SECURE E-LETTER ENTERPRISE MANAGEMENT FRAMEWORK

MOHD FIRHAN BIN MOHD SAMIAN

UNIVERSITI TEKNOLOGI MALAYSIA

SECURE E-LETTER ENTERPRISE MANAGEMENT FRAMEWORK

MOHD FIRHAN BIN MOHD SAMIAN

A project report submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia

JUNE 2012

Specially dedicated to my beloved father, Mohd Samian bin Hj Jani and my mother, Roszana binti Alias, also to Muhanizah Abdul Hamid and all my family members. Thank you to Assoc Prof Dr. Subariah binti Ibrahim, my friends and all those people who have guided and supported me throughout my journey of education.

Thank you so much & may Allah bless us..

ACKNOWLEDGEMENT

In the name of Allah, the Most Gracious and Merciful. Thanks to Allah, He who has given me strength and courage in completing my project report for Master in Information Security. I would like to take this opportunity to express my appreciation to everyone who involved in contributing for the successful completion of this project in due course of time. I am grateful for all the sacrifices, support and hope which is given to me so far.

I would like to express my deeply appreciations to my beloved supervisor, Assoc Prof Dr. Subariah binti Ibrahim for her words of encouragement, criticisms, and thoughtful suggestions. She also spends her valuable time giving me advice and guidance in writing a good report. I have learned a lot from her and I am fortunate to have her as my supervisor. Moreover, I would like to express my gratitude to Dr. Anazida binti Zainal for some comments on this work, their support and recommendation, which improved this thesis.

I am forever indebted to my parent, Mohd Samian bin Hj Jani and Roszana binti Alias for their everlasting love, endless support and patience. Also not forgotten to my special one, Muhanizah binti Abdul Hamid for her manual support, strength, help and for everything. Last but not least, I would like to thank all my friends for their assistance and cooperation and those person who are involved in completing this project.

ABSTRACT

In general, official letters are used in all organizations all over the world. An official letter will normally be written in the proper format then will seal and sent to the recipient to ensure that the letter is legitimate and pays tribute to the recipients. Nowadays, there have a system that provides a template to facilitate of creating official letter. However, the letter that has been completed will be sent to the Post Office to be signed, seal, and then sent to the destination. There is still use a lot of papers, take long time to deliver besides the confidentiality and integrity of the letter is not preserved. Therefore, a new research to create a new framework of Secure eLetter Enterprise Management System that provide a template following all attribute to enhance productivity and security of official letter. Digital signature and hash function can give a degree in level of security for the letter. In addition, access control is used in giving the confidentiality of the letter to make sure the letter only can be access by the authorized person. A new framework is design for more efficient services, faster and regular mail besides consumer safety as well as more secure.

ABSTRAK

Secara umum, surat rasmi digunakan dalam semua organisasi di merata dunia. Surat rasmi biasanya akan ditulis dalam format yang kemudiannya akan disampul dan dihantar kepada penerima untuk memastikan bahawa surat tersebut adalah sah dan memberi penghormatan kepada penerima. Pada masa kini, terdapat satu sistem yang menyediakan template untuk memudahkan mewujudkan surat rasmi. Walau bagaimanapun, surat yang telah siap akan dihantar ke Pejabat Pos untuk ditandatangani, disampul, dan kemudian dihantar ke destinasi. Sistem ini masih menggunakan banyak kertas, mengambil masa yang lama untuk menyampaikan selain kerahsiaan dan keutuhan surat itu tidak dipelihara. Oleh itu, penyelidikan baru bagi mewujudkan satu rangka kerja baru iaitu "*Secure eLetter Enterprise Management System*" yang menyediakan template bagi memenuhi kesemua ciri-ciri dan dapat meningkatkan produktiviti dan keselamatan surat rasmi tersebut. Tandatangan digital dan fungsi hash boleh memberi sudut keselamatan dalam tahap keselamatan untuk surat. Di samping itu, kawalan akses digunakan dalam memberikan kerahsiaan surat dan memastikan surat itu hanya boleh dicapai oleh orang yang tertentu. Satu rangka kerja baru ini adalah untuk mencipta perkhidmatan yang lebih cekap, lebih cepat dan teratur selain keselamatan surat dan pengguna lebih terjamin.

