NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

PUBLIC KEY INFRASTRUCTURE UTILIZATION TO PROVIDE AN ADDED LEVEL OF AUTHENTICITY TO TRANSMITTED DATA

by

Jason B. Blackmon

March 2010

Thesis Advisor:	Rex Buddenberg
Second Reader:	Thomas Housel

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2010	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Public Key Infrastructure Utilization to Provide an Added Level of Authenticity to Transmitted Data		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Blackmon, Jason B.			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

Information Systems have a need for a level of security to protect the data when being transmitted from one user to another. This thesis points out a method of protecting data utilizing an end-to-end level of security. The idea is grounded in looking at the advantages provided with the Public Key Infrastructure applied to add a level of authenticity to the data on the receiving end of a transmission. The focus of this thesis is protecting data transmitted across the Internet via e-mail using end-to-end security.

This thesis proves that applying PKI as data protection to the Information System Application Layer can be used to provide secure end-to-end connections and e-mail is the tool chosen for this thesis to accomplish this goal. The scope of this thesis is to identify authentic and/or confidential communication of data across an Internetwork. The variables to discuss are the ability to digitally sign and secure the data with the digital signature, establishing a connection to an unregulated network, and confirmation of delivery of the data by an alternate user computer. This thesis will focus on using a public key signature point out how this provides authenticity, with a bonus inclusion of the integrity.

14. SUBJECT TERMS Public Key Infrastructure, User Agent, Authenticity, Confidentiality, Integrity			**15. NUMBER OF PAGES** 65
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

PUBLIC KEY INFRASTRUCTURE UTILIZATION TO PROVIDE AN ADDED LEVEL OF AUTHENTICITY TO TRANSMITTED DATA

Jason B. Blackmon
Lieutenant, United States Navy
B.S., United States Naval Academy, 2002

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
March 2010

Author: Jason B. Blackmon

Approved by: Rex Buddenberg
Thesis Advisor

Thomas Housel
Second Reader

Dan C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Information Systems have a need for a level of security to protect the data when being transmitted from one user to another. This thesis points out a method of protecting data utilizing an end-to-end level of security. The idea is grounded in looking at the advantages provided with the Public Key Infrastructure applied to add a level of authenticity to the data on the receiving end of a transmission. The focus of this thesis is protecting data transmitted across the Internet via e-mail using end-to-end security.

This thesis proves that applying PKI as data protection to the Information System Application Layer can be used to provide secure end-to-end connections and e-mail is the tool chosen for this thesis to accomplish this goal. The scope of this thesis is to identify authentic and/or confidential communication of data across an Internetwork. The variables to discuss are the ability to digitally sign and secure the data with the digital signature, establishing a connection to an unregulated network, and confirmation of delivery of the data by an alternate user computer. This thesis will focus on using a public key signature point out how this provides authenticity, with a bonus inclusion of the integrity.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION AND PROBLEM STATEMENT....1
- A. INTRODUCTION....1
- B. THESIS GOAL....3
- C. SECURITY DEFINITIONS....3
- D. RESEARCH QUESTIONS....4
- E. MEASURABLE SUCCESS GOAL....4
- F. THESIS QUESTIONS....5
- G. BACKGROUND FOR STUDY....5
- H. THESIS ORGANIZATION....6

II. RELATED WORK....7
- A. INFORMATION TRANSMISSION....7
- B. SECURING DATA....7
- C. USING PKI....8
- D. THE TEST UNDERSTANDING....11

III. HOW TRANSMISSION WORKS IN THIS THESIS....13
- A. E-MAIL....13

IV. RESEARCH METHODOLOGY....15
- A. PRACTICAL USAGE....15
- B. DESIGN AND IMPLEMENTATION....15
- C. DEPLOYMENT AND TESTING....19
- D. SETUP....20
- E. E-MAIL SETUP....20
- F. SENDING/RECEIVING E-MAIL MESSAGES....25
- G. THE TEST....34

V. FINDINGS....39

VI. CONCLUSIONS AND FUTURE DEVELOPMENTS....45
- A. CONCLUSIONS....45
- B. FUTURE DEVELOPMENTS....45

LIST OF REFERENCES....47

INITIAL DISTRIBUTION LIST....49

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. Depiction of a Root Certificate Authority (From Newman, 2001).....9
Figure 2. Depiction of a Mesh Certificate Authority (From Newman, 2001).....9
Figure 3. Testing Example Diagram 16
Figure 4. GPS Data Flow Chart.....18
Figure 5. Screen Shot of Google Gmail Account Registration. (From Google, 2009)...21
Figure 6. Screen Capture of the New Address is to be Added to the Microsoft Office Account List. (From Microsoft, 2009).....22
Figure 7. The IMAP server type is selected for real-time updates of the messaged information that will pass from the Outlook program on the laptop to the receiving address. (From Microsoft, 2009).....23
Figure 8. The account is now put into Outlook and can be acknowledged to synchronize with Google mail when running. (From Microsoft, 2009) 24
Figure 9. Final registration setup screen. After the accounts are approved, the Finish button allows for the finalization of the account to be added for use with Outlook. (From Microsoft, 2009) 25
Figure 10. MacroMaker file setup screen. (From MacroMaker, 2009) 28
Figure 11. Timer setup for accounts. (From Microsoft, 2009).....31
Figure 12. Verizon modem software connection screen display. (From Verizon Wireless, 2009) 35
Figure 13. Verizon VZAccess Manager specifications. (From Verizon Wireless, 2009).36

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ARM	ARM – Software at http://members.ij.net/anthonymathews/macromaker.htm
ARPANET	Advanced Research Projects Agency Network – the world's first operational packet switching network, and the predecessor of the contemporary global Internet.
CA	Certification Authority – An entity that issues digital certificates and vouches for the binding between the data items in a certificate.
CAC	Common Access Card
DoD	Department of Defense
E-MAIL	Electronic Mail – a method of exchanging digital messages.
EVDO	Evolution-Data Optimized or Evolution-Data only – a telecommunications standard for the wireless transmission of data through radio signals, typically for broadband Internet access.
Gmail	Google Mail – E-mail provided by Google.
GPS	Global Positioning System
ID	Identification
IMAP	Internet Message Access Protocol – prevalent Internet standard protocols for e-mail retrieval.
LAN	Local Area Network – a computer network covering a small physical area.
MIME	Multipurpose Internet Mail Extension – An Internet protocol [R2045] that enhances the basic format of Internet electronic mail messages [R0822] to be able to use character sets other than US-ASCII for textual headers and text content, and to carry non-textual and multi-part content.
NPS	Naval Postgraduate School
OS	Operating System software (programs and data) that provides an interface between the hardware and other software
PKI	Public Key Infrastructure – A system of Certificate Authorities that perform some set of certificate management, archive management, key management, and token management functions for a community of users in an application of asymmetric cryptography.
POP	Post Office Protocol – an application-layer Internet standard protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection.

RFC	Request for CommentsOne of the documents in the archival series that is the official channel for publications of the Internet Engineering Steering Group, the Internet Architecture Board, and the Internet community in general. [R2026, R2223]
RSA	named for Rivest, Shamir and Adleman, the group who first described this algorithm – an algorithm for public-key cryptography known to be suitable for signing and encryption.
SAFECOM	Safety Communications – a communications program of the Department of Homeland Security.
S/MIME	Secure/Multipurpose Internet Mail Extensions, an Internet protocol [R2633] to provide encryption and digital signatures for Internet mail messages.
SMTP	Simple Mail Transfer Protocol – A TCP-based, application-layer, Internet Standard protocol [R0821] for moving electronic mail messages from one computer to another.
VPN	Virtual Private Network – A restricted-use, logical computer network that is constructed from the system resources of a relatively public, physical network (such as the Internet), often by using encryption and often by tunneling links of the virtual network across the real network.
WIFI	Wireless Fidelity – a trademark of the Wi-Fi Alliance that manufacturers may use to brand certified products that belong to a class of wireless local area network (WLAN) devices based on the IEEE 802.11 standards.
XML	Extensible Markup Language – a set of rules for encoding documents electronically.

EXECUTIVE SUMMARY

Information Systems have a need for a level of security to protect data during transmission from one user to another. This thesis points out a method of protecting data utilizing an end-to-end level of security. The idea is grounded in looking at the advantages provided with the Public Key Infrastructure applied to add a level of authenticity to the data on the receiving end of a transmission. The focus of this thesis is protecting data transmitted across the Internet via e-mail using end-to-end security.

Public Safety staffs (federal, state and local law enforcement, as well as fire and emergency medical service personnel) are currently unable to communicate or send information to each other over the Internet using wireless technology efficiently during crisis situations. During times of crisis, public safety organizations need the ability to transfer data/information, which includes the location of assets, to a central command organization for strategic purposes in an efficient manner. For purposes of this thesis, information security via authentication is of prime importance.

This thesis proves that applying PKI as data protection to the Information System Application Layer can be used to provide secure end-to-end connections and e-mail is the tool chosen for this thesis to accomplish this goal. The scope of this thesis is to identify authentic and/or confidential communication of data across an Internetwork. The variables to discuss are the ability to digitally sign and secure the data with the digital signature, establishing a connection to an unregulated network, and confirmation of delivery of the data by an alternate user computer.

This thesis will focus on using a public key signature point out how this provides authenticity, with a bonus inclusion of the integrity. When the information is received, how the information was compromised or the legitimacy of the source is not a concern because the design will prevent receipt of the message.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION AND PROBLEM STATEMENT

A. INTRODUCTION

Information Systems have a need for a level of security to protect the data during transmission from one user to another. This thesis intends to point out a method of protecting data utilizing an end-to-end level of security. The idea is grounded in looking at the advantages provided with the Public Key Infrastructure (PKI) applied to add a level of authenticity to the data on the receiving end of a transmission. Protecting data transmitted across the Internet via e-mail using end-to-end security is the focus of this thesis.

Public Safety staffs (federal, state and local law enforcement, as well as fire and emergency medical service personnel) currently are unable to communicate or send information efficiently during crisis situations over the Internet using wireless technology. While there are many reasons for the inability to communicate efficiently, one study cites turf battles, lack of funding and political will for the development of shared radio communications systems, lack of common standards, and shortfalls in spectrum available for public safety as reasons for this lack of ability to share (SAFECOM Baseline Survey, 2006) and this idea is backed up by various papers and studies (Schumacher, 2009; Miller, Granato, Feuerstein & Ruffino, 2005). During times of crisis, public safety organizations need the ability to transfer data/information, which includes the location of assets, to a central command organization for strategic purposes in an efficient manner. For purposes of this thesis, information security via authentication is of prime importance.

Since our most recent national attack requiring cross communications between law enforcement, fire and emergency medical services personnel on September 11, 2001, several committees, working groups, and standards committees have been formed to study how information sharing can take place. SAFECOM has taken the lead in setting the standards and creating a snapshot of the capacity and use of interoperability for first responders. Unfortunately, SAFECOM has maintained a focus only on voice

communications interoperability. SAFECOM's interoperability focus would be quite beneficial if there were more of a focus on the Information System interoperability because more end systems would be better able to work together regardless of the type of communication system; either voice or data communication systems. The intent of this thesis is to examine one tool that is available for remote assets to use when communicating with crises command centers.

A review of the basic use of computers and application systems is important before engaging in the discussion of security of information transmission among public safety personnel. This thesis will start with pointing out computer and operating system exchange, components of the Information System interoperability.

Harris (2005) provides the history and overview of computer systems, applications, and security. The book outlines the complications of systems security because: "Applications and computer systems are usually developed for functionality first, not security first. To get the best of both worlds, security and functionality would have to be designed and developed at the same time" (p. 809). Therefore, a system developer needs to include security requirements and functional requirements to ensure the computer system can safely perform the tasks it is created to accomplish. Likewise, a computer system must be developed with the ability to be monitored while functioning as designed.

