

PROJECT REPORT

FOR

MEDI-SAFE COMMUNICATIONS

(A Secure Email Pilot Program)

31 December 1999

Submitted to

Information Technologies Online Program

Information Industries Taskforce

GPO Box 9839

Canberra ACT 2601

Email: graydon.smith@noie.gov.au

Executive Summary

The MediSafe pilot has successfully demonstrated the viability of secure communications within the Medical profession. Whilst encrypted communications has been used for many years in the profession, MediSafe has deployed public key infrastructure (PKI) providing both encryption of messages and authentication of participants in an open environment using inexpensive communication mechanisms (Internet mail).

Whilst the system has proven that PKI works and is viable within the Medical profession, the trial also illustrated several detractors from widespread use of this technology:

- 1) Communication needs two parties. Initially the trial accepted participants on the basis of their desire to be involved. It soon became obvious that, unless those requiring communication were also participants, the system would not be used. In the latter period of the trial only those with a need to communicate to participants were accepted into the trial.
- 2) Communications need to be easy to use. Pilot participants were required to use a standard mail interface in order to access the system. This meant that they had to follow a convoluted process in order to send or receive an e-mail. A typical activity for a doctor was: generate a referral letter in their practice management program, exit their practice management program, generate an email, find and attach the referral letter, send the e-mail and return to their practice management program. On receipt of a response, another complicated process was required to save that response into a patient's electronic file.
- 3) The system must work first time and every time. Due to the nature of the pilot there were significant difficulties in "ironing out the bugs". This caused some practices considerable angst and productivity costs. It is very important that installation and training programs are error free so that practice disruption is kept to a minimum because target practices are operational businesses.

Despite these issues, the pilot has proven that the system works. This means that, in the opinion of the project manager, PKI will be installed across the medical profession soon. Professional and commercial organisations will be approaching doctors to get their participation in a plethora of patient care, medical databases, information repositories and practice administration products and services. Many of these services will utilise PKI for security purposes. In order to manage the impact that these services will have on their practices, the profession needs to learn from the trial and prepare for the onslaught.

A synopsis of the recommendations coming from the pilot is:

- 1) The profession must decide who they want to be their Certificate Authority (CA) (this might vary for GPs, specialists, etc.). The CA is an important function that will check the credentials of potential participants and then issue certificates containing the participant's security keys. Most PKI services will bring with them their own CA that will want to set-up a directory of medical professionals in which to store the certificate. It is likely that the first major organisation to do this will be the Health Insurance Commission. The profession must decide whether they want to control this facility or let organisations such as the HIC fulfil this role.
- 2) Consideration should be given to determining a standard communication infrastructure to which all such services must comply. General Practitioners have been somewhat abused by organisations requiring them to set-up communication processes that suit their own operations. This means that even though most computer-equipped practices have an operational e-mail service, they must maintain facilities to dial-up proprietary services to order services or get results. That implies that there will be a doubling up of communications equipment with many doctors having to dedicate facilities to communication tasks. This would be a significant cost overhead for the profession.
- 3) Now is the time for the profession to advise program developers of their preferred secure communication mechanism. Most doctor's offices operate some type of practice management software. Whilst most suppliers have been very responsive to their client's requirements and most programs demonstrate a co-operative approach to the program design. In order to meet the profession's future requirements, developers will need to know:
 - what medium is to be used (Internet, virtual private network etc.)
 - what mechanism is to be used (e-mail, web-browser etc.)
 - what private key storage mechanism is to be used (smartcard, file-based etc.)

In conclusion: the MediSafe pilot has been invaluable in gaining experience in the new world of secure messaging, public key infrastructure, Certificate Authorities and smartcards. Whilst the pilot was exclusive to the Medical profession, the lessons learnt are industry-generic. The pilot has shown that the technology works; now we'll see other industries can get it to work for them.

Acknowledgements

MediSafe gratefully acknowledges the contribution of the following parties:

- 1) The Information Technology On-Line (ITOL) program without which the project could not have proceeded.
- 2) The participants who all, in one way or another, contributed to the lessons learned during the pilot.

MediSafe sincerely regrets the system problems experienced by some participants and the frustrations experienced by most participants in the course of the trial. But lessons were learnt from all of them.

- 3) The Electrical Engineering faculty of the University of Queensland who provided office space and an Internet connection for the trial.
- 4) Software Agencies Australia which provided software licences and installation expertise to the trial.
- 5) Siemems SSE which provided software licensees and technical expertise.
- 6) Utimaco which provided equipment and technical assistance for the trial.
- 7) Nexor which provided the directory licence for the trial.

1 Introduction

General Practitioners (GPs) are the coal face workers within the health sector, and are reliant on numerous medical service providers to complete patient diagnosis and treatment. Those service providers include: hospitals; medical specialists such as surgeons, anaesthetists and psychiatrists, often housed within hospital infrastructure; and health professional service providers such as pathologists, radiographers, pharmacists, physiotherapists and psychologists.

Communication between these entities is mostly manual. Doctors request services on hand-written forms and diagnoses are returned via typed reports that are faxed or mailed to the GP. By moving to an electronic messaging system, the service provider will be assured of receiving the service request, the patient service can be scheduled immediately, and the GP can view the diagnostic report more quickly than under the current system. All relevant documentation can be filed either electronically or copied into subsequent reports.

Discussions with members of the Gold Coast's health services community revealed that the highest frequency of communications is between GPs and pathologists, radiologists and hospital administrators. Hence, it is these communication process that were targeted for trial in this pilot.

The primary focus of the pilot system was to effectively satisfy two concerns:

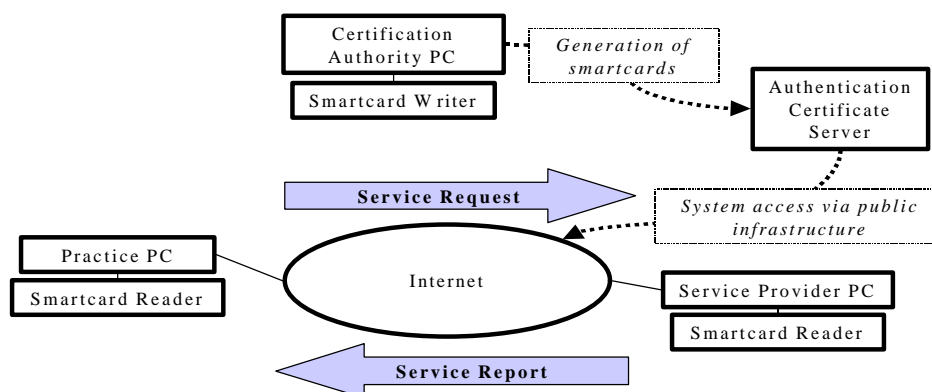
- privacy – the communication mechanism must be totally private without the possibility for anyone but the intended recipient reading a message;
- authentication – the recipients must be assured that all messages are authentic; ie, that they were definitely generated by an authorised sender.

