UNIVERSITY OF NAIROBI

SCHOOL OF COMPUTING AND INFORMATICS

A Public Key Infrastructure (PKI) for the Higher Education Institutions in Kenya

BY

PETER MAINGI MUIA

P58/75541/2012

Supervisor

Prof. W. Okello-Odongo

November 2014

Submitted in Partial Fulfilment of the Requirements of the Degree of Master of Science in Computer Science

DECLARATION

The project, as presented in this project is my original work and has not been presented for any other university award.

Student Signature **Peter Maingi Muia** **P58/75541/2012**
Date……

This project has been submitted as partial fulfilment of requirements for Masters of Science in Computer Science of the University of Nairobi with my approval as the University supervisor.

Supervisor Signature **Prof. W. Okello-Odongo**
Date……

Abstract

Public-key cryptography is fast becoming the foundation for online commerce and other applications that require security and authentication in an open network. The widespread use of public-key cryptography requires a public-key infrastructure to publish and manage public-key values. Without a functioning infrastructure, public-key cryptography is not any more useful than traditional, secret-key cryptography.

This report presents a project that was done to develop a public key infrastructure for the university community in Kenya. Firstly, a survey was conducted on the Kenyan universities to determine whether or not they needed a public key infrastructure. The results of the study showed that universities are experiencing cyber threats and PKI can be used to reduce the threats. This provided a justification for the development of the public key infrastructure and the entire development process is described in the report. With the system developed, users have a web based interface where they can request for and get digital certificates within the university environment.

The project also highlights how PKI can be used in the university environment to secure systems and electronic communication. It also highlights on the basic usage of the developed system. The project proposes the adoption of the developed system as the rootCA for the university community in Kenya with each university running its own CA based on the developed architecture.

Acknowledgments

I would like to that the Almighty God for giving me the strength and wisdom to undertake this project.

I also thank my loving family Salome and Joe, my mother Winfred, my sister Mumo, my brothers Paul and Kalulu for giving me the moral support during the entire period I was working on the project.

It was a long journey and I would not have made it were it not for the support I received from my employer, Kenya Education Network by giving me time and all the support that I needed to work on the project.

Fourthly, I would like to thank the University of Nairobi and especially my supervisor Prof. Okello Odongo for their guidance throughout the project life cycle. To all my classmates, you were very cooperative and offered great assistance when things were tough.

Thank you.

I dedicate this project to my father, the late Mr. John Muia – may his soul rest in eternal peace.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

Definitions

Cyber Security - This is information security as applied to computers and computer networks. The field covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction. Computer security also includes protection from unplanned events and natural disasters.

Cyber Attacks – This is any type of offensive manoeuvre employed by individuals or whole organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system

Cryptography - Cryptography is an art, as well as a science, that involves the process of transforming plaintext into scrambled text and vice-versa.

Symmetric key Cryptography - An encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message.

Public Key Cryptography - A cryptographic algorithm which requires two separate keys, one of which is secret and one of which is public. Although different, the two parts of this key pair are mathematically linked. The public key is used to encrypt plaintext or to verify a digital signature; whereas the private key is used to decrypt ciphertext or to create a digital signature.

Digital Signatures - A digital signature is an attachment to an electronic message that includes a mathematical digest of the message created using public key cryptography hence it is specific to both the signer of the message and the message itself

Digital Certificates - A digital certificate is an electronic identity issued to a person, system, or an organization by a competent authority after verifying the credentials of the entity. A digital certificate is a public key that is unique for each entity. A certification authority issues digital certificates.

