

Policy Formulation and Development of Secure Environment for Information Sharing

By

Shahid Iqbal

2011-NUST-MS-PHD-CSE-40

MS-11 (SE)



Submitted to the Department of Computer Engineering in fulfillment of the
requirements for the degree of

MASTER OF SCIENCE

In

SOFTWARE ENGINEERING

Thesis Supervisor

Dr. Shoab Ahmed Khan

College of Electrical & Mechanical Engineering

National University of Sciences & Technology

DECLARATION

I hereby declare that I have developed this thesis entirely on the basis of my personal efforts under the sincere guidance of my supervisor Dr. Shoab Ahmed Khan. All the sources used in this thesis have been cited and the contents of this thesis have not been plagiarized. No portion of the work presented in this thesis has been submitted in support of any application for any other degree of qualification to this or any other university or institute of learning.

Student Signature

ACKNOWLEDGEMENTS

Innumerable words of praise and thanks to Allah, the Almighty, and the Creator of the universe for carving the path for me and always helping me out in the best possible way. Without His Will and Mercy, I would not have been able to accomplish this milestone. I am grateful to my parents for their immense love, moral support, encouragement and prayers throughout my academic career.

I am deeply beholden to my supervisor, Dr. Shoab Ahmed Khan, for his continuous guidance, inspiration, and patience. His ability of management and foresightedness taught me a lot of things which will be more helpful for me in my practical life. I am also very thankful to him, for the provision of all kinds of facilities during my thesis work.

I gratefully acknowledge the help and guidance provided by Guidance and Examination Committee members Dr. Saad Rehman, Dr Muhammad Abbas, Dr Muhammad Hasan Islam. Their valuable suggestions and comments were a great source to improve the research work presented in this thesis.

DEDICATION

To my family and teachers

ABSTRACT

Flow of information among strategic and public organizations is core requirement to meet their goals and objectives. In these organizations, sharing of information in timely manner is the utmost requirement but at the same time controlled and monitored exchange of information with confidentiality, integrity and non-repudiation is also very critical objective. Other security principles like need to know, least privilege and separation of duties are also very important to consider while handling classified information during the course of sharing. Security levels and security clearance plays vital role for access control. This work presents a policy based secure collection of security mechanisms that build a secure environment to assure above mentioned security requirements. Use of proven and established security techniques and existing technologies is preferred where possible. The focus of research is on defining of security policy elements, policy enforcement and monitoring for secure and trusted sharing while providing all security essentials including confidentiality, integrity, access control, authorization, authentication and accountability.

TABLE OF CONTENTS

Table of Contents	3
List of Figures	5
List of Tables	6
1.0 Introduction	8
1.1 Introduction	8
1.2 Motivation	9
1.3 Background	9
1.4 Structure of the Thesis	10
2.0 Literature Review	12
2.1 Background	12
2.1.1 Mutual Understanding	12
2.1.2 Secure Network	12
2.1.3 Access Control	12
2.1.4 Secure Disposal	13
2.2 Previous Work	13
2.3 Gap Analysis	25
2.4 Summary	26
3.0 Policy Framework	28
3.1 Inter Organization Information Sharing (IOIS) Framework	28
3.1.1 Memorandum of Understanding	29
3.1.2 Secure Network	29
3.1.3 Access Control	30
3.1.4 Secure storage	30
3.1.5 Sharing Methodology	31
3.1.6 Hosting and Monitoring of Sharing Environment	31
3.2 Summary	32
4.0 IOIS Design	34
4.1 MOU	34
4.2 Secure Network Design	34
4.3 Proposed network Design	35
4.3.1 Compartmentalization:	35
4.3.2 Network Devices proposed	37
4.3.3 Server Machines proposed	37
4.4 Secure Transfer Application Design	37
4.4.1 Access Control	38
4.4.2 User Roles	38
4.4.3 Information Classification	38
4.4.4 Audit Trails	38
4.4.5 Storage rules	38
4.4.6 Registration Policy	38
4.4.7 User Interface	38
4.4.8 Database	38
4.4.9 Authentication Mechanism	39

4.5	PKI design	39
4.6	Secure Email Setup Design	43
4.6.1	Secure Email Benefits	44
4.6.2	Email Rules	44
4.6.3	Secure Email Deployment Design	44
4.7	Secure FTP Server	45
4.8	IOIS -Auditing and Monitoring	46
4.9	Summary	47
5.0	IOIS Implementation	49
5.1	Secure Application	49
5.1.1	Functional Rules	49
5.1.2	File sharing Methodology	50
5.1.3	Functions of each user Role	50
5.1.4	Technologies used	51
5.2	PKI System Development	52
5.3	Configuration of Secure Network.	54
5.4	Establishment of Active Directory services and Secure Email Server	55
5.5	Network and System Monitoring	57
5.5.1	System Level Monitoring	57
5.5.2	Network level Monitoring	58
5.6	Sequence of Activities	59
5.7	Evaluation And Analysis	69
5.7	Summary	73
6.0	Conclusion And Future Work	76
6.1	Contributions	76
6.2	Future Work	78
	REFERENCES	79
	APPENDIX A: MOU	84
	APPENDIX B: SECURE TRANSFER APPLICATION	86
	APPENDIX C: PKI SYSTEM DEPLOYMENT AND USAGE	92
	APPENDIX D: DEFINITIONS	100

LIST OF FIGURES

Figure 2.1: Data sharing across organizations	13
Figure 2.2: A policy Life Cycle	15
Figure 2.3 : Intelligence Information Sharing Factors	16
Figure 2.4 : Influencing Intelligence Information Sharing	17
Figure 2.5 : Architecture for Data Sharing in Campus	18
Figure 2.6 : HTTP Request – Sample	18
Figure 2.7 : Government Information Sharing -Theoretical Model	19
Figure 2.8 : Expanded Model for Information Sharing	20
Figure 2.9 : Layer Model e-GIF	22
Figure 2.10 : Information Security Policy Framework	23
Figure 2.11 : TrustStore Architecture	24
Figure 3.1 : Inter Organization Information Sharing (IOIS) Framework	28
Figure 4.1: Secure Network Design	36
Figure 4.2: Secure Application Design	38
Figure 4.3 : Authentication Mechanism	39
Figure 4.4 : CA hierarchy	41
Figure 4.5 : Certificate Path	42
Figure 4.6 : PKI Deployment	44
Figure 4.7 : Secure Email Design	46
Figure 4.8 : Secure FTP	47
Figure 4.9 : Auditing and Monitoring	48
Figure 5.1 : PKI Configuration	54
Figure 5.2 : Active Directory Deployment	56
Figure 5.3 : Email Security	57
Figure 5.4 : Network Monitoring System	58
Figure 5.5 : System starts up email	60
Figure 5.6 : User login alert mail	61
Figure 5.7 : Login to Secure Transfer Application	62
Figure 5.8 : Upload File for sharing	63
Figure 5.9 : Marking to Selected User	64
Figure 5.10: Outbox view	65

Figure 5.11 : Inbox view	66
Figure 5.12 : Email Message - Encryption	68
Figure 5.13 : Email view at Reading Pane	69
Figure 5.14 : Received Encrypted Email	69
Figure 5.15 : Security Controls Efficiency	71

List of Tables

Table 1 : Boundaries relationship and complexities	21
Table 2 : Recommendations for Validity Periods	43
Table 3 : Different Networks IPs	56
Table 4: Evaluation of Sharing Methods	74

CHAPTER 1: INTRODUCTION

CHAPTER 1: INTRODUCTION

1.1 Introduction

Information is most valuable assets for an organization. It has to be secured and properly handled when in use. High degree of trust and confidences is achieved when a trusted environment provides confidentiality, integrity and availability [8]. One way to enhance information security is to create practicable policy for required purpose and environment. Information sharing remains paramount importance among different agencies, departments and coalition networks during normal routine functions and/or in the event of crises, that may be combat operations, terrorist attack or relief operation in case of natural disaster . It is compulsory to have foolproof methodology when value added services are required to build on such data resources which are not in the control of an organization and immediate sharing of necessary information in timely and proper format is needed. To develop a policy that is acceptable to stakeholders and that encodes appropriate risk vs. benefit tradeoff [1]. A practicable policy for more than one organization needs to consider multiple factors, some of which can be in conflict with one another. Departmental privacy and security policies, cultural and technical issues and lack of knowledge about technologies and their use make timely and complete sharing of essential information difficult for governmental and public organizations. Most important the security concerns of organizations like authentication, authorization, confidentiality and integrity of data and specifically intelligent handling of information after transfer are required to be justified before start of information sharing. In reality there is conflict between data sharing and data security [2-3].

In this research work, the intent is to formulate a policy framework to simplify the information sharing among required partners which can address maxim of the security challenges faced. The framework delivers secure and tested environment with practicable security policies and technologies for enforcement of those polices which can handle the security, privacy and authorization concerns of participating organizations. This fulfills the holistic demands of all pre and post transfer concerns of information sharing. It starts with establishment of secure and monitored network among participates till secure storage and role based user access controls as per security clearance, need to know basis and security classification of information and proper accountability using available technologies which

ensures Authentication, Authorization, Accountability (AAA) and non repudiation. It also encompasses the need of physical and environmental security standards to cater threats other than information technologies.

When we talk of file sharing policies it is must cover policy for confidentiality, privacy and trust [2] and must satisfy AAA conditions [4]. The information sharing is not confined to just classification of information, encryption of data and data paths or interoperability but controlled multiuser access control in heat of crises situation [2]. Different Access control models are being used since long including Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-based Access Control (RBAC) and policy-based access control model (PBAC) [6]. These models work well in different environments mostly when controls required within one organization but when some operation among different organizations is required, there are limitations and constraints faced using these models. These models are rigid when implemented by different vendors and most popular model RBAC only cater for roles and assignments but not permission [7] and it also does not cater object security classification and subject security clearance when accessing classified information. It just look for roles as assigned once may overshadows need to know security principle. In this research combination of RBAC and MAC is used for access control and other essentials for classified information sharing are also defined. Use of real time monitoring and auditing is also incorporated to fulfill the requirements of accountability and forensics.

1.2. Motivation

File sharing and simple document sharing techniques and technologies are easily available to share at organization or team level and much of work is done for peer-to-peer sharing which consider routine information sharing. However there is no detailed methodology available to share classified data among organization basing on security classification and defined access control.

1.3. Background

As it will be discussed in more details at chapter 2 that various researchers like Douglas Harris, Latifur Khana [2] and many others have tried to improve the methods and techniques to share classified information. All the work done is to have standard and interoperable network environment for smooth exchange of information. Main emphasis is required to

build trust among the organizations. However as shown in chapter 2, already work done is basically for health sector or among worker of same organization where security requirements are different as this work has scoped sharing of classified information.

In this research work we would first define policy methodology for classified information sharing followed by development of secure environment to have proof of concept.

1.4. Thesis Organization

Chapter 2 provides background to the current research. Initially concepts of MOU, Secure network, access control and secure disposal of information are discussed. It is mentioned that how the policy is evaluated and factors which really influence the process of information sharing. Some discussing about different models of access control is also included.

Chapter 3 describes the detailed designed of proposed framework. The aim of this chapter is to provide details of all the parts of framework and understanding of the framework is made easy.

Chapter 4 highlights the detailed design process for the proposed framework. The aim of this research is design environment in which the proposed framework can be practiced.

Chapter 5 focuses of the complete implementation details of the framework as designed in previous chapter. It includes the brief description of the software along with the details of the environment in which the project was done. Comparison of the proposed framework with exiting methods and techniques of information sharing is made at end.

Chapter 6 concludes the research work and summarizes the whole work done.

CHAPTER 2: LITERATURE REVIEW

CHAPTER 2: LITERATURE REVIEW

2.1 Background:

As discussed earlier, the need of well-timed information sharing among different organizations especially in emergencies, disasters and joint operations remains an important issue. Policies and different guiding principles are always been there to manage smooth and efficient information sharing [8-10]. Information is most valuable asset in all government and public sector organizations. Information resources are accessed and utilized by the employees and other people. As most valuable asset is mostly used recourse so certain amount of security is required to ensure confidentiality, integrity, and availability of this asset. Secure and reliable sharing needs mutual understanding, secure network, robust access control and secure disposal of shared data.

2.1.1 Mutual Understanding

Mutual understanding among stakeholders for information sharing and handling of information sharing is basic element of trust. Most of the time legal agreements are not covered when financial or monetary terms are not involved. Best choice is memorandum of understanding (MOU) when legal liabilities are to be avoided. An effective and detailed MOU plays vital role in preventing disputes and misunderstanding by clarifying the expectations of stakeholders.

2.1.2 Secure Network

To ensure confidentiality, integrity, and availability during any information access process secure network is basic building block. Secure network increase confidence and trust on the system and 24 x 7 availability is ensured only through redundant and secure network.

2.1.3 Access Control

To manage access and accountability of information a robust access control system with detailed audit trails is mandatory. Different types of access control models and systems are available. Most popular access controls systems are role base access controls system (RBAC) and Mandatory Access Control (MAC) to manage access to classified information systems.

2.1.4 Secure Disposal

When classified information is shared than proper handling and disposal is responsibility of both sender and receiver. Storing at insecure storage or deleting data from storage media (hard disks, CDs, taps, USBs, etc) posses many dangers as simple deleting does not permanently destroy the information. Storage media required proper sanitization before disposal and shredding of electronic files for proper deletion.

2.2 Previous Work

Different authors have proposed different approaches for information sharing process [2-3]. To start any kind of sharing, it is evident that all the participating organizations need to work under some defined security and sharing policy so that all activities are streamlined. As emphasized by Douglas Harris, Latifur Khana at *Standard for secure data Sharing across organization* [2] that flexible architecture and techniques are to utilized particularly using standard based approaches. Figure 2.1 [2] has demonstrated the need of coordinated and standard based activities among different organizations (such as CDC: Center for Disease Control, HRSA: Human Resources and Services Administration) are working together in an emergency situation to manage crisis.

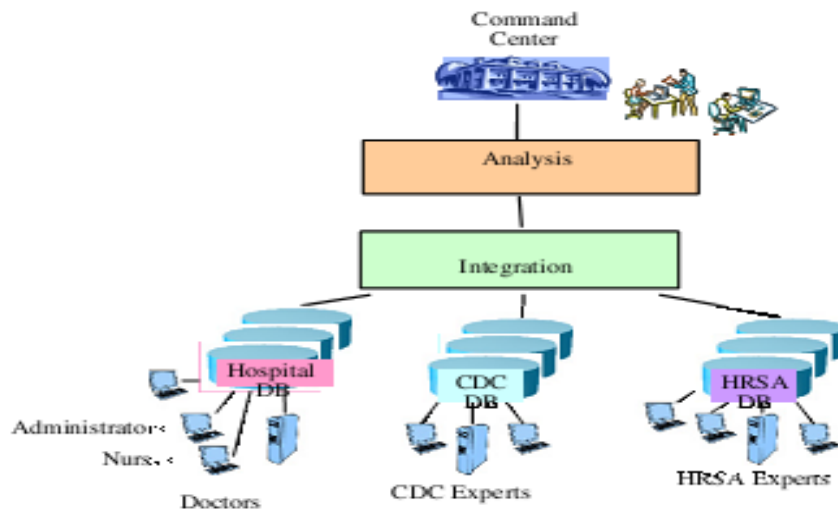


Figure 2.1: Data sharing across organizations [2]

The coordinated and standard based activates among multiple organizations required policy based approach so that all participating organizations have common platform to act and fulfill each other's demands. A policy as defined in the New Oxford Dictionary of English as “a course or principle of action adopted or proposed by a government, party,

business or individual”. The policy not only covers the future action of plan but how the information be handled during and after the sharing process. Basically, when information is accessed and stored at network, its security is at risk [8]. This risk of breach is even more considerable when multiple people are accessing it. It is very difficult to develop a policy which can cater all security risks and same time fulfills all required tasks [1]. Guidelines available for successful policy development and execution may help create a good security policy but effective and implementable policy needs few other necessary elements to consider. RFC 2196 [11], the essential guideline for security policy creation, enumerate elements and characteristics of adoptable policy. They recommend that policy must be reasonably implementable, reasonably enforceable, and must clearly define responsibility [10]. Moreover the language of policy must be realistic, understandable, approachable, and must not restrict freedom of productive critic. It must be defined that what information are need to be protected and threats to information must be reduced.

A policy must undergo all the stages of development and full analyses process as given in Figure 2.2 [12] should be followed. The analysis process is illustrated as cycle for easy understanding. This approach is considered to identify key concepts which underpin policy making process. For a policy making to be fully effective, all team members involved in policy development must have all the traditional attributes (requirements of key stakeholders, knowledge of related law and practices, ability to design and implement systems) and should also be aware of the context with in which policy have to be implemented. Policy and implementation of policy both require evaluation and analyses. Worse situations occurs, when users are granted additional access rights to meet certain operational needs at some specific time but these rights are not revoked. Conversely sometimes to facilitate information sharing, information is classified to lower sensitivity level. These are poor implementation scenarios and any good policy will not be effective. The policy must be developed and evaluated as per the needs of stakeholders and sensitivity levels of information under process. In short a fully developed policy is tweaked and improved during operations to meet the needs at real-time [1].

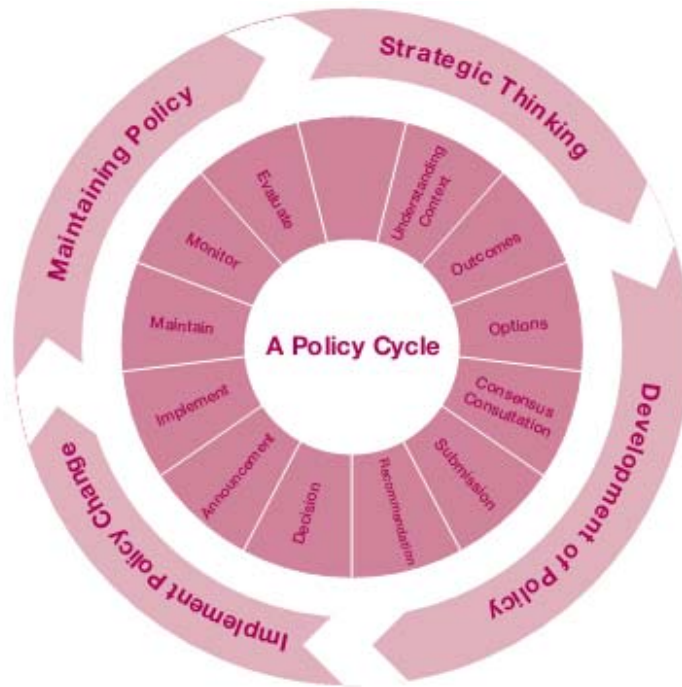


Figure 2.2: A policy Life Cycle [12]

Joseph V. Treglia and Joon S. Park at *Technical, Social & Legal Barriers to Effective Information Sharing Among Sensitive Organizations* [13] have identified three major problem areas of information sharing among different government organizations. These areas are (1) Technical (2) Social and (3) Legal as depicted in figure 2.3 [13]. In this paper authors have used interviews with field experts, literature review and experience to developed preliminary model and theory of intelligence information sharing. Within each area different factors influenced the process of intelligence information sharing. Interoperability, availability and control issues are major technical factors whereas trust, shadow networks and critical issues come under social factors. Local and governmental policies and their conflicts define the legal factors. Technical issues such as having compatible hardware, software, operating systems, secure access, high usability and system availability can be contributing factors for information sharing is not cause of information to be shared [14]. Trust and knowledge of other parties can improve overall tendency towards information sharing. Social, cultural and personal involvement of different agencies also helps in intelligence information sharing. Legal factors can be managed by having comprehensible and enforced local policy regarding intelligence information sharing. It will improve the environment that information will be shared as will increase knowledge of rules and regulations which are related to information sharing [13].

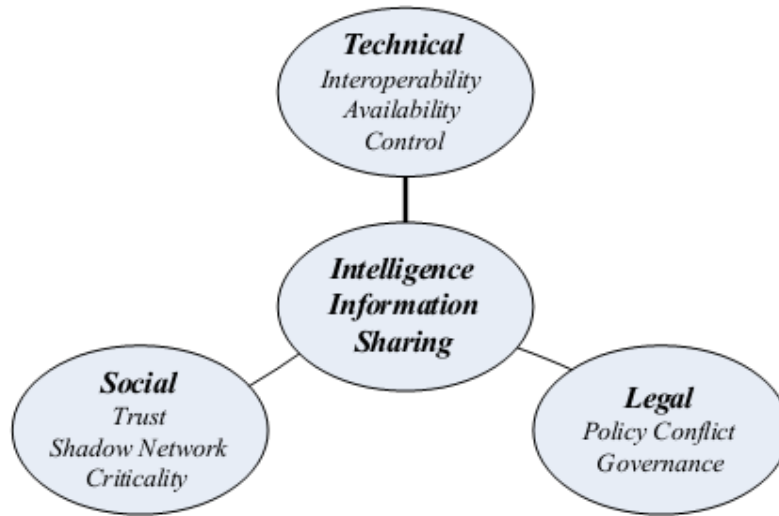


Figure 2.3 : Intelligence Information Sharing Factors [13]

Joseph V. Treglia and Joon S. Park at *Towards trusted intelligence information sharing* [15] have introduced a framework for factors effecting information sharing. This framework basically identifies the forces that influence decision making authorities. Facilitators are the forces which are driving movement for information sharing and detractors that hinder the process of information sharing. Each factor included in facilitator or detractor has potential to develop suitable or non suitable environments to share intelligence information sharing in a given perspective. Facilitators are factors which include positive pressure from problem areas already discussed containing technical, social and legal issues. On the other hand detractors are same factors resulting from technical, social and legal rule but have negative influence on the process of information sharing. Technical factors can ease the process of information sharing if will to share is present but at the same time can act as detractors as well as many organizations and agencies use different hardware or software for information management and communication and these may not be compatible to interact with each other. Normally heavy cost and lack of technical skills are major factors for standardized technical services. Some legal factors also act as detractors are security clearance issues and laws regarding privacy and secrecy may be conflicting. Third factor social bounds also behave as facilitator or detractor in any information sharing environment. It includes greater trust, mutual understanding, knowledge of other parties, and personal ties.

Basically it is matter of social networking that involves having interaction with members of other organization. The framework proposed by authors is show in figure 2.4 [15].

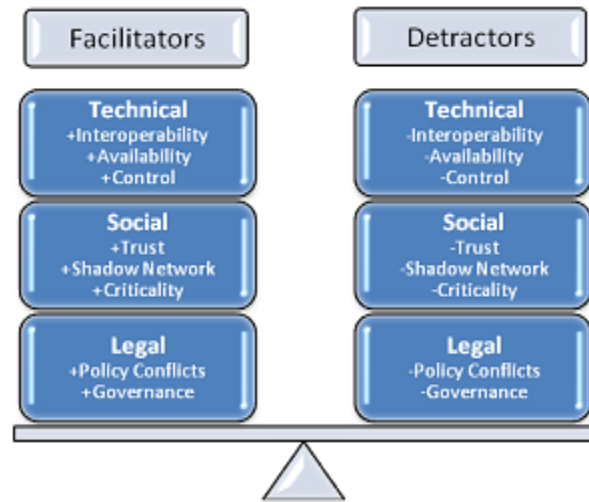


Figure 2.4 : Influencing Intelligence Information Sharing [15]

Li Ming and Luo Nianlong in *Data sharing in campus network* [16] have proposed a design to share data on network. Their design has three parties including Consumer, Data Provider and Certification server. Certificate Server is used here for authentication after basic authentication of already established directory services. The permission to access the data is granted by the Data Provider but basing on the access token issued by the certificate server. The certificate servers maintains list of all Data Providers and this list contains URI of all the web services. Every web service who acts as Consumer needs to register on Certificate Server. Certificate Server in return issues Consumer Key and Consumer Secret which essential to access Certificate Server. Entities used for data sharing process are Data Provider, Consumer, Certificate Server, Protected Data, Consumer Key, Consumer Secret, Data Provider Key, Data Provider Secret, Request Token, Access Token and Token Secret. The architecture proposed works on compass network and users have already user IDs and passwords issued to access the network resources. The design is shown in figure 2.5 [16]. This includes multiple Consumers and Data Providers with a Certificate Server which is directly connected to user database of directory service which managed separately. Use of secure web services is made to share the data and SSL protocol uses the certificate generated by same certificate server. This way the trust on user and server is controlled through single entity and certificate management is easy.