2 Project Description

The MediSafe communications pilot used secure messaging technology for electronic communications within the health sector on the Gold Coast. It utilised cost-effective, generic email systems, familiar to users, and publicly available communications infrastructure, the Internet. Privacy was ensured by encryption of the message before transmission and authentication was provided via the use of a “trusted third-party”, public key infrastructure.

Each of the medical practices and service providers participating in the pilot was equipped with a smartcard reader to be attached to the PC they used for e-mail, and each authorised user within the organisation was issued a smartcard. Those tools enable participants to safely communicate with other members of the service network. Only authenticated users were able to read or send mail via the secure system.

MediSafe Communications operates over existing publicly available Internet infrastructure. Thus a service request originating from a GP will be immediately available to the addressed service provider. Only the addressed service provider will be able to read the request and the message’s authenticity will be guaranteed. Reports returned by the service provider immediately appear in the mailbox of the requesting GP and are only readable by the addressee. If desired, reports can be electronically filed by the GP using the same encryption key.



Participants in the pilot were required to provide verification of their credentials prior to being issued key-pairs that allowed access to the system. One portion of each key-pair was provided to participants on a smartcard storage device

(floppy diskettes were also used). Smartcards were selected for the trial as they appeared to provide the best fit for *security*, they are difficult to copy; *mobility*, since participating doctors may use several PCs during the course of the pilot, and *delegation*, to enable doctors to delegate authority to a trusted employee.

The other portion of the key pair was transferred to a certificate server accessible on the Internet. When a message was first received by one of the pilot participants the system automatically accessed the server and retrieved the sender's certificate containing the matching key-pair portions to decrypt and authenticate the message. The recipient then had the option of entering the senders name and certificate in their address book to avoid the lookup in the future.

2.1 Present Status

The pilot is operational with installations in the offices of 16 doctors and four other medical professionals.

The system is used primarily for doctor-to-doctor communication, particularly GP to specialist. When communication of patient details and reports from specialists are sent between participants the messages are encrypted as they traverse the Internet.

3 Structure of the Project

3.1 Project Team

There were two components to the project structure:

1. **Administrative:** the administrative activity migrated during the project:
 - a) commencement activity consisted of activities such as organising and advertising meetings of prospective participants, plus making appointments as necessary to arrange meetings with participants (for training etc.)
 - b) once the project was in a steady state, the administrative activity consisted of periodic communication with participants and the preparation of monthly newsletters.

The administrative position is an important position within the project due to the difficulty in contacting doctors. Generally, multiple phone calls are generally required to locate the correct person within a practice, and staff rotation often makes it difficult to contact specific individuals. When a person was dedicated to this activity, it improved the efficiency of the project significantly.

2. **Technical:** there were two technical “teams”:
 - a) Infrastructure team, which administered two components of the project:
 - *certificate server* – this function designed, installed and maintained the server that stores participants public keys;
 - *certification authority* – this activity installed and maintained the system that provided the generation and maintenance of participants’ certificates.
 - b) Installation team, which performed the on-site installation for participants.

3.2 Schedule

Time	Activity
April 1999	Project Commencement <ul style="list-style-type: none">➤ System planning and network design➤ Marketing➤ Issuing invitations to participate

- Selection of twenty eligible participants (involving current systems assessment)
 - Contractual arrangements for temporary use of donated system components
 - Delivery of donated system components
 - Appointment of certification authority staff member and training
- May 1999 Project Installation and Training
- Project management
 - Presentation and sign-up of potential participants (ACIT)
 - Presentation and sign-up of potential participants (Gold Coast Hospital)
 - System training preparation
- June 1999 System launch
- Certification of initial participants
 - 1st participant installation
 - Issue of smartcards to authorised users
- July – Aug 1999
- Installation of additional participants
 - Monitoring, maintenance and feedback
- November 1999 System Conclusion & Assessment
- Results measurement
 - Project assessment
 - Project report
-

3.3 Technical Overview

The MediSafe communication system is a trusted third party, public key infrastructure (PKI) system which assures users of the authenticity of other system users and encrypts messages for communication privacy.

PKI mandates the use of key pairs for participants in the system. For each participant a “key pair” is generated which uniquely identifies that participant.

The key pair consists of a private portion that must be safeguarded by the participant, and a public key, that may be distributed freely.

The key pair is issued to a participant by an independent third party which acts as a Certificate Authority by verifying the authenticity of that participant. MediSafe is a trusted third party solution and adheres to the accepted standards for secure communications technology in the electronic world (Appendix A).

The components of the PKI system used by the MediSafe Communication System are:

- electronic mail clients with a standard security add-on for Microsoft Outlook, (Siemens and Utimaco)
- an Certificate Server, accessible via the Internet, to store public keys for project participants (Nexor) ,and
- a Certificate Authority system to issue key pairs for each participant (Siemens).

3.3.1 E-mail Client

Two packages providing standard encryption and electronic signature capabilities were trialed as part of MediSafe:

- i. *TrustedMIME* from SIEMENS CRYPTOGRAPHIC GROUP, Ireland
- ii. *Sign 'N Crypt* from UTIMACO SECURE NETWORKING

Both of these packages support message encryption using a recipient's public key which can only be decrypted using a recipient's private key, and message authentication, using a digital signature based on a sender's private key. This authenticates the sender.

3.3.2 Certificate Server

The public keys of participants are held in a certificate which is stored in a Certificate Server accessible via the Internet. For the pilot, the X.509 V3 standard was used for certificates and a full X.500 directory was implemented for the server. It was decided to implement a full X.500 directory to build local knowledge in the operation of an X.500 directory (there is very little expertise in S.E. Queensland) and there was the potential to inter-operate with the HIC PKI infrastructure (this did not occur due to relaxation of the time-line for HIC system deployment).

Certificates are accessed from the mail client via an LDAP look-up over the Internet. This requires a user to either maintain a permanent connection to their ISP, or provide for quick access via a dial-up connection..

The address of the server is inserted into the registry of the client system and the Outlook client, when access to a public key is required, issues an LDAP call to the certificate server. The server performs the directory lookup and responds with the certificate for the requested individual.

3.3.3 Private Key Storage

The private key of the participant must be securely stored by the participant. The storage mechanism is defined by the personal security environment (PSE) selected by the user. There were two such environments used in the MediSafe trial:

SmartCards

SmartCards were selected for trial since they fit the medical office environment where in doctors typically don't send their own correspondence. The use of a Card allows a doctor to delegate his or her authority to send a communication to their practice manager, and then to take back that responsibility once the function is complete.

The private key and its associated CA information is stored on the SmartCard containing a computer chip. To add a second level of security, access to the key is protected by a personal information number (PIN) that must be entered in order to complete a "read" function.

File Storage

In some cases private keys were kept on a floppy diskette (and in one case on the hard disk of the client system). This option was used in the following situations:

- the doctor had multiple systems from which mail was sent and not all systems had smartcard readers;
- the doctor feared losing the smartcard (the floppy diskette was readily copyable).

