Deploying E-Mail as an Official Communication Tool: Technical Prospect

Wasan Shaker Awad Wasan_shaker@itc.uob.bh
Department of Information Systems
Information Technology College
University of Bahrain
Sakheer, Bahrain

Abstract

Applications are spreading widely through our lives entering every field controlling some of it and enhancing other; electronic mail, or e-mail, is the best known and most popular application of the Internet. More and more people see e-mail as a way to communicate quickly and affordably. Electronic mail can also provide an advanced means of communication and enhance the recently applied e-government program. The aim of this work is to study technically the official use of e-mail for the communication between the government and citizens. This paper is mainly for proposing an e-mail exchange system that can be used to fulfill the legal requirements, and to make the usage of e-mail as official communication tool is feasible.

Keywords: E-mail, E-government, Information Security, ICT.

1. INTRODUCTION

Mankind has always had a compelling desire to communicate, that's why many evolving communication methods had emerged through the years. Communication has revolutionized from traditional means to more advanced electronic communications. As a traditional way of communication, postal mail systems and courier services are considered to be the oldest forms of mail item distribution. Wherein written letters, and also small packages, are delivered to destinations around the world. Then communication has evolved to a new concept which is telecommunications, also known as electronic communication. Telecommunication is the transmission of data and information between computers using a communication link. It began in 1844, when Samuel Morse invented the telegraph, whereby sounds were translated manually into words using Morse code. Then in 1876, Alexander Graham Bell developed the telephone, which brought telecommunication into the home, and became crucial for business life for many years. After that facsimile (fax) was developed in the 1900s, which transmits documents over telephone lines. Technology continued to expand its influence, and another technology evolved in the telecommunication field. This technology was the Internet. Internet was mainly developed for the purpose of communication. One of the very first communication means through the Internet was e-mail [1].

In general, the official communication is done through traditional ways: sending the official letters or documents by post mail, and occasionally done by contacting the person by telephone or face-to-face. The message must be delivered by the correspondent person who works in the postal office to its destination. Then the receiver should approve the receipt of the message. To cope with the modern e-application revolution, there is a need to replace the traditional method of communication with more advanced and reliable electronic communication. The electronic mail, or e-mail system are best known and most popular network-based application. It is a way to communicate quickly and affordably. From here the idea of using the e-mail as official communication has emerged.

Adopting e-mail as official communication is a critical topic. The importance of this topic emerges from the wide use of e-applications, and the rapid improvements in the e-government filed. Hopefully the study results provide some small but valuable contribution to the research quiver especially to what is related to e-government field, and can consider as a trigger for a great revolution in the official communication.

The following points are considered as reasons that's motivates using electronic communication, and stimulate the need for an official E-mail Exchange System:

- The implementation of the e-government portal.
- The need of an electronic communication means for the fast, reliable and convenient communication that also copes with the emerging e-applications.
- The need of a new mailing system that can replace the current postal system and supports the extensive official communication securely and efficiently.
- The role of the modern technologies particularly the e-mail in enhancing the communication between the government and citizens.
- The inadequacy of current electronic communication infrastructure for the exchange of the sensitive, legal and private official communication.

Communication with both citizens and organizations involves the transmission of sensitive information and legal bindings. Consequently, electronic communication has to be highly secured. Although there is an infrastructure developed for commercial use of e-mails, this infrastructure is not securely sufficient for the exchange of the sensitive, legal and private official communication. As a result, there is a need of developing a new e-mail exchange system that fulfills the security and legal requirements. Thus, the main objective of this study is to investigate the feasibility of using e-mail as official communications, during the attempt to achieve the study's main objective many sub objectives will be delivered as well, and these objectives are:

- Provide a detailed study about the e-mail technology, its advantages, disadvantages, review of same case studies that has applied e-mail as official communication.
- Investigate the ability to implement this project technically.
- Provide a proposed system that supports the technical requirements of applying e-mail effectively and efficiently.

This paper is mainly for proposing an e-mail exchange system that can be used to fulfill the legal requirements, and to make the usage of e-mail is feasible.

2. LITERATURE REVIEW

E-mail, is short for electronic mail, is just an electronic message sent from one computer to another [2]. It's hard to remember what people's lives were like without e-mail. Ranking up there with the Web as one of the most useful features of the Internet, e-mail has become one of today's standard and preferred means of communication. E-mail usage by businesses became common several years before individuals began using it at home. Yet by the late 1990s, approximately 40% of all American householders owned a computer, and 26% of those families had Internet access. An analysis in 1998 indicated that there were 25 million e-mail users sending 15 billion messages per year [3].