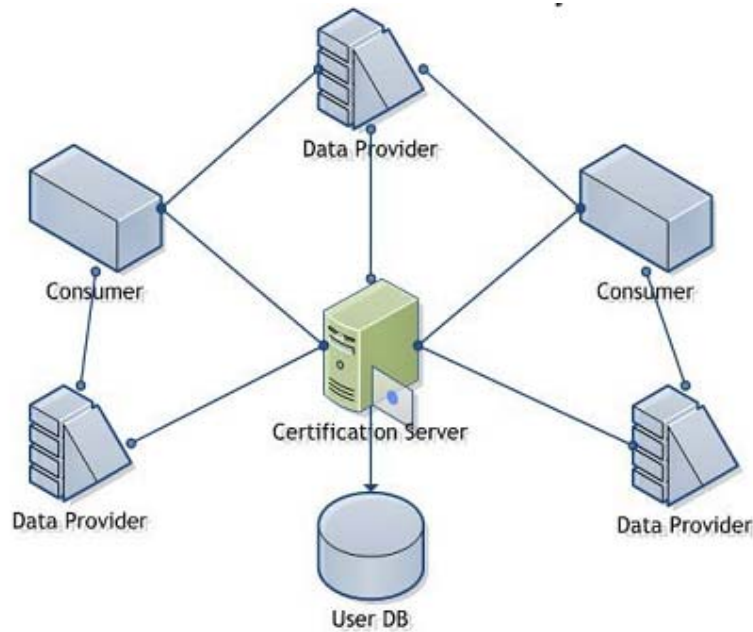


Figure 2.5 : Architecture for Data Sharing in Campus [16]

This application works on web and uses REST (Representational State Transfer) style web service. REST uses no additional data layer for messages such as SOAP is not required. It uses simple HTTP methods to send response and requests. It is stateless, saleable and lightweight protocol. Three most important web services with URI are Request Token URL, User Authorization URL and Access Token URL. An example for consumer request is shown in figure 2.6 [16] below:

```

GET /GetRequestToken HTTP/1.1
Host: https://cert.tsinghua.edu.cn
Content-Type: application/xml
Authorization: xShare
consumer_key="sanzhu.tsinghua.edu.cn",
data_scope=http://jw.tsinghua.edu.cn/transcript/,
signature_method="RSA-SHA1",
signature="wOJIO9A2W5mFwDgiDvZbTSMK%2FPY%3D",
timestamp="137131200",
version="1.0"

```

Figure 2.6 : HTTP Request – Sample [16]

Moreover as discussed by Vipin Swarup, Len Seligman, Arnon Rosenthal in *A data sharing agreement framework* [17] that data sharing is basically willingly letting the other party to use the data. At organizational level sharing of classified information are to be covered through some legal document. Normally due to organization policies and culture issues contractual obligations are avoided and Memorandum of Understanding (MOU).

These MOU also contains service level agreements (SLA) including policies regarding service level parameters. Basically MOU is to document the expectations and obligations of stakeholders to the agreement. Vipin Swarup and Len Seligman introduce Data Sharing Agreement (DSA) [17] as variant to SLA. The DSA should cover Responsive forwarding, Nondisclosure agreements and Usage notifications. As per Wikipedia definition of MOU is “a document describing a bilateral or multilateral agreement between two or more parties. It expresses a convergence of will between the parties, indicating an intended common line of action”. [18] MOU does not have legal bindings but they demonstrate degree of seriousness and mutual respect and are stronger than verbal agreements. MOUs are more in practice in multinational and international relations because, they take short time to ratify and easy to keep secret as compare to treaties [19].

Estevez, P. Fillotrani, and T. Janowski have suggested model in *Government Information Sharing – A Framework for Policy Formulation* [20] for information sharing among government agencies and explained Government information Sharing (GIS) in details. This paper also discussed two most influential theoretical models of GIS. The first model shown in figure 2.7 presents learning cycle of government agencies involved in information sharing process.

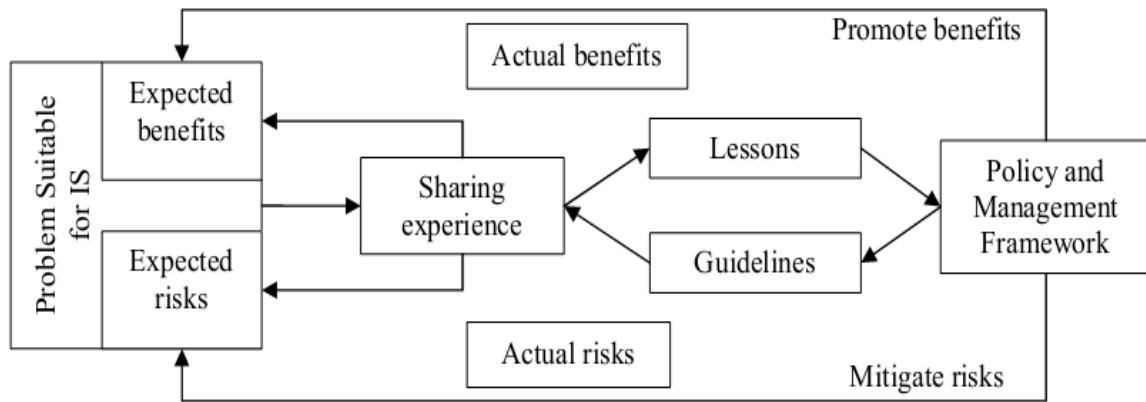


Figure 2.7: Government Information Sharing -Theoretical Model [20]

This model shown above reflects information sharing related benefits and barriers which are identified from literature. This model basically improves when participants enter their experiences using their own perceptions about benefits and risks. Every sharing experience is influenced by the policies enforced and management frameworks of the concerned organization. In turn, this sharing produces insights that help to promote benefits

and mitigating risks of future sharing experiences and ultimately help to improve the framework. This model basically focuses on the information sharing within one agency. Another model discussed in this paper is depicted in figure 2.8 [20]. This model has three stages. Stage 1 reflects on the experiences of agencies that share information and based on these experiences the model proposes building of an interoperability infrastructure in order to support information sharing.

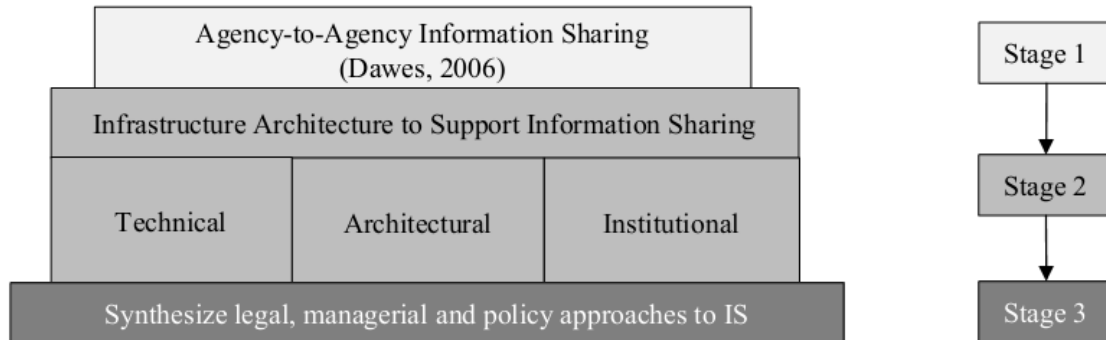


Figure 2.8 : Expanded Model for Information Sharing [20]

Stage 2 proposes three elements (1) Technical – It focuses on hardware and software compatibility, availability of standard process and integrations of best practices. (2) Architecture – These elements include meta-data infrastructure to facilitate access to information, contractual details to fulfill the inter-agency information sharing requirements at horizontal or vertical level in hierarchy of government organizations. (3) Institutional- these elements are clearinghouse of information sharing practices and formbook of contracts to cater alternatives for risk and responsibilities for information sharing. Stage 3 deals with changes to be made in laws, policies and management practices. The authors at [28] also has defined principles that will guide information sharing culture to formulate polices in government organizations. These principles include (1) defining of information sharing rules and policies, (2) social and technical procedures, (3) classification of initiatives related to information sharing including strategies and barriers. (4) Other challenges to information sharing with regards to organizational boundaries. The challenges of information sharing among organizations also introduce concepts of organizational boundaries. Same concept is explored by Zheng, Tung-Mou Yang in *“Understanding the “Boundary” in Information Sharing and Integration”* [21]. The authors have concluded that there is no defined or comprehensive definition of “boundary” in cross-boundary organizational information sharing. Different types of boundaries identified by the authors are Organizational

boundaries, personal boundaries, and geographic boundaries. These boundaries have complex relationships as shown in table 1 [21]. It said that it is hard to determine which situation is more complex for hierarchical boundaries and horizontal geographical boundaries.

Table 1 : Boundaries relationship and complexities [21]

Vertical Direction	Relationship	Illustrations
Hierarchical boundary	Non-Linear	Judging the complexity of non-vertical administrative relationship vs. vertical administrative relationship depends on from which perspective a case is viewed
Personal boundary	Linear	The complexity goes up with the degree of the vertical personal boundary
Geographic boundary	Linear	The complexity increases with the degree of the vertical geographic boundary
Development phase boundary	Linear	The complexity increases with the degree of the vertical development phase boundary
Horizontal Direction		Illustrations
Departmental boundary	Linear	The complexity goes up with the span of the departmental boundary
Personal boundary	Linear	The complexity goes up with the degree of the horizontal personal boundary
Process boundary	Linear	The complexity increases when participant organizations are not on the same process
Geographic boundary	Non-linear	It all depends. The complexity does not necessarily increase with the degree of the geographic boundary.
Development phase Boundary	Linear	Initiatives among different development phases could be more complex than among same or similar development phases

To work in network environment interoperability is essential so that all the stakeholders can operate and interact to share information. Interoperability Framework (NZ e-GIF) [22] consists of three documents including (1) Policy, (2) Resources and (3) Standards. A layer model is used to classify functions within IT system for standards. This layer model described all the components of IT and communication among these components is through neighboring levels. The four basic components are enlisted as (figure 2.9 [22]). (1) *Network*- This is most crucial area of interoperability and it covers details at datagram port level. This standard recommends protocol suit like IP v4, IP v6, LDAP, HTTP, FTP and WebDAV. (2) *Data Integration*: This layer facilitates interoperability of data exchange and processing. Standards used are UTF-8, XML, GZIP, HTML and TAR. (3) *Business Services*: This layer supports particular application level data exchange. Some standards used here are generic and other works with data integrations standards to map data to usable business information. (4) *Access and Presentation*: This layer deals with users access and presentation of systems as compiled in government standard.

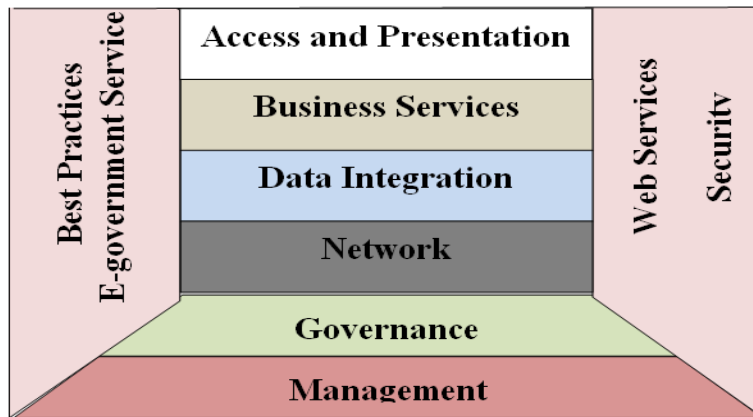


Figure 2.9 : Layer Model e-GIF [22]

The structural layers are (1) Security: This is to be included in system design not as layer and protocol recommended are SSL, S/MIME and HTTPS. (2) Best Practices: Standards alone do not ensure interoperability but just offer common approach to manage and understand the context of information sharing. This section consists of Code of Practices, Best Practices and sector focused guidelines. (3) Web Services: This service used to connect other services. It includes standard like UDDI, WSDL and SOAP which facilitate the connection and integration of web-based applications.

The standard discussed above is one of the requirements to have secure classified information sharing. However a lot of work has been done to secure the networked environments. The sharing of classified information demands comprehensive and foolproof security planning and its execution. The security should part of the design. As Vladimir Jirasek at “*Practical application of information security models*” [25] has discussed security GRC (Governance, Risk [Management], and Compliance) model. As mentioned that it is not the technology that ensures security but information security is part of information risk management. This model has three main parts (1) Security Drivers (2) Security Management (3) Stakeholders. The *Security Drivers* are the main cause of having security in place and major security drivers include Laws & Regulations, Business Objectives and Security Threats. Next *Security Management* includes three frameworks which enable an organization to achieve objectives defined in drivers section includes Policy Framework with policies, standards, and artifacts. The Process framework and security metrics framework are also part of layer model. *Stakeholders* should know what is being delivered and what is being delivered. Value of security to business is to be identified and concerns are to be addressed accordingly. *Security threats*, these are not the business drivers but they affect the level of protection. Threats come

from vulnerabilities and attackers who want to acquire information or limit the business opportunities. Security controls are needed to thwart threats. Security models are used to capture security threats and achieve security objectives and design security controls. Security intelligence is required to analyze security threats and advice actions [25]. *Information Security Policy Framework*, This document ensures the security objectives are met and proper accountability is ensured. This policy is approved by higher authorities and in line with business objectives and strategies. Information security policy framework is shown in figure 2.10 [25] below:

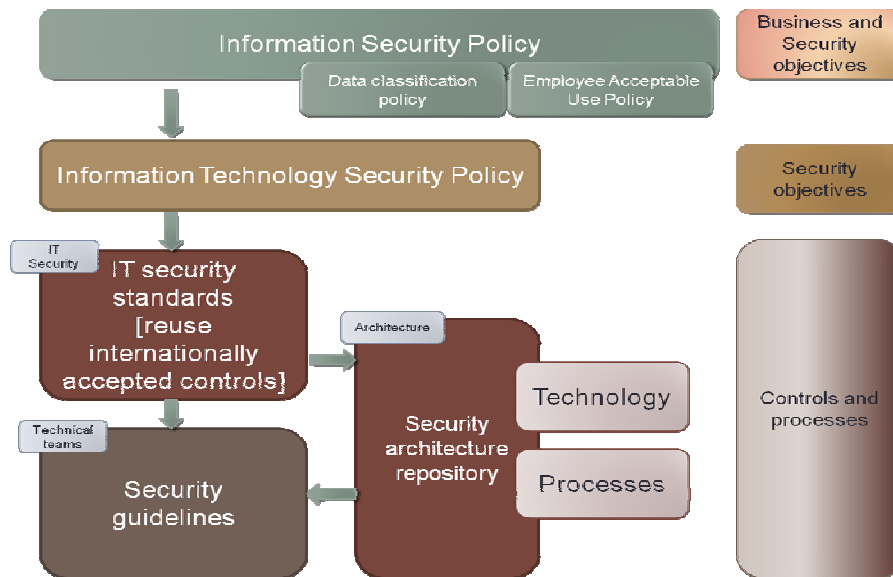


Figure 2.10: Information Security Policy Framework [25]

When information is shared the security measures are taken basing on the value and importance of the information. Information classifications helps ensure information is protected in most cost-effective manner [26]. Each classification has separate security controls and handling. For example top secret or confidential information may require access privileges of only senior members in organization.

Another requirement to have secure information sharing is secure and reliable network. Network administrators have to take several steps to secure network which includes separate network for each services and use of virtual LANs and VPNs. Use of secure protocols and special hardware such as firewalls and intrusion detectors are basic building blocks of secure network [23, 24]. Network devices are basically first security barriers for IT resources for outside threats [33, 34].

Access control is one of the main strategies to protect information assets in networked environment. Access control manages all authorizations basing on the security policy when a subject access to and object. Usually access control follows the principle of least privileges i.e. users and process have minimum operation authorities to accomplish assigned responsibilities. DAC, MAC and RBAC are most widely used access control models [27].

Auditing and monitoring is one of most important issues in host and network security. It includes monitoring, controlling and recording file access activities such as file opening, modifying, creating, deleting and moving etc. Auditing is a passive information security tool to carry out forensics and meet the legal requirements. This is used to safe guard against malicious attacks from external attackers and internal employees [29-30].

When to share data has to be stored on network accessible storage. It is more vulnerable to unauthorized access and malicious tamper. As the storage is networked and some distributed as well so the attackers can change or modify information when it is travelling on network or store on disks or tapes. Therefore securing of data is crucial when ‘data in flight’ or ‘data at rest’ and cryptography is used for such solutions [31]. The secure storage facility should cater basic security elements of confidentiality, integrity and availability. Architecture of secure storage has been presented by Surya Nepal, Carsten Friedrich, Leakha Henry, Shiping Chen [32] known as TrustStore architecture shown in figure 2.11. The TrustStore system securely store and share sensitive data in un-trusted public environments.

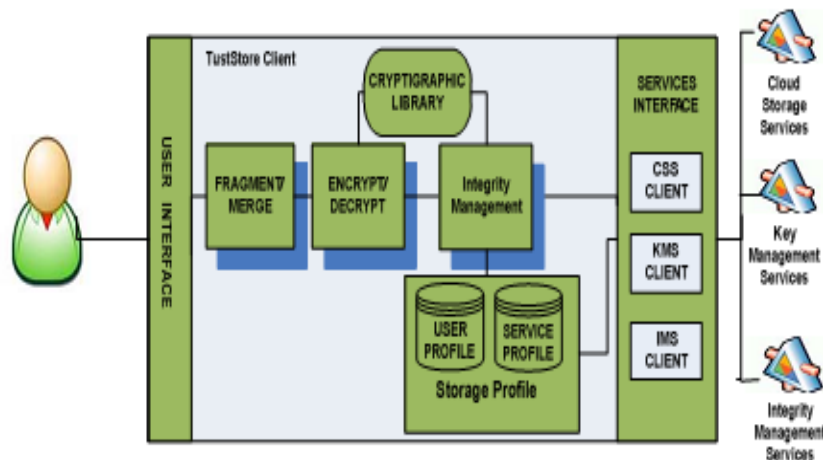


Figure 2.11: TrustStore Architecture [32]

2.3 Analysis and Gaps

Different models and standards are discussed about information sharing among organizations in this chapter and following is the analysis and gaps identified. .

- Douglas Harris, Latifur [2] at *Standards for secure data sharing across organization* have discussed requirement of information sharing only in *health-care* sector. In this work only functions are defined for which standards are necessary.
- LI Ming and LUO Nianlong [16] at *Data Sharing in Campus Network*, have also defined a design to share the information but only access control through certificate server is discussed other security requirements like, secure network, monitoring and policies are not discussed.
- A theoretical model is given by Landsbergen [20], Government Information Sharing - Framework for Policy Formulation Framework for Policy Formulation. This is three stage model and improvements are done with experience of stake holders. *It is basically theoretical model and implementation details are not covered.*
- A detailed *interoperability model* is given by Te Kōmihana O[22] . All different IT standards and protocols are defined for all areas of IT but what all should be part of implementation and how final policy will be defined and implemented is not given. *Here it is up to the user that whatever deem suitable can put into action.*
- To have maximum and trusted environment, the security principles which are required to thwart security threats faced by information sharing are given below.
 - Separation of duties
 - Least privilege
 - Defense in depth
 - Secure storage
 - Monitoring at application, system and network level.
 - Role based Access control
 - MAC
 - Physical Security
 - Intelligent use of available technologies

2.4 Summary

Sharing of information has been discussed in literature and most work is about sharing in health sector and at some government level among agencies. Information security framework and models are also available for information sharing methodologies but needs to be incorporated when designing any environment for information sharing among different organizations. At the end a gap analysis is done to find out the missing security controls in the models and standards already discussed.

CHAPTER 3: POLICY FRAMEWORK

CHAPTER 3: POLICY FRAMEWORK

The aim of this chapter is to provide the design of Policy frame work. The effort is to make a practicable policy framework which can be implemented by different organizations having intentions to share classified information satisfying organizational security policies and overall information security requirements in networked environment.

3.1 Inter Organization Information Sharing Framework:

After reviewing the literature and considering security and other cultural issues a recommended policy frame work for classified information sharing is shown at figure 3.1 below:

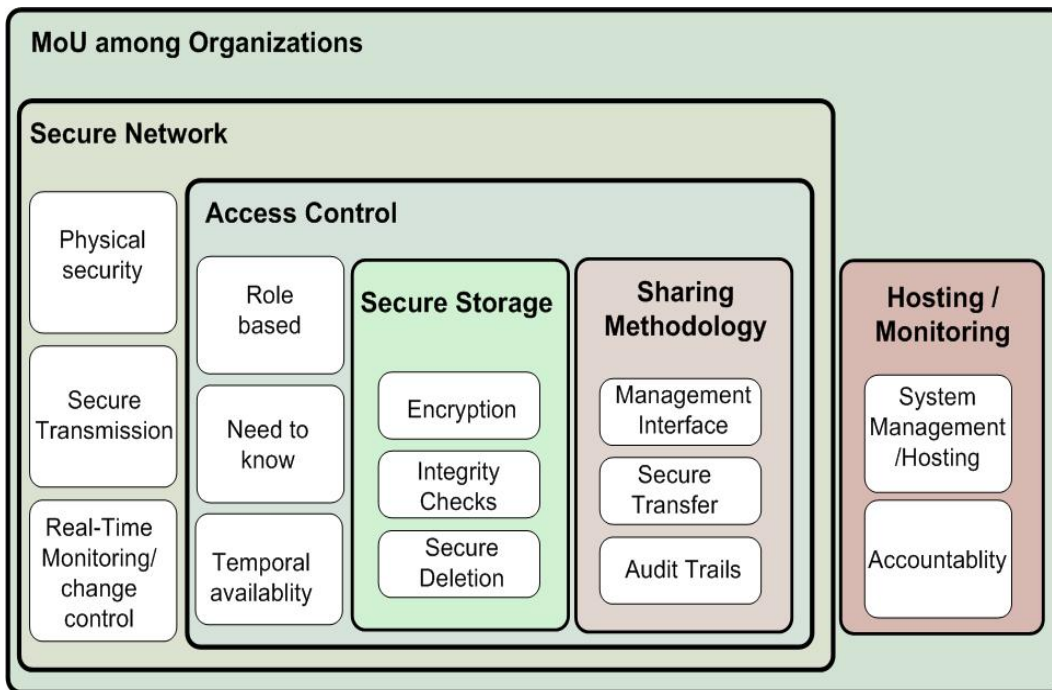


Figure 3.1: Inter Organization Information Sharing (IOIS) Framework

The above Inter Organization Information Sharing Framework (IOIS) framework for information sharing has six main parts and MOU as main part which holds in all the

other parts in it. Some parts independent but more are interrelated. All these parts are described one by one and policy principles are derived from this framework.

3.1.1 Memorandum of Understanding

Most important is will of stakeholders and that can be demonstrated through the concern shown and fulfilling documentary bindings. Some legal documents or contractual obligations may cause delays then memorandum of understanding (MOU) can be quick and viable option. MOU must be defined among the all the stakeholders' which is basically a multilateral agreement demonstrating intended common line of action.

Principle 1: Each participating organization must sign and abide by the MOU. The MOU should be legal enforceable agreement.

An effective MOU prevents confusions, disputes and misunderstandings by clarifying the expectations of the participants. MOU must include methods and pattern of information sharing. All organizations must be agreed upon network security standards, format and types of data transmission, encryption techniques, and methods to check the data integrity and above all how to manage and monitor network devices and other machines. MOU should be comprehensive and covering all necessary details.