Information Systems need to communicate freely, but they also have the need for sense, decide, and act nodes that can act independently while being monitored. There also exists a need for the system to maintain a level of security. Until recently, just providing perimeter devices, such as firewalls, intrusion detection systems (IDSs), sensors, and vulnerability scanners, was considered enough protection. Harris (2005) also identifies reasons for supporting such types of security ideas, but the one discussed in this thesis is Public Key Infrastructure and how it relates to authenticity because, "In the past, it was not crucial to implement security during the software development stages; thus, many programmers do not practice these procedures" (p. 810).

Therefore, the aforementioned challenges force a designer to ask, "Where is the best place to apply the security feature?" rather than, "How can this whole infrastructure remain protected?" In the development of an information system, Harris (2005) points out: "Security is most effective if it is planned and managed throughout the life cycle of a system or application, versus applying a third-party package as a front end at the end after the development. Many security risks, analyses, and events occur during a product's lifetime, and these issues should be dealt with from the initial planning stage and continue through the design, coding, implementation, and operational stages" (p.832). Although software development is not the central focus of this study, it is an important feature to consider when a system or application is developed. This ensures that all applications will be compatible.

B. THESIS GOAL

The goal of this thesis is to prove that applying PKI as data protection to the Information System Application Layer can provide secure end-to-end connections, and e-mail is the tool chosen for this thesis to accomplish this goal.

The use of PKI can be applied at any level but that is beyond the scope of this thesis. The focus of this thesis is end-to-end security using PKI as a solution to the authenticity security issue.

C. SECURITY DEFINITIONS

In order to identify what concepts are being described, it is important to know what the key terms are being discussed. The following definitions are taken from RFC2828, which provides a foundation for information systems terms usage:

- authenticity: The property of being genuine, verifiable and trustworthy.
- confidentiality: information is not made available or disclosed to unauthorized individuals.
- integrity: The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.

This thesis will focus on using a public key signature point out how this provides authenticity, with a bonus inclusion of the integrity. When the information is received, how the information was compromised or the legitimacy of the source is not a concern because the design will prevent receipt of the message.

D. RESEARCH QUESTIONS

The scope of this thesis is to identify authentic and/or confidential communication of data across an Internetwork. The variables to discuss are the ability to digitally sign and secure the data with the digital signature, establishing a connection to an unregulated network, and confirmation of delivery of the data by an alternate user computer.

Beyond the scope of this thesis are the communications interoperability, networking technology, and data fusion into information. All of these are important features, but beyond the scope of this thesis.

Information communicated over the Internet can be by voice or data communications. Either can be sent across the Internet via Internet Protocol packet. The assertion made in the thesis can be applied to either communication. This thesis only concerns itself with the end-to-end securing of the data over the Internet.

E. MEASURABLE SUCCESS GOAL

The method designed for this thesis demonstrates the ability to securely transmit information using existing wireless devices and technology, thus protecting data from being exposed while being transmitted from sender to receiver. This process allows for the data to have an end-to-end level of security. Therefore, the success metric is achieved by identifying where the data is no longer in a protected form.

F. THESIS QUESTIONS

The questions to be addressed are:

1. Can First Responders use PKI to provide security for information that comes from a sensing tool that is transmitted across the Internet via wireless means?
2. Does it have value?
3. If it has value, then to whom?

G. BACKGROUND FOR STUDY

For some years, NPS Information Technology Management Department personnel engaged in communication with the Monterey County Law Enforcement and Fire Department to discuss the use of Information Technology tools to improve the efficiency/effectiveness of their responses to crisis management situations. Rex Buddenberg presented an overview of these conversations, as well as previous research projects undertaken for this partnership to our class. His previous work contributed to the idea to study how one tool, a tracking system (sensor), would be advantageous to the local Monterey fire department, a public safety organization and the testers of the theory proposed in the thesis.

Common security approaches usually incorporate the security of the sensors used on the network by creating a completely separate network. This approach is not the most efficient when the same desired result can be accomplished by providing end-to-end security over the existing Internet utilizing proper security protocols. In the case of this thesis, the idea that end-to-end security can be accomplished is presented with the use of PKI.

H. THESIS ORGANIZATION

Chapter I provides a brief overview of the study's purpose and a listing of the original set of study questions for the thesis. Chapter II reviews the literature delineating the extent and practicality of using such a component in the development of the architecture of a network. This will provide the basis for why using PKI in development of the network architecture is important from various security points of view. Chapter III details the research methodology used in the study. Chapter IV provides the findings of the study and explains how everything works together. Chapter V provides conclusions and recommendations for use of this study for future research.

II. RELATED WORK

A. INFORMATION TRANSMISSION

Traditionally, information was transferred orally from person to person or from one person to many via public meetings or settings. As society expanded, and with the advent of mail service, printed/written words were used to communicate out to individuals or the masses. Information that was confidential in nature was sent via private messenger or some secure means. Sometimes, upon delivery of that information, the messenger was killed. This act assured the sender that the message and its contents remained confidential (i.e., dead men tell no tales).

Today, information in our society is transmitted in many forms, including the use of large and small electronic devices. Communication transmissions have evolved from words on paper to electrons passing data from person to person, device to device. The Internet was developed for this purpose. Initially, security was not an issue because only those with reception devices could obtain the messages. The first users of the Internet were agencies within the DoD (ARPANET). They used it as a means of transmitting data from one point to another. With technological improvements and the availability of electronic transmission to anyone with the hardware to transmit (via landlines or wirelessly), security of transmissions via the Internet has become very important.

B. SECURING DATA

A discussion of ways to secure data is necessary before moving forward.

1. **Physical security**. Access can be limited to electronic information by physically separating the information from any other interested party via barriers such as locks, walls and doors. Information can also be protected by other safety mechanisms such as fire extinguishers and alarm devices to indicate if the information is in possible danger.

2. **Network security**. The information can receive an individual section of protection as it passes down the layers of information structuring. These layers include the Application Layer, Transport Layer, Network Layer, and Data Link Layer. Each step can provide another layer of electronic security while information travels on the designated network.

For the purposes of this thesis, an Application Layer of security is applied over the network and all other forms of security are ignored.

C. USING PKI

PKI is an infrastructure for providing key pairs. A key pair provides only the user with a private key and authentically advertises the user's public key. PKI utilizes RSA; which allows the PKI to be practically useful. RSA (named for the inventors, Rivest, Shamir and Adelman) is a cryptography procedure that capitalizes on the large prime factorial problem and allows for the separation of keys into public and private (the asymmetric part) ones. RSA allows the user to digitally sign an object with a private key and anyone to test the validity of that signature with your public key. PKI provides the proper keys in the appropriate places to do RSA, thereby guaranteeing authenticity is always achieved through a required digital signature,

A case where emergency services require only authenticity is in own position reporting. Confidentiality may be an issue for some police services trying to maintain a low profile; otherwise, just maintaining the authenticity remains the priority. In order to uphold this concept, the user has to have the PKI to hold up the RSA digital signature process. The same PKI holds up the encryption process, so that requirement delivers for free.

Determining how to develop the network infrastructure consisting of a trusted environment can be very confusing. The network infrastructure can either be developed by the network developers or outsourced to a more established organization to monitor and maintain this setup. The pros versus the cons are pointed out by Newman (2001) and the bottom line establishes that it is a matter of trust as to who is to

develop, monitor and maintain the certificates in the infrastructure. The keys must be maintained and is either in a hierarchical design as follows (Figure 1).

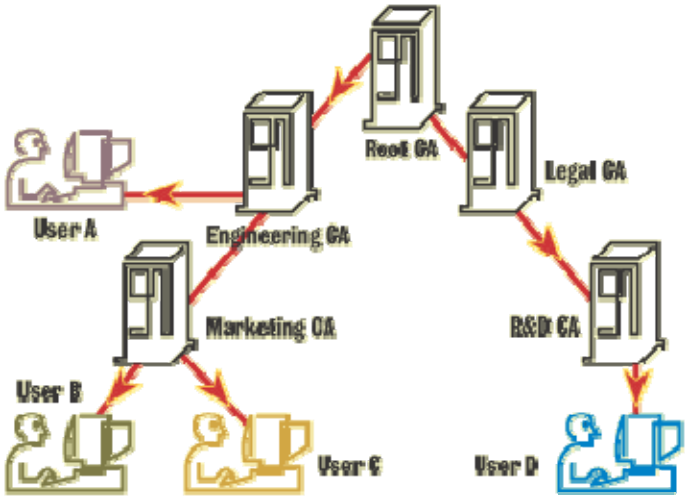

Figure 1. Depiction of a Root Certificate Authority (From Newman, 2001)

Figure 1 demonstrates how a key certification process is maintained using a top-down infrastructure. This setup designates a top level designator of the key generations used in the PKI for the organization. The alternate method is a mesh organization, as shown in Figure 2.

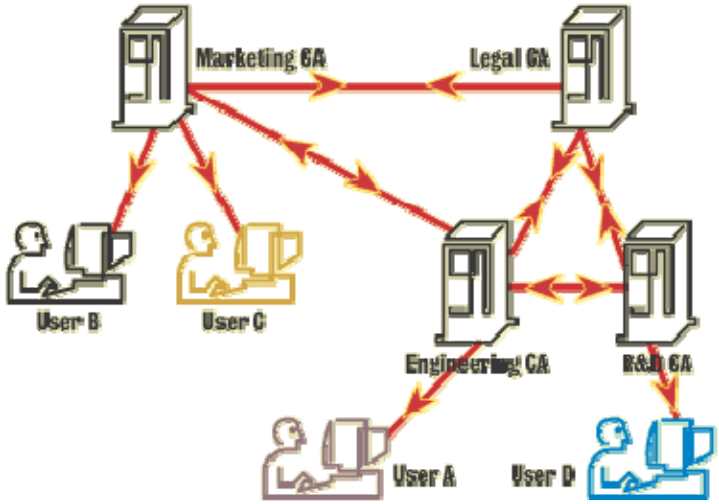

Figure 2. Depiction of a Mesh Certificate Authority (From Newman, 2001)

In Figure 2, the keys are shared among a group of authorities and this design can allow for a back-up of the way the system is maintained, less control over the dominant station controlling the certificates used to establish keys is not as well maintained. As with the question as to who is maintaining and monitoring the infrastructure, control of who is responsible becomes the main concern and can lead to a definite bias towards the Root Certificate Authority (CA) to maintain control over where keys and certificates are provided from a single source.

The projected end state for this study is the determination that a PKI can assist in the development of an information system and not conflict with the interoperability of the components connected to the network where the information system resides. PKI is an established, available system and this study has a goal of demonstrating the value that can be added when incorporating this type of security with an interoperable system. The explanation as to how to implement a PKI will be examined and explained. Finally, a simple demonstration will be set up to demonstrate how the confidentiality, integrity, and authenticity of an information system have value added with a PKI.

When using cryptography to protect information, the sender cannot deny sending the information and the receiver has a valid reason to believe that the information originated from the listed sender. The process of encryption is a process of using designated values to encode information from both the user and sender; these values are known as keys. Information that has been encoded can be translated using the key that provided for the now encrypted information.

The public key cryptography algorithms and implementations live in protocols like S/MIME (which pretty much come automatically in your operating system distribution these days). But the public key INFRASTRUCTURE is not—you need the actual key pairs to make the crypto algorithms work. In DoD, the local PKI artifact lives in your CAC, not your computer's OS.