TABLE OF CONTENT

LIST OF TABLE

LIST OF FIGURE

LIST OF ABBREVIATION

XHTML	Extensible HyperText Markup Language
HTTPS	Hypertext Transfer Protocol Secure
DMS	Document Management System
ELETTER	Electronic Letter
SEPT	September
CC	Copy Carbon
REF	Reference
NO.	Number
PDF	Portable Document Format
SMTP	Simple mail transfer Protocol
POP	Post Office Protocol
IMAP	Internet Message Access Protocol
EXE	Executable file
NeAF	National e-Authentication Framework
PKI	Public Key Infrastructure
DSA	Digital Signature Algorithm
RSA	Rivest, Shamir, and Adleman
XML	Extensible Markup Language
UML	Unified Modeling Language
SDLC	System Development Life Cycle
HDD	Hard Disk
SQL	Structured Query Language
CA	Certificate Authority

CHAPTER 1

INTRODUCTION

1.1 Introduction

Letter is a written message from a person to another person in other meaning for communication between two people in another location. In an organization, letter is send formally or informally with important subject and message to other people or client in order to dealing with a business, personal or diplomatic reason. As a various communication technology evolved, posted letter that being a routine form of communication has become less important because of the time taken to print it out, sending it as a hardcopy format to the destination. For person where outside from the country, it takes longer period to make the letter delivered.

In early, a paper-based signing process is written by handwritten message or typed by the typewriter on a piece of paper. With the information of sender and receiver like name and address at the top of letter to ensure that letter are from who and for who the letter want to be sent. Followed by the date, subject and the content of message to represent the reason letter are sent. At the end of the letter, there is name including the handwritten signature of sender as the confirmation and proof that the letter is from sender.

Since computer technology is designed to sequentially and automatically carry out a sequence of arithmetic or logical operations and have been used daily, the electronic world has typically begin with a paper-based signing. A document in the most correspond software application is created such as Microsoft word is suitable for build a text, Excel works for budgets and XHTML is used for Web forms makes all the work become easier. Then the document created electronically and digitally is printed to a paper and their handwritten signature is applied.

Handwritten signature look simple enough, but the significant of the signature is quite substantially. That signature represents permission and identifies of the signer. The ink binds the signature to the paper permanently so that it's almost impossible to remove it. These purposes are the establishment of the legal requirements for signing in other words, in a court of law, that signature makes for a legally enforceable contract.

Nowadays, computer technology and internet are becoming the first thing in human daily activities. Nowadays, everywhere there have been new technologies approaches. The particular sequence of operations can be changed readily, allowing the computer to solve more than one kind of problem. For an example, letter are now can be delivered through technology without go to the post office.

Electronic letter, commonly called "eletter" or "e-letter" is a method of exchanging digital messages from an author to one or more recipient and will operate across internet or other computer network. This increased of technology makes the time for letter delivered to recipient shorter and the letter can be accessed anywhere and anytime since the recipient open it as long as the recipient have an internet access. In additional, electronic letter can help the environment consumption based on complying with the Paperless Office Concept provide functionality which satisfies the requirement for traceability of administrative actions especially as regards the principle of placing things on record.

E-letter can be considered a special form of e-business. E-commerce can be defined from the several perspectives of business such as communications, commercial, business process, service, learning, collaborative and community. From business process, service and communication perspective, e-commerce is an enable of online service and communication in an organization.

E-letter is commonly used in two purposes; for the personal user or enterprise reason. The services that provided to personal user is allows to build a quality mail communications and electronically transfer them for printing, enveloping, address validation, barcoding and lodgments without leaving the desk. User are not required to go to the post office to send a letter, putting it in an envelope, write the address destination and waiting for the envelope to be collected and delivered to the recipients.

It's about bringing online capabilities and physical mail together in a "hybrid" solution. The idea of hybrid mail is a simple one which is being able to send all the data for a direct mail campaign electronically to one central location and then having that mail actually printed and lodged as close as possible to its destination. All the work that needs to be done on the data is therefore undertaken at the central location before it is sent directly to production. Not only is this much more efficient, it's also a more environmentally friendly solution because much less fuel is used in transportation.