3.1.2 Secure Network

Second part of IOIS framework is establishment of secure network. Secure Network can be established by (1) Physical Security (2) Secure Transmission (3) Real time monitoring and Change control.

Principle 2: Each participating organization must ensure security of network by applying measures for physical security, transmission security and real time monitoring.

Dedicated optical fiber or leased lines can resolve majority of security risks and satisfy the stakeholders. Network devices should be physically secured and properly accounted for through inventory controls. Use of different networks for different purposes and configuring networks into LANs (Local Area Networks) can isolate more secure networks from internet or other public networks [24]. To ensure secure transmission outside data centre virtual private network (VPN) must be configured [23]. Properly configured VPN using IPsec provides secure virtual “tunnels” among multiple

organizations and data is encrypted and secure while on move. Real-time monitoring should be carried out through network performance monitors (NPM). NPM simplifies detection and resolution network issues and tracks availability, response time, uptime of network devices. Real time port level monitoring provides statistics of network traffic and any change in traffic patterns can be monitored and investigated. Configuration management and change control can be achieved through use of Network Management Systems (NMS). Using NMS policy violations and other configurations changes can be controlled and monitored automatically. It guards against unauthorized, erroneous and unscheduled configuration changes.

3.1.3 Access Control

Third part of IOIS framework consists of access control mechanism. The access control should ensure access to the shared information as per roles and need to know bases which can be achieved by applying RBAC and MAC while considering security classification of data [6].

Principle 3: Each data file shall be marked with access control list taking into account the security classification and need to know requirements with time limits.

Shared data should be available for allowed time period only as this environment is being established for sharing of classified information not for storage or permanent hosting. It recommended that the access to shared information should be:

- Based on user roles.
- Principle of need to know and least privileges should be satisfied.
- Information should be classified and access is to be granted basing on security clearance level.
- Information should be available at shred place for specified time.

The access control is implemented under secure and reliable network environment for access to shared information.

3.1.4 Secure storage

Next is secure storage which is basically placed in secure network and behind proper access control. Secure storage can be achieved by using good encryption and integrity techniques. This requirement introduces next principle information sharing framework.

Principle 4: Each shared file should be encrypted, satisfy integrity and securely disposed off from shared area.

The information stored at shard media should be encrypted to meet the confidentiality requirements. It should be digitally signed or hash information be attached to satisfy integrity requirements. Every document placed should have specified time of availability at shared area and after that removal or deletions should be permanent using some shredding utility and activity be properly logged.

3.1.5 Sharing Methodology

After establishment of secure and reliable network and roust access control mechanism, sharing methodology or technique is discussed in framework. This part of IOIS framework is core of whole sharing environment. Adopted sharing methodology must satisfy AAA security principle. The next principle of information sharing work is:

Principle 5: Sharing technique should have management interface for secure and audit trails of transferred information.

Best sharing can be achieved using customized secure sharing application which fulfills all security needs of confidentiality, Integrity and Availability (CIA) triad and other security principles. Sharing policies and relevant audit trails must be part of this application. Options available for secure sharing are:

- Special application made as per the requirements and agreed upon practices in MOU.
- Secure email using Public Key Infrastructure (PKI) technology and applying security filters on inbound and outbound emails.
- Use of secure FTP protocol by implying SSL and user certificates for authentication through PKI technology.

3.1.6 Hosting and Monitoring of Sharing Environment.

The secure environment can be hosted at mutually decided place as in MOU. Separation of Duties principle is an important standard of security can be implemented for Management of the shared environment.

Principle 6: Each activity at secure environment should be logged and monitoring is visible to all stakeholders.

All activates at each tier i.e. (1) network, (2) system (3) application must logged and monitoring console be available to all stake holders.

3.2 Summary

All the above mentioned principles of IOIS framework are the recommendations and every part of the framework need deliberate effort to design and standardized so that security and privacy requirements are satisfied. As it is a policy framework and policies are improved and modified with respect to change of environments. Developments and introduction of new technologies can introduce modifications and improvements in framework definition of implementations.

CHAPTER 4: IOIS DESIGN

CHAPTER 4: IOIS DESIGN

Information sharing framework is purposed and explained in previous chapter and now the design and adopted methodology is described in this chapter. Sample or design of all the parts of information framework is presented here.

4.1 MOU

As discussed in the previous chapter MOU is formal agreement among different parties who want to be part of any collective activity. A MOU for sharing of information should include all the necessary details which are deemed for information sharing. A general MOU should cover following:

- Overall intent of the participating parties.
- The parties included in the sharing process.
- Assignments and responsibilities.
- Disclaimers
- Financial arrangements if any required.
- Risk sharing
- Signature

A sample MOU is attached as Appendix A

4.2 Secure Network Design

Secure networks and their proper operations are very crucial for information systems as nearly all operations work on network environment. The reliability, security and performance of network are basis of trustworthy IT operations. During design to achieve cost effectiveness and avoid errors set and recognized principles should be taken into account as described below [33]:

- Compartmentalization
- Defense in depth
- Adequate protection through security devices.

- Principle of least privileges
- Weakest link in the chain
- Security Zones
- Intrusion prevention

A comprehensive and appropriate network design provides following advantages:

- Low trust networks are isolated
- Security breaches are reduced
- Accurate access control, proper monitoring, and resource management.
- speedy identification of incidents
- Cost optimization by applying all the recognized principles

4.3 Proposed network Design

By considering the network security principle discussed above and requirements of security and reliability as mentioned in the information sharing framework in previous chapter a comprehensive network design is along with network devices and other services is proposed. This network design includes network security devices, network monitoring and configuration devices, and access control and encryption services as shown in figure 4.1.

4.3.1 Compartmentalization: The proposed design has different compartments or networks (VLAN) for every service. Every part has different purpose and network. Following are different parts of the network;

4.3.1.1 Demilitarized Zone: It is a neutral zone between outside world and internal network. It consists of exchange server for outbound emails and web and FTP servers.

4.3.1.2 Local Domain: This basically hosts Forest controller, domain controller to manage users and their groups through directory services.

4.3.1.3 Secure Sharing Application: This is main application and it manages all file sharing activities. The design of this application is discussed subsequently.

4.3.1.4 Public Key Infrastructure: To generate public and private certificates to have following uses

- Encryption and non-repudiation services for email
- Encryption and integrity check of documents
- Digital signatures
- Use for secure communication protocols i.e. SSL , IKE

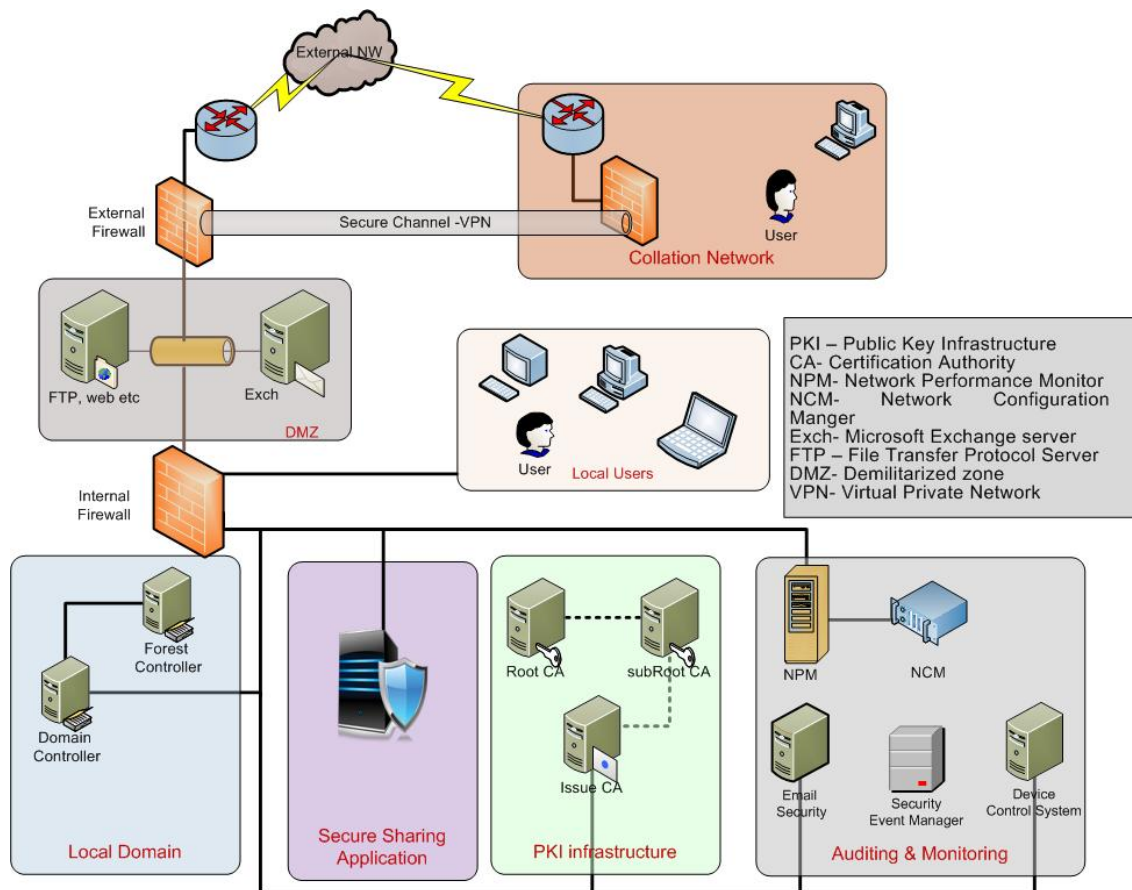


Figure 4.1: Secure Network Design

4.3.1.5. Auditing & Monitoring: This part of network is not to provide any service to the users but it provide real time monitoring and policy enforcement. It has multiple services combined in it. All the services are provided by different devices and security solutions.

- Network performance monitor (NPM)
- Network Configuration Manager (NCM)

- Email security
- Security Event Manager
- Device Control System

4.3.1.6 Local User Group: This part of network consists of local user or we can say internal employees. These are users authenticated by directory services and get security certificate from certificate server and all the monitoring of these employees is done by security event manager.

4.3.1.7 Collation Network: This network is outside of local network and it consists of other organization or agency network connecting through some public network using some secure channel i.e. VPN and proper firewall /routing policies.

4.3.2 Network Devices proposed

- Firewall with VPN, IDS / IPS functionality
- Network Routers
- Network switches for compartmentalization

4.3.3 Server Machines proposed

- Domain Controllers
- Exchange servers
- PKI setup servers
- Application servers
- Monitoring machines

4.4 Secure Transfer Application Design

To have secure transfer of file so that confidentiality and integrity of information is not compromised. An application for secure transfer of information as per the requirements prescribed at framework is taken into consideration while designing secure transfer of information in any format. The secure transfer application maintains consistency of user roles, security clearance of subject (users) and classification of objects (files) is matched before grant of access. Following is list of information security requirements included in the design of application shown at figure 4.2.

4.4.1 Access Control: Access control to the application is based on user role and then to access the shared file security clearance level of the document is matched before access is granted.

4.4.2 User Roles: User roles as per tasks assigned are made as user, organization administrator and master administrator.

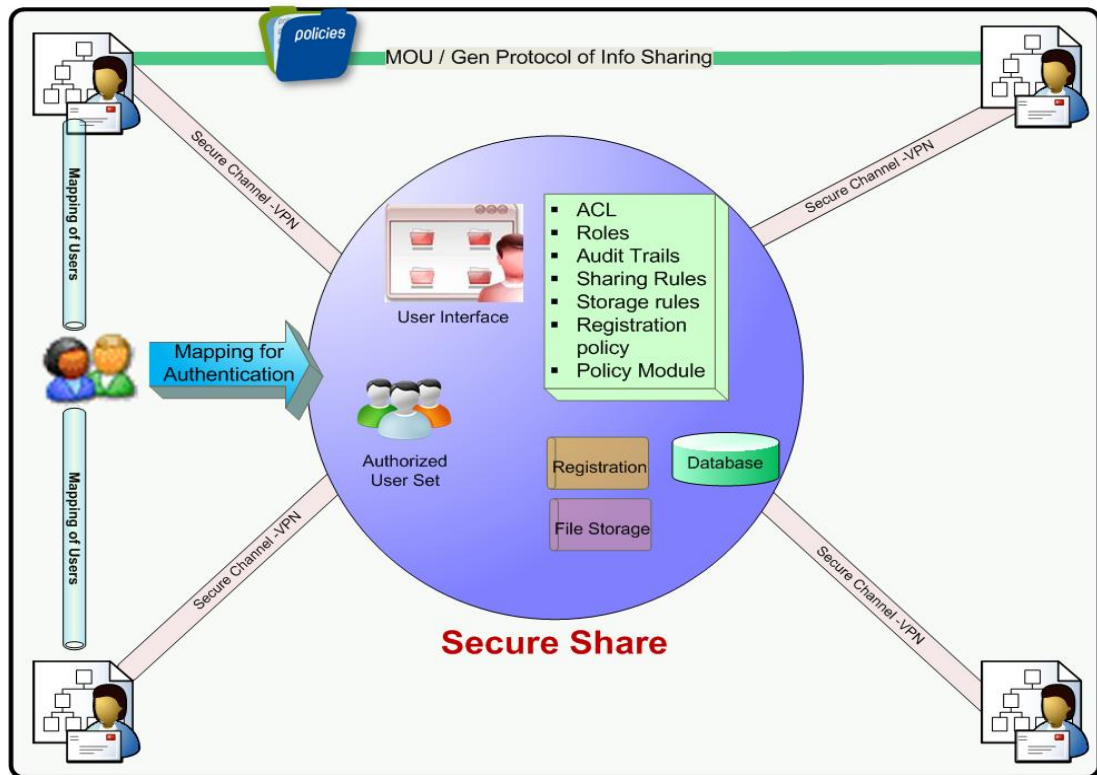


Figure 4.2 : Secure Application Design

4.4.3 Information Classification: Information to be shared is classified as per security level.

4.4.4 Audit Trails: A proper audit trail of all activities of users of all the roles is maintained so the requirement of accountability and forensics is met. Following activities of all users are logged :

- Organization Added by master administrated.
- Any change made to organization profile.
- User created by organization administrator.
- User profile modified by the organization administrator.
- File uploaded for sharing.

- File shared by users.
- File downloaded by users.
- Shared file entry deleted.

4.4.5 Storage rules: As this application is made for sharing of information so the storage of information is made for temporary time and will be deleted after specified interval.

4.4.6 Registration Policy: Users' creation and addition of organization will depend up policies defined in MOU.

4.4.7 User Interface: An easy to use Graphical User Interface (GUI) is proposed so that all the respective tasks are performed easily.

4.4.8 Database: A database system is used for file storage and keeping record of all audit trails etc.

4.4.9 Authentication Mechanism: Authentication is main point of decision for granting any access to information system. Basing on the authentication and matching with roles and security clearance level access is given to the user to logon the application. Sequence and mechanism of authentication is shown in figure 4.3.

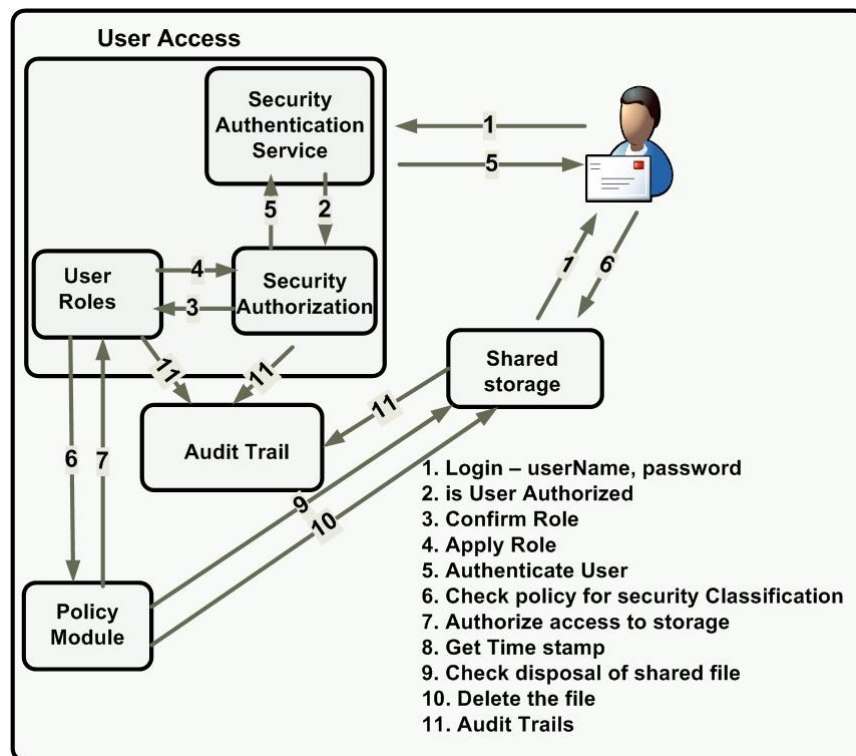


Figure 4.3 : Authentication Mechanism

4.5 PKI design

To have secure email which satisfies requirements of confidentiality, integrity and non repudiation Public Key Infrastructure (PKI) setup is essential. As mentioned in the Information Sharing Framework that second option to share information securely is by use of secure email. PKI provide the abilities to manage publish and use keys easily. The certificate issued by PKI service can be used for secure wireless LAN, encrypted file system, smart card Logon, secure email, document signing, web service security and IP Sec. PKI certificate for the above purpose can be purchased from any commercial certification authority or own private PKI setup can also be established . Hierarchical deployment design of PKI is most suitable and options available are

- Single –Tier PKI Hierarchy
- Two- Tier PKI Hierarchy
- Three-Tier PKI Hierarchy
- Four Tier PKI Hierarchy

Keeping in view the security and confidentiality and management issues three-Tier certification Authority hierarchy is proposed for secure information sharing.

4.5.1 Three Tier PKI Hierarchies: Three-tier hierarchy certification authority (CA) provides flexibility and best security as shown in figure 16 .A three tier CA consists of following

- An offline Root Certification Authority deployed as standalone CA
- Offline Policy subordinate certification Authority as standalone subordinate CA
- One or more Issue Certification Authority.

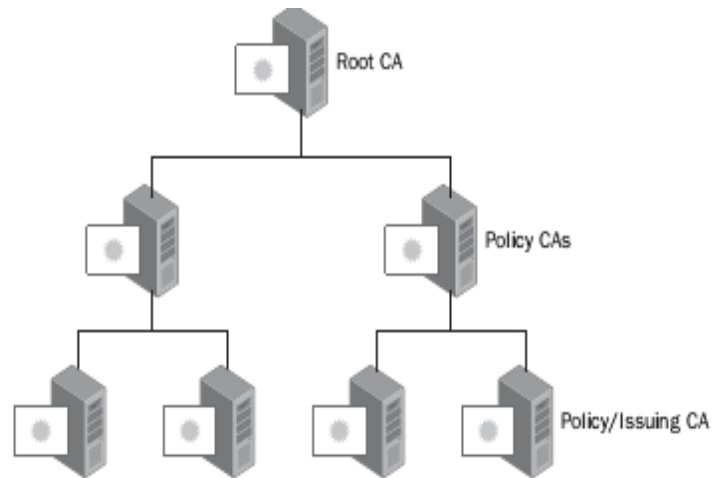


Figure 4.4 : CA hierarchy [35].

To deploy the PKI services in actual environment as required by Information Sharing Framework one machine will be used for each tier of CA. Root CA and sub root CAs will be offline and Issue CA also known as Enterprise CA will be online. Offline CAs will be place in secure vault and only be made available to issue new certification revocation list (CRL) after specified interval or to issue new certificate. Root CA is main CA which issues certificate to itself and sub root CA get its CA certificate form Root CA. Issue CA gets its certificate from sub root CA. The Certificate path will as shown in figure 4.5.

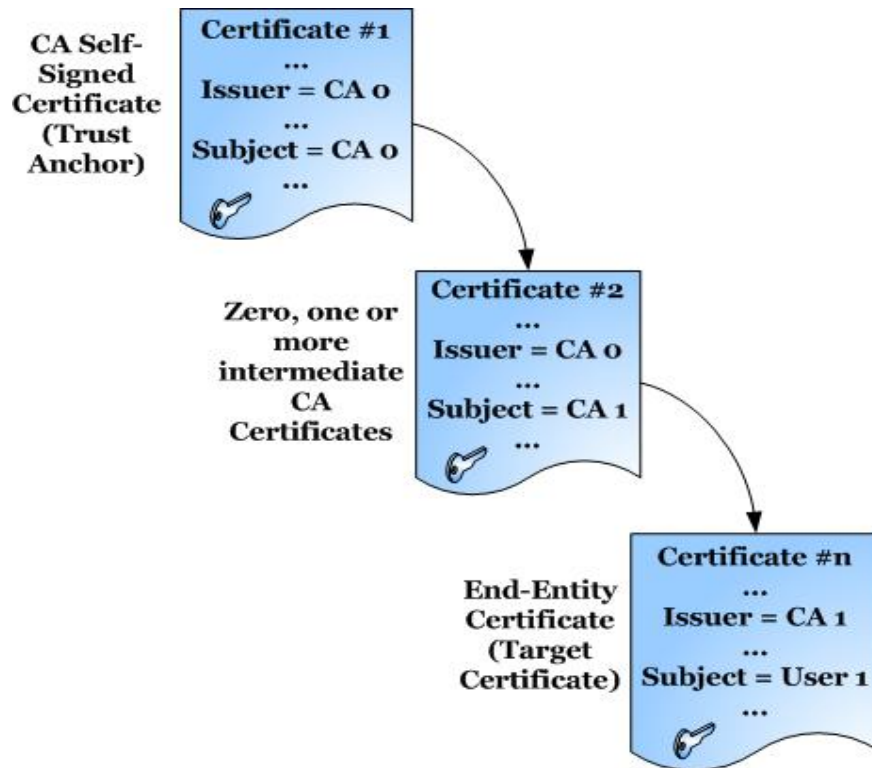


Figure 4.5 : Certificate Path [35]

Each certificate issued by any CA has life time and before expiration is required to be renewed from issuing CA so that normal functionality is not hampered. Proposed life time of each certificate as hierarchy is mentioned at Table 2.

4.5.2 Certificates Administrators

- EFS recovery certificates
- Key Recovery certificate.
- Smart card enrollment agent certificates

4.5.3 Certificates for end users

- S/MIME signature certificates
- S/MIME encryption certificates
- 802.1X client authentication certificates
- Smart card logon certificates
- EFS certificates

Table 2 : Recommendations for Validity Periods

Purpose of Certificate	Certificate Life	Private Key Renewal Strategy
Stand-alone root CA. (4096-bit key)	16 years	Renew at least every 8 years to ensure that Issue CA certificates can be issued with lifetimes of 8 years. Renew by using a new key at least every 8 years.
Enterprise issuing CA s for medium security certificates (2048-bit key)	8 years	Renew at least every 4 years to ensure that child-issuing CAs can be issued for 4 years. Renew by using a new key at least every 4 years.
Secure mail and secure browser certificates	2 year	Renew by using a new key at least every 2 years.
Smart card certificates (1024-bit key)	2 year	Renew by using a new key at least every 2 years.
Administrator certificates (1024-bit key)	2 year	Renew by using a new key at least every 2 years.
Secure Web server certificates (1024-bit key)	2 years	Renew by using a new key at least every 2 years.

The certificate types required for management of PKI setup and utilization of PKI services following certificates are recommended.

4.5.4 Certificates for Machine

- IPsec certificates
- Domain Controller certificates
- SSL certificates

4.5.5 PKI deployment pattern: As per the information sharing framework the deployment under secure networked environment using directory services of Microsoft will be as shown in figure 4.6.