E-mail is no longer just a method of communicating in business; it's a way of doing business. It has become an integral part of workers' lives. Most employees have Internet access at their work, and an e-mail account to help them in collaborating with their colleagues and customers, in order to be more productive at their work. A portion of those e-mails probably replaces the telephone calls or faxes or traditional mails [4]. For example, Western Provident Association (WPA) [5] which is one of Britain's leading health insurers, who insure over 500,000 people and more than 5,000 companies.

The main reason why people connect to the Internet is to communicate by e-mail. Traditional methods of communication are now converging onto the Internet – text messages, phone calls and video images can all be sent via the Internet. Furthermore, the growth in mobile communication and the continuing improvements in mobile communication devices means that e-mail is now accessible just about anywhere. So why e-mail taking the communication world by storm? These are the main benefits [6]: It is relatively low cost, easy to copy a message to many people at the same time, easy to

distribute information such as reports, spreadsheets, presentations and other files, personalized, convenient, relatively quick, and it does not sleep.

E-mail is a great tool used to communicate with others, however, with the added great advantages of e-mail, also comes some disadvantages such as: Viruses, Spamming, Flaming, Phishing, and E-mail Privacy and Security, such that, without some security protection can be compromised because [6]:

- E-mail messages are generally not encrypted.
- E-mail messages have to go through intermediate computers before reaching their destination, meaning it is relatively easy for others to intercept and read messages.
- In some business, e-mail messages of employees are monitored.
- Many Internet Service Providers (ISP) store copies of senders e-mail messages on their mail servers before they are delivered. The backups of these can remain up to several months on their server, even if the receiver deletes them in his/her mailbox.
- The received headers and other information in the e-mail can often identify the sender, preventing anonymous communication.

Although e-mail has several disadvantages, most of these can be solved easily. For example using an anti virus program provides protection from e-mail viruses, or some web mails provide message scanning for viruses. Spamming and phishing can also be handled by some web mail services. Moreover, most web mail services warn the user before opening an anonymous mail. Furthermore, there must be new rules and regulations to govern the use of Internet services, and to organize the exchange of the information across the world wide information net, mainly those information that are related to the official treatment and correspondences.

The problem of deploying email as official communication tool has been considered by a number of organizations and researchers. On November 6 and 7, 1997, with the sponsorship of the Markle Foundation, RAND convened a workshop in Washington, D.C. to begin a discussion of the character of the required infrastructure, who might plausibly provide it, how it might be financed, and what other policy changes (institutional, legal, programmatic) might be necessary to support secure communication between government and citizens. Attendees at the workshop included managers, policymakers, and analysts from a variety of government agencies at the state and federal levels and representatives of private-sector concerns that are users or providers, current or potential, of secure communications services [7].

At the Summit on the 21st Century Workforce, held June 20, 2001, in Washington, D.C., Secretary Elaine L. Chao announced the creation of a compliance E-Mail Initiative to ensure that the Department of Labor answers on a timely basis all electronic inquiries from DOL customers. This policy required all DOL agencies to establish and advertise electronic public contact mechanisms on DOL public Websites for collecting general comments, suggestions, or inquiries from the public and to develop procedures for handling electronic correspondence in accordance with this policy. This initiative provides the option for agencies to integrate electronic correspondence procedures with existing paper correspondence procedures [8]. The main purpose of this step is the establishment of OSHA E-Correspondence system, which provides for processing, routing, tracking, and responding to the public on general safety and health questions received through OSHA's public Website. The scope of this project was OSHA-wide. The project was based on the following basics:

- Department of Labor Electronic Correspondence Policy.
- Secretary's Order 2-2000, Department of Labor Internet Services, Section 6a.
- OSHA Instruction of Internet/Intranet Policy & Procedures of December 15, 2000.
- OSHA Instruction of Policy Issuances of December 11, 2000.
- OSHA Instruction of Non-Policy Issuances of December 11, 2000.

In order to achieve the above purpose the state must:

- Develop a system that ensures timely response to inquiries received through the OSHA E-Correspondence system.
- Notify OSHA through the Directorate of Cooperative and State Programs of any changes to the e-mail address designated to receive electronic correspondence.
- Maintain records of correspondence received and their responses to that correspondence.