Public Key Cryptograph is the use of an asymmetric algorithm to create a public and private key pair, perform a key exchange or agreement, and generate and verify digital signatures. PKI utilizes the assumption that the identity of one end user can be

verified through a "certificate" by a certificate authority and uses the algorithm of the asymmetric algorithm (Public Key Cryptography) to carry out the key exchange. The certificates are generated and maintained by those that can identify users, thus allowing for encrypted communication and authentication between users as stated by Harris (2005).

So, if the idea is appealing, the next step is to gain a certificate for use. As previously mentioned, there are two ways to go about maintaining a PKI for an information system, either by home grown development or by outsourcing to established certificate authority organizations. Before assuming PKI is the solution to all security related problems, Schneier (2000) reminds security personnel that, "Long keys don't make up for an insecure system because total security is weaker than the weakest component in the system." Therefore, overall security must be accounted for and not to place all eggs in one PKI basket. Continuing with the development of a Public Key Infrastructure, the process can be achieved by reviewing Network Working Group Request for Comments (RFC): 4158, which provides guidance for developing a public key certification path within a given application.

D. THE TEST UNDERSTANDING

This test looks at the requirements for an accurate First Responder Information System. The current requirements only involve similar communication bands of frequencies to be able to share information. Telling another user a location such as, "I'm in the bathroom" or "I'm in the master bedroom" does have validity to providing the other user where the first is located. The case reviewed here looks at that idea from a slightly more specific point of view.

The Merriam-Webster dictionary defines *accuracy* as follows: (Merriam Webster, n.d.)

1. freedom from mistake or error: correctness

2. a. conformity to truth or to a standard or model: exactness
   b. degree of conformity of a measure to a standard or a true value: precision

The definition that best describes in the case presented is one of being free from mistake or error. Using a computer Information System to accurately identify the correct sender of the information can be expanded to the idea that the correct information has been transmitted and not that which might be generated from another user. The test case used the digital signature to ensure this idea and the test concerns of validity are proven with that information.

III. HOW TRANSMISSION WORKS IN THIS THESIS

A. E-MAIL

Electronic mail is the universal method of transmitting information across the Internet. Since it is widely available and accepted as a form of information transfer, e-mail has been used as the communications means in this study. It has the following available protocols and standards:

i.) Simple Mail Transfer Protocol (SMTP) specifies the handling of e-mail and it specifies the format for the e-mail message header. The specifics for the protocol, as outlined in RFC822, do not specify the requirements of the message body itself.

ii.) Multipurpose Internet Mail Extension (MIME) supplements SMTP by articulating the body parts of a messing. Now there is an identifiable object so data security measures (sign, crypt) can be applied to it.

iii.) Secure Multipurpose Internet Mail Extension (S/MIME) is a standard for signing/encrypting electronic mail parts. Taking a step backwards, the Multipurpose Internet e-Mail Extension (MIME) is simply a specification that indicates how multimedia data and e-mail body portions of the message are to be transferred by dictating the encapsulation of the data for processing. Secure MIME is just an extension of the encapsulation process that will be understood by the networking protocols allowing for the e-mail to be encrypted in the process. S/MIME provides confidentiality through the user's encryption algorithm, integrity through the user's hashing algorithm, authentication through the use of public key certificates through cryptographically signed message digests (Harris, 2005, p. 663).

THIS PAGE INTENTIONALLY LEFT BLANK

IV. RESEARCH METHODOLOGY

A. PRACTICAL USAGE

Getting the security set up is now overviewed with a few guides towards creating an original PKI certificate authority, the other option is to purchase a certificate from VeriSign, Entrust, GlobalSign or any other certificate monitoring authority. For a fee, someone else can maintain the certificates and ensure all required updates and requirements are up to date.

Demonstrating this idea will be with the application of the idea that a simple blue force tracker will be developed and the information will be transmitted over the Internet using a secure means. This provides the example that the process is quite simple.

Using a Garmin Global Positioning System (GPS) receiver, a laptop, an Internet capable cell phone, and an automatic e-mail system utilizing Microsoft Outlook to send the information from the GPS receiver will do accomplishing this task.

B. DESIGN AND IMPLEMENTATION

The tools for demonstrating a simple solution were selected were based upon a first responder in need of transmitting information from an end system to the base monitoring location; keeping in mind that the goal of sending this information was to not be extremely complicated and difficult to implement. The information could include data regarding location, equipment needs, observations made, anything considered vital to the current environment and operation.

The first tool selected was the Garmin GPS receiver so that location information could be sent to a monitoring station as a baseline for the type of information to be transmitted. Since the unit was only a receiver, the data collected by the receiver needed to be saved on a computer, from which the saved information could be transmitted to the monitoring station. In order to accomplish this task, a laptop running Microsoft Windows was utilized while running the Garmin GPS location software, which was

downloaded from the Garmin Web site (www.garmin.com). This same software was loaded onto a stationary desktop computer so that the updates could be received and the data could be displayed as the updates came in from the laptop computer. A temporary certificate was requested from VeriSign so that there was a certificate loaded on to the laptop's version of Microsoft Outlook, and therefore could be verified by the monitoring computer. The actual data from the GPS receiver had to be set up to be saved automatically in a fixed interval of time and then e-mailed to the receiving computer.

The information from the laptop computer was initially sent to the second computer via a non-automated process. Automation of the process is capable with such script writing programs as Macro Scheduler, a Microsoft Windows based script editor. In the Linux environment, various open sourced script editing programs (such as Script Editor 3.0 for example) can be utilized to automate this process in a Linux environment. A basic depiction of the test scenarios was in accordance with Figure 3.

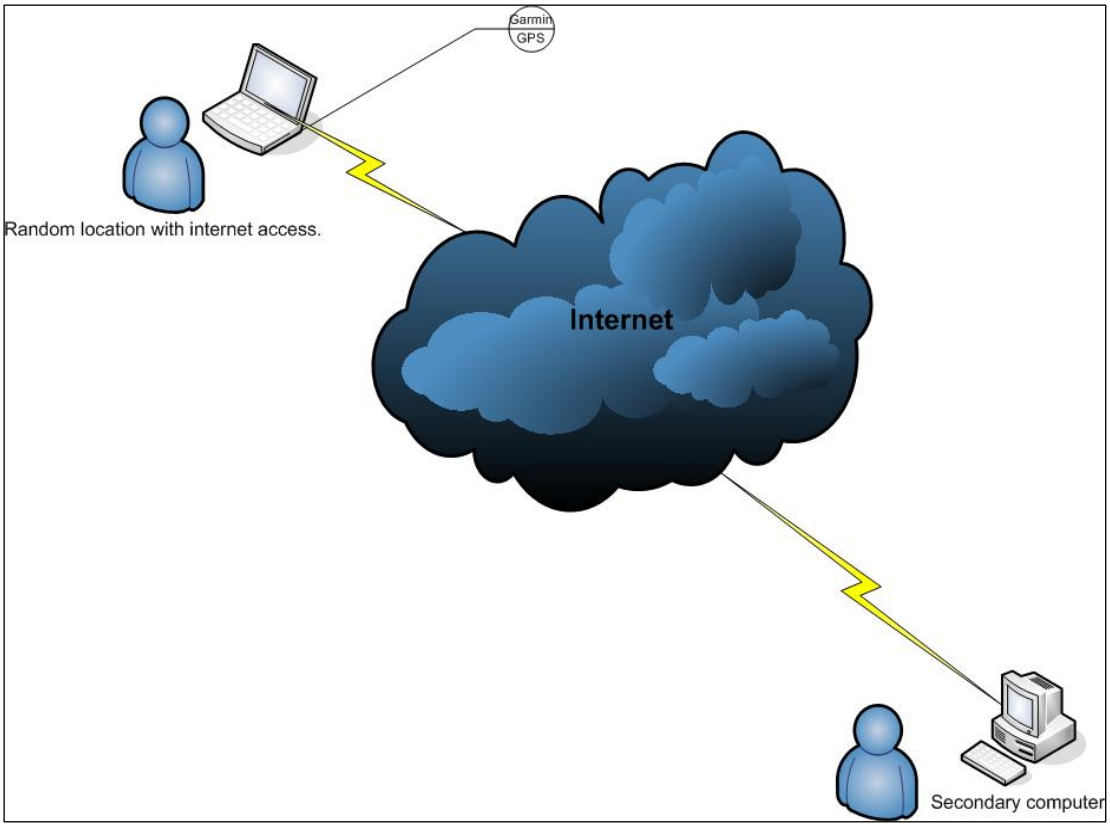

Figure 3. Testing Example Diagram

A random location with Internet access was chosen, the coordinates were saved in the file location on the laptop computer. That information was then digitally signed using the security feature on the laptop's Microsoft Office Outlook computer program, and then transmitted to the secondary computer. This information was transmitted and then received by the secondary computer.

Figure 4 displays that the two computers are connected to the Internet and transmitting information between one another via the Internet. The different systems that can possibly make up the cloud of the Internet, which connects the two separate networks, demonstrate the Internet's interoperability capability.

The other members on the Internet have no need to be specified as being on the local network, just having an established Internet connection. The idea that two User Agents can talk to one another along a common infrastructure is easy to understand. Information on the Internet can be transmitted from one User Agent to another because the architecture that comprises the Internet is already established. The required information is the source and destination addresses to determine where the information came from and where it is going and the Internet protocols work out by binding the system together.

The authenticity of the information is not dependant on the originating location of the information or where it is being sent. The validation information can be various other applications that simply feed into the way the information is securely transmitted – simply another program on the computer. The data to be transmitted stands by itself and only needs a vessel to encapsulate it as a form of protection. In this case, the end user program is Microsoft Office Outlook, which uses the digital signature to provide authenticity. Authenticity of the data is an end-to-end function and should not depend on any bit-hauling infrastructure.