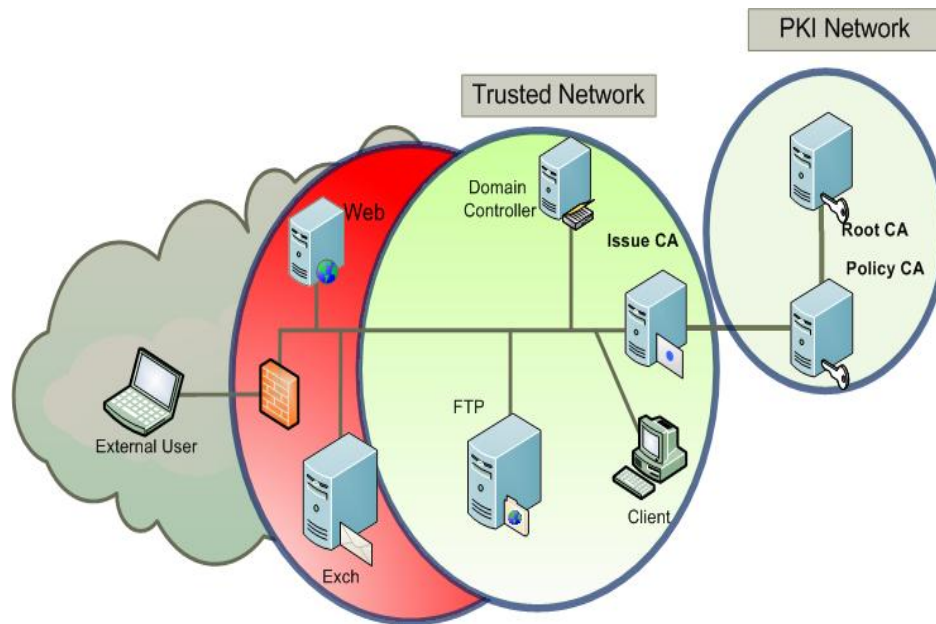


Figure 4.6: PKI Deployment

4.6 Secure Email Setup Design

Electronic email, commonly known as email is a facility to exchange messages and other documents from one sender to one or many recipients. It is fast and cheap method to exchange information due to easy access to internet at every IT enabled device. It has many features including send one message to many people simultaneously, message reaches to everyone in short duration of time, send attachments and can store messages at server and client side. But traditional email system has some inherent disadvantages as well which include:

- Email can carry virus.
- Difficult identify identity of sender
- Cannot be used as signed document so cannot be used as legal authority.
- No restriction on sender about content and recipient filtration.

4.6.1 Secure Email Benefits. Above mentioned limitation are to removed and new design will provide the following:

4.6.1.1 Eliminate

- e-mail Tampering

- Spoofing.
- Repudiation
- Sniffing & other attack methods

4.6.1.2 Enable

- End to End Security with confidence.
- Message Authentication, Document Authentication.
- Non-Repudiation, Integrity, Confidentiality, Authorization.

4.6.2 Email Rules. Keeping in view the above limitation of email system and requirement of sharing of classified information secure email designed is proposed as under:

4.6.2.1 PKI system be used for every email as following.

- Every user will have digital certificate.
- Every email will be signed and encrypted.

4.6.2.2 Email content checking and filtering to control.

- sensitive content sending
- Attachments as *.exe, *.vbs or any sensitive content in attachment
- Apply antivirus on all incoming and outgoing emails.
- Checking of Microsoft word document macros.

4.6.3 Secure Email Deployment Design. The deployment design of secure email is shown in figure 4.7. All the users using email will have digital certificate for following services

- EFS recovery certificates
- Key Recovery certificate.
- Smart card enrollment agent certificates.

Every email will be passing through email security application and content filtering and multiple virus engine scan will scan every inbound and outbound email message. The content filtering will be enabled on attachments as well. Sender control will be done with help of digital certificates and users without digital certificate will not be able to send and receive encrypted email and will be able to send digital signed emails.

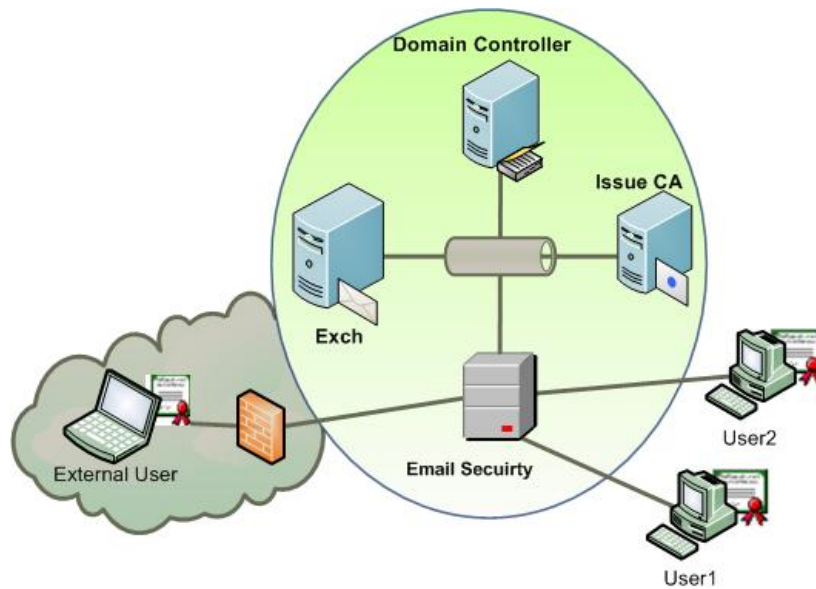


Figure 4.7 : Secure Email Design

4.7 Secure FTP Server

File Transfer Protocol (FTP) is a standard protocol to transfer files over network. It is an efficient way to transfer files over network but it some inherent disadvantages as it is not secure protocol. It can be attacked during transfer and breach of confidentiality and integrity can have severe effects. Use authentication services as basic rule can help to overcome these disadvantages. Username and password authentication is very common method to identify a user on website. However to have more secure transfer of files over network use of PKI services can help to meet the information security requirements i.e. confidentiality and integrity. A secure FTP design is shown at figure 4.8. To enable Secure Socket Layer (SSL) and user authentication using PKI certificates following is required:

- Web server Certificate will be issued to server machine.
- Every user will have digital certificate for identity authentication.
- SSL will be enabled on web server for secure transfer of files.
- User authenticate using certificate option will also be enabled at web server.
- All transmission done using SSL protocol.

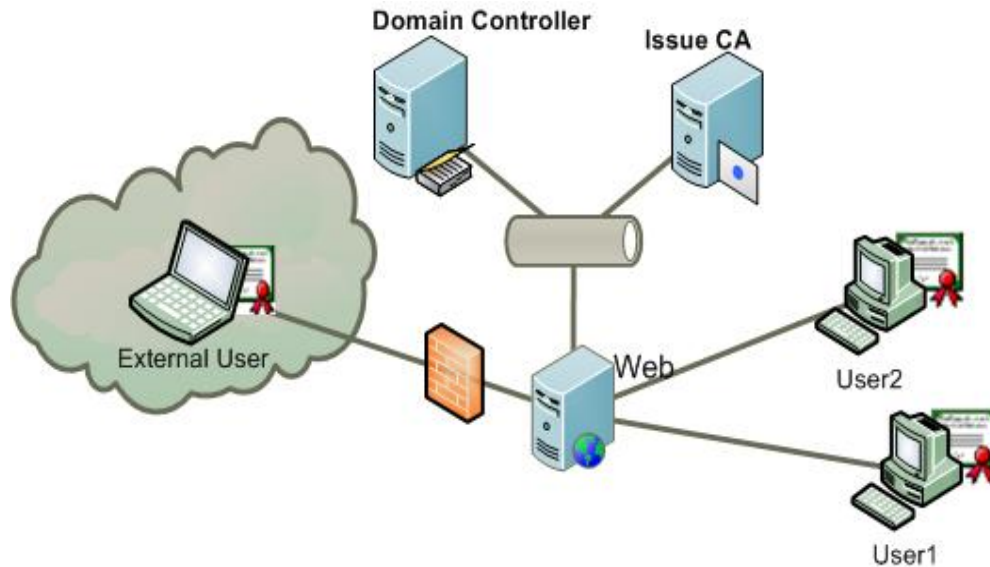


Figure 4.8: Secure FTP

To access the files through FTP server, authentication of user and computer of user will be done as the private certificate of the user will be available at the location only. This made the access to information location and hardware dependent. Following is sequence of information sharing:

- User to login with username and password of directory service as controlled by domain controller.
- SSL connection to be established between client and FTP server.
- User authentication using digital certificate is completed at web server.

4.8 IOIS -Auditing and Monitoring

To meet AAA requirement as required in IOIS framework a comprehensive logging and monitoring solution is required to be in placed so that all the activities which are not according to the policy invoked are identified. This is a process to identify any incident at initial stages. Security events and application events generated by users and machines provide complete picture of the activities with timestamp. As IOIS is designed to share classified information, all activities of all users required to be logged so that auditing and accountability is possible. The auditing and monitoring design for IOIS is shown in figure 4.9.

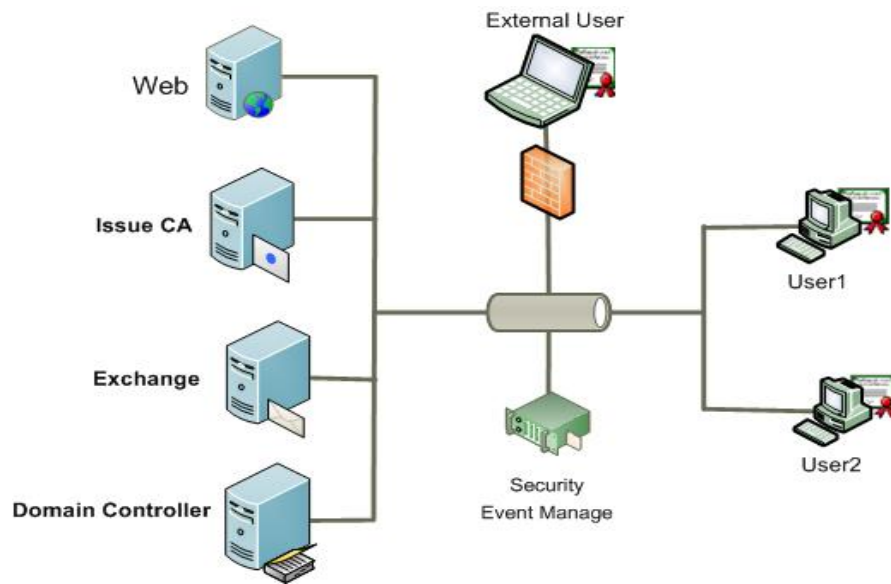


Figure 4.9: Auditing and Monitoring

4.9 Summary

This chapter has discussed complete design of secure environment. The design includes secure network in details incorporating compartmentalization and security services like PKI, application for sharing, real time monitoring of systems and network. At the end email security design with content filtering is also presented.

CHAPTER 5: IOIS IMPLEMENTATION

CHAPTER 5: IOIS IMPLEMENTATION

The aim of this chapter is provide detailed view of how IOIS framework was implemented. Implantation is done in different parts as IOIS framework has different principles to be implemented for secure sharing of classified information. The implementation is divided into following parts.

- Development of application to securely share information among different organizations.
- Development of PKI system for generation digital certificates which can be used for secure email, SSL, user authentication.
- Configuration of secure network.
- Establishment of Active Directory services and email server.
- Deployment and configuration of network and system monitoring system

5.1 Secure Application

To share different files on network as design given in previous chapter a web based application is developed using available application development technologies.

5.1.1 Functional Rules: The application is developed by keeping in view following rules:

- Access Control using user name and password authentication.
- User role are implemented as
 - **Master Administrator** to manage organization registration.
 - **Organizational Administrator** to manage user's registration within organization.
 - **User** is created to share information to other users of same or different organization
- Security Classification of object and security clearance of subjects
- Audit trails of all the activities carried out by all the users maintained
- File deletion and storage rules
- Separate User Interface for all roles.

- Sharing based on security classification of information and security clearance of users

5.1.2 File sharing Methodology: The methodology used to share file among users is as under:

- A user can upload any type of file using interface provided in the application.
- Once upload file is saved at secure folder which does not have access by any user.
- The file load is categorized as the security classification.
- Time limit is applied on the file so that it deleted from share area.
- After upload, the file is shared to the user who has security clearance level equal or higher than the file.
- Log of sharing activity is generated.
- Receiver can download and delete the file from share area.

5.1.3 Functions of each user Role: Functions of each role are defined as following:

5.1.3.1 Master Administrator. It is basically administrator at application level and it performs following tasks:

- It can register organization.
- It can reset the properties of the organization
- It can create administrator of organization.
- It can reset the properties of the organization Administrator.
- It can view logs
- It cannot manage or create organization users
- It cannot share, view or download files / documents.,

5.1.3.2 Organization Administrator. It is administrator at organization level and can perform following tasks.

- It can create user at organization level.
- It can reset properties of users at respective organization level.
- It can view logs

- It cannot share, view or download files / documents.

5.1.3.3 Organization User. It is basic entity to share information using this application. It can perform following tasks.

- It can upload file
- Share file to user by name
- Download files shared for him.
- Delete file shared by him
- Delete files received by him.
- It cannot view or download file not shared for him.
- It cannot receive file having security classification level higher than his security level.
- It cannot perform any user level tasks.

5.1.4 Technologies used: To develop secure transfer application following technologies are used :

- **Java:** It is a programming language and state-of-the-art programs, application, utilities and games can be developed using JAVA.
- **Java Server Faces.** It is standard java EE web framework. It is used to build component based user interfaces for web application. It is well designed and easy to use framework [37].
- **Prime Faces.** It is an open source JSF component suit. It has rich set of components including HTML editor, AutoComplete and dialog.
- **Oracle XE Database.** Oracle database 11g is used to maintain data of secure transfer application.
- HTML 4.0
- Glass Fish web server
- Web browser (IE or Firefox).
- NetBeans as IDE

Screenshots of allocation are placed at Appendix B.

5.2 PKI System Development

A PKI setup is deployed to generate digital certificates using Microsoft server. Three tier hierarchal CAs are configured as designed discussed in previous chapter. In this design root CA and sub root CA are offline and Issue CA is on line available for issuance of certificates to users and machines and publishing of certificate revocation list (CRL).

5.2.1 Hardware / Software requirement. To configure three tier model following software and hardware are enquired:

- 1 x Server with operating system Windows server for Root CA
- 1 x Server with operating system Windows server for Sub Root CA
- 1 x Server with operating system Windows server for Issue CA

5.2.2 Configuration sequence. To configure hierarchal PKI setup is shown in figure 5.1 and following sequence was followed.

5.2.2.1 Configuration of Root CA. Root CA was configured at Microsoft server and it has self signed root CA certificate to be used for initiating of trust with low level and any other PKI setup. The properties of Root CA are as under:

Following software modules are installed before installation of certification authority

- Server 2003
- Application server
- Internet Information server
- World wide web service

Root CA has following properties.

- Key Length – 4096
- Certificate life – 8 years

5.2.2.2 Configuration Sub root CA. Sub root CA is configured after Root CA as certificate of sub root CA is issued by Root CA. installation steps and requirements are same except.

- Key Length – 2048
- Certificate life – 8 years

5.2.2.3 Configuration Issue CA. Issue CA is configured after sub root CA and it has root certificate of root CA and sub root certificate of sub root CA with following properties

- Key Length – 2048
- Certificate life – 4 years

5.2.2.3 CRL distribution point. CRL is issued by every CA to check the validity of the certificates issued by the respective CA. The access to the CRL for all the PKI based application is compulsory.

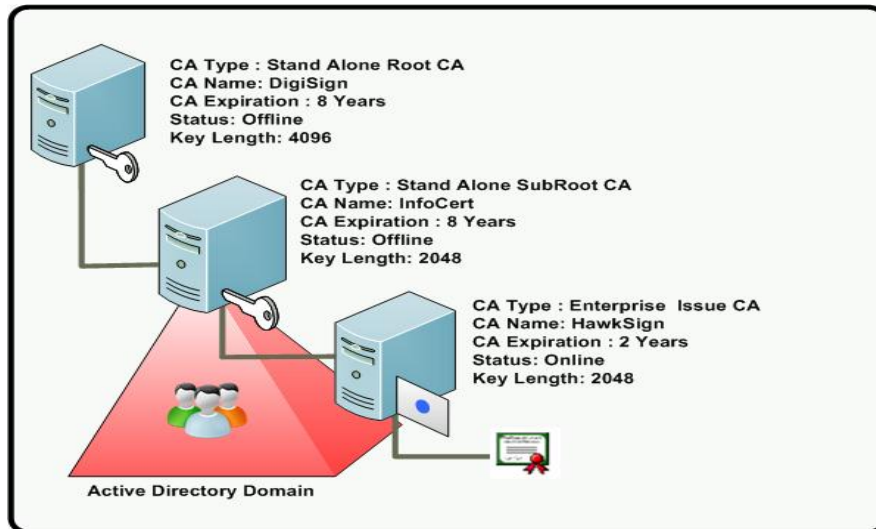


Figure 5.1: PKI Configuration

5.2.3 Certificate Type. Following is the list of certificate template types and their uses to be issued to users and machines.

- **Administrator.** It allows the holder to send secure email, encrypt and decrypt files used under Encrypting File System (EFS) and user authentication.

- **Computer.** This allows one computer to authenticate in network with other computer and user.
- **Domain Controller.** This allow domain controller in Active Directory to authenticate with other computers.
- **EFS Recover Agent.** This is used for recovery of files encrypted by EFS and holder has also designated it as recovery agent.
- **IP Sec.** Use to in IP Sec protocol for encrypt and decrypt network communication.
- **Root Certification Authority.** This template certificate allows the CA to work as root certification Authority.
- **Subordinate Certificate Authority.** This template certificate allows the CA to work as subordinate certification Authority in CA hierarchy.
- **User.** It permits the certificate holder to digitally signed and encrypted email and authenticate on network.
- **Web Server.** Use for SSL and proves identity of web server to clients and encrypt network communication.

Screen Shots of PKI setup are placed at Appendix C

5.3 Configuration of Secure Network.

To have secure environments for secure sharing of classified information a secure network was configured as per design given in previous chapter. Off the shelf hardware was used to establish the network. Following hardware was used to establish network.

- Two firewalls of Juniper Networks
- One Cisco router
- One managed switch for VLAN configuration.

Each network service has its own different network to build the concept of compartmentalization. VLAN are configured at switch and communication among different networks is controlled by routers. To communicate through un-trust networks VPN is created among firewalls. One firewall is placed ay boundary of friendly network and other firewall is places at boundary of other organization. IP scheme for every part was different as shown in table below.

Table 3 : Different Networks IPs

SNo	Service	IP Scheme
1	DNS	10.10.0.0/24
2	Network Monitoring	10.10.1.0/24
3	Active Directory	172.18.1.0/24
4	PKI Server	192.168.0.0/24
5	User Network	172.16.1.0/24

5.4 Establishment of Active Directory services and Secure Email Server

To share the information among organization second option given IOIS framework is use of secure email. To demonstrate the concept of secure email, a proper user environment is established using Microsoft Active Director and Microsoft Email Server. The design of Active Directory is shown in figure 5.2.

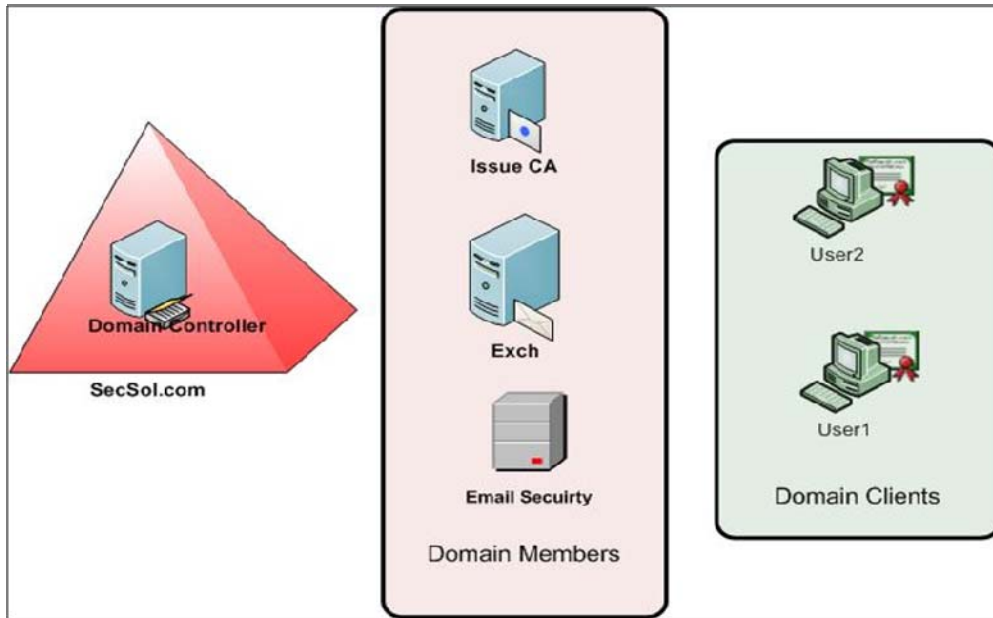


Figure 5.2: Active Directory Deployment

5.4.1 To implement secure email from one user to another user following are mandatory steps:

- Every user is member of domain secsol.com
- Each user should have email box created at email server
- Each user has certificate issued from the domain certification Authority
- Certificate of user should have installed on his computer.
- Email Client (Microsoft Outlook) is installed and configured on computer.

5.4.2 To implement further security on the emails, email monitoring and filtering solution GFI email security was installed. All the emails initiated and received are scanned first through GFI email security and then delivered to user. To monitor the email filter and action rules were configured as under:

- Content filtering basing on sensitive words in subject and body of the email
- Filtering on attachment types as *.exe or *.vbs can carry virus or worms.
- Multiple virus scan engines.
- On matching of filter the email is quarantined and information is send to administrator and sender.
- Default attachment checking rules are as under

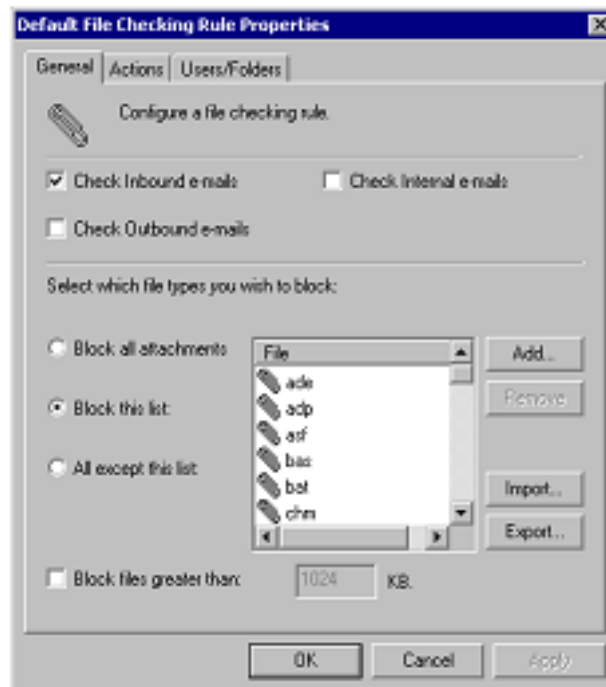


Figure 5.3: Email Security [39]

5.5 Network and System Monitoring

To meet the requirement of auditing and monitoring a proper logging system is required at any network. Real time monitoring is also required at IOIS framework.

5.5.1 System Level Monitoring. To monitor user activities and machine security and application event logs are collected and reports are generated with help of GFI event log manager. The deployment of event manager is made as shown in figure 5.4 [38].

