheduling services, referring patients and, where the telecommunications services performance permit, also transmitting medical images and their associated expert readings, either written or oral.

Another level of sophistication of the uses of Information and Communications Technologies is **Telemedicine**, which is "the provision of medical care using audio, visual and data communications", including the actual diagnosis, examination and even care of a patient who is remotely located. Telemedicine is an important and growing field and is expected to change many of the traditional approaches in Health Care; indeed it is the start of a new paradigm in medical care.

Another area that is relatively speaking not recent, but will usefully expand with the spread of Telematics support, is the access to and uses of **knowledge-based systems**. These systems, which are also known as expert systems and decision support systems, are systems that provide expert advice and guidance on medico-scientific issues and procedures. For example, given a patient's coordinates and symptoms, it could provide diagnostic support, suggest additional tests or propose a treatment.

All the above cited developments are also having a major impact on the relevant **Management Information Systems** needed for and used in the health sector, e.g. Hospital MIS. These are no more systems for the administrative management of hospital care to patients, from admission to discharge/transfer, but include a multitude of intelligent, medical-staff-friendly interfaces to, for example, clinical decision support systems, Telemedicine links, Website portals, etc…

Two other recognised realities of Health Care staff and patients should also be cited: their **mobility** and their need for having their **hands free** and thus dedicated to the medical care itself. The mobility feature means that they can get to the medical information required, e.g. an **Electronic Patient Record**, or to a tool or instrument, from any remote location and whenever necessary subject to their verification, within a building or a town, but within whole countries and between countries. And, the hands free feature means that solutions have to be found for identification and authorisation that do not engage the medical worker in a manual intervention, e.g. to open a door or to key onto a computer keyboard.

Thus, Health Care is a profoundly information-intensive sector, in which the collection, flow, processing, presentation and distribution of health, and health-related, data and information, are key to the **efficacy, efficiency and economy** of the operations and development of the Health Care services, within a country and between countries.

A crucial requirement is that all such flow must be fulfilled **securely and confidentially**, and in strict adherence to **ethical and legal rules and regulations**.

The Public Key Infrastructure (PKI) Technology

All communications over electronic networks are susceptible to all sorts of security breaches, especially open networks such as the Internet. In the case of the Internet, the Transmission Control Protocol/Internet Protocol (TCP/IP) is used. TCP/IP allows any kind of data to be sent from one computer to another through a variety of intermediate computers and separate networks before it reaches its destination.

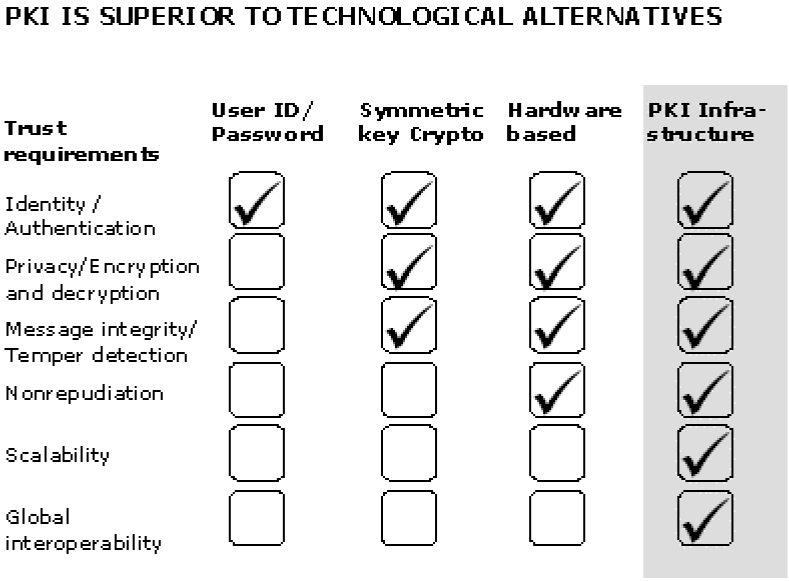
The great flexibility of TCP/IP has lead to its worldwide acceptance as the basic Internet and Intranet communications protocol. At the same time, the fact that TCP/IP allows information to pass through intermediate computers makes it possible for a third party to interfere with communications in the following ways:

- Eavesdropping. Information remains intact, but privacy in compromised (e.g., someone learns a credit card number, records a sensitive conversation or intercepts classified information)
- Tampering. Information in transit is changed or replaced and then send on to the recipient.
- Impersonation. Information passes to a person who poses as the intended recipient

A set of techniques and standards known as **public-key cryptography** make it relatively easy to avoid such unwanted interferences as it facilitates the following tasks:

- *Identity/Authentication* allows the recipient of information to determine its origin – that is, to confirm the sender's identity.
- *Privacy/Encryption and decryption* allows two communication parties to disguise information they send to each other. While in transit, the encrypted information is unintelligible to an intruder.
- *Message integrity/Tamper detection* allows the recipient of information to verify that it has not been modified in transit.
- *Non-repudiation* prevents the sender of information from claiming at a later date that he didn't send this information.
- *Global interoperability:* The PKI Technology allows global cross-recognition and interoperability between CAs.

In comparison to other well-known technologies, PKI is able to cover all of the essential security challenges that such technologies cannot overcome.



PKI IS SUPERIOR TO TECHNOLOGICAL ALTERNATIVES

Trust requirements	User ID/ Password	Symmetric key Crypto	Hardware based	PKI Infra-structure
Identity / Authentication	☑	☑	☑	☑
Privacy/Encryption and decryption	□	☑	☑	☑
Message integrity/ Temper detection	□	☑	☑	☑
Nonrepudiation	□	□	☑	☑
Scalability	□	□	□	☑
Global interoperability	□	□	□	☑

Public key cryptography (also called asymmetric encryption) involves a pair of keys – a public key and a private key. Each public key is published, whereas the private key is kept secret (e.g., on a smart card or on a token, in the future also on a PDA or mobile phone). In general, to send encrypted data to someone, a person encrypts the data with the recipient's public key, and the person receiving the encrypted data decrypts it with the corresponding private key. Public-key encryption is used to sign data – an important requirement for electronic commerce.

A **digital certificate** binds public key and a private key to an individual or organisation. The main purpose of the PKI infrastructure is to issue and manage digital certificates. Digital certificates associate the identity of a person with a virtual identity. The fundamental responsibility of the PKI infrastructure is to vouch for the correspondence between these two identities. Rules and procedures to be followed for operating a PKI infrastructure are defined in a Certification Practice Statement (CPS), which ensures a common quality basis for digital certificates international and cross-sector interoperability. In simple terms, a digital certificate is a message that, at least, states the name, identifies the certificate's operational period, contains a certificate serial number, the name of the organization which authenticated the identity of the user/holder of the private key (Certification Authority, see below) and specifies the legal framework and limitation of usage. One could say that digital certificates are the electronic counterparts to a passport and personal signature.

The binding of the keys to an individual or organisation has to be certified by a trusted source: the **Certification Authority** (CA).

What type of PKI for eHealth?

Through its chaining of certification authorities, the PKI reproduces a hierarchical structure of the real world, whether it's a geopolitical hierarchy (regions-countries-states-localities), or thematic (Health-Medicine-Surgery-Specialized surgery-suppliers, etc). Furthermore, due to the fact that the Health sector is ubiquitous, hierarchical far-reaching and increasingly interactive across frontiers, the definition of a standardised PKI for health is becoming a manifest necessity.

The technical interoperability of health systems has to be assured by the exhaustive use of technology standards. These standards, such as the ITU X.509, have already been adopted by most security solutions providers. Being user authentication a critical application that is dependent on local information, the freedom to choose a given Public Key Infrastructure should not affect the capacity of the user to interoperate with persons certified by other Public Key Infrastructures in the health sector (which of course extends to at least a minimum standardisation regarding access control and other related policies of the health sector). To achieve this, different strategies can be put in place that could include the cross-recognition of the different infrastructures or the use of a common root. The adoption of technology standards, the technical interoperability of the different infrastructures and the standardisation of certain policies will guaranty a fully efficient and integrated environment for the world wide health transactions.

For more information, please contact:

Salah Mandil, WISeKey SA. Phone: +41 79 753 7301

Jérôme Darbellay, WISeKey SA. Phone: +41 22 929 5757