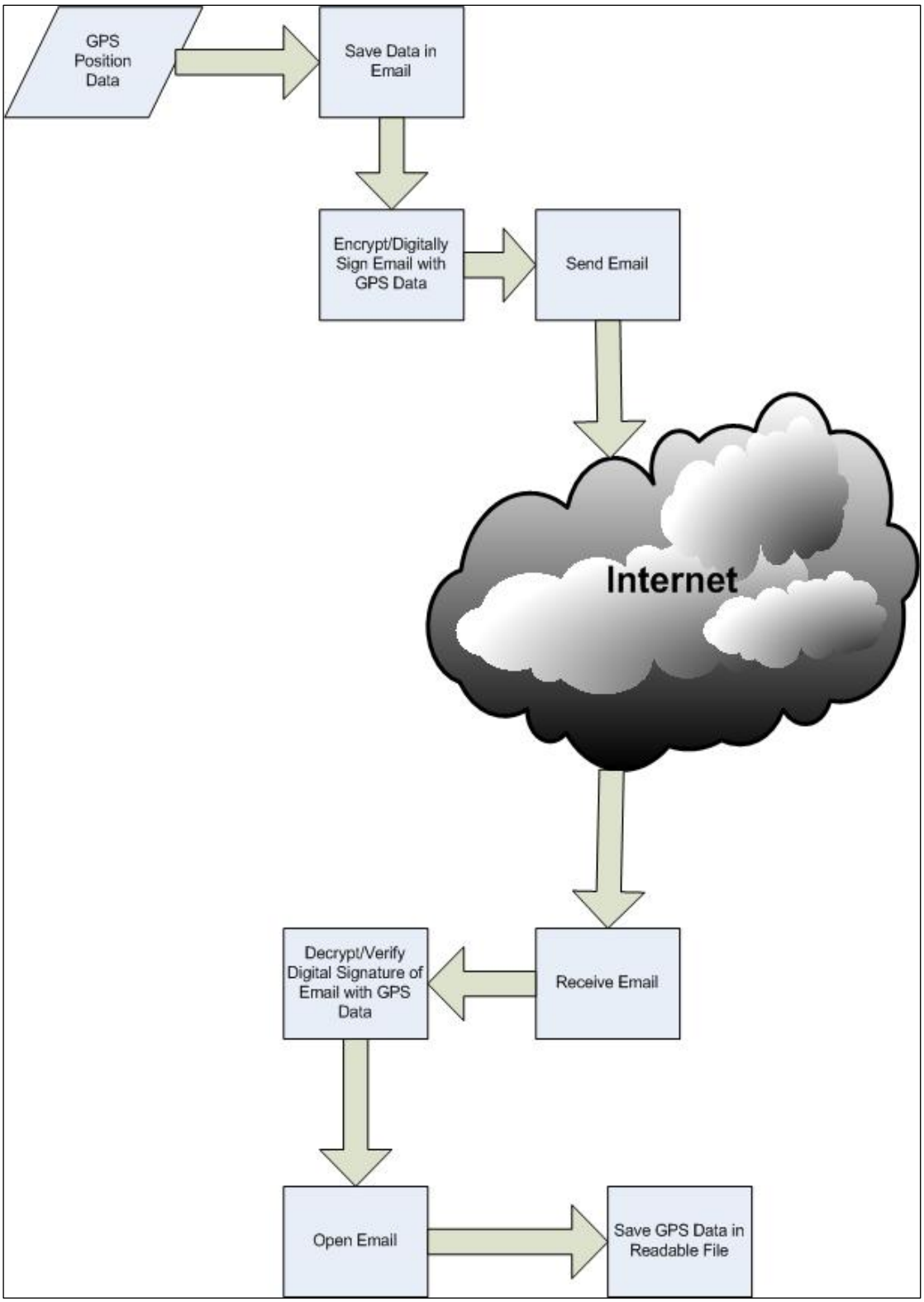

Figure 4. GPS Data Flow Chart

C. DEPLOYMENT AND TESTING

The actual testing of the developed system worked quite effectively for such a rudimentary design. The end resulted in the information being transmitted from the traveling laptop computer to a stationary computer using a Verizon cell phone as the laptop's modem.

The results demonstrate that using one User Agent attached to any connection node on an inter-networked system can properly communicate the intended information to another User Agent through another inter-networked system securely. The preferred standards for protecting the information to be stored is required to be specific to the end system, because the data is the only part that needs the security protection across the inter-networked Information Systems.

Here the test involved using GPS information and the Microsoft Office Outlook computer program as a means to provide an easy to follow example. Any other data transfer program can be inserted to provide for similar results because how the information can be transmitted is not important. For this test, the information was saved from one file, attached to an e-mail document, digitally signed, sent, received, downloaded and resaved on a second computer by an individual user. Where the users were connected to the Internet was of no importance because the different local area networks used the Internet Protocol to traverse across different connected networks and again demonstrating the option of using the Internet as the interoperable network of networks as a means to connect different users together.

The use of a GPS sensor accomplished two tasks as the data is passed from the laptop user to the other. First, because of GPS technology, data from the location of the sensor provides a very accurate or precise set of coordinates as to the location of the user using this end system. Second, the digital signature provides for integrity of the information originating from the desired source when received by the second user.

The following is the specific setup of the experiment.

D. SETUP

A User Agent was established with a laptop computer. The User Agent's purpose was to roam while sending out information of interest about itself (the User Agent). The information about the User Agent was the GPS information file that was stored on the laptop. The location of the User Agent is updated continuously, therefore a save interval of the information had to be established. The established update period of once every minute was established. The most recent GPS location was stored in a file directory and could be exported as desired by the User Agent.

E. E-MAIL SETUP

Microsoft Outlook was chosen to be the information export device because of its versatility for use with all types of e-mail programs. An e-mail address for sending the information was chosen "SenderBlackmonThesis@Gmail.com" and set up for use with the Microsoft Outlook program. A Google Mail (Gmail) account was chosen due to the fee requirements of setting up a Microsoft Hotmail account with Microsoft Outlook. A simple yet strong password was established as "JbB2009!" so that the account could be monitored as needed. In the Gmail account, certain settings had to be changed so that it would work properly with Microsoft Outlook. Under the Forwarding and POP/IMAP tab in the settings menu, IMAP had to be enabled in order to be able to synchronize with the Microsoft Outlook Application.

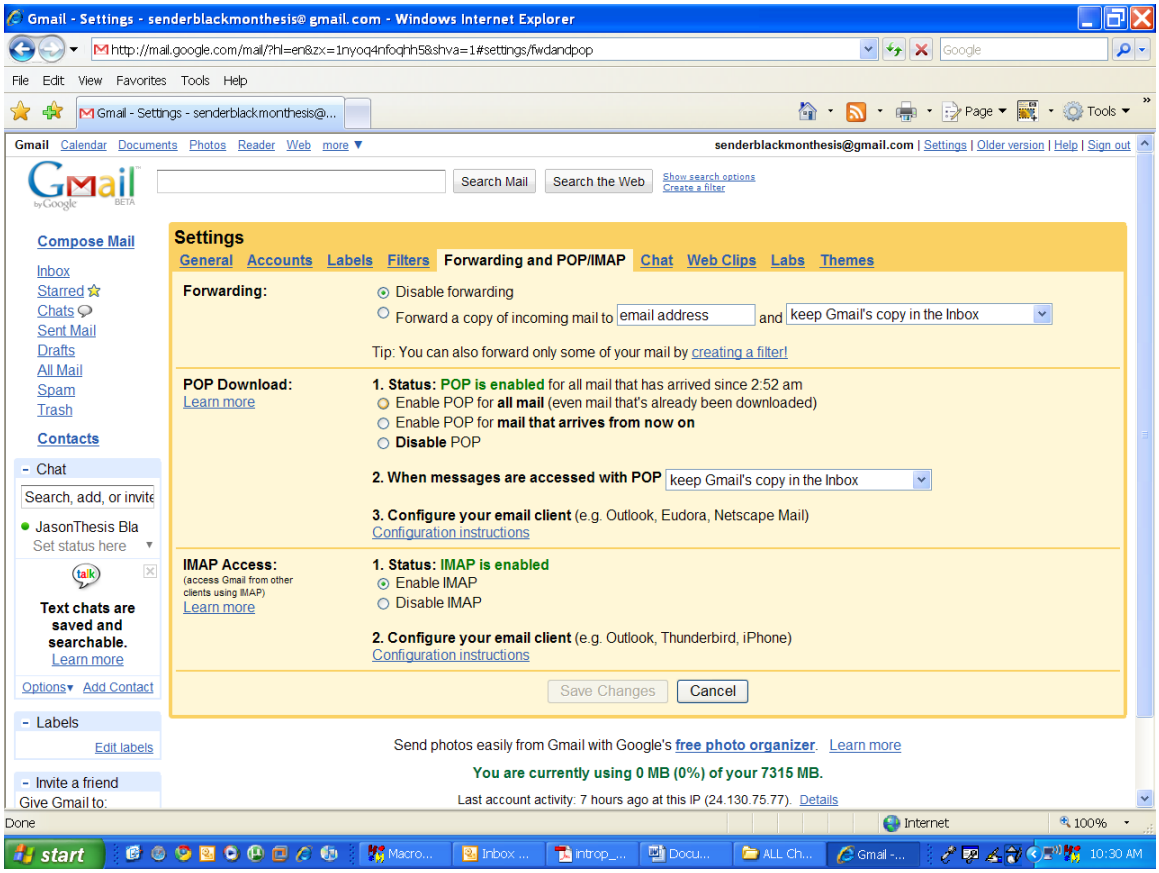

Figure 5. Screen Shot of Google Gmail Account Registration. (From Google, 2009)

Now that the Google Mail account was set up, the other part of the User Agent had to be set up so that the laptop could access this account and use the Microsoft Outlook application. In the Microsoft Outlook application, a new address had to be added and is easily done so using the Microsoft Add E-mail Accounts wizard.

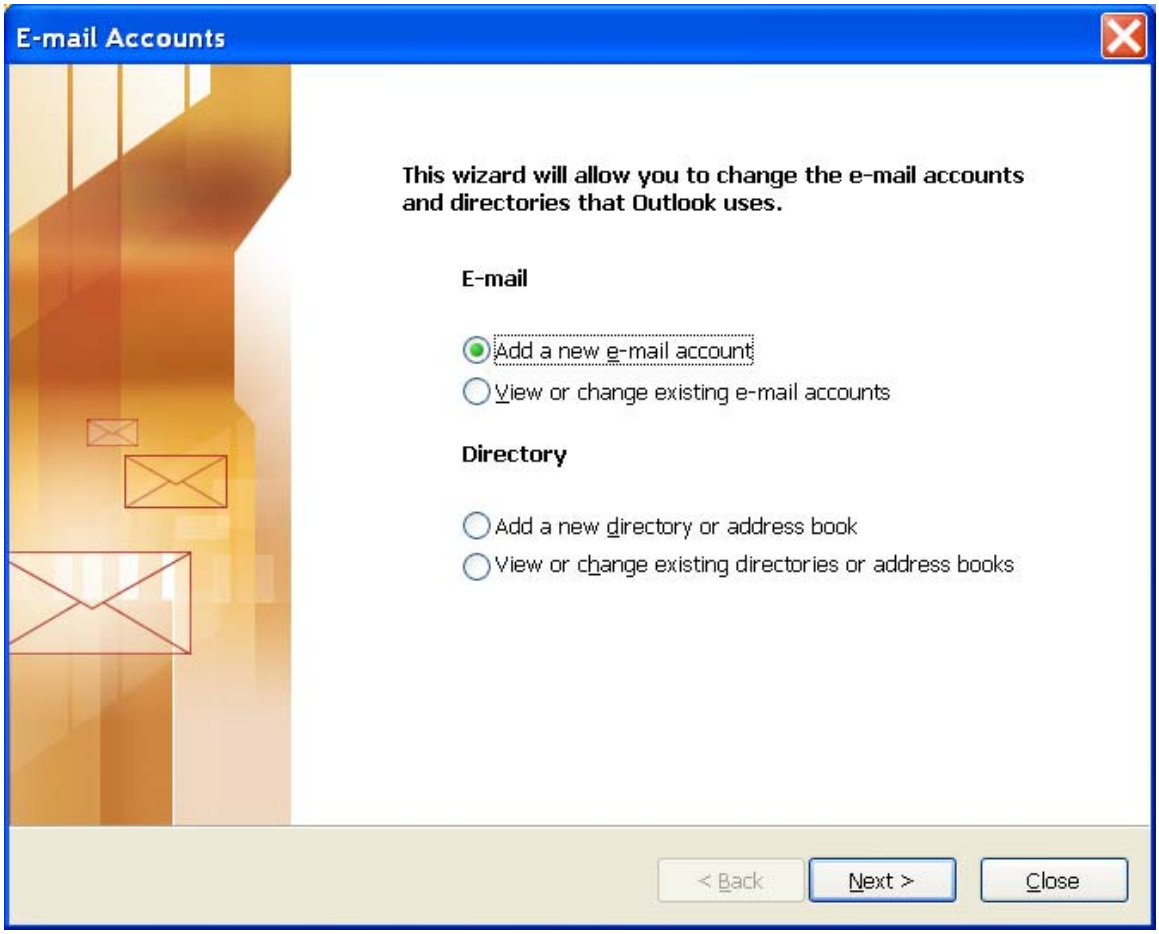

Figure 6. Screen Capture of the New Address is to be Added to the Microsoft Office Account List. (From Microsoft, 2009)