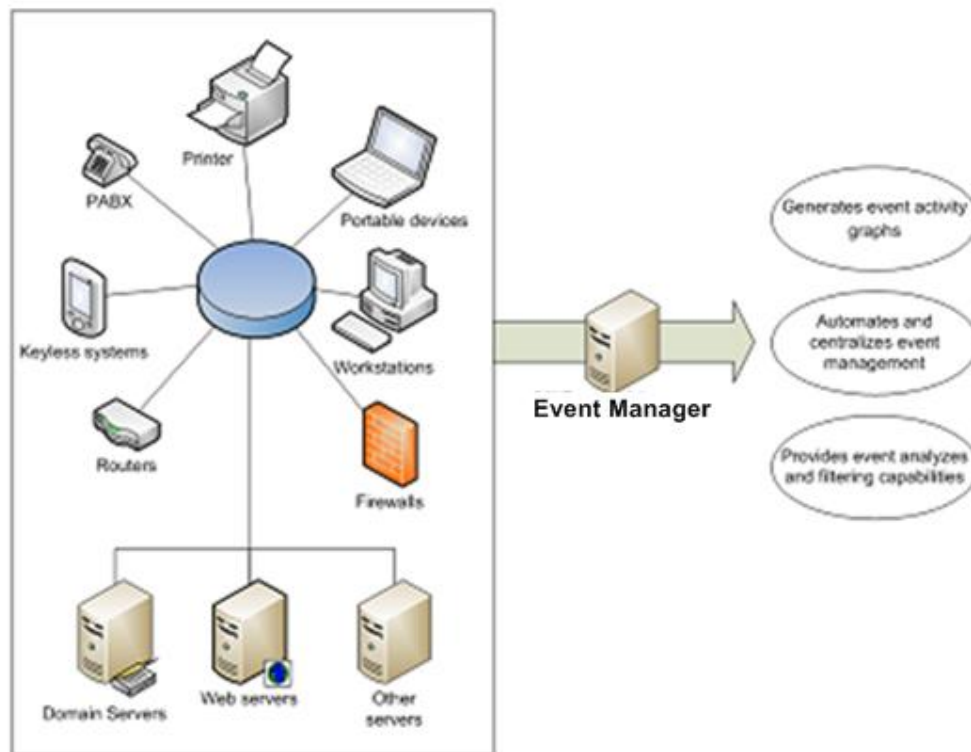


Figure 5.4: Network Monitoring System [38]

Using GFI event manager all sorts of events logs of server machines and client computers are collected at single database. The events include.

- User login and logoff events
- Computer startup and shut down events
- Any changes made in user account.
- Bad password attempts.
- User login after office timings or on weekends.

- Any policy violation.
- Multiple Reports are generated

5.5.2 Network level Monitoring. To monitor real time network round the clock a professional level network performance monitor is required. To create secure network for IOIS, NMP of solar winds is used. The NMP helps the following for network:

- It provides real time view of network availability.
- It performs automated network discovery.
- It also generates real time alerts.
- Real time alerts when any devices are down or restarts.
- Port level traffic volume monitoring.

5.6 Sequence of activities in IOIS

Step by step execution of IOIS

5.6.1 Scenario 1: Use of a secure application to share file among different organizations basing the classification of information and security clearance of the receiver.

Step 1

Action: intention to share information

Security Principle: MOU – Mutual Agreement basing on operational requirements and security requisites

Security Control: Policies and procedures

Technical Measures: Development of environment as per standards agreed upon at MOU

Step 2

Action: Approach to secure place

Security Principle: Physical Security

Security Control: Access control

Technical Measures:

1. Smart card
2. Video Surveillance

Step 3

Action: Startup System

Security Principle: Physical Security, Monitoring

Security Control: Access control

Technical Measures:

1. System security logs
2. Alert and Report of system startup including all necessary details

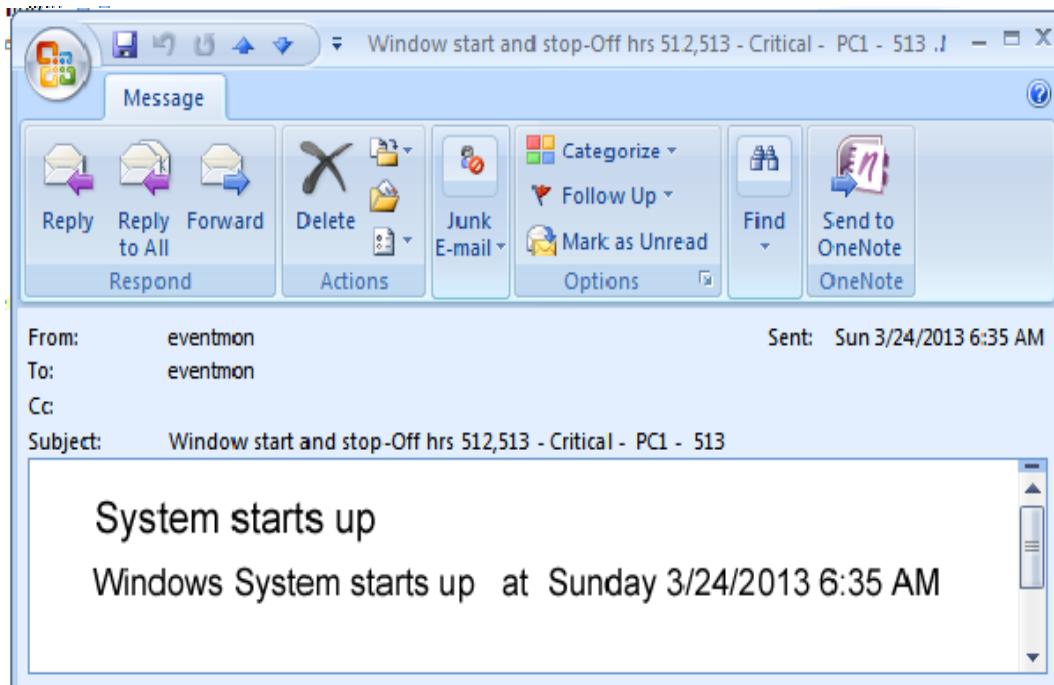


Figure 5.5: System starts up email

Step 4

Action: Login to Active Directory

Security Principle: Identification, Authentication, Monitoring

Security Control: Access control

Technical Measures:

1. Authentication Mechanism
 - a. Username /password
 - b. Digital certificates

- c. Biometrics
- 2. System security logs
- 3. Alert and Report of system startup including all necessary details

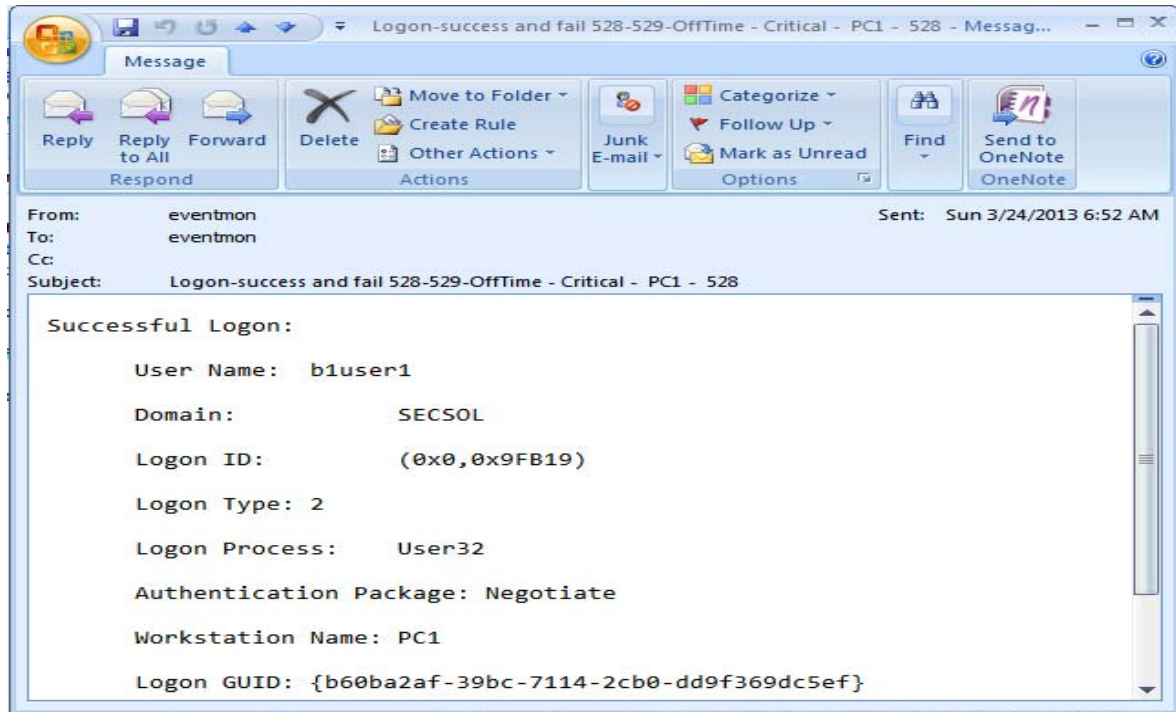


Figure 5.6: User login alert mail

Step 5

Action: Access to file to be shared

Security Principle: Storage, Authorization, Security Classification, Confidentiality, Integrity, Monitoring

Security Control: Access control, Encryption, Hashing,

Technical Measures:

- 1. Symmetric encryption
- 2. Asymmetric encryption
- 3. Access monitoring- logs

Step 6

Action: Transfer of Information

Methodology: Secure sharing application

Security Principle: Identification, authentication, Security Clearance, Monitoring, Application deployment.

Security Control: Access control – RBAC

Technical Measures:

1. Username / password
2. Access monitoring- logs
3. SSL

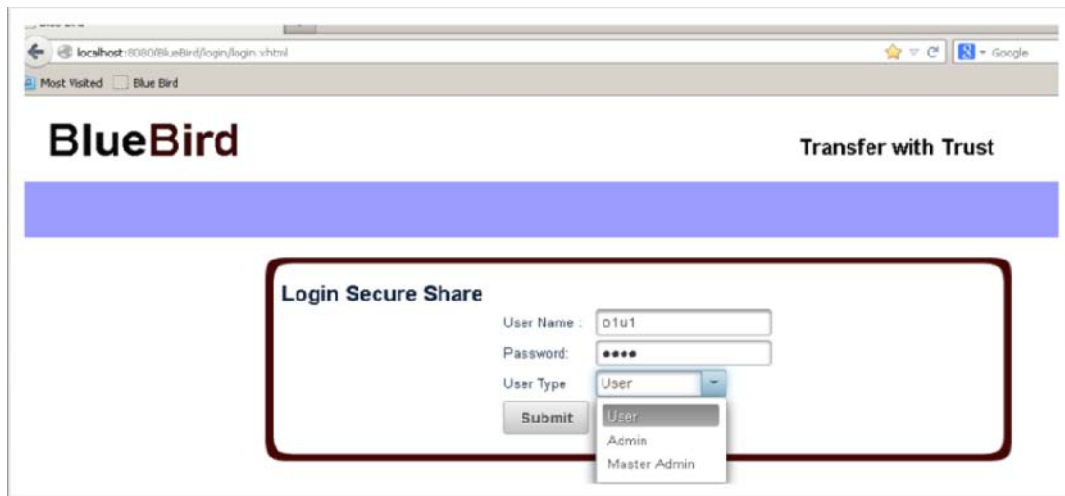


Figure 5.7 : Login to Secure Transfer Application

Step 7

Action: Upload File

Security Principle: confidentiality, integrity, security classification, Monitoring

Security Control: Access Control

Technical Measures:

1. Logs
2. Encryption
3. Hashing
4. Security classification

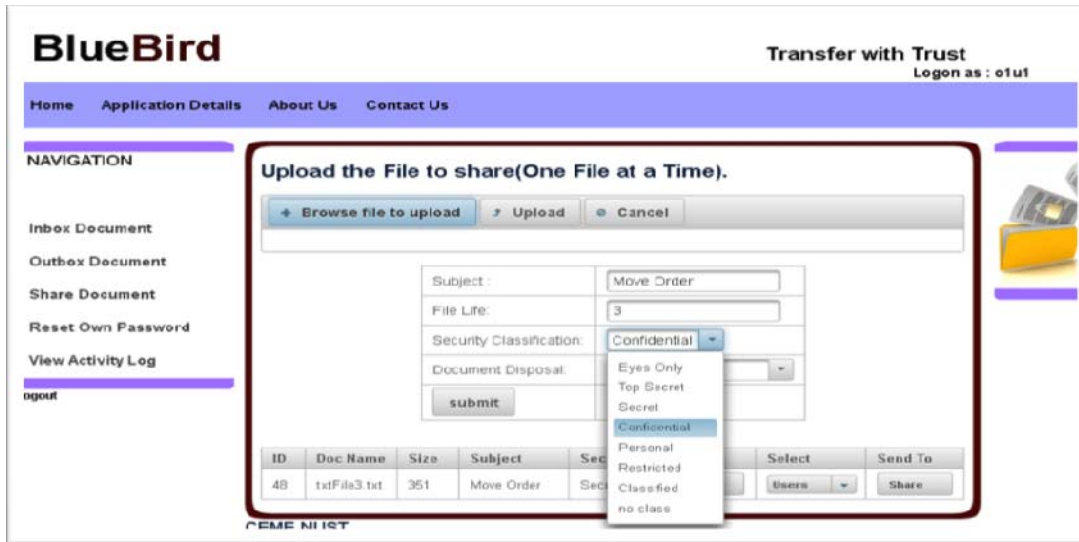


Figure 5.8 : Upload File for sharing

Step 8

Action: Marking of File

Security Principle: security classification, Monitoring, Identification of Receiver

Security Control: Access Control

Technical Measures:

1. Logs
2. Security Clearance

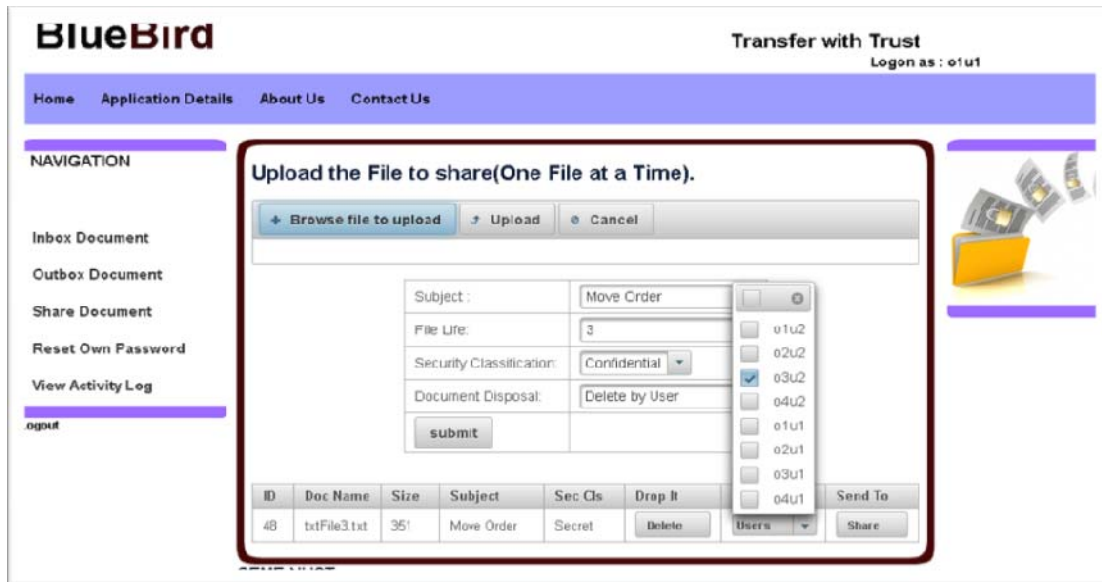


Figure 5.9 : Marking to Selected User

Step 9

Action: Send File

Security Principle: Monitoring, Network security

Security Control: Network security Controls

Technical Measures:

1. VPN
2. Network Devices Monitoring – Configuration changes etc
3. Network physical security
4. Logs
5. Configuration management
6. Secure Routing
7. File policies

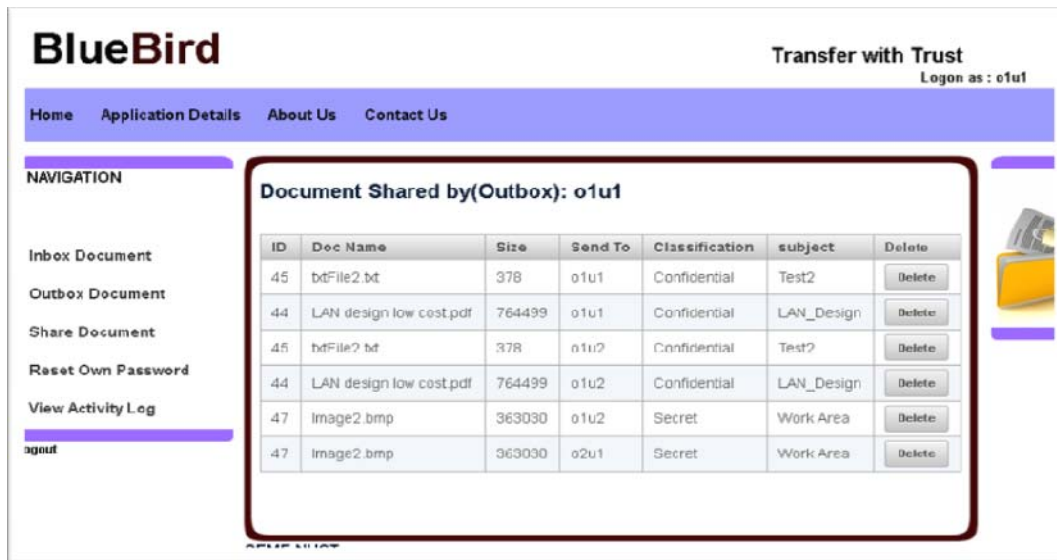


Figure 5.10 : Outbox view

Step 10

Action: Receive File

Security Principle: security classification, Monitoring, Identification of Receiver, Authorization

Security Control: Access Control

Technical Measures:

1. Security clearance check
2. Logs
3. Decryption
4. Integrity checks
5. Non- repudiation

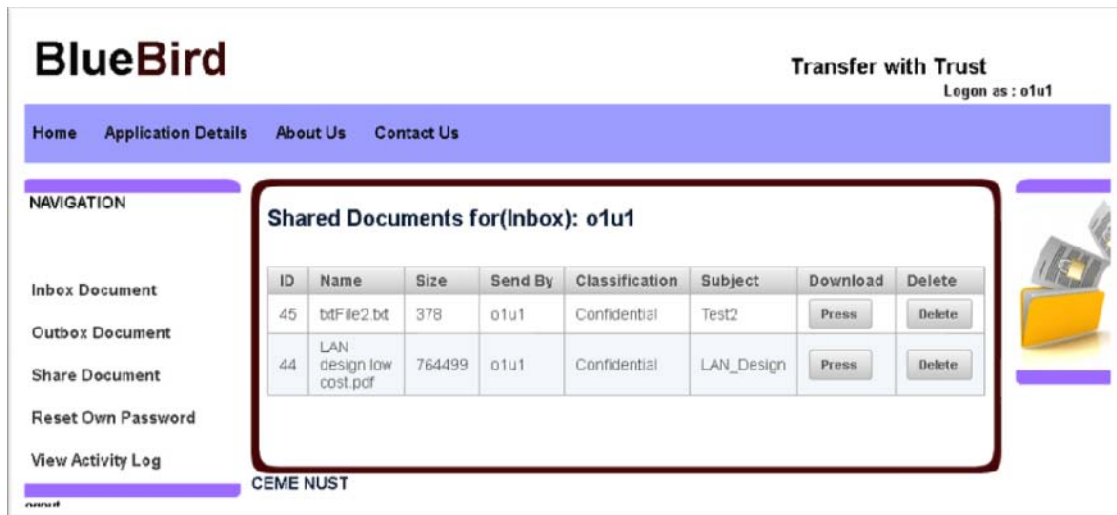


Figure 5.11 : Inbox view

Step 11

Action: View File

Security Principle: Non-repudiation, integrity, confidentiality

Security Control: Access Control

Technical Measures:

1. Hash matching
2. Logs
3. Decryption

Step 12

Action: Secure Disposal

Security Principle: Monitoring, Destruction

Security Control: Access Control,

Technical Measures:

1. Declassification
2. File eraser
3. Logs

5.6.2 Scenario 2: Use of secure email to share file among different organizations basing the classification of information.

Steps 1 to 5 are same as in scenario 1 and further sequence of activity will be as under:

Step 6

Action: Transfer of Information

Methodology: Secure email

Security Principle: Identification, authentication

Security Control: Access control

Technical Measures:

1. Email client /server
2. Username / password
3. Digital Certificate

Step 7

Action: Write message and upload file

Security Principle: confidentiality, integrity, security classification, Monitoring

Security Control: Access Control, Encryption, Digital signature,

Technical Measures:

1. Digital certificate
2. Encryption
3. Hashing
4. Email filter



Figure 5.12 : Email Message - Encryption

Step 8

Action: Receive email

Security Principle: Non-repudiation, integrity, confidentiality

Security Control: Access Control, Digital signature, encryption

Technical Measures:

1. Digital certificate
2. Encryption
3. Hashing
4. Email filter

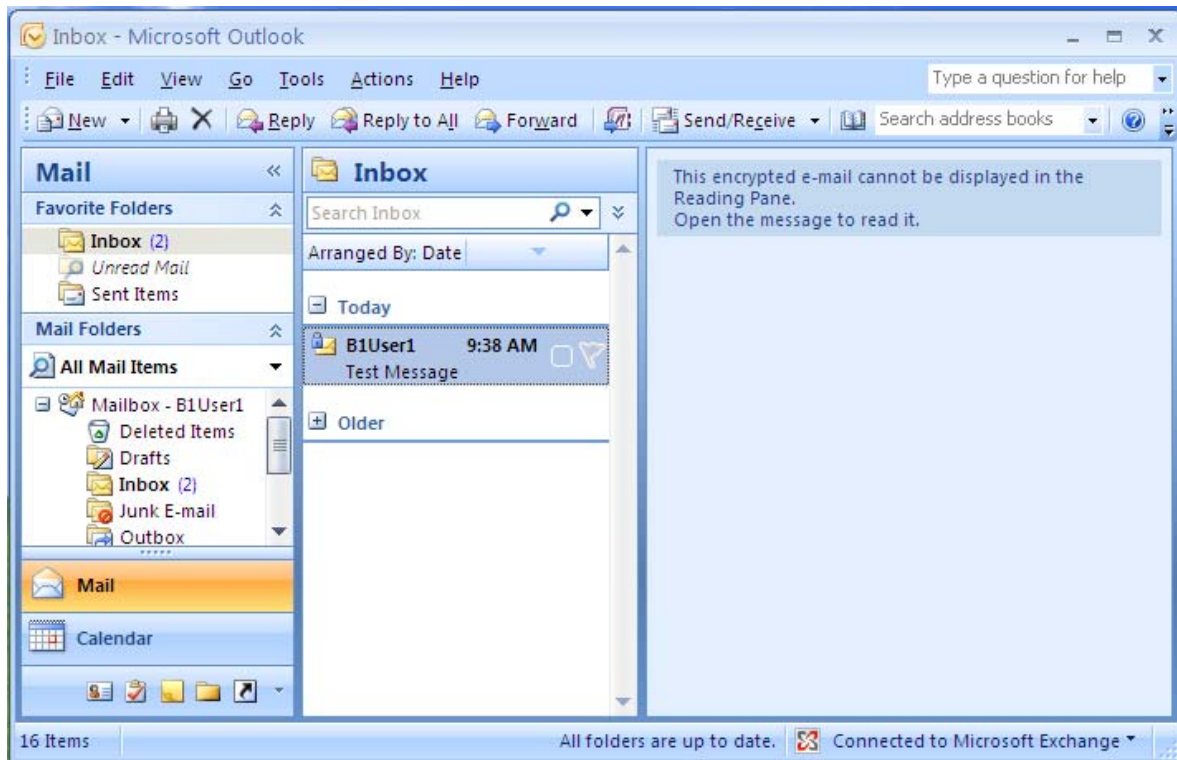


Figure 1 : Email view at Reading Pane

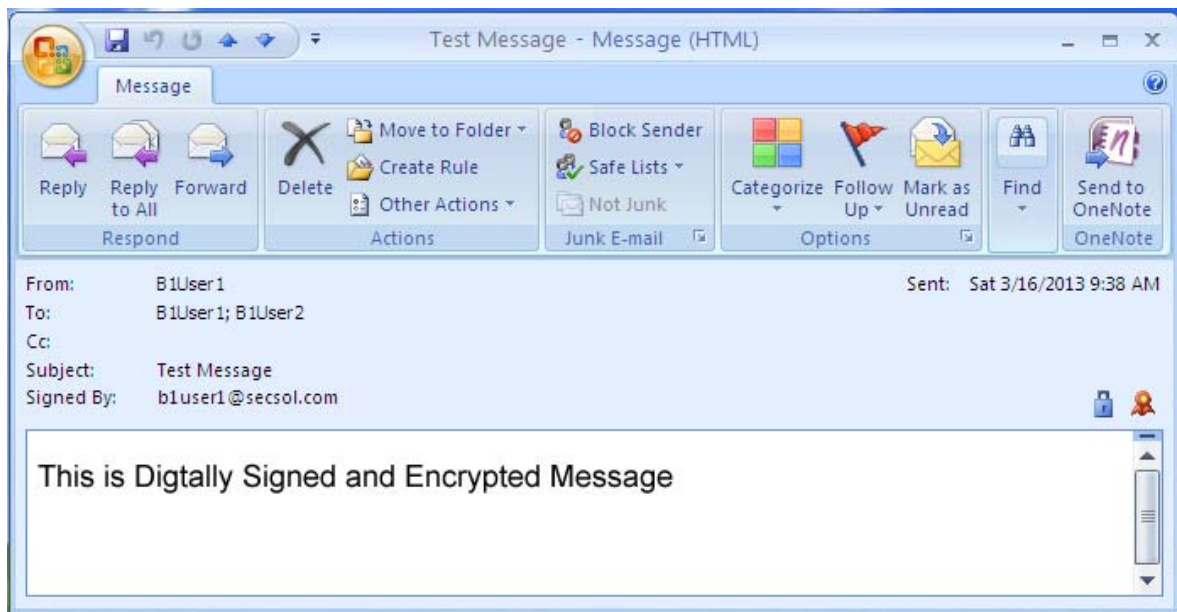


Figure 5.14 : Received Encrypted Email

5.7 Evaluation and Analysis

The aim this section is to evaluate and analyze the IOIS with respect to security, efficiency and trust building. The expected result or any other outcome of any policy is achieved after true implementation for some duration of time and applying it at environment for which it is formulated. When to cater for security requirements of sharing environment different controls are applied according to risks present. To evaluate the performance of IOIS we can apply following methodologies