3.4 System Operation

There are two components of the system's operation:

Authentication:

In order to use the system all prospective participants must first present their credentials to the authenticating party.

In Medisafe's situation this was accomplished during the system installation. The prospective participants of the system were authenticated as certified users by MediSafe acting as the "trusted third party". MediSafe then generated a key pair for each validated user that consisted of a public and a private key, and produced a certificate as proof of the authenticity of the key owner. These keys were generated by the MediSafe CA at the time of authentication.

Prior to installation, the public key was transferred to the MediSafe directory, which was accessible via the Internet. The directory also contained some general information about the users such as name, area of specialisation and e-mail address. The private key was stored on a SmartCard. Each user was issued with a smartcard containing their unique private key at the time of installation.

Operation

When a user wants to send a message to another user, the sender's private key is read from the SmartCard and used to digitally sign the message. The security utility searches the directory for the recipients certificate, encrypts the message into cipher text, checks the CA, who generated the certificate (which is also stored in the directory) and then sends the message to the recipient. If either the person specified, or the CA is not present in the Directory, the send operation fails.

When the recipient receives the message, he/she checks the signature and confirms that the message came from the right person. The SmartCard is then used to decrypt the body of the message into plain text. Because the recipient is the only person who has the SmartCard with his private key, there is no way any one else can read the message. And because he checks the signature of the message, he is assured that the message came from the right person.

Thus the whole system can work as a secure electronic mailing system. Take the following example-

Alice wants to send an email to Bob: both Alice and Bob have their own private keys and public keys. The public keys are kept on a database that both can access while each keep their private key safe on a SmartCard. Alice proceeds to write an email to Bob then she inserts her SmartCard into the reader attached to her computer. She selects the sign and the encrypt option available in TrustedMIME under her email program. TrustedMIME prompts Alice to enter her private PIN in order to access her private key. Once TrustedMIME has verified that the user is indeed Alice, it uses her private key to sign her email.

Next *TrustedMIME* looks up the recipient in Alice's Addressbook, in this case the recipient is Bob. The system then searches the common

directory available on the Internet, for Bob's public key. Once found, it uses Bob's public key to encrypt the email. Now the email is both signed and encrypted and can be sent to Bob. Along with the email, Alice's public key is also sent.

Upon receiving the email on Bob's computer, Bob's *TrustedMIME* will look at who has sent the email; in this case it is Alice. If Bob's *TrustedMIME* has not associated Alice's public key with Alice in his Addressbook, *TrustedMIME* will do so. In that way any further email from Alice can be processed more quickly.

Now since Alice has encrypted the email with Bob's public key only Bob's private key can decrypt it, this ensures that only Bob will be able to read Alice's email. To gain access to Bob's private key the system requires that Bob insert his SmartCard into the reader attached to his system. *TrustedMIME* then uses his private key to decrypt the email.

Finally, *TrustedMIME* uses Alice's public key to ensure that it really is Alice's digital signature. Once it has verified the signature, Bob can be certain that the message was sent by Alice.

4 System Description

4.1 Client

4.1.1 Hardware

Each participant was responsible for the provision of a satisfactory client computer system for the pilot. A minimum configuration was considered:

- Pentium processor
- 32 Mb RAM
- Modem and ISP service

4.1.2 Software

The software required on the client was MS Outlook. If this was not available then it was loaded on to the system.

The secure plug-in used for the trial was TrustedMIME from Siemens.

The lack of support for other mail clients was detrimental. One site preferred Pegasus, but agreed to use Outlook for the purposes of the pilot. Another site required Groupware mail. A formal request was made to Siemens to develop a Groupwise interface to TrustedMIME. Non-disclosure agreements were signed but a change in management at Siemens delayed the progress of this initiative.

4.2 Certificate Server

4.2.1 Hardware

The certificate server was:

- Pentium processor
- 64 Mb RAM
- Modem and permanent Internet connection

4.2.2 Software

The server operated an X.500 database for storage of the certificates. The software was provided by Nexor.

The operating system was WindowsNT Server Version 4. x

4.2.3 Interface to the Directory

Management and administration of the directory is a web browser interface. This utility comes with the *Messageware* directory software and forms part of the configuration when implemented. There are two parts to the interface:

- The Messageware Directory Manager (MDM)

- The Messageware Directory Browser (MDB)

Both components are required to operate and control the directory efficiently and to facilitate directory management from a remote location. These applications use *The Internet Information Server (IIS 4.0)* HTTP service for Windows NT.

Web-browser access is protected via username and password. Once accepted, a user is asked which directory they want to connect to. Once connected, a framed homepage is displayed with various options for data management. Mostly Options are self-explanatory.

There is also a command line interface for directory management that uses DISP commands for management tasks.

Access to the management facility was only granted to directory administrators. Future implementations would allow users to enter the directory and access limited functions, e. g. modify their own entries and read all entries.

4.3 Certificate Authority

4.3.1 Hardware

The certificate authority system was:

- Pentium 133
- 32Mb
- 2 smartcard readers

The CA system was kept in a locked office, only two personnel had the system password.

4.3.2 Software

The operating system was Windows 98. The system was dedicated to this task; i.e, no other applications were resident on the system and the unit was not on any network.

4.3.3 Participant Authentication

Authentication of participants is the process of verifying a person's credentials and issuing of a certificate validating that person as a user of the system. In the absence of an appropriate medical body, MediSafe performed both verification and authentication of the pilot participants. In this way MediSafe acted as the "trusted third party".

In the Certification/ Policy issued by MediSafe (Appendix E) there are three levels of possible certification. For the pilot, only the medium level was utilised.

Certification Policy

The three levels of certification used to classify different user categories according to their security needs are:

- *Strong-* for doctors who need patient data security and authentication for the ordering of services or HIC submissions. One Hundred identification points are required to validate a user at this level. This authentication procedure is expected to be performed by medical organisations with knowledge of their membership; e.g. the *Gold Coast Division of Medical Practitioners (GCDMP)*.
- *Medium-* for doctors and medical organisations who do not need strong authentication for activities such as HIC submissions, but who still need patient data security. Fifty points of identification are required to authenticate these participants. This authentication was done by MediSafe.
- *Basic-* for miscellaneous participants in the pilot such as suppliers without the need for encryption of patient data,. These people did not require any form of data security to be part of the pilot. 25 points of identification were required to verify their credentials and admit them as participants.

4.3.4 Authentication Procedure

Once a participant is authenticated, their key pair was generated and a certificate issued. The certificate was stored in the directory under the MediSafe organisational unit. The private key on the other hand was downloaded onto the Smartcard to be used by the participant.

Public Key

Public keys were stored in the form of an X.509 certificate that resided on an X.500 *Public Key Infrastructure (PKI)* database located in a so that it could be accessed via the Internet.

All clients have a public key and any client may retrieve another client's public key. The public key is used to encrypt email and verify digital signatures.

Private Key

A Personal Security Environment (PSE) file contains the subject's private key and certificate and, with the exception of SESAME PSEs, the CA's public key. The PSE resides in a smartcard and can only be accessed with a subject's private PIN. The PSE is used to digitally sign email and to decrypt incoming email.