Acronyms

PKI – Public Key Infrastructure

CA – Certificate Authority

TCP/IP – Transmission Control Protocol/ Internet Protocol

IP – Internet Protocol

DES – Data Encryption Standard

RSA - Ron Rivest, Adi Shamir and Leonard Adleman

RA – Registration Authority

ICT – Information Communication & Technology

CCK – Communications Commission of Kenya

LDAP - Lightweight Directory Access Protocol

CHAPTER 1: INTRODUCTION

1.0 Background

The Internet has led to an increase in online communication which has in turn led to issues of computer and network security. Where previously isolated small networks did not have connections to the outside world, today every small network is connected to the Internet. So it is possible that from all parts of the world unknown persons, whether with good or bad faith, can connect to any network. This is because packet-oriented protocol suite TCP / IP was designed specifically to allow an end-to-end connection for all stations on a network. However, this prevailing decentralized structure of the Internet allows little control over the way to take the data packets from one end to the other.

Before the invention of computers, secret messages had to be transmitted by using a key or method known only to those who were meant to share in the contents of those messages. In such systems, there were always difficulties in distributing these keys or systems so that they did not fall into the wrong hands. The need to protect information in transit is justified today by the overwhelming means of communication available today and by the continuously increasing amount of critical data that is no longer processed on paper.

The higher education community in Kenya is finding more ways to provide better services and cutting costs by use of electronic delivery of data. As students, universities, service providers and the government transitions from the traditional paper to electronic data exchange over the Internet, security has become a major challenge to all the stakeholders including the data senders, receivers and the general public. Mechanisms must therefore be put in place to provide security assurance for online data transactions and exchanges. Encryption and digital signatures achieved by the use of public key infrastructure can satisfy these required security attributes.

Asked about whether they felt that PKI could help those better secure university systems, 90% of university ICT directors interviewed strongly agreed, 10% moderately agreed while none disagreed. On the other hand, when asked whether there existed a PKI infrastructure for managing certificates within the university, 10% agreed while the majority, 90%, disagreed. This shows that although the universities appreciate the role that PKI would play in securing systems and electronic communication within the universities, they do not have any PKI implemented for the Kenya University Community.

Table 1 : A table showing response of ICT directors when asked if they felt digital certificates can be used to secure university systems and electronic data communication

I feel digital certificated can be used to secure university systems and electronic data communication	**Frequency**
Strongly Agree	90 %
Moderately Agree	10%
Agree	0 %
Moderately Disagree	0 %
Strongly Agree	0 %

Table 2: A table showing the response of ICT directors when asked about the existence of a platform for managing digital certificates within the University Community

There is no system in the university where students can register to request for digital certificates	**Frequency**
Strongly Agree	50 %
Moderately Agree	10%
Agree	30 %
Moderately Disagree	10 %
Strongly Agree	0 %

1.2 Problem Statement

With the increase in the penetration of the Internet after the landing of the fiber optic cables in Kenya, there has been an increase in the usage of online services within the university community in Kenya (Meoli & Waema, 2014). Universities in Kenya are currently consuming about 3Gbps of International bandwidth up from around 100Mbs in 2008. Consequently, this has led to an increase in cyber threats in the higher education sector as well (SERIANU, 2012). Some of the services that are online include email, student management systems, the university websites, and eLearning systems among many others. These services run on public servers on the background that need to be secured and communication is over an open network and through the Internet. Most of these systems carry very critical data for the university that needs to be secured and any interrogation to the systems also need to be secured.

There are many potential opportunities for unauthorized access to information on a university network. A person can attempt to monitor or alter information streams such as file transfers, electronic commerce transactions, and e-mail. The University may work with partners on projects of limited scope and duration, with unknown employees, but who, nonetheless, must be given access to some of the information resources. Additionally if users have a multitude of passwords to remember for accessing different secure systems, they may choose weak or common passwords to more easily remember them. This not only provides an intruder with a password that is easy to crack, but also one that will provide access to multiple secure systems and stored data. The most commonly used mode of authentication, passwords, is prone to dictionary attacks, login spoofing, replay attacks and man in the middle attacks. Additionally hosted sites can be prone to phishing attacks.