The main offices and agencies that are involved in this project are National Office, Regional Offices, Area Offices, and State Plan States. These offices and agencies must implement the policies and

procedures contained in this project in order to ensure the consistency of the Correspondence. In addition to USA, Perry presets the use of e-mail in different countries [9]. Also, Yayehyirad [10] studied the possibilities offered by E-Government to Africa by documenting few initiatives on the continent that have developed innovative models that contribute to governments' efficiency, accessibility, transparency and accountability through the implementation of ICT based services. He also presented an application to provide a secure online email service to high level government officials. This implied the design and deployment of a corporate mail system for the government including the delivery and setup of mail servers.

This paper differs from previous studies by providing a general framework for deploying e-mail as an official communication tool between citizens. Although they presented an infrastructure for commercial use of e-mails, this infrastructure is not securely sufficient for the exchange of the sensitive, legal and private official communication. Consequently, developing a new e-mail exchange system that fulfills the security and legal requirements is needed.

3. THE OFFICIAL E-MAIL EXCHANGE SYSTEM LEGAL REQUIREMENTS

Deploying e-mails for official communications will be successful if:

- A number of legal rules and regulations should be set in order to govern the use of e-mail and the other e-communication means, and to organize the exchange of the information across the world wide information net.

- There is an awareness of the legislation interventions – locally and globally- to deal with the illegal and unlawful behaviors that it's performed via the e-mail and the other e-communication ways. In addition, there must be appropriate penalties against the individuals who cause those behaviors.

- There must be constraints that restrict the way of using e-mail in the official communication. The main purpose of these constraints is the assurance of the accuracy and the reliability of information being exchanged through such way of communication, at the same time these constraints are used to prevent the misuse of the citizen's sensitive information. Consequently, if these constraints were skipped there will be a stiff government penalties as well as civil suits. The responsibility in the e-communication field dose not confines on the management responsibility, but it includes the civil responsibility as well as the malefaction responsibility.

    a) **The Management Responsibility**: the management responsibility represented in the various penalties that usually issued by the management parties which has the role of mentoring and supervising the other parties that work in the E-communication field.

    b) **The Civil Responsibility**: regarding to the e-communication filed the civil responsibility is basically means the adherence of the individual citizens and the other parties that are involved in such communication to compensate the damages and harms they caused.

    c) **The Criminal Responsibility**: criminal malefaction responsibility is the inculpation of some of the actions that are related to the field of collecting, processing and distributing data.

- There must be continuance supervision and monitoring activities on the use of e-mails as the official communication, along with the ability of deciding on the legal responsibilities in case of skipping one or more of the rules and constraints that governs the use of e-mail as an official communication.

- There must be mechanisms to confirm that the message originated from its originator and that can take the place of the hand written signature usually used in the paper based official correspondent.

- There must be mechanisms for protecting the e-mail message that contains sensitive information, and to protect the behalf of the sender and the receiver, the sender and the receiver must agree upon a mechanism to confirm the reception of the e-mail message by its appropriate recipient [11].

4. THE OFFICIAL E-MAIL EXCHANGE SYSTEM SECURITY TECHNIQUES

The satisfaction of the above requirement requires the use of the following security techniques:

- **Message Encryption:** Protects the privacy of the message by converting it from plain, readable text into cipher (scrambled) text [12, 13].

- **Digital Signature:** An electronic, encryption-based, secure stamp of authentication on a message. The signature confirms that the message originated from the signer and has not been altered. Digital Signature provides Authentication, Non- repudiation and Data Integrity [14, 15].

- **Digital Certificate**: A digital means of proving your identity, using a public and private key pair. The private key is the secret part kept on the sender's computer that the sender uses to digitally sign messages to recipients and to decrypt (unlock) messages from recipients. Private keys should be password protected. The public key is sent to others or published in a directory, so that others can use it to send you encrypted messages. Mainly there the system will use two types of digital certificate: Identity and Authority Certificate [16].

    a) **Identity Certificate:** is the process of associating a public key with a particular user and establishing his identity.

    b) **Authority Certificate:** is the process of granting the user whose can now be verified, *authority* to access information, to make use of services, to carry out transactions, or whatever.