5.7.1 Evaluation methodology A

Effectiveness of applied security controls is used to evaluate performance against security risks. To calculate the total effectiveness, each control is evaluated individually and then product of is used. As any single security control cannot provide 100% security and availability so combination of security controls is deployed. IOIS provide multiple layers of security. Each layer provides considerable security but not 100%, so by deploying right combination of security controls we can very close to 100%. Here is simple effectiveness measurement equation to for security controls [40].

$$\text{Effectiveness}_{\text{total}} = 1 - ((1-E_1)*(1-E_2)*(1-E_3)...) \quad (5.1)$$

Here E1, E2 presents effectiveness of single security control applied against security threats. If E1 (Security polices) is applied and it gives 80% and to cater for rest 20% we apply E2 (Network security) which again provides 80% of 20% than the resultant security is

$$\text{Effectiveness}_{\text{total}} = 1 - (1-80\%) * (1-80\%) = 96\% \quad (5.2)$$

By applying all the security controls as indicated in IOIS as E3 (Access control), E4 (Secure storage) and E5 (Monitoring and auditing) we get following results

$$\text{Effectiveness}_{\text{total}} = 1 - (1-80\%) * (1-80\%) * (1-80\%)*(1-80\%)*(1-80\%) = 99.97\% \quad (5.3)$$

This is very close to the required level of security as total risk cannot be eliminated but we try to reduce the risk to acceptable level.

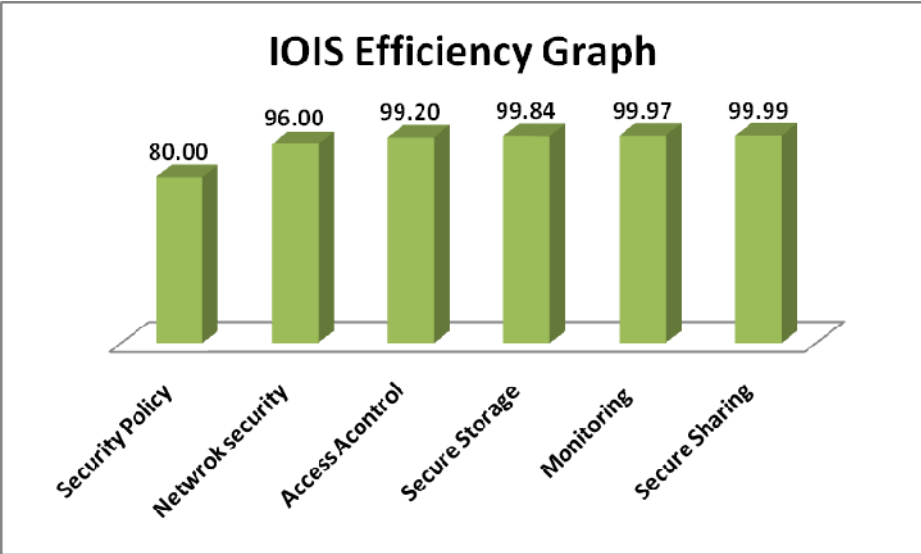


Figure 5.15 : Security Controls Efficiency

- Government Information Sharing – A Framework for policy formulation* [20], is a theoretical model for information sharing. Authors have focused on four aspects Technological, Organizational, Inter-organizational and Environmental. Within technical concepts information security standards are mentioned which include encryption (secure storage), network security, and access control and secure sharing. The total effectiveness value for four type security controls is as under

$$\text{Effectiveness}_{\text{total}} = (1 - ((1-80\%)*(1-80%)*(1-80%)*(1-80\%))) * 100 = 99.84 \% \quad (5.4)$$

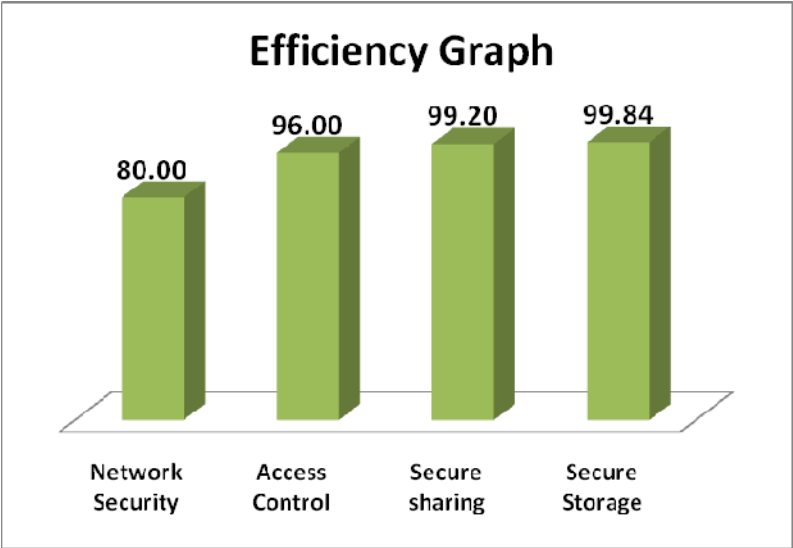


Figure 5.16: Security Efficiency graph for Government Information Sharing Policy Framework

- Requirements different security measures for information sharing have been highlighted at *Standards for secure data sharing across organization* [2]. Basically authors have focused only at problem areas for which standards should be made before sharing. As for security control and mechanism are concerned main emphasis is made on use of encryption (for storage), secure sharing application and policies.

The total effectiveness value for three type security controls is as under

$$\text{Effectiveness}_{\text{total}} = (1 - ((1-80\%)*(1-80%)*(1-80\%))) * 100 = 99.20 \% \quad (5.5)$$

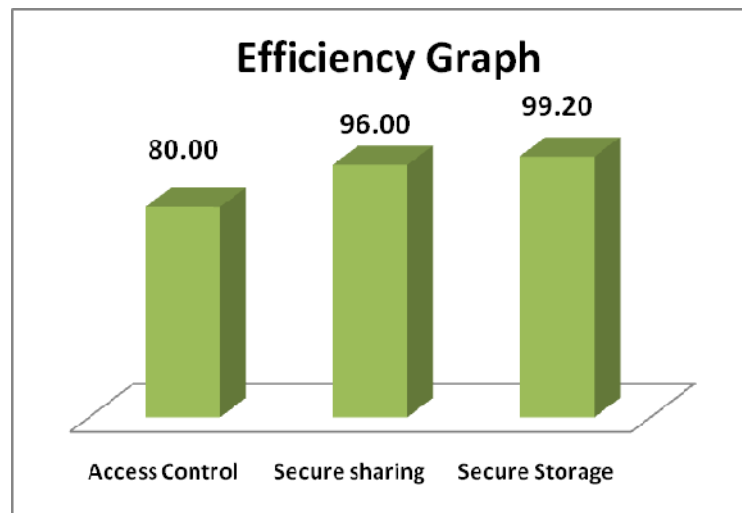


Figure 5.17: Security Efficiency graph for Standards for secure data sharing across organization

Data sharing requirements have also been elaborated by LI Ming and LUO Nianlong [16] at *Data Sharing in Campus Network*. Authors have mainly discussed use of digital certificate server to manage access control and encryption for security. Total effectiveness of these controls can be determined as under:

$$\text{Effectiveness}_{\text{total}} = (1 - ((1-80\%)*(1-80\%))) * 100 = 96.0 \% \quad (5.6)$$

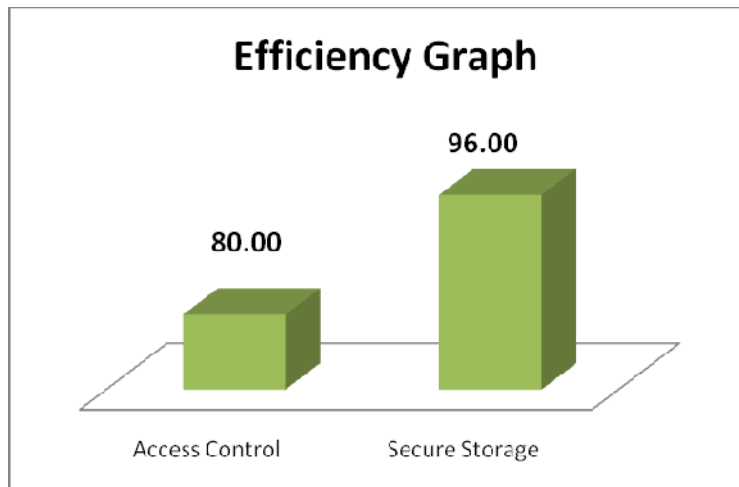


Figure 5.18: Security Efficiency graph for Standards for Data Sharing in Campus Network

5.7.2 Evaluation methodology B

To analyze IOIS in more details, the comparison is made with methods and techniques available to share information among different organizations. Following is the list methods available to share information:

- P2P - Peer to Peer File Sharing
- Email
- Online Sharing Services
- Removable media
- FTP File Transfers
- Instant messaging.
- The web
- Any special application for sharing of information

Normal practice at local departments used to share the information is use of email or removable media especially use of USB disk and CD which have some advantages but many inherent draw backs. Normally some personal is used carrier to carry remove able disk from one place to another and data is copied. Some time the classified data is removed from the disk and it causes big security breaches.

5.7.2.1 Evaluation Criteria.

To evaluate the IOIS with existing practices following criteria parameters are used and evolution values are presented in table:

- Security
- Ease of Use
- Cost
- Availability of Technology
- Availability of Expertise.
- Monitoring / Auditing feasibility
-

Table 4: Evaluation of Sharing Methods

Sno	Technique	Size Limit	Cost	Ease of Use	Expertise	Availability of Tech	Security	Auditing Monitoring	Speed
1	P2P	No	Less	Yes	Not much	Yes	No	No	Yes
2	Public Email	Yes	Less	Yes	Not much	Yes	No	No	Yes
3	Removable media	No	Less	Yes	Not much	Yes	No	No	Yes
4	FTP File Transfers	No	Less	Yes	Not much	Yes	No	No	Yes
5	Instant messaging	Yes	Less	Yes	Not much	Yes	No	No	Yes
6	The web	Yes	Moderate	Yes	Not much	Yes	Moderate	yes	Yes
7	special application	No	Moderate	Yes	Required	Yes	Moderate	Yes	Yes
8	IOIS	No	High	Yes	Required	Yes	High	Yes	Yes

5.8 Summary

Detailed implementation of IOIS framework as designed in the previous chapter is described. At start development of secure application using JAVA and JSF as main technology is explained. After that hierarchical PKI is developed using Microsoft server and details of all certificate templates with usage is covered. Deployment of network according to services

with different subnets is for each service is described in details. Environment for secure email and real-time monitoring comprises of active directory is explained. After that two scenarios are depicted to explain all the security controls of IOIS. At the end of this chapter two methodologies are used to evaluate and analyses the IOIS framework

CHAPTER 6: CONCLUSION AND FUTURE WORK

CHAPTER 6: CONCLUSION AND FUTURE WORK

6.1 Conclusion

For smooth and efficient completion of joint assignments information sharing among different government and civil organizations and agencies is necessary. To have reliable information sharing among stakeholders, first and most important is will to share without fear and network interoperability. It also includes availability of technical expertise and efforts to protect safeguard it from unauthorized access and modification. In short all necessary measures should be taken from security perspective. When sharing information, other than securing information, it should also be accessible, understandable, interoperable, trusted, and safeguarded. In this research by designing IOIS framework, the considerations are practical challenges in information sharing by system administrators, network administrators and stakeholders. By implementing all the measures and security principles as discussed in IOIS framework secure and trusted information sharing is possible and can help to improve the organizations work in more productive and swift manners especially in emergency situations. Use of network security and monitoring at all levels provides reasonable protection against external and internal security threats.

In this research work, effort has been made to incorporate multilayer security with view to achieve secure and trusted information sharing environment. Work already ready done in this domain is briefly described at literature review section which comprises of different standards and guiding frameworks for information sharing. Frameworks and standards related information sharing and information security are analyzed and a gap analysis is also made at end of literature review.

After literature review IOIS policy framework is explained and all the parts of frame work are elaborated so that main theme of IOIS framework is made clear. All the parts of IOIS with respect to security requirements and methodologies to fulfill these requirements are discussed. Every principle is explained with rational and necessary implementing

methodologies. This framework basically revolves around the understanding among stakeholder is expressed as MOU document, secure network with physical security and real-time monitoring, access control, secure storage and proper disposal of shared information. Benefits of these technologies and how secure sharing is improved is described in details. These principles are implemented in isolation and then by use of information security policy, cohesive secure environment is developed by uniting properties of all the principles and security controls.

In next part design details of the framework are explained so the desired results from the proposed framework are achieved as expected. The design part has incorporated all necessary details about network, system and application. Design for network including DMZ, different working domains, separate service network and comprehensive monitoring and logging. To satisfy the critical security principles like confidentiality, integrity, non-repudiation and authentication design of secure PKI system discussed with implementation values. To share information through email, design for secure email system based on real time content filtering is proposed.

Chapter 5 is basically implementation of design part so that framework can be implemented and tested. Each principle of framework is implemented in lab environment basing on design made in previous chapter. All implementation details including deployment methodologies and technologies used are explained with screenshots. Necessary hardware and software required to get the required results are mentioned with configuration details. At the end of this section evaluation and analysis of IOIS with other available frameworks and methods in practice is done. Two evaluating methodologies are used to evaluate the strength and efficiency of IOIS framework and design. Methodology A uses effectiveness of security controls in form of percentage and aggregate effectiveness is calculated to evaluate the design strength. Second evaluating methodology is comparison with exiting practices being used at different government and civil organizations.

Success of any policy framework depends upon the interest and support of the higher authorities. It is the job of senior management of the organization to support and ensure the implementation of all the policy points.

IOIS frame is basically made to have a reliable, secure and trusted environment. It is an effort to build trust to share classified information by judicious use of tested and renowned technologies. To make the sharing an reliable and secure activity all applicable security

measures are incorporated which includes (1) Multilayer security (2) Monitoring at all levels (3) RBAC and MAC (4) PKI system and (5) security classification. User confidence is built using security management principles like least privilege and need to know. However security any environment is ongoing process and continuous efforts and vigilance is required with due care and diligence.

6.2 Future Work

Research can be extended for more smooth and dynamic access control so that only authorized access is ensured with object level detailed monitoring. The system should be able to accommodate dynamics of information sharing among collation organizations. As access to the information is very critical and in real world user role constraints are enforced due to shortage of expert personal and these role constraints can compromise access to critical information. Therefore more work is required to incorporate role delegation and user constraints at access control level.

Other dimension which can be explored is intelligent storage and search of shared information with respect to the role and area of responsibility of each organization involved.

REFERENCES

- [1]. **Dynamic security policy learning.** Yow Tzu Lim, Pau-Chen Cheng ,Pankaj Rohatgi ,John A. Clark. 2009. New York : ACM, 2009. Proceedings of the first ACM workshop on Information security governance. pp. 39-48.
- [2]. **Standard for secure data Sharing across organization. [Journal].** Douglas Harris, Latifur Khana, Raymond Paulb, Bhavani Thuraisingham, January 2007, Computer Standards & Interfaces - CSI , vol. 29, no. 1, pp. 86-96, 2007
- [3]. **Automated Military-Civilian Information Sharing.** Dourandish, R. Quimba Software, San Mateo, CA Zumel, N. ; Manno, M. 2006. s.l. : IEEE, 2006. Military Communications Conference, 2006. MILCOM 2006. pp. 1-5.
- [4]. **Harris, Shon. 2009.** Access Control. *CISSP All in one Exam Guide.* 5th . : Mc Graw Hill, 2009.
- [5]. **Information sharing and security in dynamic coalitions.** Charles E. Phillips, Jr. T.C. Ting, Steven A. Demurjian. 2002. New York : ACM, 2002. SACMAT '02 Proceedings of the seventh ACM symposium on Access control models and technologies. pp. 87-96.
- [6]. **Research on Policy-based Access Control Model.** Lin Zhi, Wuhan Commanding Commun. Acad,Wuhan Wang Jing, Xiao-su, Chen and Lian-Xing, Jia. 2009. s.l. : IEEE, 2009. Networks Security, Wireless Communications and Trusted Computing, 2009. Vol. 2, pp. 164 - 167.
- [7]. **Access control models for business processes.** Karimi, Vahid R.Cowan, Donald D. 2010. s.l. : IEEE, 2010. Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference. pp. 1-10.
- [8]. **Guidelines for an Information Sharing Policy.** Chris Gilber. 2011. ver. 1.4b option 1, s.l. : SANS, Jan 10, 2011, SANS Institute InfoSec Reading Room, Vol. GSEC.
- [9]. **Group-Centric Models for Secure and Agile Information Sharing.** Ravi Sandhu, Ram Krishnan, Jianwei Niu, and William H. Winsborough. 2010 . s.l. : ACM, 2010 . MMM-ACNS'10 Proceedings of the 5th international conference on Mathematical methods, models and architectures for computer network security . pp. 55-69 .
- [10]. **Automated Military-Civilian Information Sharing.** Dourandish, R. Quimba Software, San Mateo, CA Zumel, N. ; Manno, Military Communications Conference, 2006. MILCOM 2006. IEEE. pp. 1-5.
- [11]. **"RFC 2196: Site Security Handbook."** Fraser, B. (Editor), Various (Authors). Key fingerprint = AF19 FA272F94998DFDB5DE3DF8B506E4A1694E46 URL: <http://www.ietf.org/rfc/rfc2196.txt>? Number=2196 (25 Feb. 2013).

- [12]. **A Practical Guide to Policy Making in Northern Ireland.** *Office of the First Minister and Deputy First Minister.* [Online] Aug 2011. [Cited: Feb 20, 2013.] <http://www.ofmdfmni.gov.uk/practical-guide-policy-making - amend aug 11.pdf>.
- [13]. **Technical, Social & Legal Barriers to Effective Information Sharing Among Sensitive Organizations.** Joseph V. Treglia, Joon S. Park. 2009. Chapel Hill, NC, USA. : ACM, 2009. Conference'09.
- [14]. **Exploring the causes and effects of inter-agency information sharing systems adoption in the anti/counter-terrorism and disaster management domains.** JinKyu Lee, H. Raghav Rao. 2007. [ed.] Digital Government Society of North America. s.l. : ACM, 2007. roceedings of the 8th annual international conference on Digital government research: bridging disciplines & domains . pp. 155-163. ISBN:1-59593-599-1 .
- [15]. **Towards trusted intelligence information sharing.** Joseph V. Treglia , Joon S. Park. 2009. s.l. : ACM, 2009. CSI-KDD '09 Proceedings of the ACM SIGKDD Workshop on CyberSecurity and Intelligence Informatics . pp. 45-52 . ISBN: 978-1-60558-669-4 .
- [16]. **Data sharing in campus network.** Li Ming, Luo Nianlong. Aug, 2009. [ed.] IEEE. Beijing, China : IEEE, Aug, 2009. IT in Medicine & Education, 2009. ITIME '09. IEEE International Symposium on Comput. & Inf. Vol. 1, pp. 601-605.
- [17]. **A data sharing agreement framework.** Vipin Swarup, Len Seligman, Arnon Rosenthal. Dec 2006. [ed.] Vijayalakshmi Atluri Aditya Bagchi. Kolkata, India : Springer-Verlag Berlin, Heidelberg ©2006,. Information Systems Security, ICISS 2006. Vol. 4332, pp. 22-36. 978-3-540-68963-8.
- [18]. **Memorandum of understanding.** Wikipedia. , *the free encyclopedia.* [Online] [Cited: Feb 25, 2103.] http://en.wikipedia.org/wiki/Memorandum_of_understanding.
- [19]. **Memorandum of understanding (MOU or MoU).** Margaret Rouse. 2011 *WhatIs.techtarget.com.* [Online] Jan 2011. [Cited: Feb 23, 2013.] <http://whatis.techtarget.com/definition/memorandum-of-understanding-MOU-or-MoU>.
- [20]. **Government Information Sharing – A Framework for Policy Formulation** [Book Section] / auth. E. Estevez, P. Fillottrani, T. Janowski, and A. Ojo // E-Governance and Cross-boundary Collaboration: Innovations and Advancing Tools / ed. Y. - C. Chen and P. - Y. Chu. - [s.l.] : IGI Global, 2011. - EISBN13: 9781609607548
- [21]. **Understanding the “Boundary” in Information Sharing and Integration** [Conference] / auth. Lei Zheng, Tung-Mou Yang ; Pardo, T. ; Yuanfu Jiang // System Sciences, 2009. HICSS '09. 42nd Hawaii International Conference on System Sciences - [s.l.] : IEEE, 2009. - pp. 1-10.
- [22]. **Interoperability Framework** (2008, February). New Zealand e-Government Interoperability Framework (NZ e-GIF) Version 3.3. Retrieved February 10, 2013, from e-Government in New Zealand : <http://www.e.govt.nz/library/e-gif-v-3-3-complete.pdf>

- [23]. **A new VPN routing approach for large scale networks** [Conference] / auth. Houidi, Z.B. Orange Labs., France Meulle // Network Protocols (ICNP), 2010 18th IEEE International Conference. - Kyoto Japan : IEEE, 2010. - pp. 124-133.
- [24]. **Towards Safe and Optimal Network Designs Based on Network Security Requirements** [Conference] / auth. Nihel Ben Youssef Ben Souayah and Adel Bouhoula // Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference. - Liverpool UK : IEEE, 2012. - pp. 573-579.
- [25]. **Practical application of information security models** [Journal] / auth. Vladimir Jirasek // Information Security Tech.. - Oxford : Elsevier Advanced Technology Publications, February 2012. - 1-2 : Vol. 17. - pp. 1-8.
- [26]. **Harris, Shon. 2009.** Information Security and Risk management . *CISSP All in one Exam Guide*. 5th . : Mc Graw Hill, 2009.
- [27]. **Study on the access control model in Information Security** [Conference] / auth. Bai Qinghai, Zheng Ying // Cross Strait Quad-Regional Radio Science and Wireless Technology Conference (CSQRWC). - Harbin, China : IEEE, 2011. - Vol. 1. - pp. 830-834.
- [28]. **Interoperability and information brokers in public safety: an approach toward seamless emergency communications** [Journal] / auth. Andreas Kuehn, Michael Kaschewsky, Andreas Kappeler // Journal of Theoretical and Applied Electronic Commerce Research. - Chile : [s.n.], April 2011. - 1 : Vol. 6. - pp. 43-60.
- [29]. **System Design of Unified Auditing and Monitoring Based on Complex Network** [Conference] / auth. Liu Lianzhong ; Li Chunfang ; Li Xiangyu // Intelligent System Design and Engineering Application (ISDEA), 2012 Second International Conference . - Sanya, China : IEEE, 2012. - pp. 1144 - 1147.
- [30]. **The monitoring and auditing method of Windows File manipulations** [Conference] / auth. Naval Acad; Chen Houwu ; Liu Fuqiang // Information Management, Innovation Management and Industrial Engineering (ICIII), 2012 International Conference . - Sanya, China : IEEE, 2012. - Vol. 3. - pp. 366 - 368.
- [31]. **Secure Remote Storage through Authenticated Encryption** [Conference] / auth. Fangyong Hou, Dawu Gu ; Nong Xiao ; Yuhua Tang // Networking, Architecture, and Storage, 2008. NAS '08. International Conference. - Chongqing, China : IEEE, 2008. - pp. 3 - 9.
- [32]. **A Secure Storage Service in the Hybrid Cloud** [Conference] / auth. Surya Nepal, Carsten Friedrich, Leakha Henry, Shiping Chen // Utility and Cloud Computing (UCC), 2011 Fourth IEEE International Conference. - Melbourne, Australia : IEEE, 2011. - pp. 334 - 335.
- [33]. **Network Security Architecture** [Journal] / auth. Stawowsk Mariusz // The ISSA Journal. - [s.l.] : ISSA, May 2009. - 5 : Vol. 7.
- [34]. **The Principles of Network Security Design** [Journal] / auth. Stawowski By Mariusz // The ISSA Journal. - [s.l.] : ISSA.org, October 2007.