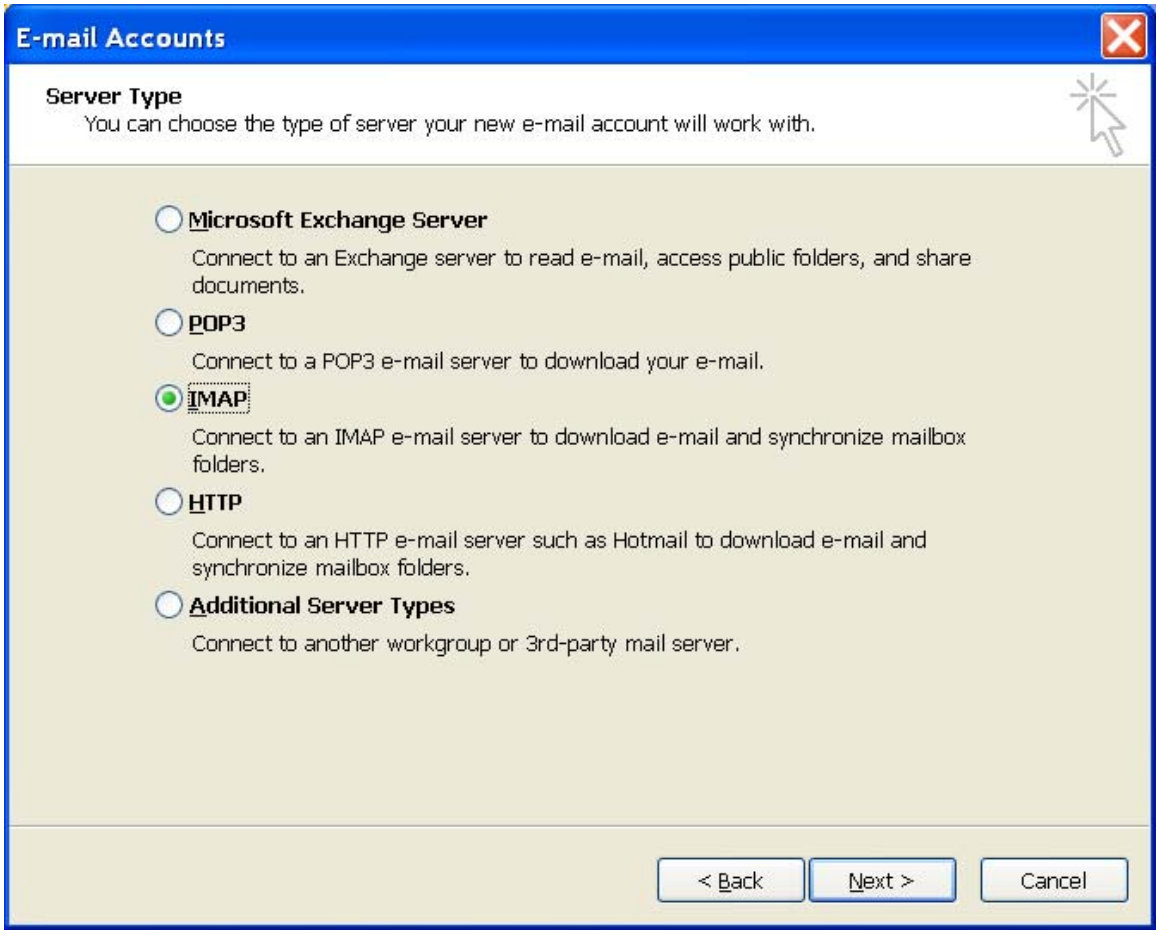

Figure 7. The IMAP server type is selected for real-time updates of the messaged information that will pass from the Outlook program on the laptop to the receiving address. (From Microsoft, 2009)

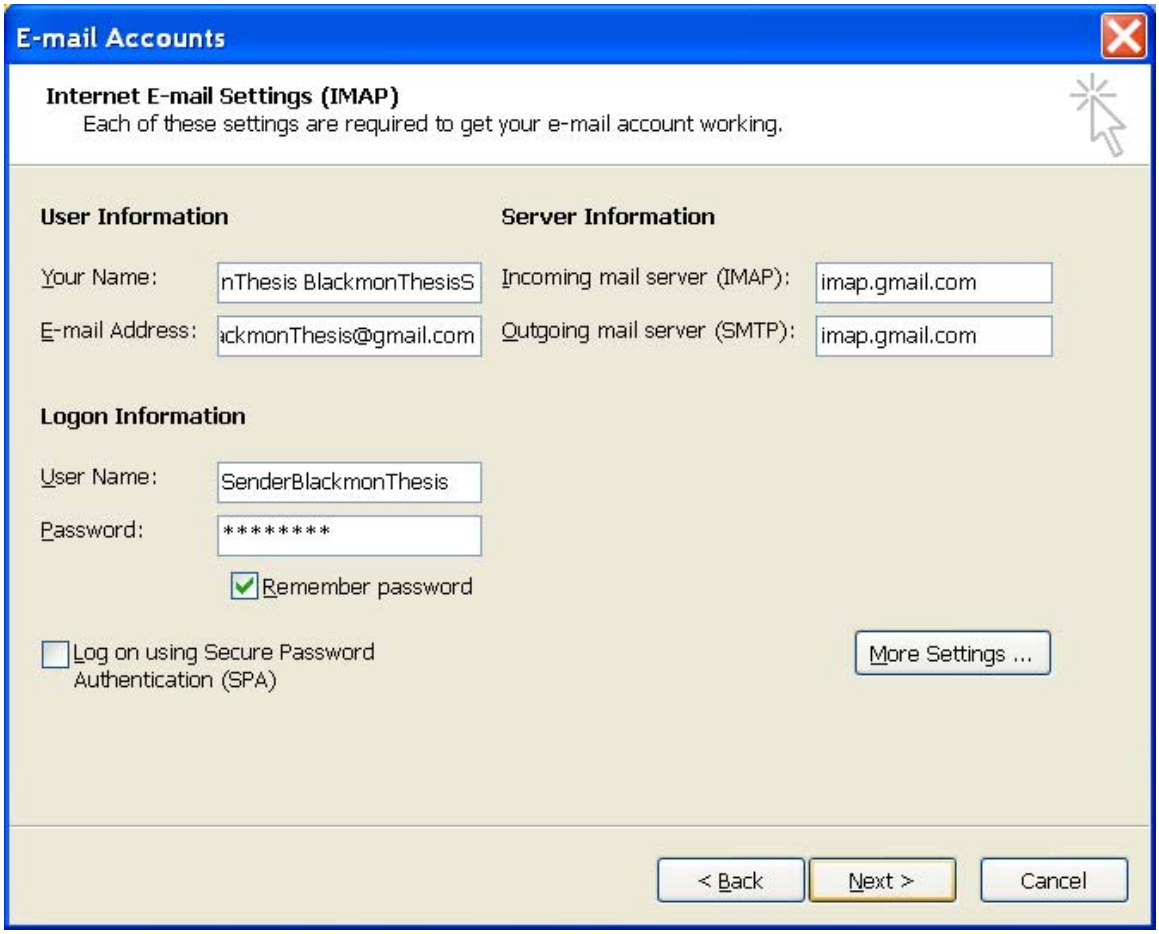

Figure 8. The account is now put into Outlook and can be acknowledged to synchronize with Google mail when running. (From Microsoft, 2009)

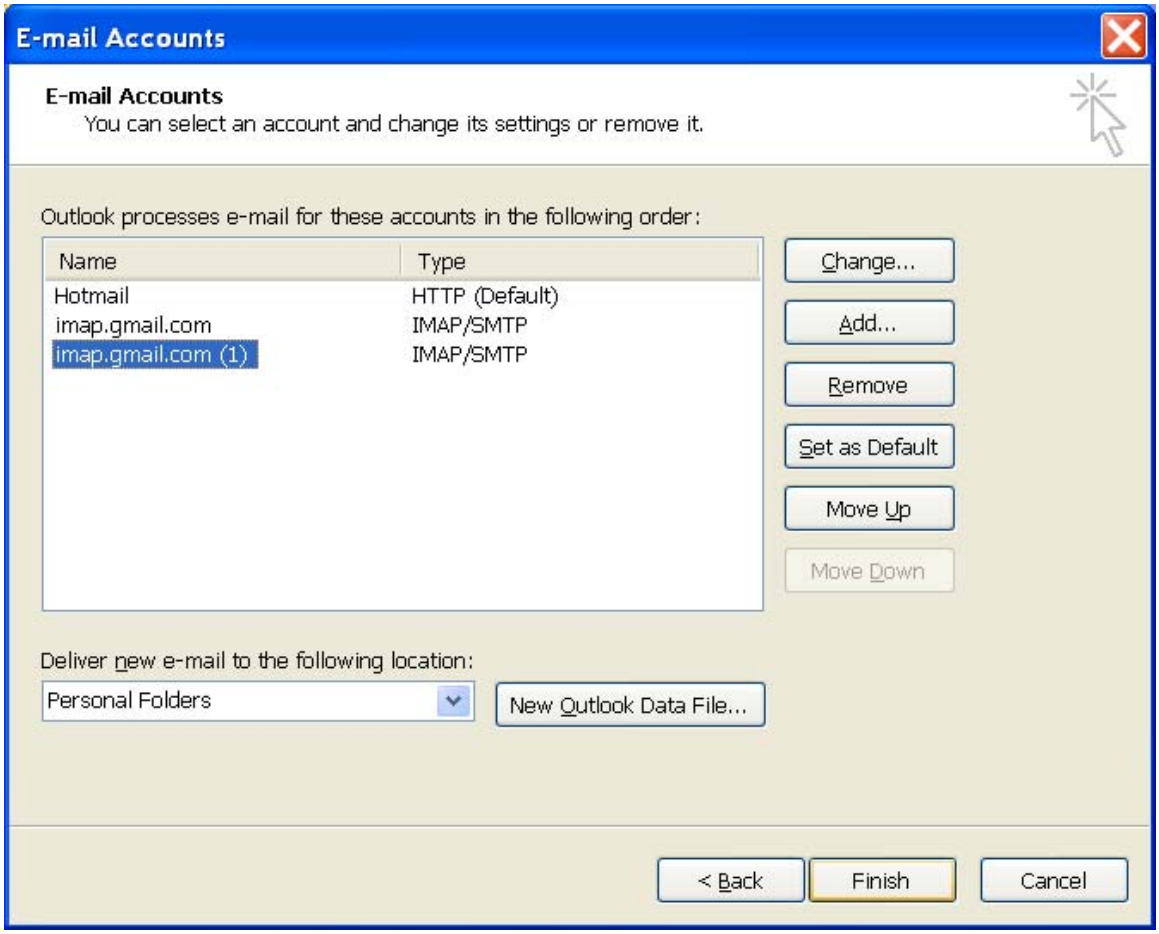

Figure 9. Final registration setup screen. After the accounts are approved, the Finish button allows for the finalization of the account to be added for use with Outlook. (From Microsoft, 2009)

F. SENDING/RECEIVING E-MAIL MESSAGES

The next stage is to automate the sending process. Setting up the ability to send information was developed over a several stages. The stages were as follows:

1) Send e-mail to a predetermined address automatically
2) Send e-mail with an attachment to a predetermined address automatically
3) Exporting the data file from the GPS nRoute software
4) Receive e-mail automatically
5) Download attachment from received e-mail automatically
6) Importing the GPS data file from the e-mail

The send e-mail feature was pursued with the help of using Visual Studio and programming in the Visual Basic computer programming language. This language was chosen for its close association with Microsoft Outlook since macro (in-house automated) programs can be developed using the Visual Basic editor built in to the Microsoft Outlook program.