  Although this two functions (establishing identity Certificate and establishing authority Certificate) are distinct and quite separable and usually are initiated by different entities, in some cases they are initiated by the same entity, a government agency for example.

- **Conformation Mechanism:** An e-mail not reaching their destination is a growing problem, in case of the official communication this problem become more serious. Therefore there must be some mechanisms that can help both senders and receivers of emails to make sure their official emails are not lost. There are several confirmation mechanisms that can be used to ensure Official E-mail Exchange System delivery capabilities [17, 18]:

    a) **First: User Generated Feedback** is used to determine if Email is not flowing through the system. If no feedback is received then the system is presumed to be operating normally.

    b) **Second: Test Message Monitoring** is a variation of the user based feedback method. Instead of depending on user to notice non-delivery of E-mail messages, an administrator will periodically send a message through the E-mail system to a testing account. If the message is successfully delivered, the administrator assumes that the system is functioning properly.

    c) **Third: Looped Message Monitoring** is a variation of the test message monitoring method. An administrator still manually generates a message to test the E-mail system. The message is used to test the system by sending it through a loop to more than one testing accounts in different regions. If the test messages are successfully delivered, the administrator assumes that the system is functioning properly.

d) **Fourth: Automated Looped Message Monitoring** is a variation of the Looped Message monitoring method. Test message generation is automated by third party software. If the test messages are successfully delivered, the administrator assumes that the system is functioning properly.

e) **Fifth: Tracking Method** is based on using a tracking method such as the Pixel Tags. Pixel Tags are tiny invisible graphics (or minute embedded images) tucked away in HTML content distributed via e-mail that contain a set of instructions. When HTML-enabled e-mail clients open the HTML content, the pixel tag is instructed to contact a particular web server to receive a unique identifier code. This code is added to a special server log that records details of the machine and user receiving and opening the message. If the HTML content is forwarded to another HTML-enabled e-mail client, the pixel tag will perform similar functions, although it is limited in its ability to provide information on the referring machine. The information sent to servers can also be done by Web Bugs. Web Bugs are like the pixel tags described above. The affected e-mail clients at this point include Outlook 2000, Outlook Express, and Netscape 6 Mail Messenger, or any client which has JavaScript-functionality turned on by default.

f) **Sixth: Confirmation Software** using some of the confirmation software such as *Mailinfo* is another confirmation mechanism**.** Mailinfo allows the senders of emails to verify that the email messages have actually been received and notifies him/her the message has been read.

5. THE OFFICIAL E-MAIL EXCHANGE SYSTEM

This section suggests an official e-mail exchange system, which is a proposed solution to address all the necessary requirements in an official mailing system. The use of e-mail instead of the current postal system requires an e-mail exchange system with the following technical requirements:

- **Confidentiality:** Confidentiality means keeping information protected from unauthorized party.
- **Data Integrity:** Massages data is protected from unauthorized changes.
- **Authentication:** The process of identifying an individual**.** Citizens and government agencies must be sure that they are in fact communicating with the intended party
- **Non- repudiation:** A proof that a transaction occurred, or that user sent or received a message.
- **Access controls:** They are predicated on a system of identification and authentication -- that is, "Who are you?" and "Can you prove it?"
- **Confirmation of receiving and reading messages**.

Thus, the official E-mail exchange system can be implemented using a framework comprises three main technologies. These technologies are:

- Exchange server.
- E-mail client.
- (PKI) Public key infrastructure.

These technologies are interacting together to provide a secure environment for the exchange of the official communications [16]. Each of these technologies is used to meet some of the official e-mail exchange system requirements and to implement one or more of the security services introduced previously.

- **Exchange Server.** Exchange server is messaging and collaborative software. Exchange's many features consist of electronic mail, calendaring, contacts and tasks, and support for the mobile and web-based access to information, as well as supporting data storage. Exchange server act as an access point for sending and receiving messages. The e-mail client should be accommodated with one or more of the previously mentioned confirmation mechanism.

- **E-mail Client.** E-mail client is a front-end computer program used to manage email. The E-mail client should be accommodated with software confirmation mechanism.

- **Public key infrastructure (PKI).** Public key infrastructure is an arrangement that used to manage keys and certificates. In such systems, each user has one or more key pairs, each comprising a "public" key that is known to his or her correspondents, and a "private" key known only to the user. These keys can be used as encryption keys and as signing keys.