- [35]. **Windows server PKI Certification Authority** [Book] / auth. Komar Brain. - Washington : Microsoft Press, 2008. - 1 : p. 800.
- [36]. **The Security and Trust Services API (SATSA) for J2ME** [Online] / auth. Ortiz C. Enrique // ORACLE Sun Developer Network. - ORACLE, September 2005. - Mar 5, 2013. - <http://dsc.sun.com/mobility/apis/articles/satsa2/>.
- [37]. **What is JSF (JavaServer Faces)** [Online] / auth. Emailed Baski // JAVA Samples. - Java-samples.com, July 2009. - February 25, 2013. - <http://www.java-samples.com/showtutorial.php?tutorialid=466>.
- [38]. **GFI EventsManager®** -[Online] // GFI. - 2012. - Feb 25, 2013. - <http://www.gfi.com/eventsmanager>.
- [39]. **GFI Email Security®** - [Online] // GFI. - 2012. - Feb 25, 2013. - <http://www.gfi.com/exchange-server-antispam-antivirus>
- [40]. **Multi-Layer Security Revisited** [Online] / auth. Gianna David. - NetSPI, Aug 23, 2010. - March 10, 2013. - <http://www.netspi.com/blog/2010/08/23/multi-layer-security-revisited/>

APPENDICES

APPENDIX A: MOU

SAMPLE MOU

Organization Name/Title

City, Province, and Zip Code

MEMORANDUM of UNDERSTANDING

BETWEEN

THE ORGANIZATION AND SERVICE PROVIDER

SUBJECT: Sample and Details of a Memorandum of Understanding

1. **Purpose.** This heading defines, in as short paragraph with few words, the purpose of the memorandum of understanding and outlines the requisites of the agreement.
2. **Reference.** This heading will list the references that are directly related to the MOU of stakeholder.
3. **Problem.** This is core of whole MOU. It should be clear and concise statement of the problem may include a brief background history.
4. **Scope.** Add a concise statement specifying the area of the MOU.
5. **Use of Technology:** What type of technology and how to deploy among the participants?. How will bear the cost and who will manage it.
6. **Monitoring.** How the monitoring will be done and what will be included in monitoring? Who all are eligible to view and analyses the logs generated?
7. **Cost Effects:** the cost of equipment and resources in terms of local currency and head of payment be specified.

8. **Documentation Required:** support and resource needs, mutual understandings and, agreements. List all necessary understandings, agreements and supportive documents of the parties or agencies involved in the MOU.

9. **Responsibilities:** responsibilities of all the stakeholders and resources to be provided be included in this portion

10. **Time – Duration:** Specify the time and duration of contract. Start and end date must be specified taking in account of fiscal year start and end dates.

11. **Effective date.** Enter the date the MOU will become effective.

SIGNATURE BLOCK
XXXXXXXX, XXXX
XXXXXXXX, XXXXXX

SIGNATURE BLOCK
XXXXXXXX, XXXX
XXXXXXXX, XXXXXX

(Date)

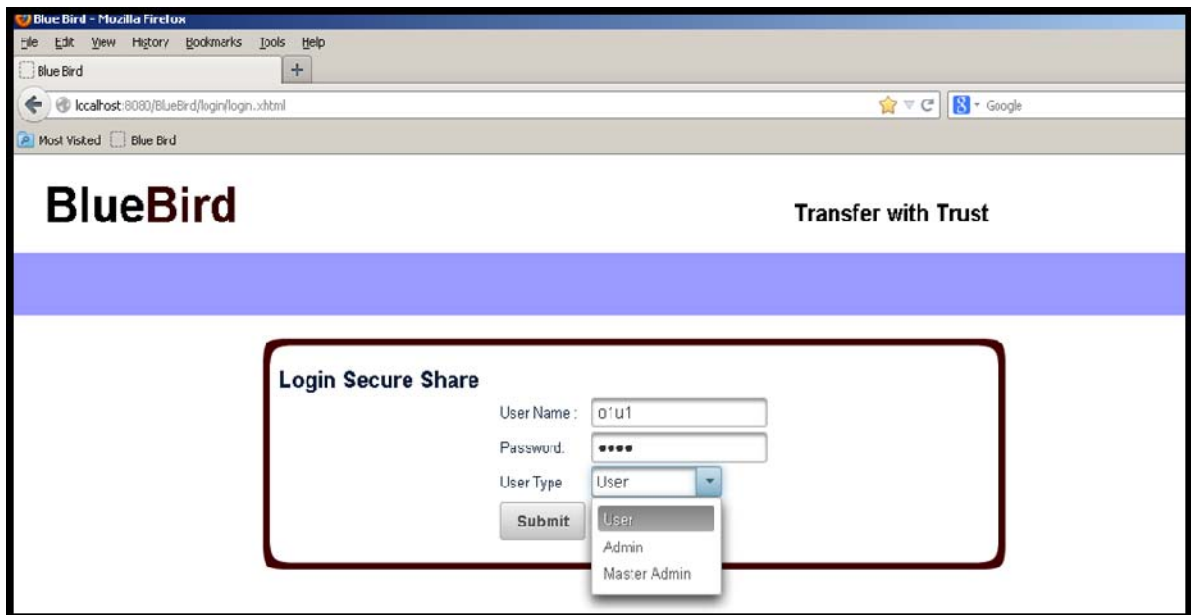
(Date)

APPENDIX B

SECURE TRANSFER APPLICATION

Screenshots of Secure Transfer application are displayed below.

1. Logon Screen is given below and logon options are show with dropdown menu.



2. Master Admin can add the organization to the application.

BlueBird Transfer with Trust
Logon as : MasterAdmin

Home Application Details About Us Contact Us


NAVIGATION

- List Organization
- Add Organization
- Modify Organization
- List All Users
- Reset Admin Password
- Reset Password
- View own Activity Log

Logout

Add New Organizations

Org Name :	<input type="text" value="Red Works"/>
Discription:	<input type="text" value="Parts Provicers"/>
Location:	<input type="text" value="Islamabad"/>
Code:	<input type="text" value="45"/>
City Code:	<input type="text" value="46"/>
Org Status:	<input checked="" type="radio"/> Active <input type="radio"/> Inactive
<input type="button" value="Submit"/>	



CEME NUST

3. List of all the organization in the application.

BlueBird Transfer with Trust
Logon as : MasterAdmin

Home Application Details About Us Contact Us


NAVIGATION

- List Organization
- Add Organization
- Modify Organization
- List All Users
- Reset Admin Password
- Reset Password
- View own Activity Log

Logout

Registered Organizations

-ID	Org Name	Discription	Location	Status	Admin User
11	O1	C1-org	O1-Loc	Active	O1Admin
12	O2	C2-org	O2-Loc	Active	O2Admin
13	O3	C3-org	O3-Loc	Active	O3Admin
14	O4	C4-org	O4-Loc	Active	O4Admin



CEME NUST

4. List of all users from all the organizations

BlueBird Transfer with Trust
Logon as : MasterAdmin

Home Application Details About Us Contact Us


NAVIGATION

- List Organization
- Add Organization
- Modify Organization
- List All Users
- Reset Admin Password
- Reset Password
- View own Activity Log

Logout

User List

ID	First Name	Last Name	User Name	Status	Organization	Sec Classification
15	Org1	Admin	O1Admin	Active	O1	no class
16	Org2	Admin	O2Admin	Active	O2	no class
17	Org3	Admin	O3Admin	Active	O3	no class
18	O1u1	O1u1	o1u1	Active	O1	Top Secret
19	O1u2	O1u2	o1u2	Active	O1	Secret
20	O1u3	O1u3	o1u3	Active	O1	Confidential
21	O2u1	O2u1	o2u1	Active	O2	Top Secret
22	O2u2	O2u2	o2u2	Active	O2	Secret
23	O2u3	O2u3	o2u3	Active	O2	Confidential
24	O3u1	O3u1	o3u1	Active	O3	Top Secret
25	O3u2	O3u2	o3u2	Active	O3	Secret
26	O3u3	O3u3	o3u3	Active	O3	Confidential
27	Org4	Admin	O4Admin	Active	O4	no class
28	O4u1	O4u1	o4u1	Active	O4	Top Secret
29	O4u2	O4u2	o4u2	Active	O4	Secret
30	O4u3	O4u3	o4u3	Active	O4	Confidential



5. Master Admin can view the log of complete application

BlueBird Transfer with Trust
Logon as : MasterAdmin

Home Application Details About Us Contact Us


NAVIGATION

- List Organization
- Add Organization
- Modify Organization
- List All Users
- Reset Admin Password
- Reset Password
- View Activity Log

Logout

Activity Log

ID	Action	Date Time
1	A Draft Document Entry is deleted by o1u1	Feb 21, 2013 2:43:02 PM
2	A Draft Document Entry is added by o1u1	Feb 21, 2013 2:56:27 PM
3	A Draft Document Entry is deleted by o1u1	Feb 22, 2013 9:56:59 PM
4	A Draft Document Entry is deleted by o1u1	Feb 22, 2013 10:04:03 PM
5	A Draft Document Entry is deleted by o1u1	Feb 22, 2013 10:06:55 PM
6	A Draft Document Entry is added by o1u1	Feb 22, 2013 10:23:18 PM
7	A Draft Document Entry is deleted by o1u1	Feb 22, 2013 10:36:25 PM
8	A Document Mark Entry is made by o1u1 and Document is marked to nullDocument Name is LAN design low cost.pdf	Feb 22, 2013 10:36:38 PM



6. Organization Admin can view all users of his organization only

ID	First Name	Last Name	User Name	Status	Organization	Sec Clearance
18	O1u1	O1u1	o1u1	Active	O1	Top Secret
19	O1u2	O1u2	o1u2	Active	O1	Secret
20	O1u3	O1u3	o1u3	Active	O1	Confidential

7. Organization Admin can add organization user only.

First Name :	Shahid
Middle Name:	
Last Name:	Iqbal
User Name:	O1user4
Password:	*****
Telephone:	92513476525
Security Classification	Top Secret
Status:	<input checked="" type="radio"/> Active <input type="radio"/> Inactive
<input type="button" value="Submit"/>	

8. User inbox view

BlueBird Transfer with Trust
Logon as: o1u1

Home Application Details About Us Contact Us


NAVIGATION

- Inbox Document
- Outbox Document
- Share Document
- Reset Own Password
- View Activity Log

Logout

Shared Documents for(Inbox): o1u1

ID	Name	Size	Send By	Classification	Subject	Download	Delete
45	btFile2.txt	378	c1u1	Confidential	Test2	Press	Delete
44	LAN design low ccst.pdf	764499	c1u1	Confidential	LAN_Design	Press	Delete



CEME NUST

9. User outbox view

BlueBird Transfer with Trust
Logon as: o1u1

Home Application Details About Us Contact Us


NAVIGATION

- Inbox Document
- Outbox Document
- Share Document
- Reset Own Password
- View Activity Log

Logout

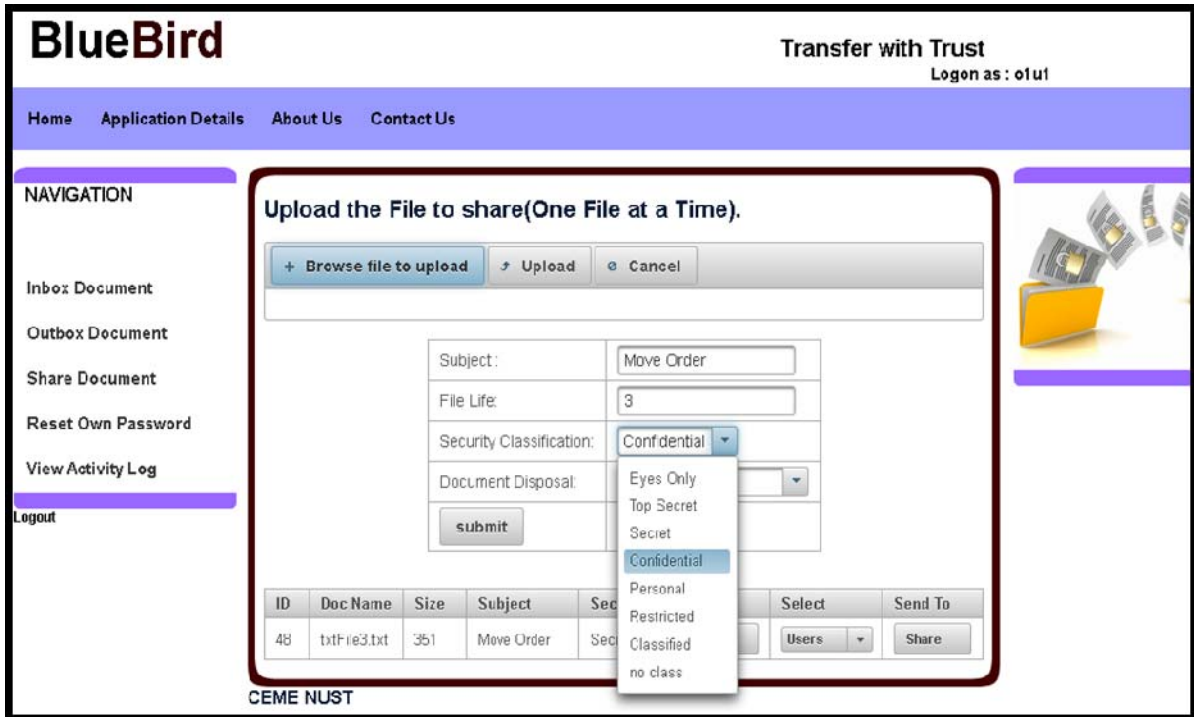
Document Shared by(Outbox): o1u1

ID	Doc Name	Size	Send To	Classification	subject	Delete
45	btFile2.txt	378	o1u1	Confidential	Test2	Delete
44	LAN design low cost.pdf	764499	o1u1	Confidential	LAN_Design	Delete
45	btFile2.txt	378	o1u2	Confidential	Test2	Delete
44	LAN design low cost.pdf	764499	o1u2	Confidential	LAN_Design	Delete
47	Image2.bmp	363030	o1u2	Secret	Work Area	Delete
47	Image2.bmp	363030	o2u1	Secret	Work Area	Delete

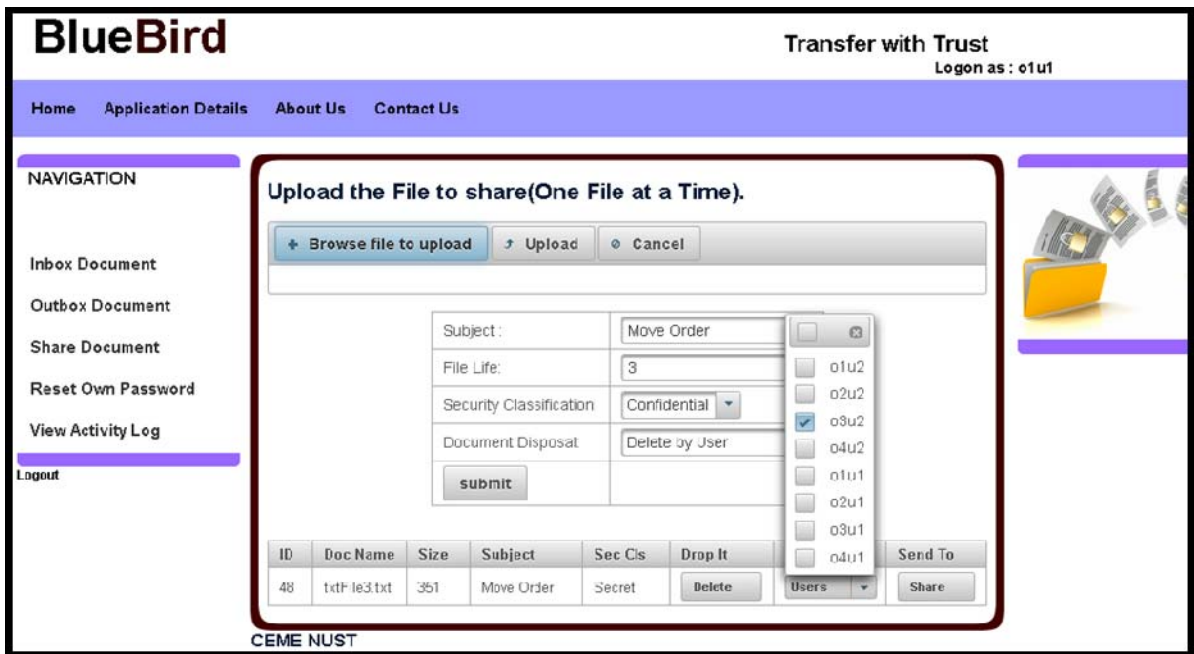


CEME NUST

10. User can upload and share a file as follow:



11. Mark the users to be shared



12. User can view his own log

NAVIGATION

[Inbox Document](#)

[Outbox Document](#)

[Share Document](#)

[Reset Own Password](#)

[View Activity Log](#)

[Logout](#)

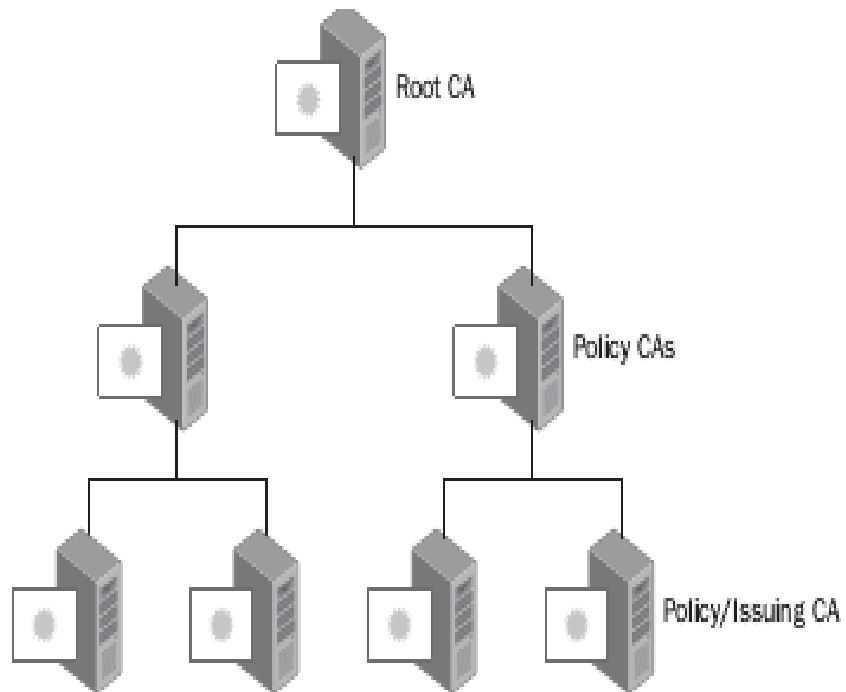
Activity Log Report: o1u1

-ID	Doc Name	Action	Date Time
1	10 Excel Tricks.pdf	A Draft Document Entry is deleted by o1u1	Feb 21, 2013 2:43:02 PM
2	Image1.bmp	A Draft Document Entry is added by o1u1	Feb 21, 2013 2:56:27 PM
3	btFile1.bt	A Draft Document Entry is deleted by o1u1	Feb 22, 2013 9:56:59 PM
4	btFile1.bt	A Draft Document Entry is deleted by o1u1	Feb 22, 2013 10:04:03 PM
5	Image1.bmp	A Draft Document Entry is deleted by o1u1	Feb 22, 2013 10:08:55 PM
6	LAN design low cost.pdf	A Draft Document Entry is added by o1u1	Feb 22, 2013 10:23:18 PM
7	stages_ &_ steps.pdf	A Draft Document Entry is deleted by o1u1	Feb 22, 2013 10:30:25 PM
8	LAN design low cost.pdf	A Document Mark Entry is made by o1u1 and Document is marked to nullDocument Name is LAN design low cost.pdf	Feb 22, 2013 10:38:38 PM
9	LAN design low cost.pdf	A Document Mark Entry is made by o1u1 and Document is marked to nullDocument Name is LAN design low cost.pdf	Feb 22, 2013 10:38:38 PM