5 Implementation

5.1 Infrastructure

The first issue was the placement of the certificate server. Since the Technical team was primarily made up of university students an approach was made to the University of Queensland to house the server at its main campus. Following some discussions it was agreed that the project would provide invaluable expertise to the students involved, particularly regarding the X.500 standard and directory installation issues that were likely.

The server was located in one of the research rooms in the Electrical Engineering building and was connected to the staff network. The router configuration for the network was modified to allow LDAP and HTTP traffic from the Internet.

The Certificate Authority software was installed on a PC at the offices of The Competitive Option on the Gold Coast. The unit was located in the accounting office and was not connected to the network.

5.2 Participant Installation

Installation at a participant site was accomplished as follows:

- 1) The Certificate Authority system was used to establish a key pair for the participant. The private key was written to the smartcard and the certificate (with the public key) was written out to a floppy disk.
- 2) The certificates were physically transferred to the certificate server and installed several days prior to software installation at the participant's practice. i
- 3) On the day of installation a technician travelled to the participant's office or surgery, verified the authenticity of the participant and completed the following procedure:
 - Installation of the smartcard and driver software;
 - Installation of Outlook (if not already on the system);
 - Installation of TrustedMIME;
 - Modification of the registry for LDAP call address;
 - Installation of the root certificate (from floppy or LDAP call to the directory);
 - Testing of the system operation.

5.3 Training

Training on a system typically occurred within two weeks of it's installation.

A submission was made to the Australian College of General Practice for inclusion of MediSafe training in the Continuing Medical Education (CME) program. The training for MediSafe was assessed by the college and a 2pt per hour classification was assigned to the training. The training program was to take 3 hours for a total of 6 points.

No doctor availed themselves of this training, preferring a quick 20 minute introduction to the system. Sometimes this training was provided to the receptionist of the practice manager, rather than the doctor.

It is noted that one of the areas in which the survey of participants indicated that improvement was needed was in MediSafe training.

5.4 Installation Difficulties

Significant difficulties were experienced in completing installations:

Administrative

Working at a technical level with medical practices is fraught with difficulties. Staff in most practices were unable to determine the operating system of their systems, they typically have no knowledge of the computer facilities beyond the practice management software they usually use. This meant that a technical person needed to visit the practice several days before the installation to verify the system operation, check that a comms port was available and determine the type of e-mail service being used.

Getting appointments to visit practices was time-consuming. Typically, visits needed to be approved by the contact doctor and this required leaving a message and an inevitable telephone tag.

Typically the contact doctor was the only one familiar with the use of e-mail, yet the training in MediSafe was given to receptionist or practice management staff. This required additional training and, since the use of e-mail was an addition to their duties, the system was infrequently used.

5.5 Technical Difficulties

One of the major impediments to the project was the poor state of systems and knowledge of systems in the medical practices into which the secure infrastructure was installed.

Of the twenty three installations, not one proceeded smoothly and as planned. A summary of the situations that were experienced is as follows:

- user software conflicts 1

- broken hardware 2
- system instability 5
- system configuration problem 5
- Windows 95 smartcard problem¹ 8

It was observed that, in general, systems in doctors offices were not adequately administered, nor was there appropriate documentation.

The overhead associated with rolling out devices in doctors offices is a significant logistics exercise.

¹ This was a technical problem with the smartcard reader driver. Whilst this was no fault of the doctor's system, it caused immense difficulty during the installation phase.

6 Pilot Evaluation

Initially the pilot was to be evaluated via a comparison between two questionnaires, one taken at the beginning of a participant's trial of the system and one taken after approximately three month's use of the system.

There are two reasons for the failure of this methodology:

- 1) Only two, out of 23 participants completed the pre-pilot questionnaire. Whilst some attempt to have completed forms returned was made, there was difficulty in determining who in a medical office should complete the questionnaire and in obtaining sufficient dedication of time from this person. The questionnaire survey form required the respondent to make some subjective evaluation of the types of communication used by the practice; some were reluctant to do this. In retrospect, the survey should have been conducted in-person at the time of installation and the post-survey conducted at an appropriate point after significant exposure to the system.
- 2) The pre-post Pilot questionnaire methodology anticipated a measurable alteration in the communications patterns for participating medical practitioners. For the reasons noted above that did not happen. The evaluation methodology was therefore flawed.

6.1 Telephone Survey

It was therefore determined to use another mechanism to evaluate the Pilot. An independent marketing communications organisation was engaged to undertake a telephone-based survey during which ten questions were asked:

6.1.1 Survey Results

The results were mixed, with only 7 respondents providing detailed responses. A synopsis of the findings is as follows:

1) With whom is there regular communication?

All respondents nominated the Gold Coast Hospital (or Tweed Hospital), and most also indicated Pathologists and Radiologists. Two mentioned specialists, one mentioned other GPs, but another advised that communication with other GPs was rare. One communicated regularly with the Division of GPs.

2) What is the primary method of communication?

Most respondents used standard letters, one used e-mail referrals to the Gold Coast Hospital

3) What are the primary frustrations with current communication methods?

Answers ranged from “most specialists are not computerised” to “the time it takes to get a response”. One respondent felt that patients being able to read a referral letter was a problem.

4) What is Email best suited for?

E-mail is definitely best suited for communication with pathology and radiology. One respondent indicated that it was not suitable for patient communication.

5) With whom has secure e-mail been used?

All respondents indicated that they had just sent trial messages to other participants.

6) What frustrations have been experienced with MediSafe?

Answers were quite varied. Smartcards were seen as an inconvenience by two respondents (see Question 7). Two respondents considered the system too complex to set-up. One mentioned that he was put off by the error messages he received on the screen.

7) Is the storage of private keys on smartcards suitable for medical practices?

The answers for this question were skewed by the size of the practice. Comments were that it was a great concept for a solo practice but two larger practices indicated that readers would be needed on all machines and that the smartcard was inconvenient in this scenario.

8) Will secure e-mail be a technology that medical practices will adopt?

Answers to this question revealed that medical practices would adopt the technology but that the “program” must fit the routine of the practice.

7 Findings

7.1 Operational Considerations

7.1.1 Smartcard

Smartcards are readily accepted by doctors for the storage of their private keys. It is the considered opinion of the project administrators that the Smartcard storage of keys best fits the operation of most medical practices.

Much correspondence is generated by the practice manager or clerical staff. The smartcard allows the doctor to review at correspondence prior to electronically signing it. Smartcards also allows a doctor to delegate his or her signing authority to a staff member for a specific routine operation, such as submission of MedClaims, and then enable them to take back that authority once the operation has been completed.

Whilst there was concern initially by some doctors that they would leave their smartcard at home, or otherwise mislay it, rendering secure communications impossible; this did not prove to be a problem during the course of the pilot. It is noted that the low usage of the system possibly made this less of an issue.