The sending of the information using Visual Basic was chosen because of the concept that the programming language would be easily able to draft and send the required information from the intended User Agent with little difficulty of interaction with the Microsoft Office Software. The actual development of the Visual Basic program was broken down into smaller parts. The sections of development were to 1) create a program to send e-mails using Microsoft Outlook and 2) attach a program to the e-mail being sent. The original program of sending the e-mail was developed using a form with a button that utilized the following code:

```
Imports System.IO
Imports System.Collections
Imports Microsoft.VisualBasic
Imports System.net.Mail
Imports Microsoft
Private Sub Email_Btn_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles Email_Btn.Click

    'Create OL App object
    Dim objOLApp As Object
    Dim objMsg As Object

    Dim strRecipient As String = "SenderBlackmonThesis@Gmail.com"
    Dim strSubj As String = "temp"
    Dim strBody As String = "test to send"

    objOLApp = CreateObject("Outlook.Application")
```

```
        If objOLApp Is Nothing Then
                MessageBox.Show("Could not create OL App.  Shutting Down")
                Exit Sub
        End If

        'Create a new mail item
        objMsg = objOLApp.CreateItem(0)
        If objMsg Is Nothing Then
                MessageBox.Show("Could not create Mail Item.  Shutting_ Down")
                Exit Sub
        End If

        'attach each file attachment
        objMsg.Attachments.Add(filename)

        'Set basic message parameters
        objMsg.To = strRecipient
        objMsg.Subject = strSubj
        objMsg.Body = strBody

        'Send the message
        objMsg.Send()

        'Free up the space
        objOLApp = Nothing
        objMsg = Nothing

End Sub
```

As soon as the sending of the e-mail was proven possible with the above code, the following line was added just after the strBody variable was declared:

```
Dim filename As String = "c:\Documents and Settings\Jason\My_
Documents\thesis\update.gdb"
```

And the following line was added to attach the file after the create new mail item line was added:

```
'attach each file attachment
objMsg.Attachments.Add(filename)
```

The code searched through and sent the information as desired.

The next step was to automate the process of sending the information. This was accomplished with the assistance of a macro builder program called MacroMaker which is developed by ARM Software and can be downloaded from the Web site http://members.ij.net/anthonymathews/macromaker.htm. After being downloaded and installed, the Figure 10 displays what the Web site looked like:

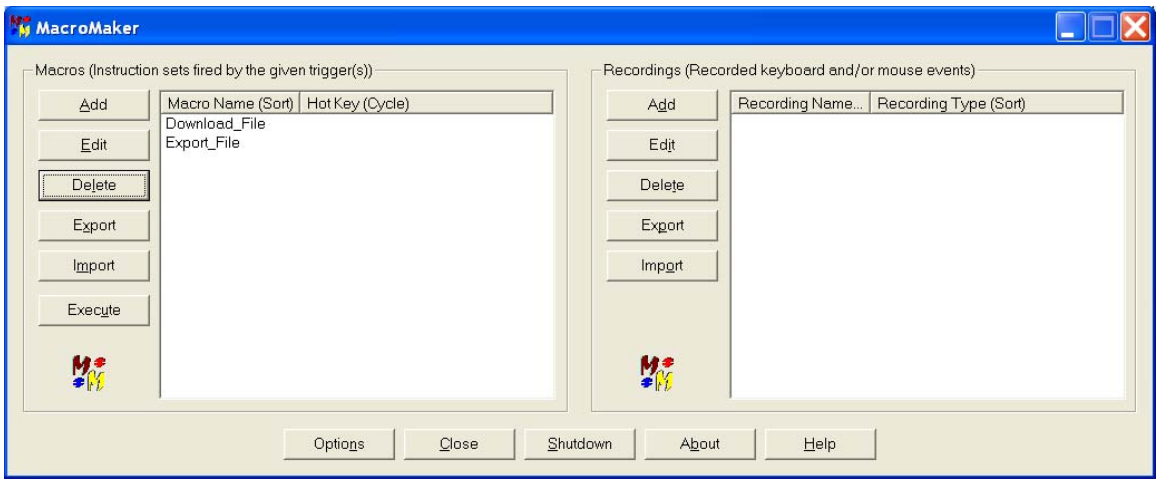

Figure 10. MacroMaker file setup screen. (From MacroMaker, 2009)

The original program to send files was named Export_File and the commands according to MacroMaker were as follows:

- SET FOREGROUND(Start Button)
- SET FOCUS(Start Button)
- MOVE MOUSE POINTED(REL/WIN: 6963,31538)
- LEFT BUTTON DOWN
- LEFT BUTTON UP

The above commands executed the automated sending of the e-mail, and with the help of the scheduler feature of the MacroMaker program, the e-mails could be sent automatically in one minute intervals. If any type of delay was required, a DELAY command is easily inserted with the intended delayed amount of time input in milliseconds.

Next, the process of automatically exporting the data to be sent needed to be mastered. This was accomplished in the Export_File program with several commands input into the Macro body. The commands utilized:

- RUN(C:\Garmin\nRoute\nRoute.exe)
- SET FOREGROUND(nRoute)
- SET FOCUS(nRoute)
- DELAY 2000 millisecond(s)
- CTRL(Down)
- eE(Down)
- eE(Up)
- CTRL(Up)
- uU(Down)
- uU(Up)
- pP(Down)
- pP(Up)

- dD(Down)
- dD(Up)
- aA(Down)
- aA(Up)
- tT(Down)
- tT(Up)
- RETURN(Down)
- RETURN(Up)

These commands allowed for the file export function to be called in the nRoute GPS tracking software and saved to a file named update which was automatically saved as a Garmin gdb file type. The process of sending the information was now a matter running the created macro program and the e-mails get automatically sent from the intended information supplier.

The next step in this process is the receiving of the information. The first step is determining how often are updates desired and in the case of this example a five minute update time was implemented in Figure 11 with the Send/Receive --> Send/Receive Settings menu in Outlook:

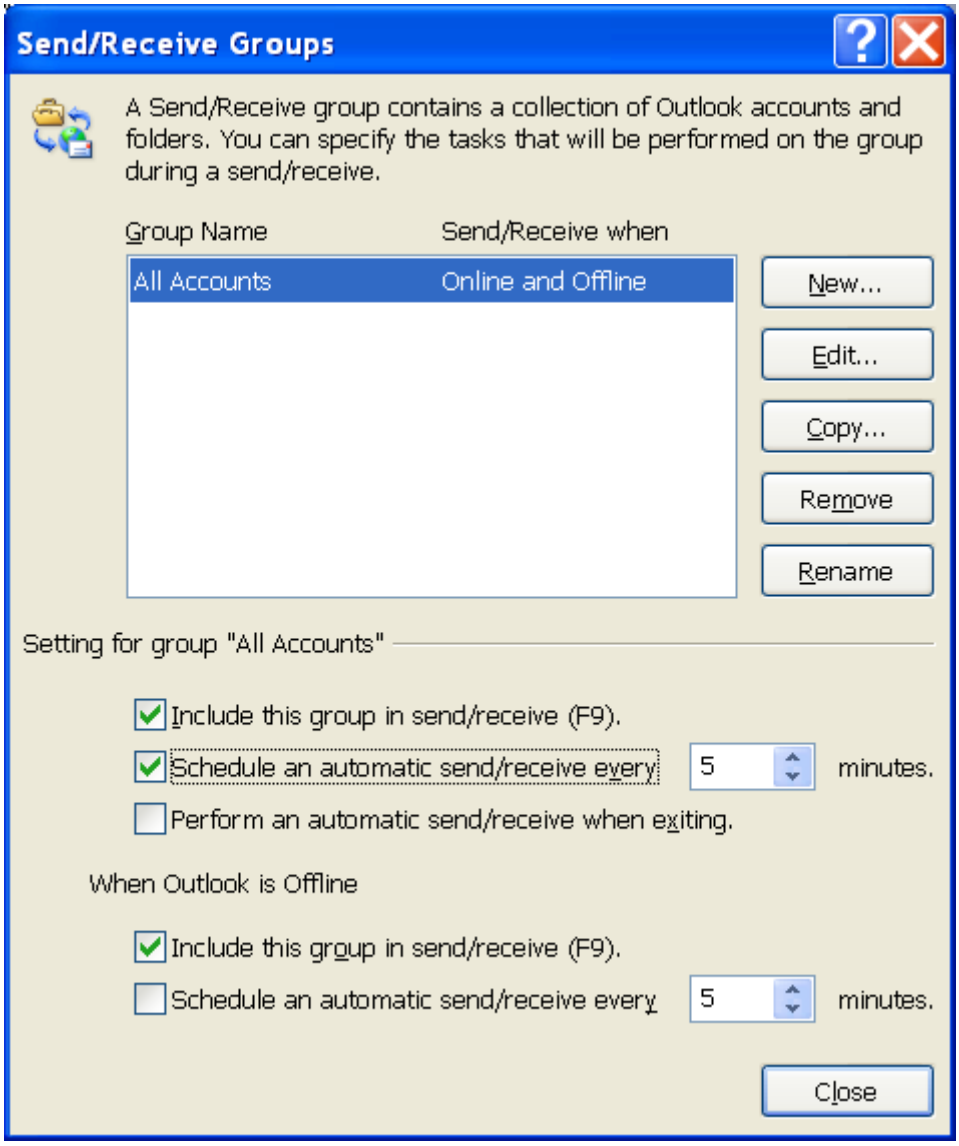

Figure 11. Timer setup for accounts. (From Microsoft, 2009)

A receive e-mail account was set up with the following e-mail address, ReceiverBlackmonThesis@Gmail.com. The password for this address is the same as the sender address to keep down complexity. The receive macro was developed in a similar fashion to the sender macro. This macro was broken down into two parts, the download file part and the import file to nRoute part.

The download from file part was conducted using the MacroMaker program and various mouse clicks at various relative locations on the open Outlook window. The following commands are how the file is downloaded:

- DELAY 300000 millisecond(s)
- SET FOREGROUND(Inbox – Microsoft Outlook)
- SET FOCUS(Inbox – Microsoft Outlook)
- MOVE MOUSE POINTER(REL/WIN: 4351,25872)
- LEFT BUTTON DOWN
- LEFT BUTTON UP
- MOVE MOUSE POINTER(REL/WIN: 3788,25940)
- LEFT BUTTON DOWN
- LEFT BUTTON UP
- MOVE MOUSE POINTER(REL/WIN: 17510,14677)
- LEFT BUTTON DOWN
- LEFT BUTTON UP
- MOVE MOUSE POINTER(REL/WIN: 31385,14335)
- RIGHT BUTTON DOWN
- RIGHT BUTTON UP
- MOVE MOUSE POINTER(REL/WIN: 32101,18022)
- LEFT BUTTON DOWN
- LEFT BUTTON UP
- WAIT FOR WINDOW(Save Attachment)
- MOVE MOUSE POINTER(REL/WIN: 4351,25872)
- LEFT BUTTON DOWN
- LEFT BUTTON UP
- LEFT BUTTON DOWN
- LEFT BUTTON UP
- RETURN(Down)
- RETURN(Up)

The second part of the command lines for the program are to import the downloaded file into a running nRoute GPS monitoring window that will provide updates to the ‘update.gdb’ file every five minutes.

- SET FOREGROUND(nRoute)
- SET FOCUS(nRoute)
- CTRL(Down)
- iI(Down)
- iI(Up)
- CTRL(Up)
- uU(Down)
- uU(Up)
- pP(Down)
- pP(Up)
- dD(Down)
- dD(Up)
- aA(Down)
- aA(Up)
- tT(Down)
- tT(Up)
- eE(Down)
- eE(Up)
- .>(Down)
- .>(Up)
- gG(Down)
- gG(Up)
- dD(Down)
- dD(Up)
- bB(Down)
- bB(Up)

- RETURN(Down)
- RETURN(Up)

The command to run this macro is triggered every minute with a three-hundred thousand millisecond (5 min) delay. Now the most recent updates of a GPS position as sent by the receiver can be received and viewed by the monitoring (receiving) secondary station.