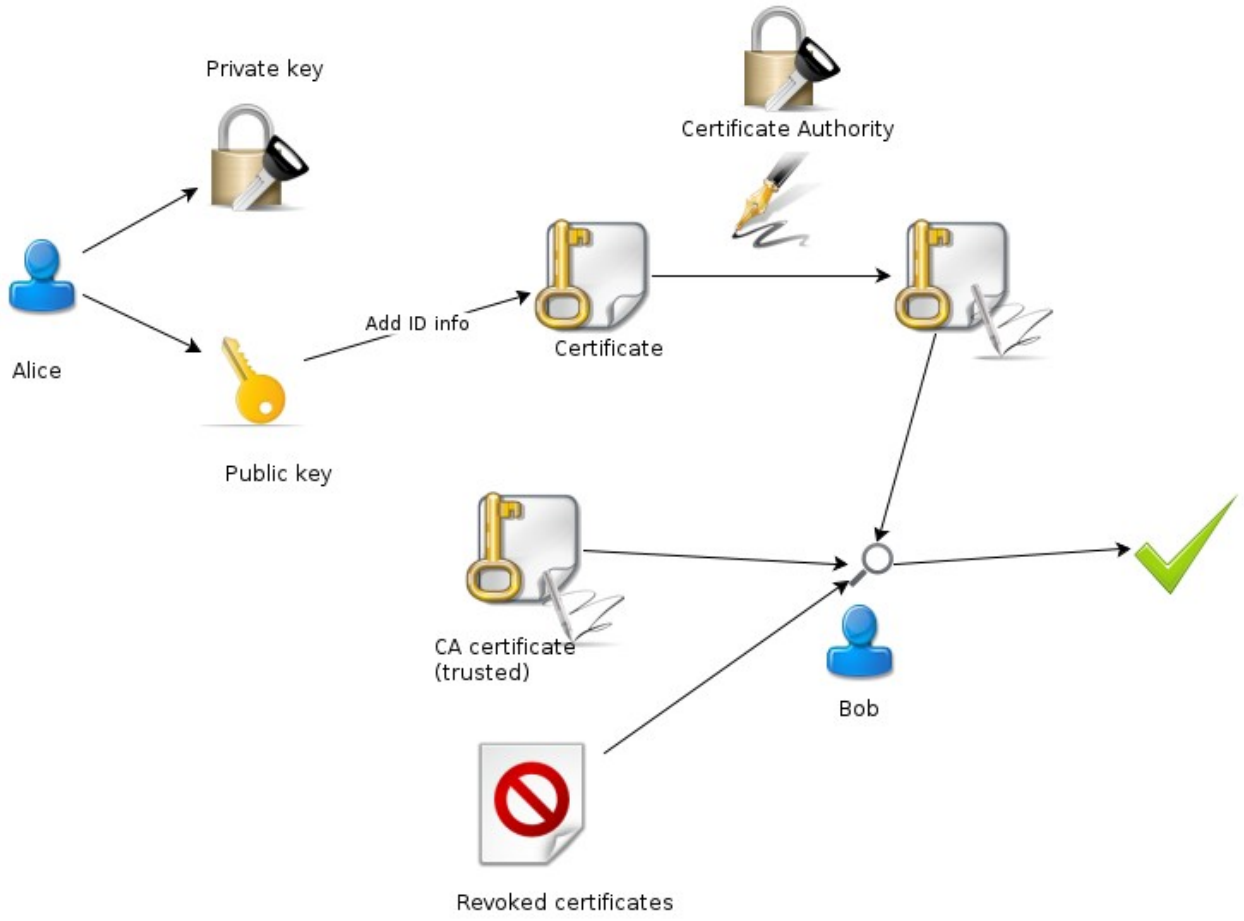
Traditional cryptography has usually involved the creation and sharing of a secret key for the encryption and decryption of messages. This secret or private key system has the significant flaw that if the key is discovered or intercepted by someone else, messages can easily be decrypted. For this reason, public key cryptography and the public key infrastructure is the preferred approach. A university PKI will provide a mechanism for securely issuing and distributing keys and certificates in a university environment.