Some poor operational practices were observed:

- Whilst the smartcard fitted the application well (temporary delegation of signing authority), doctors tended to leave their smartcards in the cardreaders attached to their computers. Completion of the smartcard read operation requires the operator to type in their PIN number. Once this number is known, the security of the system is compromised.
- Once the smartcard has been inserted and the PIN has been entered, the operator may send authenticated mails until either the smartcard is removed from the reader, or the session is terminated. Failure of the doctor to be vigilant in the removal of their smartcard, safeguarding their signature, leaves the system open to fraudulent operation.

7.1.2 Communications

There is little doubt that electronic communication within the medical profession is increasing exponentially. The profession has been a heavy user of electronic communication in the area of pathology for many years. Currently most general practice offices on the Gold Coast communicate to the following services:

Service	Type	Encryption
Queensland Medical Laboratory	dial-up	PGP
MedNetwork (for Sullivan Nicolaides)	dial-up	PGP
South Coast Radiology	dial-up	PGP

Observation is that these services are generally installed on one PC in the office that is the “communications” PC. This unit is usually a workstation (in 2 instances it was the file server). Experience shows that once set-up, these services are reliable and generally cause the practice little trouble, although there is no update of security keys.

However, communication over the Internet is becoming more important. Two practices in the trial had permanent connections to the Internet, one was from a Linux server and one was a dedicated Internet server. In these practices two telephone lines were dedicated to data communications.

It is desirable that the profession determine the preferred mechanism for communication and requires service providers to adhere to a model that minimises the costs and complexity of GP systems.

7.1.3 Public Key Infrastructure

To date the profession has been an early adopter of secure communications. This has resulted in a large installation of dial-up services using PGP-based communication. For those services, security keys are set-up by the service provider when the service is installed. There is no mechanism for the update of the keys and so this rarely occurs. This is possibly not a concern for pathology since the service request accompanies the specimen, the PGP keys are therefore only providing encryption of the data transmission.

However, for Radiology services, although the service request may be made by e-mail, the patient must present with a valid (signed) instruction from the doctor. The secure communications is currently only providing encryption services.

Once the HIC alter their regulations to recognise digital signatures, the service request from the doctor will suffice for the radiologist and dependence on secure communications will rise. When this occurs current practice-based authentication will be insufficient. Doctors will then need to be able to order services individually with a valid certificate that the HIC can cross-reference to a valid provider number. It will also be important that the validity of the digital signature periodically expires and that immediate revocation of a signature be possible in the event of doctor de-registration.

MediSafe has demonstrated that PKI can fulfill these requirements of the medical profession and can adequately accommodate dynamically managed, key-pair issuance and validity. The features of PKI that enable better control of authentication are:

- the ability to assign a certificate validity period after which the certificate must be re-issued;
- the ability to dynamically revoke a certificate;
- the ability to re-issue a certificate in the instance of smartcard loss.

7.1.4 Dual Keys

MediSafe used single key operation. That meant that the same key used for signing an outgoing document was used for decrypting an incoming document. That meant that encrypted documents entering a practice could only be decrypted with the doctor's private key.

Dual key operation is therefore mandatory in the health sector. It is not acceptable to encrypt at the individual level since no-one would be able to read a patient's results if the doctor was away or left their smartcard at home. The medical profession therefore require both *personal* authentication and *practice-level* encryption.

7.1.5 Internet connection latency

Two locations maintained a permanent connection to the Internet. In this instance the operation of the system was quite acceptable. For instances when an encrypted mail was being sent to a new recipient, the length of time for the certificate look-up was excessive. Although the look-up time on the server was very good (usually less than ten seconds), when the commencement of an internet connection was required the look-up time was excessive (>30 seconds) even when a successful connection was made. In several instances a failure of the ISP connection was observed and the encrypted mail operation was aborted. The reasons for a failed connection were typically busy signals or unstable communication lines causing authentication errors. In three cases the ISP account set-up was incorrect, requiring additional visits to the doctor's offices to set-up the connection correctly.

It was soon found that off-line transfer of recipient certificates from the server to the sender's address book was necessary. This function was accommodated by the mail client software via the Certificate Manager feature.

7.2 Issues

Several issues arose during the trial:

- 1) The number of doctors using e-mail One of the basic tenets of the trial was low-impact on processes used in medical offices.
- 2) The trial determined not to incur significant expense in integrating the secure communications mechanism into the processes utilised in medical practices. The secure client utilised for the trial was an Outlook plug-in and it was deemed to be sufficient for the trial.

It was considered that requiring the sender to open the Outlook application would be satisfactory. This was not the case; it required the sender to enter into a convoluted process that detracted from using the communications mechanism on a regular basis. For instance, if the practice used Medical Spectrum, (MSS) practice management software, the following process was required:

- a) a referral letter would be written and saved within MSS and the software would either be exited or minimised;
- b) Outlook would be started on the communication PC and an e-mail generated;
- c) the referral letter would then be attached to the e-mail; this was accomplished by attaching it to the system on which MSS files are stored and locating the documents (MSS uses a combination of letters and numbers by which to file documents) that had been generated at the time in question. If several referral letters had been written at the same time, the order in which they had been generated needed to be known. The selection of the correct letter was usually verified by opening the attachment before the mail was sent.
- d) the mail was then sent and the secure mail screen would be presented. If the mail was being sent to another participant the mail could be “sealed” as well as “signed”. For sealed (encrypted) mail the system would expect to have the certificate of the recipient attached to an address book entry.

This process was too complicated for regular use. For widespread use of PKI to occur, the secure e-mail client must be integrated into the medical practice software to provide a seamless operation for medical office staff.

- 3) There is a need to include the Gold Coast Hospital’s Outpatient Department in the trial. One of the regular requests by participants was for details regarding outpatient activity for their patients. Having an electronic communication facility with the Outpatient unit would allow GPs to track a patient’s attendance for diagnostic tests and would facilitate electronic

receipt and storage of test reports. Whilst discussions were undertaken with the Outpatients Department concerned there were several issues which detracted from progress on this issue:

- a) the Gold Coast Hospital uses Novell Groupwise for their desktop environment and neither the TrustedMIME client from Siemens nor the Sign'nCrypt client from Utimaco currently support Groupwise².
 - b) At the time of the Pilot the Hospital was heavily involved in year 2000 activities which precluded any intensive involvement with another project.
- 4) It is important that the position of the Certification Authority within the medical field is well understood. Two entities declined to perform the CA function for the trial due to the potential liability associated with the performance of this function. The CA entity is a seminal component of secure electronic communications and will be a pivotal point in medical practice administration in the future. It is important to realise that the organisation that maintains the certificate server will populate the server with more than just certificate information. At the very minimum, medical specialities and e-mail addresses will be maintained and it is likely that the server operator will wish to expand the data repository to names, addresses and marketing information that can be used by the public to locate appropriate medical services. An additional source of revenue might therefore accrue from allowing doctors to purchase advertising on the site. That means that whoever owns the directory owns a basic data repository of medico-details: The medical fraternity needs to decide whether or not they wish to control this function.
- 5) A related issue is the need to establish a security policy for each Certificate Authority (Appendix E). It is likely that there will be separate CAs for GPs, radiologists, pharmacists, etc. and that participants with CAs will want to communicate with each other and have their certificates recognised when they access another discipline's web site. This means that CAs will need to establish trusted relationships between one another. To do this CAs will have to review each other's security policy to determine the mapping between security levels. Medical professionals should have input into the determination of the security policy governing the CA for their particular group.