Using this service, the mail or document shall be lodge electronically today and delivering to the mail of recipient in a day without go out to the post office. The documents will securely be lodged by email, direct file transfer or the internet (HTTPS) and be able to get a return email for validation of lodgments. Once that service receive the lodgment, the addresses are validated and then the documents are barcoded, pre-sorted, printed, enveloped and lodged.

For other purpose, organization use e-letter for enterprise reason. Most of organizations are changeover from the traditional, time consuming paper processes and finding new and innovative technology to increase efficiency. Normally heard the name of ‘letter head’ that organization uses to communicate or deliver something important message formally.

The duty officer received instructions to type and sends the letter to client in other organizations through the system provided. The most common security risk of intrusion of an access control system is for authorized users, such as user passwords, screen saver passwords and limiting access to shared network drives to authorized staff. Strategic design created to enhance interaction and encourage response. Functional of creative execution that demands attention such as form methodology and template for selection type of business. Firstly format the data into required communication template including addresses which is one of the components of the letter. Documents are then electronically sent to the Mail Exchange Server.

A document management system (DMS) is a computer system (or set of computer programs) used to track and store electronic documents and usually also capable of reporting and keeping track of the different versions created by different users (history tracking). Reference number is a unique number represent the letter and to differentiate to another letter. All the letter that have been sent have a reference number before the document stored in a database as a backup to make sure the document can be access if needed or restored when disaster happened.

An Electronic Process Signature is a new form of electronic signature technology developed by (Silanis, 2005) for Web-based transactions and electronic document automation. In fact of delivering the document including the review, signing and acceptance will grab and keep the entire Web sequence of programs and its contents. At the final transaction, the document is stored and need to sign and will be delivered by an electronic document automation system.

Businesses that have been reaching a successful achievement not only give the best services in order to make the transaction run smoothly. The consideration and focusing in security issues that increasing day by day must be include performing an efficient business provider. Beside the improvement of the effectiveness between communications to both customers and prospects, shorter process cycle times, accelerated customer service and drastic cost savings, the ability in secure the data during designing, transaction and deliver must be in priority.

Authentication, integrity and non-repudiation are closely interrelated during the data transaction.

Digital signatures can significantly benefit to organizations. The ability to immediately sign and seal documents and electronic transactions results in a shorter cycle time processes, customer service, and rapid and drastic cost savings. The digital signature provides improved for both customers and organizations, at the same time reduce application processing time.

The objective of sign the paper digitally is like sign the paper with handwritten signature. For paper based signing, pen and paper is used while digital signature uses digital keys (public key cryptography). Handwritten signature on a piece of paper is attached the identity and originality of signer and also digital signature represent the identity of the signer to the document and records a binding commitment to the document. The main reason of using digital signature is digital signature is impossible to be forged unlike the handwritten signature.

Digital signature is embedded in the e-letter that can be used to authenticate the identity of the sender of the message or the signer of a document and to ensure that the original content of the message or document that has been signed is unchanged.

1.2 Problem Background

In the name of technology, letters are still being the intermediation particularly by law firms and businesses, for official (public) notifications, sometimes used for advertisement. A paper-based signing process is use based on signing with handwritten signature on the paper. The subject, content and message are proven by a handwritten signature.

The advantage of using paper-based signing process with no special device is needed in which almost all people who have homes or other places where he can receive e-mail. Mailbox is what the requirements intended recipients, unlike e-mail or phone call, in which the intended recipients need access to a computer and sender e-mail or phone respectively. "Catch-all" advertisement is not like e-mail, in which the recipient's e-mail requires an individual to receive the message, individuals not need to be selected, with a relatively wide can cover any or all the address given place. Important messages that need to be maintained in the physical records (for an example is invoices; government such as tax notices or immigration) can be stored with relative ease and safety.

There have advantages but also have weaknesses using paper-based signing process. Paper is used in all printed document which can increased the cost besides the physical record are using space to store the file. Time spent too long hunting through stacks of paper for an invoice or searching through paper files. The handwritten signature is open and can be copied from unauthorized person. Authentication, integrity and non-repudiation from this paper-based signing process are not secure.