1.3 Proposed Solution

The solution that was proposed to the problem described above was the development of a web based Public Key Infrastructure for the University community in Kenya. The PKI system that has been developed includes a set of hardware, software, people and procedures needed to create, manage, store, distribute, and revoke digital certificates in a university environment in Kenya. The general user will at least have a web browser that he/she will be able to use to register at the University and to follow some basic instructions outlining how to obtain her digital certificate and to generate her private key.

The diagram below shows how certificates are created and how they work.

Figure 1: How PKI works



A certificate is comprised of the public key, together with data that identifies who the public/private key belongs to. This certificate also has signatures attached that are generated by

the private keys of other certificates. If both Alice and Bob know a public key (certificate) of a party they both trust, then Alice can send her own certificate, signed by this trusted party, to Bob. Bob then validates the signature on this certificate (using the public key he has of the trusted party). If the signature is fine, then Bob verifies if the certificate isn't in the list of revoked certificates (which is managed by the University Community Certificate Authority). If that isn't the case, then Bob knows that the certificate he got is indeed from Alice (because the trusted party says so) and of which the private key is not known to be lost or stolen (otherwise it would have been mentioned in the revocation list). The list of certificates that are trusted (the certificates of the Certificate Authority) are stored in a trust store.

A malicious person now has a more difficult task. If a wrong certificate is generated, then the trusted party will probably not sign it. As a result, Chris cannot "fake" a certificate because both Alice and Bob will check the signature of the certificate and the certificate revocation list before they agree that it is a valid certificate. The system will serve the university community in Kenya.

Registration Authority (RA)

The RA keeps logs of certificate requests and mediates the requests to the Certificate Authority (CA). Physical/human initial authentication will be devolved to multiple RAs around the Universities, or at individual universities schools or colleges.

The Certification Authority (CA)

The CA performs the role of signing certificates on the basis that the applicants have been through the appropriate registration procedures.

1.4 Project Objectives

The overall goal of the project was to develop a model that could be used by the University community in Kenya to implement public key infrastructure. The following were the major project objectives.

1. To study and understand the security implementations and mechanisms used by the higher education community in Kenya to secure their systems. This would be achieved by:-
    - Exploring and describing the experiences and perceptions of using the available security systems in place.
    - Identifying whether universities in Kenya have employed the use of Public Key Infrastructure to secure systems.
    - Identifying whether PKI technology would be acceptable in the University environment in Kenya.
2. To develop an architecture for developing a PKI system for the university community in Kenya.
3. To design and implement a PKI system for the university community in Kenya. It was assumed that universities in Kenya are similar in terms of structure and organization therefore a similar model can be adopted in any of the universities.

1.5 Project Justification

Internet usage in Kenya has grown rapidly in the last couple of years (SERIANU, 2012). There were approximately 17.38 million Internet users in Kenya as at December 2011. As the Internet usage continues to grow in the country, so does the number of security incidents reported. This has exposed Kenyan organizations to premeditated security threats with possibly disastrous effects. They become prime targets for insider attacks as well as cyber criminal acts.

The universities in Kenya have identified Infrastructure, ICT and Library Services as one of the key strategic issues. The universities see ICT infrastructure to be a contributing factor towards providing an enabling and conducive environment for them to provide quality services. All the online systems deployed by the universities are prone to cyber attacks or abuse from users or any other malicious persons.

From the study conducted on the universities, only 10 % have secured their systems using digital certificates but 100% are aware of digital certificates and the benefits that can be accrued by using them. 50% of the universities have experienced successful cyber attacks in one way or the other and they believe use of digital certificates could have helped to deter these attacks.

Although electronic mail has replaced many paper-based communications, more sensitive documents are still sent the old-fashioned way for greater security. PKI based Trusted Messaging allows sensitive documents to be sent by e-mail, eliminating the processing costs, mailing costs, and time delays associated with traditional regular mail. Additionally PKI provides a powerful security benefit by protecting access to web applications. While passwords might be easily guessed or sniffed, intercepted en route to the application, or revealed by a brute force attack, PKI-based authentication is very difficult to break.