² Siemens agreed to have MediSafe develop an API for Groupwise, non-disclosure agreements were signed but changes in management within Siemens delayed this activity.

8 Appendix A – System Configuration and Standards

Certificate Server	Windows NT	<p>Nexor X.500 Directory</p> <ul style="list-style-type: none"> - 1993 ITU X.500 and ISO 9594 compliant - fully support DAP & LDAP V3 access protocols
Certification Authority	Windows 98	<p>Siemens Trusted CA</p> <ul style="list-style-type: none"> - PKAF X.509 V1 & V3 Certificate and CRL profile compliant - RSA 512-2048 bit keys - PKCS-12, PEM & PGP PSE formats
Secure Mail Client	<p>Window 95, 98 or NT Workstation</p> <p>Outlook 97 or 98</p>	<p>Siemens TrustedMIME</p> <ul style="list-style-type: none"> - S/MIME compliant - Multiple Trust Model (self-signed, commercial & Local CAs) - X.509 V1 & V3 compliant
Smart Card	<p>Windows PC/SC</p> <p>CardOS</p>	<p>Siemens SLE44CR808 RSA format</p>

9 Appendix B- Installation Issues

Omitted for confidentiality purposes.

10 Appendix C – Project

10.1 Technical Team

The technical group involved consisted of five undergraduate students from the Computer Science and Electrical Engineering department of the University of Queensland. They were -

- i. *Kenneth Walpole* (final year Computer System Engineering student)
- ii. *Tony Troung* (final year Computer System Engineering student)
- iii. *Luis The* (third year Computer System Engineering student)
- iv. *Jonathon Sheelings* (third year Computer System Engineering student)
- v. *Shahriar Rahman* (third year Electrical Engineering student)

Each of the students had sufficient technical background to undertake a project of this complexity and the outcome was a fully operational, trusted third party system. The students performed most of the installations.

Graham Williamson of THE COMPETITIVE OPTION (TCO) was as the project leader and he coordinated most of the work. He is the person responsible for the whole project.

Julian Lawrence of SOFTWARE AGENCIES AUSTRALIA (SAA) in Melbourne acted as an active technical assistance to the project. He assisted the group members to solve many technical problems, which came up with the software supplied by SAA.

Peter McCully from Siemens Cryptographic Group based in Ireland and *Marcel Strung* of Utimaco Secure Networking in Denmark were the others who provided assistance with their software numerous times during the project.

Administration Team

Anita Wildman - provided administrative assistance for the commencement of the project and organised the prospective client presentations

Kylie Anstey - provided administrative support in the later portion of the project. This involved contacting participants to get the appropriate feedback and

arrange technical visits as appropriate. Kylie also maintained the monthly newsletters during the latter portion of the project.

Appendix D – Technical Infrastructure

The X500 Standard Internet Directory

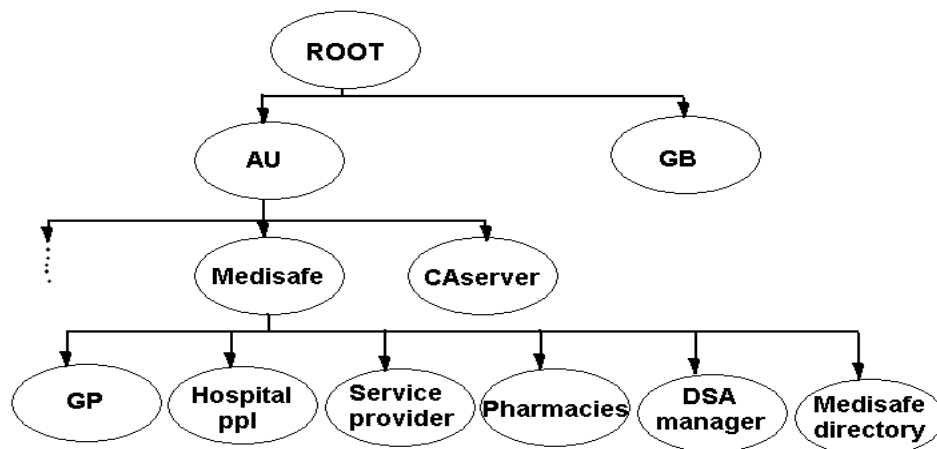
A set of systems produced to facilitate the interconnection of information processing systems to provide directory services together with the directory information which they hold, can be viewed as an integrated detailed listing of the participants. This is called a directory. The information held by the directory, collectively known as the *Directory Information Base (DIB)*, may be used to facilitate communication between, with or about objects of the trial, such as participating GP's. It can also be publicly available on the Internet.

The software used for this purpose is *Messageware 3.02* produced by NEXOR based in the UK and supplied by SAA in Australia. This is standard directory software and is currently running off the departmental network of the CSEE Department of UQ. It is located at the following address-

<http://130.102.97.61/> or <http://www.medi1.elec.uq.edu.au/>

The Directory Information Tree (DIT)

The Directory Information Tree (DIT) has been implemented using International X500 standards and fully complies with the standards X500, X501, X520 and X521. The central design of the DIT follows from the root directory down to the entries under *MediSafe* organisation. Under the country entry, the organisations appear and options are available to include the *GPnetwork* and other Health CAs willing to enter into a trust relationship and be added to the DIT at this organisational level. At the moment, *MediSafe* will act as the only current organisation in the directory. *MediSafe directory* holds the directory information and *DSA manager* is the administrative point of this directory.



Currently there are four divisions under the *MediSafe* organisation, which are 'General Practice', 'Hospital Personnel', 'Service Providers' and 'Pharmacies'. All the population of the directory will reside under one of these four units. Like the organisation, the units are also flexible to add.

The *CAServer* entry was moved up from under *MediSafe* to just under the country entry. This was primarily to conform to the standards. Secondly to allow other Certification of Authorities, e. g. HIC, to generate certificates acceptable by the directory, which can later interact with the directory and the messaging system. This will also avoid any possibility of object class violation within the directory. Because the directory will be accessed by the client software, it is also easier for the encryption software to check the authenticity of the public key by checking the *CAServer* at this level.

Object Classes of the Directory

Object classes used in this directory are-

- country
- organization
- certificationAuthority
- organizationalUnit and applicationProcess
- dSA and applicationProcess
- directory and applicationProcess
- person and organizationalPerson and strongAuthenticationUser and thornPerson and thornObject

Attribute Types in the Directory (while no Local OID)

Attribute types used for the `participants` entries of the directory are as follows.