G. THE TEST

Now the guts behind what is making the program run have been revealed and must be put into action for demonstration. On Thursday, April 14, 2009, the laptop was placed in a car and driven around the local Monterey area with the Garmin GPS receiver with nRoute monitoring software running, Microsoft Office running, the send e-mail Visual Basic program running, and the Export_File macro running as well. The information was saved and recorded. If an Internet connection was not available the e-mail was sent into the Outlook Outbox folder and as soon as an Internet connection was re-established, the folder downloaded the file.

Because of the frustration of waiting for the laptop computer to re-establish a network connection, another alternative was sought out. A Verizon cellular with mobile broadband access to the Internet was utilized. This was accomplished using the Verizon wireless VZAccess Manager software. This allowed for the laptop User Agent to utilize the 3G capabilities with the Verizon EVDO Internet capabilities.

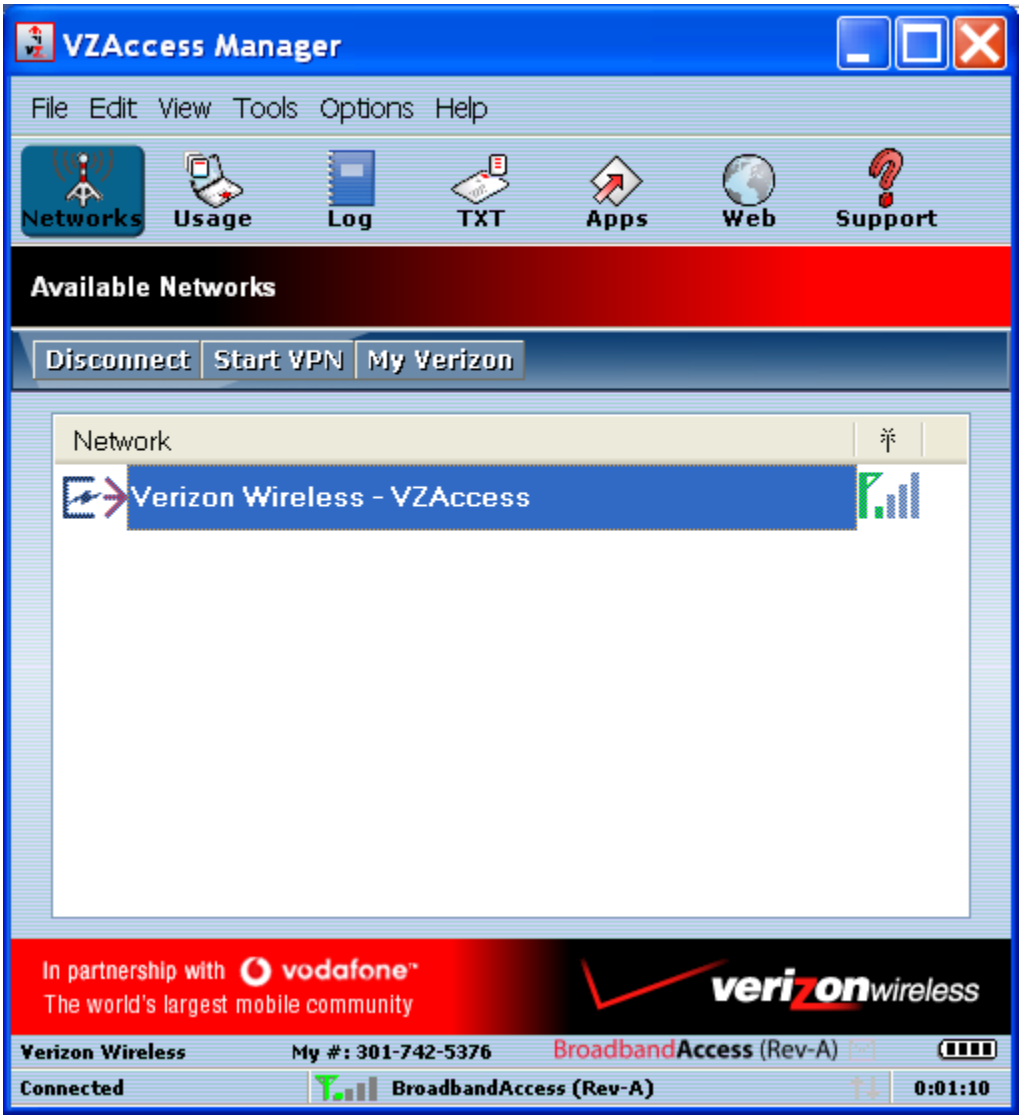

Figure 12. Verizon modem software connection screen display. (From Verizon Wireless, 2009)

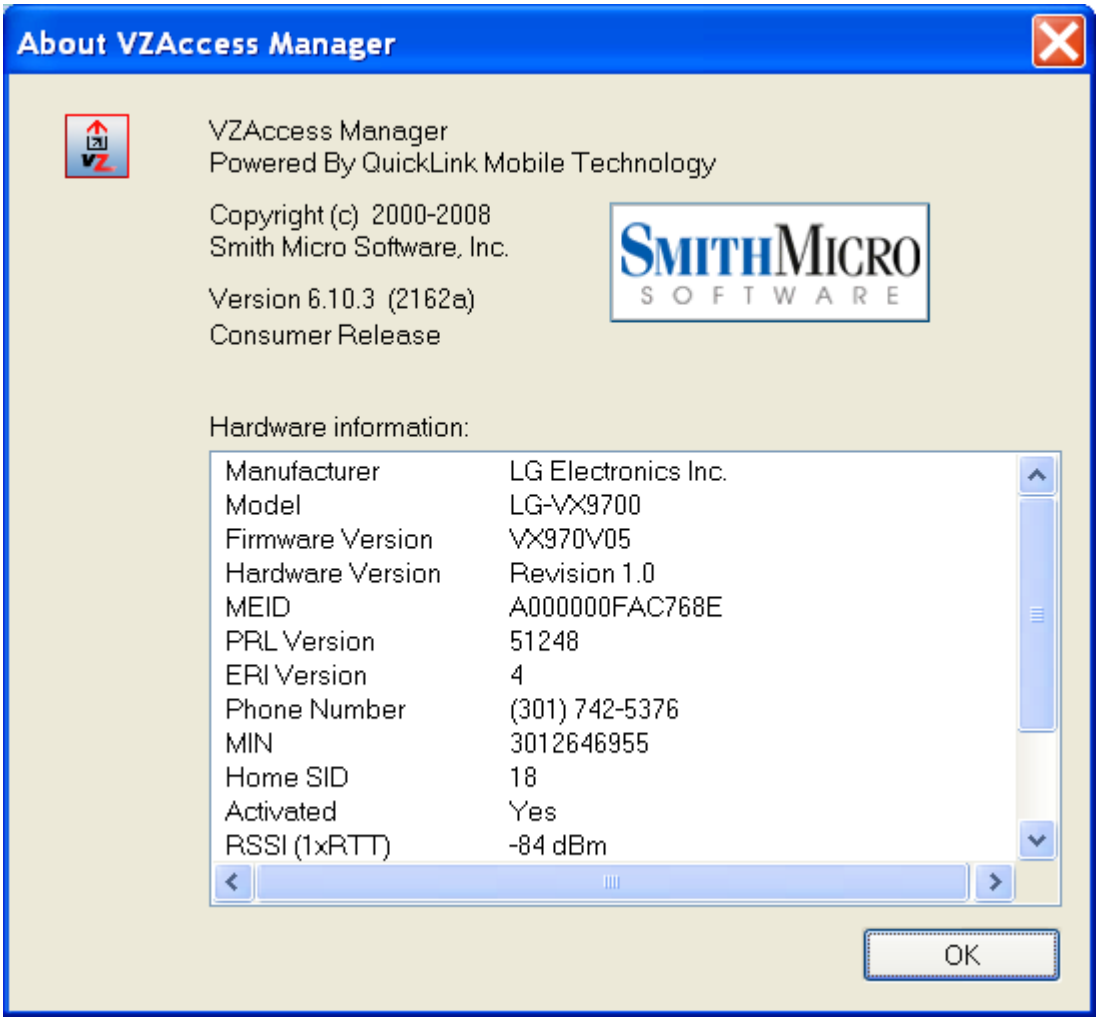

Figure 13. Verizon VZAccess Manager specifications. (From Verizon Wireless, 2009)

The simple idea of plugging in the laptop computer to a cellular phone with Internet capability to act as a modem provided a simple solution to the complex idea of keeping the User Agent in constant contact with the extremely powerful Internet.

When the course was completed and the updates were sent via the laptop User Agent to the monitoring User Agent, update.gdb files followed the transmission path as in Figure 4, going from the GPS receiver to the laptop computer; saved to the file; attached to the e-mail; authenticated using PKI; transmitted via the cellular phone modem; traveled across the Internet; received by the monitoring location; verified authentication by the receiving station; opened and viewed by the receiving station. The

test metric was successfully proven because the data transmitted successfully from end to end. The data is unprotected on the ends of the transmission (on the transmitting laptop and the monitoring station) but protected once transmitted in the e-mail format. Anyone that wants to interfere with the transmission of the data in the middle cannot do so because that is where the protection is located with security “bubble” around the data.

A very noteworthy point is even though the signal was not consistent throughout the sending of the location data, the security was not compromised because it was protected before transmission and had the protection removed by the receiving computer. This security concept is applicable for any WIFI or EVDO wireless transmitted computer because only the end users can strip away the security around the data.

THIS PAGE INTENTIONALLY LEFT BLANK

V. FINDINGS

The results indicate using one User Agent attached to any connection node on an inter-networked system can communicate the intended information to another User Agent through another inter-networked system properly and securely. The preferred standards for protecting the information to be stored is must be specific to the end system, because the data is the only part requiring security protection across the inter-networked Information Systems.

The validity of the test, the purpose behind this thesis, was proved successful because the transmission of data was successfully across the Internet utilizing the transmission flow in Figure 4. The use of secure e-mail eliminates users' concerns and minimizes the exposure of unprotected data within the Operating System in the end systems.

There was difficulty developing the system due to a lack of familiarity with Visual Basic, plus the involvement of a script editor was used to help in the automation of the process. Trial and error was involved in the development of the system. After initial programming bugs resolved the network capability was confirmed and later tests were successful. Ultimately, Microsoft Outlook was the e-mail application tool chosen based upon its availability and certificate incorporation ability.

However, potential drawbacks still existed. Such drawbacks included the possibility of being hacked and keeping the computer safe from outside sources was still a definite concern. Therefore, a non-Hotmail e-mail account was designed because a connection fee was required to establish a Microsoft Outlook—Hotmail account connection for any Hotmail account developed after 2004. This fee was removed after the test in September 2009.

In the end, the following research questions were answered: 1.) Can First Responders use PKI to provide security for information that comes from a sensing tool that is transmitted across the Internet via wireless means? 2.) Does it have value? 3.) If it has value, then to whom? First Responders can use PKI to provide security for

information coming from a sensing tool that is transmitted across the Internet via wireless means to a central site. Current Information Technology in use can be easily altered to use PKI, especially if they use a VPN today. The test use case provided a visual demonstration that this can happen. The fact that there are organizations dedicating time and resources to enhance the capability of using PKI in mobile platforms definitely proves that there is value in evolving the use of this possibility. In the use case section, e-commerce, mobile platform software developers, XML communication developers, and federal organizations all have proven interest in using PKI for more hardware and software applications.