The growth of e-letter in recent years has not been as robust as expected for several reasons. One of these is undoubtedly the inability to ensure security and online authentication in online services environment. Since the Internet is exposed to various types of security breaches, the discussion on the operation of a robust e-mail and confirmation is not complete without taking into account safety as a key aspect of an online signature or digital signature (Shiralkar, 2003). Many emerging technologies are being developed to provide online authentication. One may consider a digital signature as a type of electronic authentication (Shiralkar, 2003).

Digital signature data attached to or included in the message that proves the identity of both documents and content of the message (Alan, 2007). Digital signatures try to ensure the integrity of both the message and also provide evidence that the messages coming from a particular sender. The digital signature allows the public to sign digital documents by providing features a handwritten signature. They must meet the following attractive features such as a handwritten signature authentication, integrity and non-repudiation (Schneier, 1996). In the case of handwritten signatures, both the signature and the document are physical things, which make it difficult for the 'signatories' to claim the signature is not their own. In order to provide a secure digital signature scheme, these properties must be satisfied (Tulu et al., 2004).

A transaction between users through the Internet requires a protocol to provide confidentiality and authentication of both the sender identity and message content (Alan, 2007). One issue frequently arises as organizations seek to promote e-letter is the validity of electronic transactions and other electronic documents. This issue has some aspects (James, 2003):

i. Authenticate a person that have never met face to face is the person he claim to be.
ii. To make sure the integrity of message will be preserved if there have one party (or hacker in a communication stream) trying to change the content of a document.
iii. Make sure that a party cannot deny or repudiate an agreement by claiming that he never sent the message, arguing, for example, someone else was impersonating to be him online.

These problems can be solved by security technologies. The largest remaining problem with doing serious work in e-letter over Internet that is its current anonymous nature and the corresponding lack of accountability. The rapid development of e-mail raises the need for online security and authentication. To be a successful services platform and meet the organization online business goals, the e-letter system should be a highly secure performance and trusted environment.

Intrinsic electronic signature that is different from the handwriting that they can take advantage of various security measures increase. Associated technologies offer, which is the means to ensure data integrity, non-repudiation and confidentiality, the relevant characteristics of both a pure security perspective enhance technical, and the handwritten signature must be replaced in the different types of electronic networks.

1.3 Problem Statement

How to design a secure eLetter Enterprise framework that can enhance the level of security which fulfils the requirement of official letter besides improve enterprise letter management efficiently and securely and reduce the manual process.

1.4 Project Objective

The objective of this project is to develop and implement a new framework for a secure e-letter enterprise management to secure the data confidentiality, integrity, authentication and non-repudiation of e-letter.

i. To study on manual letter management in an organization.
ii. To study an electronic letter, its components and workflow of eLetter system as well as manual letter management.
iii. To design a framework of a secure e-letter management for an enterprise that provides confidentiality, authentication, integrity and non-repudiation.
iv. To implement and test the secure e-letter management system as a proof of concept for proposed framework.

1.5 Project Scope

The scope of this project is to secure the e-letter management system for an enterprise based on three security issues which are:

i. Security services address are confidentiality, integrity, authentication and non-repudiation.
ii. Template gives usability and flexibility with following the proper format of writing official letter.
iii. Totally paperless that can promote green technology which reduce cost, time and save environment.

1.6 Significant of Project

Based on the assessment and initial expectations, it is hoped the new framework that will develop can bring benefit and interest to the parties involved, namely the administration and users of the system itself. Here are the importance and benefits found in this system:

i. Letter will be sent to the recipient easier, faster, secure and can save the used of paper which can reduce the cost and save the environment.
ii. This framework will increase the degree of security which is confidentiality, integrity, authentication and non-repudiation of the letter and the user itself.
iii. Template is being used to give usability and flexibility for user and make sure the official letter produced is following the format before it sends to the recipient.

1.7 Organization of Report

Chapter 1 explains the introduction of the development in project, the introduction includes the overall explanations of the purposes of the project. In addition, this chapter includes the problem background, problem statement, objectives and the scope of project. While chapter 2 discuss about the literature review, where it explains the current systems or application that similar to the developed project. This chapter also explains about technique, method, equipment that has been used in this developed project.