- commonName
- surname
- givenName
- countryName
- title
- description
- streetAddress
- localityName
- postOfficeBox
- stateOrProvinceName
- postalCode

- ❑ telephoneNumber
- ❑ mobileNumber
- ❑ facsimileTelephoneNumber
- ❑ rfcMailbox
- ❑ uniqueIdentifier

For the `organization` or `organizationalUnit` object classes the following attributes are used.

- ❑ commonName
- ❑ organizationName
- ❑ organizationalUnitName
- ❑ description
- ❑ uniqueIdentifier

All standard syntax and methods are used to store information in the Directory. For more on these, please see the x500 standard references from ITU and Nexor documentation.

Email Clients

MediSafe Pilot anticipated usage of various common email packages for its clients. Initial considerations were given to the following packages-

- i. Microsoft Outlook*
- ii. Pegasus Mail*
- iii. Novell Groupwise*
- iv. Eudora Mail, and*
- v. Netscape Mail*

But at this point, *Microsoft Outlook* is the only client being used. This is due to limitations of secure email software. *Microsoft Outlook* is a standard personal email package widely used and works smoothly with both secure client software in use. Especially, it provides an excellent interface for the user with all necessary features of an email package, such a file attachment, carbon copy, etc.

Other packages are now under consideration for development to generate plug-ins of the secure client so that they work with other packages as well.

System Administration

System administration is an important activity to ensure sound operation of the system. Monitoring and maintenance of data and debugging of any problems with configuration must be done with care. This section outlines basic operation of the administrative part of the system.

Administrators

Currently the major part of the system administration involves maintaining and updating the *Messageware Directory*. The other part, although minor, is the *CA Server* and SmartCard administration. The rest of the system is installed at client sites and should only attract occasional update and check-ups. Currently assigned administrators for the directory are *Luis The* and *Shahriar Rahman*.

10.2 Common Operations in the Directory

Assuming no structural part of the DIT should change, common operations on the directory are-

- ❑ Browsing the directory
- ❑ Adding, modifying, and removing objects
- ❑ Access Control

Browsing the directory is simple in both *MDM* and *DISH*. In *DISH*, follow the following procedure-

- At command prompt type `<dish>`
- When bound to the Directory, type `<ls>` or `<list>` or `<dir>` to list entries.
- When the entries appear with their entry numbers, bind as a DSA Manager by typing `bin -sim <entry number (DSA Manager)>` e. g. `bin -sim 5` if entry number is 5.
- Enter the valid password. This should let you in.
- Now browse through the directory tree.
 - Use `mov <entry number>` to move within directory
 - Use `sh <entry number>` to display details for an entry

To add an object type add `-objectclass "cn=<objectName>" -draft <draftFile>`.

Make sure to have a valid `draftFile` in the same directory from which Dish is invoked. We recommend using a `draftFile`, which can be obtained when modifying an object at the same level. For example, use the `draftFile` to add an `organizationalPerson`, which is obtained when modifying another current `organizationalPerson` in the Directory. To obtain this file, simply type the modify command (given below) and copy the contents of the `draftFile` to another file and call it the `newDraftFile`.

To modify an object type- `mod <entry number>` or `modify <entry number>` and answer No to the question.

To remove an object type- `delete <entry number>` or `remove <entry number>`

To move an object from current level type-
`modifydn <entry number> -superior <entry number>`

Access controls utilities are currently under investigation.

Other Directory Administrative Activities

Other activities to administer the Directory are updating the *Certificates Revocation List (CRL)*, the software and patches, keeping regular backups, monitoring Directory accesses and hits, etc.

CRL is a list of certificates subject to revocation, which might have resulted from non-use, or lost card, or forgery. This list should be manually updated in the Directory, which is actually accessed by the secure client when sending a mail. This is to make sure that the recipient is still current in the system. This is a procedure using LDAP query and the secure client should handle it automatically. However, at the current time, *TrustedMIME* is not able to check an Internet Directory for CRL, although it can do so on a local CRL database (this utility should come up later in the year).

So the following policy has been adopted to deal with the issue. This is to create a CRL database on client's local machine. *TrustedMIME* supports this scheme and it can successfully check a CRL located on a local machine when sending each message. Now the obvious question is how to update this list every time a new certificate is added. It has been

decided that the administrators will update the Directory every-time a new entry is made to CRL and send a copy of the list to each of the system users. Users will then replace the old list with the new one.

This scheme is only temporary and will be replaced as soon as *TrustedMIME* becomes capable of the LDAP search for CRL on the Directory.

- Software update and patches will be handled by the administrators. Most of the other activities are simple updates and changes in various configurations. These will be implemented as need arises.

SmartCard PIN Administration

The SmartCard is protected by two pins which allow certain access to the card. The first is the administrator the second is the user PIN.

The administrator PIN is required to put a private key on a SmartCard. The PIN is set by the manufacturer and cannot be changed by the sample test program. Currently (July 1999) the UTIMACO Administrator default PIN is: 87654321. Please note that this PIN will not allow users to send email only by putting private keys on the SmartCard. This PIN must be changed before using the SmartCard. Contact the manufacturer for more information.

User SmartCard PIN can be changed by using the sample C++ program provided by the *CardOS C++ SDK* as follows.

1. Go to *Start -> Programs -> CardOS Service Provider SDK -> C++ Sample*
2. Select *Load the COM Vendor Wrapper* and click *Perform Request* (perform req.)
3. Select *Attach OwnLCC* and perform request
4. Select *ChangeCode* and perform request
5. Enter in the user old code (default is 12345678 for *SIEMENS* SmartCard, but contact your provider if default PIN does not work)
6. Enter in new code.

Certificate of Authority (CA) Administration

The CA typically resides on a portable machine, such as a Notebook computer. Only one CA was used by MediSafe and this was administered by The Competitive Option. It was maintained by a responsible person and was located in a secure location. In this way the CA is completely separated from rest of the system, and its protection against compromise over the network.

Client System Installation

Client system installation involves installing the Email package, secure Email client and the SmartCard reader with a SmartCard attached to it.

Email packages

Installing email packages are similar to any other Microsoft products and need only to follow the on-line instructions.

Security software

Follow the simple procedure described below.

1. Run *TrustedMIME.exe*
2. Follow on screen instruction.
3. When running Outlook for the first time *TrustedMIME* will ask for how PSE will be read.
4. Choose SmartCard.
5. In Outlook from the *TrustedMIME* menu choose

Certificate Transfer->Import a Certificate

6. Import in the *CA Cross Certificate* which should be provided by your CA Trust Center.
7. Run *regedit* from windows *Run* command line.
8. Go to *HKEY_LOCAL_MACHINE -> Software -> SSE -> TrustedCMF -> Catalogs -> Default*
9. Right click *LDAP Provider* and select modify.
10. Change the setting to-

```
"C:\ <PATH OF SYSTEM DIRECTORY>\CMPDirectory.dll,  
1,  
<LOCATION OF DIRECTORY>; <PORT NUMBER>;;  
(mail=%NAME%); o=ORGANISATION,c=COUNTRY;0"
```

The items in '<>' are replaced with your local information. For

example, <PATH ...> would be where your operating system's system directory resides (*Windows '95* it would be simply `C:\WINDOWS\SYSTEM\`). `LOCATION` => Directory location (usually the name of the computer it reside on if on network or IP address). `PORT NUMBER` => is defaults to 389, but may change if any other Port is used for *LDAP* search.