At the heart of the PKI there should be one or more Certificate Authorities (CAs) also known as trusted third party (TTP). Certificate Authorities are trusted institutions or organizations that will mainly certify that a particular public key is associated with a particular user. Usually, Some Certificate Authorities (CAs) will make use of the S/MIME (Multipurpose Internet Mail Extensions) which is a standard for public key encryption and signing of e-mail to perform the following functions:

- The establishment of identity certificates.
- The use of the public key information to encrypt messages.
- The use of the public key information and the standard to verify the digital signature of a message, which was made using the signer's private key.
- For others to have confidence in this identity, a CA must also be able to provide nearly instantaneous verification that a particular user/public key pairing is still valid (that the user or other authority has not for some reason canceled a public key).
- CA will also provide customer services such as replacing certificates that have been lost or compromised, publishing directories of public keys, and assisting users who experience difficulties.

Other Certificate Authorities that may or may be the government represented by the Central Informatics Organization will use the same S/MIME standard for establishing the authority certificates by associating each electronic identity with specific records or in our case specific e-mail account. Note that the two functions of (establishing identity Certificate and establishing authority Certificate) can be performed by the same Certificate Authorities in some cases.

6. WHO CAN ACT AS CERTIFICATE AUTHORITIES FOR THE GOVERNMENT AGENCIES?

The previous sections considered the definition and the main functionalities of the Certificate Authorities, and concentrate on their role in the official e-mail exchange system. But the question now is "Who Can Act as Certificate Authorities for the Government Agencies?" Certificate Authorities can be any government agency or commercial institution that can meet the following criteria [7]:

- **Highly reliable identification of agencies and users.** The official communications usually include the transmission of extremely sensitive information. Government agencies and citizens will require a very high degree of confidence that they are in fact each communicating with the intended party.

- **Local Presence**. To ensure reliable identification of users, CAs may require in-person interactions and perhaps the physical presentation of certain documents. This in- person interaction may have to be repeated periodically to maintain the validity of the digital certificate. If secure electronic communication is to be available to any citizen who desires it, then every citizen will have to have easy access to an office of a suitable CA.

- **Extensive customer service.** Official E-mail Exchange System requires a robust customer service operation **(**to answer questions, to guide infrequent and perhaps unsophisticated users, and to restore or to replace lost or compromised certificates as examples).

Examples of the commercial institution that may be positioned to provide CA services for secure official communication are:

- **Specialist Firms have begun to offer CA services.** This kind of firms is established to serve relatively small and specialized populations**,** so they expand their operations to the entire population**.**

- **Banks.** Banks have ongoing trusted relationships with their customers and already go to some lengths to establish customers' identities. Banks have many points of presence in almost all

communities and, at least occasionally, deal face-to-face with their customers. Finally, many banks are moving toward creating electronic banking systems to serve their own customers. It may turn out that such bank infrastructures can be exploited for communications with the government at minimal additional cost**.**

- **Other institutions that maintain continuing relationships with individual citizens might also be able to provide CA services.** Consider, for example, large health insurance providers or health maintenance organizations. Such organizations routinely establish basic identity information on their members and patients. Increasingly, these organizations may desire to communicate sensitive information (e.g. diagnostic test results, payment information, and appointment verifications) to doctors and patients electronically, and they may develop secure communications systems for their own purposes. Electronic identities established for these purposes might be sufficiently reliable for the transmission of sensitive government information.

In carrying out their missions, some government agencies and quasi-governmental entities have frequent or regular interactions with large numbers of citizens. They may, therefore, be plausible candidates for providing CA services to a broad population.

7. GETTING FROM THE CURRENT MAILING SYSTEM TO THE OFFICIAL E-MAIL EXCHANGE SYSTEM

Secure e-mail communication between government agencies and individual citizens will not become a reality overnight. Considerable groundwork must be laid: standards for privacy, integrity, and authentication must be established; certificate authorities must be identified or established; a host of institutional, administrative, and policy questions have to be resolved; and, most important, accumulating experience and maturing laws, regulations, and practice norms will have to provide a foundation for trust in using official e-mail exchange system for sensitive communications. The task of creating a capability for secure communication between governments and citizens can be accomplished by [7]:

- **An incremental, experimental approach.** The likelihood that we will get the system entirely right on the first try is vanishingly small, and there is little point in trying at the outset for a system that will meet all government demands. Much better to concentrate on functional requirements, and to experiment, starting with relatively undemanding applications and relatively no sensitive information, and then to gradually strengthen systems and procedures until we are confident that we can handle the most complex transactions and the most sensitive data.