Chapter 3 discuss about the overall approach and framework chosen for research and development of developed project. The content of this chapter can hold the operational framework, methods, technique or approach that is used during design and implementation of the project. Chapter 4 discuss of the proposed framework for securing sending eLetter for an enterprise, selected security features and conceptual framework for the developed project.

Chapter 5 discuss about the design interfaces and code function that related to the selected security features, system implementation and testing. The implementation and testing is to verify the performance, reliability and functionality of developed system. Chapter 6 is discusses about the achievements and result that have gain from developing system.

REFERENCE

Carol Poster and Linda C. Mitchell, eds., Letter-Writing Manuals and Instruction from Antiquity to the Present (Columbia, SC: U of South Carolina Press, 2007).

Richard Walker. *White Paper: Achieving The Paperless Office.* USA. Efficient Technology Inc. (2009).

United States Environmental Protection Agency (USEPA), *Municipal Solid Waste In The United States: 2005 Facts and Figures,* Office of Solid Waste (2006).

Jon S. Gardner, Juin J. Wang, Matthew V. Scott. Messaging and document management system and method. (2009).

Zhang Xianhong. Principle and Technology of Digital Signature[M]. Beijing: Machinery Industry Press, 2004: 15-98.

Chen Tianhuang, Digital Signature In The Application Of E-Commerce Security, School of Computer Science and Technology, Wuhan. 2010.

Chen XiangLin. Digital signature technology and algorithm. Fujian PC, 2007, 6: 58-59

Miles Tracy, Wayne Jansen, Karen Scarfone, and Jason Butterfield, Guidelines on Electronic Mail Security, NIST Special Publication 800-45 Version 2, 2007.

Jones,M.R. Cooking The Data? Science News 8. 1990. 878-891.

Smith,J.P. Studying Certainty. Science And Culture 9. 1989. 442-463

Nancy Flynn, Tom Flynn, Writing Effective E-Mail, Fifty-Minute Series, 1998.

Silanis, “How Much Security Is Enough? Security in Electronic Documents and Signatures”, Silanis Technology Inc. Whitepaper, 2005.

Shiralkar and Vijayaraman, “Digital Signature: Application Development Trends In E-Business”, Journal of Electronic Commerce Research, VOL. 4, NO. 3, 2003.

Schneier, B., Applied Cryptography, John Wiley & Sons. 1996.

Alan G. Konheim, Computer Security and Cryptography, John Wiley & Sons. 2007.

Tulu et al., “Design and Implementation of a Digital Signature Solution for a Healthcare Enterprise”, Proceedings of the Tenth Americas Conference on Information Systems, New York, August 2004.

James X. Dempsey, “Creating the Legal Framework for Information and Communications Technology Development: The Example of E-Signature Legislation in Emerging Market Economies”, 2003.

Eero Huvio, John Gronvall, Kary Framling. Tracking and Tracing Parcels Using a Distributed Computing Approach, Helsinki University of Technology, 2005.

National e-Authentication Framework (NeAF). Department of Finance and Deregulation, Australias Goaverment Information Management Office, Australia. 2009.

Voydock, V.L., Kent, S.T, “Security Mechanisms in High-Level Network Protocols”, ACM Computing Surveys, Vol. 15, No. 2, Jun 1983, pp. 135-171.

ISO 7498-2, “Information Processing Systems - Open Systems Interconnection - Basic Reference Model”, Part 2: Security Architecture, International Organization for Standardization (ISO), Geneva. 1989.

Weippl Edgar, Security in E-Learning, Springer Science + Business Media, Inc. 2005a.

NIS, National Information Systems Security (INFOSEC) Glossary (1992), Federal Standard 1037C, NSTISSI No. 4009, June 5, 1992.

Richard E. Smith, Basic Glossary from Internet Cryptography, Addison Wesley. 2003.

Miles, H. and Huberman, M., Qualitative Data Analysis: A Sourcebook, Sage Publications, Beverly Hills, CA. 1994.