The test involved using GPS information and the Microsoft Office Outlook computer program as a means to provide an easy to follow example. The method of information transmission proved unimportant. Any other data transfer program could be inserted to provide similar results. For this test in this thesis, the information was saved from one file, attached to an e-mail document, digitally signed, sent, received, downloaded and resaved on a second computer by an individual user. The users connected to the Internet were of no importance because the different local area networks used the Internet Protocol to traverse across different connected networks. Once again, demonstrating the option of using the Internet as the interoperable network of networks as a means to connect different users together.

The use of a GPS sensor accomplished two tasks as the data is passed from the laptop user to the other. First, because of GPS technology, data from the location of the sensor provided dynamic information that was constantly updated by the user using this end system allowing for multiple updates with new information. Second, the digital signature provides for integrity of the information originating from the desired source when received by the second user.

This test provided a proof of concept that a simple solution to the blue force tracker idea can be developed utilizing a Network Citizen that maintains itself in accordance with a few basic requirements. The LAN interface presented here is the wireless network card or the broadband wireless cell phone maintaining the laptop's connectivity with the Internet. The packaging interface of the information is the e-mail

MIME structure of sending information in an e-mail format from a source to its destination. The PKI interface is determined with the Microsoft Outlook program which harnesses the power of using a digital signature in order to maintain confidence that the information is arriving from a trusted source. The Quality of Service is maintained by monitoring the network for particular hang-ups and ensuring those hang ups don't delay the routing of important information. In the case of this test demonstration, the use of the Verizon wireless cellular phone as a modem and using the Verizon wireless broadband Internet access instead of waiting for a random wireless network connection to be established. The management interface is the monitoring of the updates by the monitoring station and a lack of timely updates can provide insight into a possible problem with the network or User Agent active connection.

This test meets the requirements of a good network citizen and maintains a sense of modularity with the ability to maneuver around freely and provide these GPS updates. The basis for using this example as a model to for any other system of information sharing shows how important this test has been. The idea of stove piping an updating system is proven unnecessary due to the simplicity of this demonstration. The User Agent can be any information system and not remain limited to GPS receiver data because the information in the file e-mailed can be of any type. Therefore, this test demonstrates the ubiquity of using a similar setup for any other type of information that has a need to be shared and monitored.

The results indicate using one User Agent attached to any connection node on an inter-networked system can communicate the intended information to another User Agent through another inter-networked system properly and securely. The preferred standards for protecting the information to be stored is must be specific to the end system, because the data is the only part requiring security protection across the inter-networked Information Systems.

The validity of the test, the purpose behind this thesis, was proved successful because the transmission of data was successfully across the Internet utilizing the

transmission flow in Figure 4. The use of secure e-mail eliminates users' concerns and minimizes the exposure of unprotected data within the Operating System in the end systems.

There was difficulty developing the system due to a lack of familiarity with Visual Basic, plus the involvement of a script editor was used to help in the automation of the process. Trial and error was involved in the development of the system. After initial programming bugs resolved the network capability was confirmed and later tests were successful. Ultimately, Microsoft Outlook was the e-mail application tool chosen based upon its availability and certificate incorporation ability.

However, potential drawbacks still existed. Such drawbacks included the possibility of being hacked and keeping the computer safe from outside sources was still a definite concern. Therefore a non-Hotmail e-mail account was designed because a connection fee was required to establish a Microsoft Outlook—Hotmail account connection for any Hotmail account developed after 2004. This fee was removed after the test in September 2009.

In the end, the following research questions were answered: 1.) Can First Responders use PKI to provide security for information that comes from a sensing tool that is transmitted across the Internet via wireless means? 2.) Does it have value? 3.) If it has value, then to whom? First Responders can use PKI to provide security for information coming from a sensing tool that is transmitted across the Internet via wireless means to a central site. Current Information Technology in use can be easily altered to use PKI, especially if they use a VPN today. The test use case provided a visual demonstration that this can happen. The fact that there are organizations dedicating time and resources to enhance the capability of using PKI in mobile platforms definitely proves that there is value in evolving the use of this possibility. In the use case section, e-commerce, mobile platform software developers, XML communication developers, and federal organizations all have proven interest in using PKI for more hardware and software applications.

The test involved using GPS information and the Microsoft Office Outlook computer program as a means to provide an easy to follow example. The method of information transmission proved unimportant. Any other data transfer program could be inserted to provide similar results. For this test in this thesis, the information was saved from one file, attached to an e-mail document, digitally signed, sent, received, downloaded and resaved on a second computer by an individual user. The users connected to the Internet were of no importance because the different local area networks used the Internet Protocol to traverse across different connected networks. Thus, once again, demonstrating the option of using the Internet as the interoperable network of networks as a means to connect different users together.

The use of a GPS sensor accomplished two tasks as the data is passed from the laptop user to the other. First, because of GPS technology, data from the location of the sensor provided dynamic information that was constantly updated by the user using this end system allowing for multiple updates with new information. Second, the digital signature provides for integrity of the information originating from the desired source when received by the second user.

This test provided a proof of concept that a simple solution to the blue force tracker idea can be developed utilizing a Network Citizen that maintains itself in accordance with a few basic requirements. The LAN interface presented here is the wireless network card or the broadband wireless cell phone maintaining the laptop's connectivity with the Internet. The packaging interface of the information is the e-mail MIME structure of sending information in an e-mail format from a source to its destination. The PKI interface is determined with the Microsoft Outlook program which harnesses the power of using a digital signature in order to maintain confidence that the information is arriving from a trusted source. The Quality of Service is maintained by monitoring the network for particular hang-ups and ensuring those hang ups don't delay the routing of important information. In the case of this test demonstration, the use of the Verizon wireless cellular phone as a modem and using the Verizon wireless broadband Internet access instead of waiting for a random wireless network connection to be established. The management interface is the monitoring of the updates by the

monitoring station and a lack of timely updates can provide insight into a possible problem with the network or User Agent active connection.

This test meets the requirements of a good network citizen and maintains a sense of modularity with the ability to maneuver around freely and provide these GPS updates. The basis for using this example as a model to for any other system of information sharing shows how important this test has been. The idea of stove piping an updating system is proven unnecessary due to the simplicity of this demonstration. The User Agent can be any information system and not remain limited to GPS receiver data because the information in the file e-mailed can be of any type. Therefore, this test demonstrates the ubiquity of using a similar setup for any other type of information that has a need to be shared and monitored.

VI. CONCLUSIONS AND FUTURE DEVELOPMENTS

A. CONCLUSIONS

This thesis demonstrates that information can be secured with a digital signature from end-to-end across the Internet.

a.) The type of network that was available was irrelevant, and therefore did not impact the availability of the data during transmission. The only requirement is having a connection to the Internet, which is accomplished using the EVDO Verizon capability. Particularly noteworthy is that no need exists by the user to know anything about the type of Internetwork except that it is connected to the Internet. With the digital signature/PKI capability, the network can be either a hand radio or digital information and there is assurance of content security. In the end, there is a simple solution, and that solution is usually the correct one.

b.) In this experiment, information was sent and received using the tools provided. For this test case, position information was the information chosen to be transmitted, but this security procedure can apply to any case. The information does not need to be limited to what was performed here in order to meet the security levels demonstrated here. That is the advantage of this basic system setup.

B. FUTURE DEVELOPMENTS

A simple solution exists for ensuring security capability across the Internet that can utilize a simple solution to the authenticity of information transmitted across the Internet. First responders should take advantage of the simple solution provided by the current PKI capability to address security issues.

1. All end systems should only transmit data that is digitally signed. If confidentiality is required, then the end systems should transmit data that is encrypted. No end system should unconditionally accept data unless it a valid digital signature is detected.

2. The goal of future systems should be to move toward a similar design as presented here. If there is a requirement for the information to be sent across the network, investment should be along ensuring that the protection capability meets the simple requirements presented here. Early planning addresses many possible future security related issues. Using this already-established security concept provides a simple solution without complicating the how to talk from end to end. The end-to-end levels of security allow the designing/procuring of a system to have fewer issues down the line.

First responders have a need for information that contains these capabilities. All future systems to be developed need to require digital signatures for all network transmissions. The new focus on true systems interoperability would be achieved across local, county, state, and federal lines in a more cost-effective manner.

LIST OF REFERENCES

Buddenberg, R. (2006, July) Of Good Network Citizens and Internet toasters.

Buddenberg, R. (2007, December) Emergency services interoperable communications: Aka Internet and mobility for a model county.

Denning, D.E. (2001). *Information warfare and security*. New York: Addison-Wesley.

E-commerce, (2009). Retrieved May 15, 2009, from PKI Web site: http://www.ecommercepki.com

Elbaz, L. (2002, October) Using Public Key Cryptography in Mobile Phones. Discretix Technologies Ltd. White Paper.

Ellison, C. Schneier, B. (2000) Ten risks of PKI: What you're not being told about public key infrastructure. *Computer Security Journal*, *XVI* (1).

Final Report of the Public Safety Wireless Advisory Committee (PSWAC Final Report). September 11, 1996.

Google. (2009). Retrieved May 15, 2009, from Google Gmail account setup Web site: https://www.google.com/accounts/NewAccount?service=mail&continue=http%3A%2F%2Fmail.google.com%2Fmail%2Fe-11-11a0735fa97e454016b56c1597cc0f78-3963bc4a21dd2ef7b20205c1988979d6756b48cb&type=2

H. Gilbert Miller, Richard P. Granato, John W. Feuerstein, Louis Ruffino, "Toward Interoperable First Response," *IT Professional*, vol. 7, no. 1, pp. 13–20, Jan./Feb. 2005, doi:10.1109/MITP.2005.20

Harris, S. (2005). *CISSP: All in one exam guide*. Emeryville, CA: McGraw-Hill/Osborne.

Housel, T. J. (2008, January). Achieving interoperability in homeland security communications and operations: A "model county" field test.

Internet Security Glossary, Network Working Group Request for Comments: 2828. May 2000.

Internet x.509 Public Key Infrastructure: Certification Path Building, Network Working Group Request For Comments: 4158. September 2005.

Kiaer, M. (2007, May). A Microsoft PKI Quick Guide. Retrieved May 9, 2009, from WindowsSecurity.com Web site: http://www.windowsecurity.com/articles/Microsoft-PKI-Quick-Guide-Part1.html.

Merriam Webster Online Dictionary. (n.d.) Retrieved May 15, 2009, from Web site: http://www.merriam-webster.com/

Microsoft, 2009. Retrieved from Microsoft Office 2003 Outlook Setup Web site: http://office.microsoft.com/en-us/outlook/fx100647201033.aspx?ofcresset=1.

Morgan, M., Levitt, R.E., & Malek, W. (2007). *Executing your strategy: How to break it down & get it done.* Boston, MA: Harvard Business School Press.

National PKI: The Foundation of Trust in Government Programs. Verisign White Paper. March 2009.

Newman, D. (2001). PKI: Build, Buy or Bust. Retrieved May 9, 2009, from NetworkWorld, Inc. Web site: http://www.networkworld.com/research/2001/1210feat.html

PSWN Program's Analysis of Fire and EMS Communications Interoperability. Public Safety Wireless Network Program. April 1999.

Railsback, K. 2001 PKI is key to secure e-commerce. Retrieved May 11, 2009, from ITWorld.com Web site: http://www.itworld.com/print/39277.

SAFECOM 2006 National Interoperability Baseline Survey. December 2006.

Schumacher, L.J. (2008, December) Interoperability: Why the Current Definition is Wrong, and a Proposal to Adopt NATO's Definition of Interoperability for First Responders.

Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1, Network Working Group Request For Comments: 3851. July 2004.

State and Local Law Enforcement Wireless Communications and Interoperability: A Quantitative Analysis. National Institute of Justice. January 1998.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California