- **Citizens should be able to "opt in."** At least during a transition period when the security and reliability of on- line communication with government agencies is still being demonstrated, citizens must be able to "opt in" to such communications arrangements, positively choosing for their records or accounts to be accessible on-line. It is unreliable to assume that citizens have sufficient understanding of the implications of on-line access and of procedures to control this access to make on-line access the default option.

- **"Out of band" communication will continue to be important.** To provide adequate assurance of the identity of an individual, it is often useful to use a separate channel of communication for verification. For example, although application for a digital identity certificate might be made on-line or in person, the password or personal identification number (PIN) unlocking or activating the certificate might be sent by postal mail to the correspondent's registered home address. All of this suggests that policy should aim to maintain and to utilize multiple channels for electronic communication: the Internet, automated telephone services, bank ATM networks, and the like.

- **Success will depend on education and training**. Successful development and deployment of mechanisms for digital communications between citizens and governments will require extensive efforts to educate citizens regarding the advantages of new communications modes and associated protections for sensitive information. Training in how to establish, use, and

protect a digital identity will also be key. Equally important will be establishing realistic expectations among users; just because e-mail can be transmitted nearly instantaneously.

8. CONCLUSION

This paper considered the problem of using e-mail as an official communication tool. This problem should be investigated from different prospective. Here, only technical one has been considered. This study presented that the adoption of e-mail as an official communication is legally tolerable. Also, this study has suggested a reliable e-mail system that can be applied as an official communication, which has met all the requirements, by deploying a number of security mechanisms.

9. REFERENCES

[1] Connell S., and Galbraith I. A."*The Electronic Mail Handbook: A Revolution in Business Communications*", Great Britain, Kogan Page Ltd, (1982)

[2] Hayden M., and Brad H. "*The On-Line/E-Mail Dictionary*", New York, Berkley Publishing Group, (1997)

[3] Abbate J. "*Inventing the Internet*", Boston, MIT Press, (1999)

[4] Lerner M. How Stuffs Work [Online]. Available at: http://www.learnthenet.com/english/html/20how_2.htm, [Accessed April 2008]

[5] Whelan J. "*E-mail @ Work*", Great Britain, Biddles Ltd, (2000)

[6] Computer Desktop Encyclopedia. Electronic mail [Online]. Available at: http://www.answers.com/Electronic+mail?cat=technology [Accessed May 2008]

[7] Neu C. R., Anderson R. H., and Bikson T. K. E-Mail Communication between Government and Citizens - Security, Policy Issues, and Next Step. RAND science and technology organization [Online]. Available at: http://www.rand.org/pubs/issue_papers/IP178/index2.html, [Accessed April 2008]

[8] U.S. Department of Labor. Occupational Safety & Health Administration Public Website. OSHA E-Correspondence system [Online]. Available at: http://www.osha.gov/, [Accessed April 2008]

[9] Perry T. S. "*Forces For Social Change".* IEEE Spectrum, 29(10):30 – 32, 1992

[10] Yayehyirad Kitaw. "*E-Government in @frica Prospects, challenges and practices*". Swiss Federal Institute of Technology in Lausanne (EPFL), 2006

[11] Abu Al Lail E. A. "*Legal issues of eTransactions*". Kuwait, Scientific Research Council, 2003

[12] Dam K.W. and Lin H.S. "*Cryptography's Role in Securing the Information Society*". National Research Council, Washington D.C., 1996

[13] Schneier B. "*Applied cryptography*", 2ed edition, New Jersey, John Wiley and Sons, (1996)

[14] Forouzan B. A. "*Cryptography and network security*", New York, McGraw-Hill, (2008)

[15] Stallings W. "*Cryptography and Network Security*", 4th edition, New Jersey, Prentice-Hall, (2006)

[16] Budd C. "*Exchange Server 2003 Message Security Guide*", Microsoft, (2004)

[17] Charles E. M. "*Ensuring Electronic Mail System Delivery Capability*". In Proceedings of the IEEE military communications conference. Atlantic City NJ, 1999

[18] Mailinfo Ltd. Don't let your emails get lost in spam! [Online]. Available at: http://www.mailinfo.com/web [Accessed May 2008]