`ORGRANISATION` => your organisation, must match data, that is in the Directory, `COUNTRY` => the country must match what is in the Directory.

SmartCard Reader Installation

Following are the instructions for SmartCard Reader installation.

1. Run *Scbase* to install base files from disk 2. Choose 'NO' to rebooting.
2. Run *Sclib* to update the drivers from disk 2. Reset the computer.
3. Run Setup from disk 1.
4. If running on *windows95/98* use the detect new hardware feature from *Control Panel* and follow it through.
5. If asked for the directory of the driver (on *Windows NT*), point to disk I.
6. Run the *CardOS* setup
7. Follow on screen instruction, for the serial number enter in any word or digits as currently this software is free for the project.

CA System installation

Make sure you have the files *setupCA.W02*, *setupCA.W03*, *setupCA.W04*, *setupCA.W05* and *setupCA.exe*.

1. Run *setupCA.exe*
2. Follow on-screen instructions
3. Choose typical installation
4. When finished run *TrustedCA*
5. In the *Tools* -> *Customize* menu tick the *PC/SC SmartCard* option.
6. Under *Certification* menu choose *Generate CA*
7. Enter in the name of your CA
8. Choose *CA keylength*, usually *1024* for medium or *2048* for high security.
9. Enter in random characters for the *SEED*.

Appendix E - Certificate Policy

MediSafe Secure Email Pilot

Certification Policy

Revision 1.0

1 Introduction

This document defines the certification policy associated with the MediSafe secure e-mail pilot.

MediSafe is based on a trusted third party, public key infrastructure model for the management and use of both encryption and ensuring (digital signatures) electronic messages.

This policy adheres to the IETF X.509 framework.

1.1 Definitions

Certificate	an electronic record certifying the identity of its owner signed by the Certification Authority which issued it
Certification Authority	a trusted body that authenticates a user and issues a certificate attesting to the identity of the user.
Certificate Policy	the definition of the applicability of a certificate to its use within a particular community or class of application with specific security requirements
Certificate Revocation List	the list of digital signatures that are no longer valid
Digital Signature	an electronic record appended to a message that allows recipients to be assured of the originator's identity
Key	a variable length value that allows for the electronic deciphering of a message or message attachment
Non-repudiation	the ability of a recipient of a document to rely on the validity and irrevocability of that document
Private Key	a key that is stored and protected by the owner as the value necessary for the production of a secure message
Public Key	the key that is stored in a publicly accessible place to allow for the encryption of originating messages and authentication of received message, it is typically stored on a certificate server accessible to the pertinent network of users

2 Policy Specification

2.1 Purpose of Issue

The issuance of key pairs to MediSafe participants is for the purpose of:

- authentication for such requirements as the request of medical procedures and the submission of claims for financial remuneration;
- encryption of private communications including patient file details.

The primary use of MediSafe key pairs is for secure e-mail using the S/MIME protocols. The same keys will be used in some cases for SSL web browser security.

2.2 Key Management

Separate keys will be utilised for encryption and authentication. Two modes of operation will be supported:

- **Individual:** both encryption and authentication private keys will be stored on a smartcard issued to the participant at the time of authentication;
- **Practice:** the authentication private key will be kept on the individual's smartcard, the encryption private key will be stored on the computer system at the practice, protected by a PIN. This enables the viewing of encrypted documents by anyone with a valid PIN.

Note: in either scenario authentication keys will be associated with individual participants or functions and will be maintained on smartcards in the individual's possession. No authenticated e-mail can be sent without the presentation of a valid private key.

2.3 Key Strength

The following key strengths will be used:

- Encryption Key pair 128Bit
- Signature key pair modulus 1024

2.4 Participation Levels

MediSafe will maintain three levels of user authentication:

2.4.1 Basic

The basic level is for all participants of MediSafe that do not fall into the medium or high categories. Users at the basic level will demonstrate a need for secure

communication within the health profession, but are not providing medical services to the public and will not normally be transferring individual patient-care information.

2.4.2 Medium

Participants in the medium level will be medical practitioners, i.e. persons providing medical service to the public, who have no need to be authenticated for submission of claims to the HIC.

2.4.3 High

Participants at the high level are those practitioners providing health care to the public and submitting to the HIC or participating on the GPNetwork.

2.5 Certification Requirements

2.5.1 Basic

Validation Type	Authentication Entity	Certificate Authority
Proof of name and address - one Secondary item	MediSafe Administration	MediSafe

2.5.2 Medium

Validation Type	Authentication Entity	Certificate Authority
Proof of name and address proof of professional qualifications 50 point check	MediSafe Administration	MediSafe

2.5.3 High

Validation Type	Authentication Entity	Certificate Authority
Proof of name and address proof of professional qualifications	HIC Regional Office personnel Gold Coast Division of	HIC MediSafe

qualifications	General Practice	
Health Provider number		
100 point check		

3 Operational Requirements

3.1 CA/RA Administration

Multiple Certification Authorities will be maintained as follows:

Medium and Basic levels	MediSafe
High level	MediSafe
High Level	HIC & MediSafe

Each CA will have a mutual trust relationship with the other CA. The HIC will operate multiple Registration Authorities. The requirements for a trust relationship between HIC and MediSafe will be explored during the trial with the other CAs.

3.2 CRL Administration

Two revocation list options will be trialled:

3.2.1 On-line Certification Server Protocol (OCSP)

OCSP will be the primary method of certificate revocation. In this scenario the CRL file will be sent to participants on an as-required basis. On encryption of an e-mail for a participant for whom a certificate is held, the revocation list will be checked to ensure the certificate has not been revoked. For encrypted mails for a new recipient, the certificate server will be accessed. For received mail the local CRL list will be checked prior to authenticating a message to ensure that the originator's certificate has not been revoked.

3.2.2 Certificate Revocation List (CRL).

A small number of participants will be configured to use CRLs. In this scenario the CRL on the certificate server will be accessed whenever a mail is to be encrypted or a received mail is to be authenticated.

The certificate life will be one week.

Replication of the CRL to multiple sites will be tested.

4 Security Controls

4.1 Physical

The system upon which the Certification Authority software operates will be stored in a locked area to which there is no access to unauthorised personnel. The CA software will be protected by a PIN.

Access to the system and knowledge of the PIN will be given to two persons employed by the CA organisation.

4.2 Technical

The master password providing access to the CA software will be at least eight characters in length.

The system upon which the CA software operates will not be on network. Periodic connection on a dial-up basis is permitted; certificates will normally be transported to the certificate server via floppy disk.

Addendum – Project Financials

Please refer to report addendum.