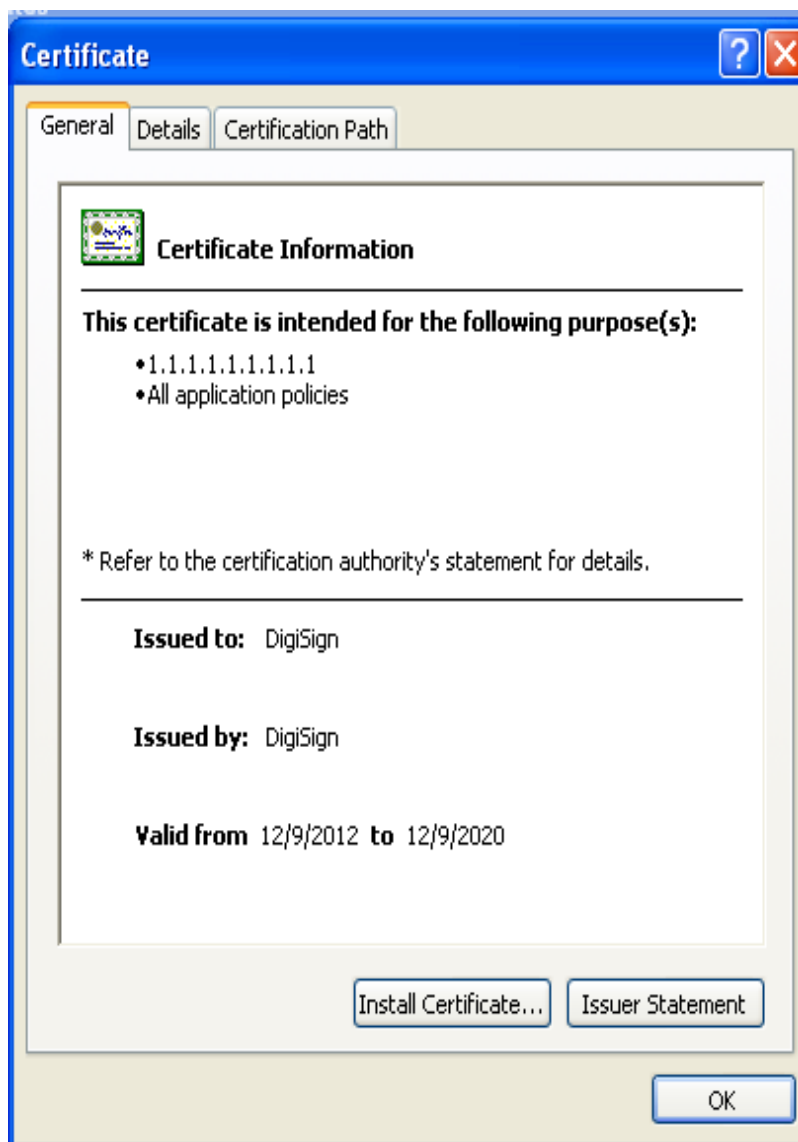
PKI SYSTEM DEPLOYMENT AND USAGE

1. Following PKI system is deployed as follow
 - a. Microsoft Server
 - b. Root Certification Authority
 - c. Sub Root Certification Authority
 - d. Issue Certification Authority



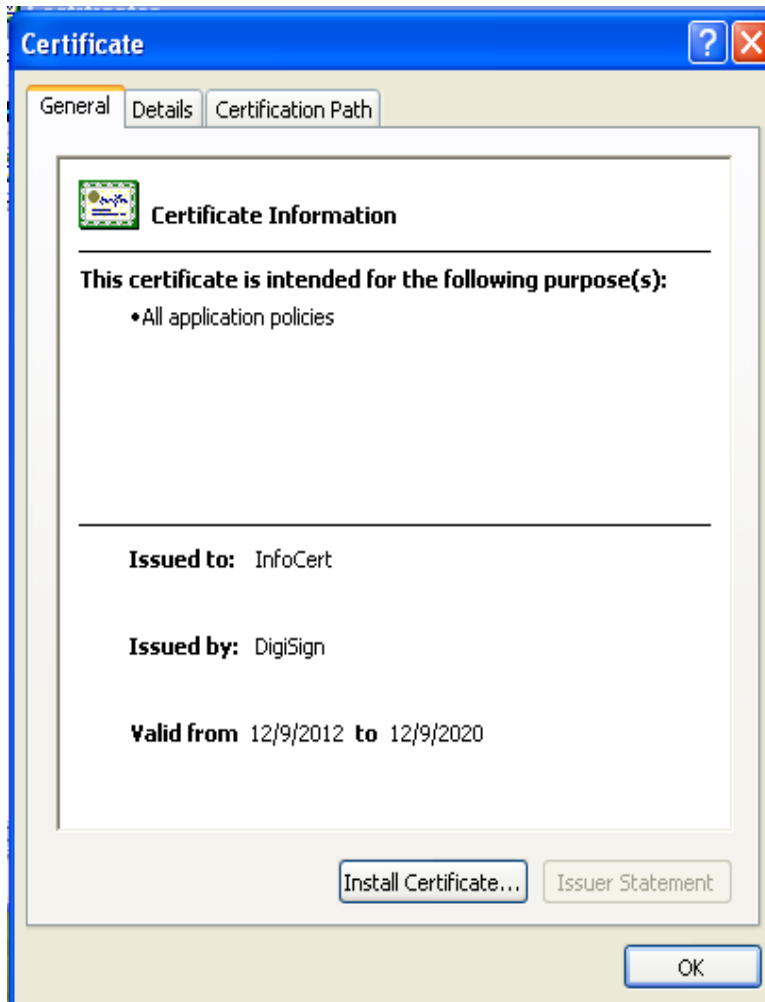
2. Certificate of Root CA is self signed and issues by same CA.

- a. Issued by root CA
- b. Signed by Root CA
- c. Validity - Maximum
- d. Key Length -- 8192

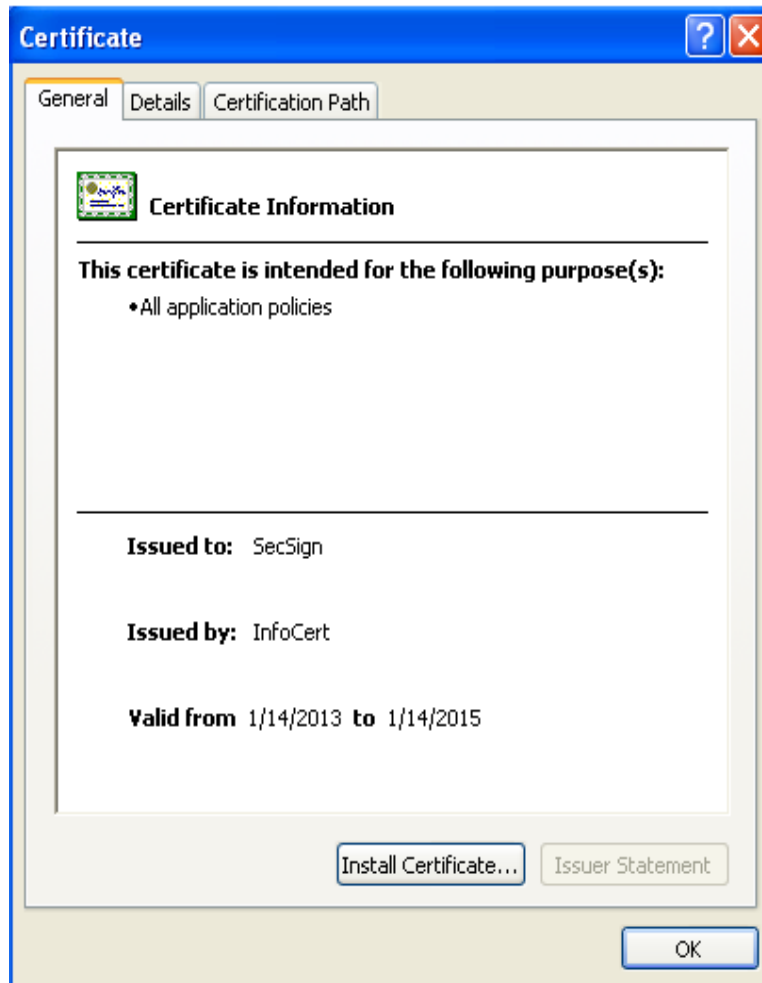


3. Sub root CA certificate

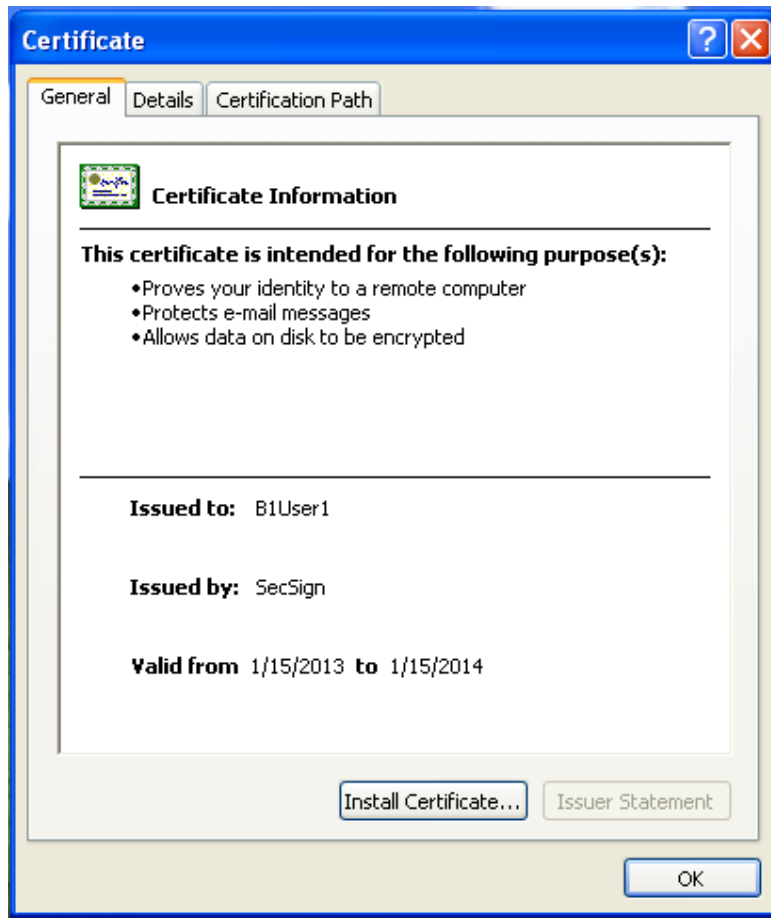
- a. Issued by root CA
- b. Signed by Root CA
- c. Validity Time equal to Root CA
- d. Key Length – 4096



- 4. Issue certification Authority Certificate
 - a. Issued by sub root CA
 - b. Signed by sub root CA
 - c. Validity Time less than sub root CA
 - d. Key Length – 2048

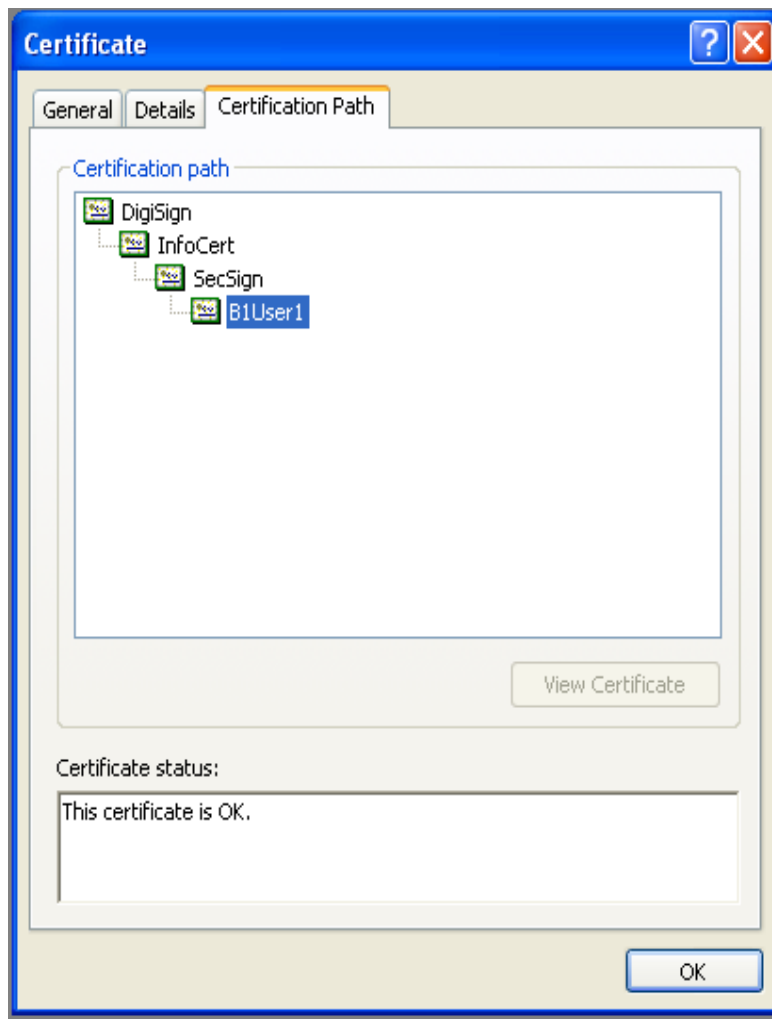


5. User certificate
 - a. Issued by issue root CA
 - b. Signed by issue root CA
 - c. Validity Time less than issue CA
 - d. Key Length – 1024



6. Certificates Path

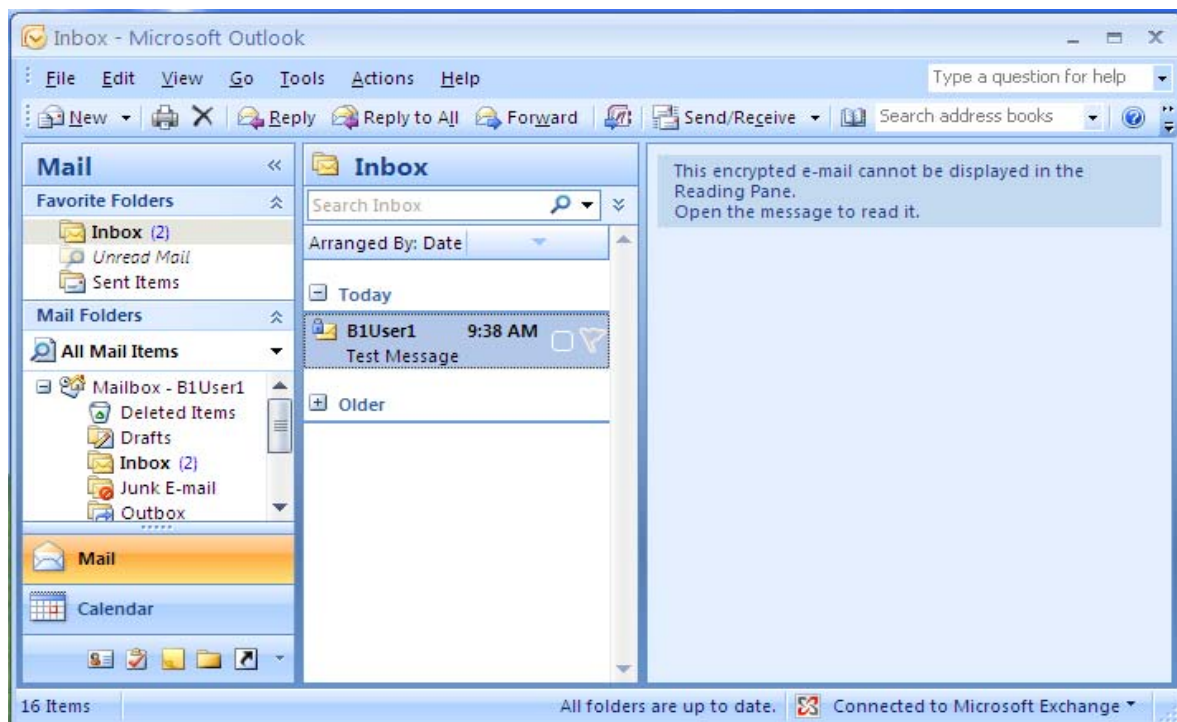
- a. Allow to manage trust of all the certification authorities in the hierarchy
- b. Allow to manage and validate CRL
- c. Policy management of revocation and certificate is controlled by certificate path



7. Digitally Signing email using user certificate
 - a. Outlook is used to signed email with digital certificate.
 - b. Certificate is installed on the computer
 - c. Certificate is validated with the help of on line CRL
 - d. Enable button of Digital Sign and Encrypt button



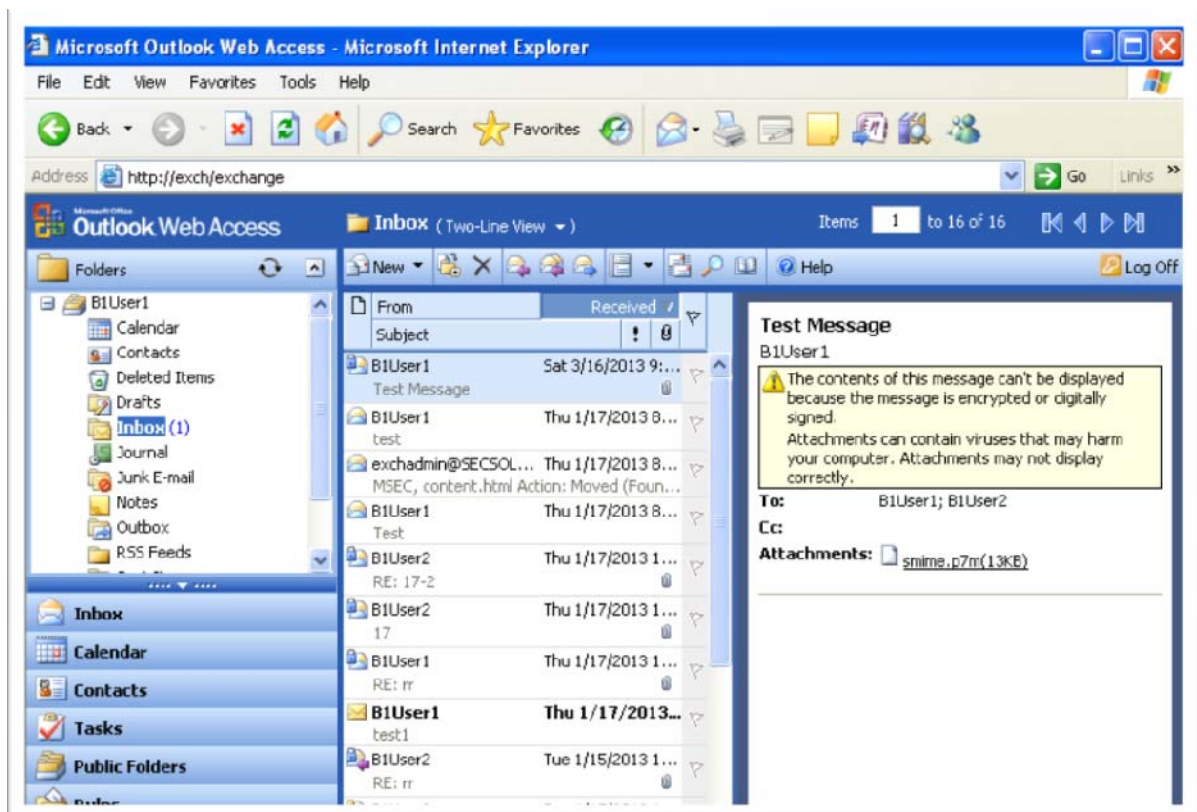
8. Received email at outlook, encrypted email does not open in normal reading pane



9. Properly received digitally signed and encrypted email.



10. Digitally signed and encrypted message without certificate



APPENDIX D

DEFINITIONS

- **Access control**

An access control limits the use of a resource. Only those people, programs or devices that are specifically permitted to use the resource will have access. In addition, an access control will usually limit use to specific types of access; someone can read a file but not change it,

- **Auditing**

Auditing is the information gathering and analysis of assets to ensure such things as policy compliance and security from vulnerabilities

- **Authentication**

Authentication is a process where a person or a computer program proves their identity in order to access information. The person's identity is a simple assertion, the login ID for a particular computer application, for example. Proof is the most important part of the concept and that proof is generally something known, like a password; something possessed, like your ATM card; or something unique about your appearance or person, like a fingerprint.

- **Authorization**

Authorization is the act of granting a person or other entity permission to use resources in a secured environment. This is usually tightly linked to authentication. A person or other identity first authenticates and then is given pre-determined access rights. They now have the authority to take specific actions.

- **Certification authority (CA)**

A certification authority, or CA, holds a trusted position because the certificate that it issues binds the identity of a person or business to the public and private keys (asymmetric cryptography) that are used to secure most internet transactions.

- **Certificate Revocation List (CRL)**

A Certificate Revocation List (CRL) is a signed data structure that contains information about revoked certificates.

A certificate is the signed digital assertion by a Certification Authority (CA) that allows a trust relationship between a client and a server. Although a certificate has a limited lifetime, there are certain events that may make it invalid before it expires. For example, if information contained in the certificate about the domain or its owner changes; the certificate can no longer be trusted and should be revoked. Another event that requires the certificate to be revoked is when the private key, which is linked to the public key in the certificate, is compromised.

- **Confidentiality**

Confidentiality is the need to ensure that information is disclosed only to those who are authorized to view it.

- **Demilitarized Zone (DMZ)**

In computer security, in general a demilitarized zone (DMZ) or perimeter network is a network area (a subnetwork) that sits between an organization's internal network and an external network, usually the Internet. DMZ's help to enable the layered security model in that they provide subnetwork segmentation based on security requirements or policy. DMZ's provide either a transit mechanism from a secure source to an insecure destination or from an insecure source to a more secure destination. In some cases, a screened subnet which is used for servers accessible from the outside is referred to as a DMZ.

- **Digital certificate**

In general use, a certificate is a document issued by some authority to attest to a truth or to offer certain evidence. A digital certificate is commonly used to offer evidence in electronic form about the holder of the certificate. In PKI it comes from a trusted third party, called a certification authority (CA) and it bears the digital signature of that authority.

- **Domain Name System (DNS)**

The domain name system (DNS) is the way that Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.

- **Firewall**

A logical or physical discontinuity in a network to prevent unauthorized access to data or resources.

- **Hash Function**

An algorithm that computes a value based on a data object thereby mapping the data object to a smaller data object.

- **IPSec**

IPSec, which is short for "IP Security" is the name of a security architecture and set of protocols commonly used to construct a VPN. These services work at the IP (Internet Protocol) or network layer and provide confidentiality and authentication as the packets move through networked devices.

- **Least Privilege**

Least Privilege is the principle of allowing users or applications the least amount of permissions necessary to perform their intended function.

- **Mandatory Access Control (MAC)**

Mandatory Access Control controls is where the system controls access to resources based on classification levels assigned to both the objects and the users. These controls cannot be changed by anyone.

- **Non-Repudiation**

Non-repudiation is the ability for a system to prove that a specific user and only that specific user sent a message and that it hasn't been modified.

- **PKI**

Public-Key Infrastructure (PKI) is the infrastructure needed to support asymmetric cryptography. At a minimum, this includes the structure and services needed to do the following:

- Register and verify identities,
- Build and store credentials,
- Certify the credentials (issue digital certificates),
- Disseminate the public key, and
- Secure the private key and yet make it available for use.

The infrastructure will also need to have the structure and services to renew keys, recover keys, and to notify others when a key is revoked.

A set of highly trusted certification authorities must be able to certify other CAs, this includes being able to make and assert decisions based on use and policy.

- **RBAC (Role Based Access Control)**

Role Based Access Control (RBAC) is the establishment of access rights based on a user's role in the organization. When an organization looks at the job of provisioning thousands of users and thousands of network devices for hundreds of applications, it can be daunting. One of the ways to simplify this task is to implement access controls for a limited number of roles instead of for each individual.

- **SSL-VPN**

Although the Secure Sockets Layer (SSL) is a protocol designed specifically for web browsers to securely access web-based applications, the fact that it encrypts information and that it authenticates at least one of the parties, also makes it a Virtual Private Network (VPN). One of the best things about this protocol is that most computers have a browser; that means that no new software needs to be added to the client in order to use this method.

- **VPN**

Virtual Private Networks (VPNs) allow private use of a public network. They enable mobile computers and other devices to connect to a company's private network by creating an encrypted tunnel from the network that's owned by the company, over the Internet and to the remote device on the other end. The most commonly used technologies to do this are Secure Sockets Layer (SSL) and IP Security (IPSec). These effectively extend the company's network, creating a Virtual Private Network.

Reference: The definitions and explanation is taken from ***RSA Security – Information Security Glossary***. URL: - <http://www.rsa.com/glossary/> and from **SANS - Glossary of Security Terms** . URL <http://www.sans.org/security-resources/glossary-of-terms/>