In Kenya the Communications Commission of Kenya is developing a root CA for a Public Key Infrastructure for the country, Each sector such as the education, judiciary, banking, National Intelligence Service (NSIS) among others are supposed to build their own PKIs. The proposed project will be a model that can be used by the education sector. The proposed university PKI will be an infrastructure that uses digital certificates as an authentication mechanism and it will be built to better manage certificates and their associated keys.

1.6 Scope of the project

The project entailed conducting a research of the cyber security threats and the mechanisms employed to mitigate the threats on systems in the higher education sector in Kenya. The research highlighted the various threats that the systems deployed by the institutions face and how a PKI can be used to mitigate these risks. The research provided a justification for the design of a PKI system for the Universities.

PKI architecture suitable for a university was designed and implemented for the university community in Kenya. Finally, a PKI system that uses the proposed architecture was developed. The developed system address threats of confidentiality, integrity, access control, authentication, and most importantly, non-repudiation of the systems within the university. The system has the following components:-

- A certificate authority (CA) whose responsibility is to issue and verify digital certificates.
- A registration authority (RA) that acts as the verifier for the certificate authority before a digital certificate is issued to a requester
- One or more directories where the certificates (with their public keys) are held
- A certificate management system - the management system through which certificates are published, temporarily or permanently suspended, renewed or revoked.

The system is used to issue certificates that can perform the following tasks:-

1. Digital certificate authentication
2. Securing e-mail from unintended viewers.
3. Enabling secure connections between computers connected via the Internet.
4. Securing web servers

CHAPTER 2: LITERATURE REVIEW

2.0 Introduction

Computer security has been evolving especially in the last three decades. Researchers have put a lot of effort in developing security methodologies, models and standard definitions of security services. However, we still experience systems insecurity. The need for user authentication has become mandatory in e-government, e-commerce, and e-business applications because of the sensitivity of the information exchanged by these systems.

Rivest, Shamir, and Adleman (1978) discovered the first practical public-key encryption and signature scheme, now referred to as RSA. The RSA scheme is based on a mathematical problem, the intractability of factoring large integers. This application of a hard mathematical problem to cryptography revitalized efforts to find more efficient methods to factor. In their paper, R.L. Rivest, A. Shamir, and L. Adleman presented an encryption method with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences:

- Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only he can decipher the message, since only he knows the corresponding decryption key.
- A message can be signed using a privately held decryption key. Anyone can verify this signature using the corresponding publicly revealed encryption key. Signatures cannot be forged, and a signer cannot later deny the validity of his signature.

2.1 Cryptography Concepts

2.1.0 Cryptography

Cryptography is an art, as well as a science, that involves the process of transforming plaintext into scrambled text and vice-versa. The purpose of cryptography is to conceal the confidential information from unauthorized eyes and ensure immediate detection of any alteration made to the concealed information.

2.1.1 Symmetric Cryptography

In traditional cryptography, the sender and receiver of a message know and use the same secret key; the sender uses the secret key to encrypt the message, and the receiver uses the same secret

key to decrypt the message. This method is known as symmetric cryptography. The main challenge is getting the sender and receiver to agree on the secret key without anyone else finding out. If they are in separate physical locations, they must trust a courier, a phone system, or some other transmission medium to prevent the disclosure of the secret key. Anyone who overhears or intercepts the key in transit can later read, modify, and forge all messages encrypted or authenticated using that key. The generation, transmission and storage of keys is called key management and all cryptosystems must deal with key management issues.

Because all keys in a secret-key cryptosystem must remain secret, secret-key cryptography often has difficulty providing secure key management, especially in open systems with a large number of users. Algorithms that implement Symmetric cryptography are not secure and are prone to the man in the middle attack.

The biggest obstacle in successfully deploying a symmetric-key algorithm is the necessity for a proper exchange of private keys. This transaction must be completed in a secure manner. In the past, this would often have to be done through some type of face-to-face meeting, which proves quite impractical in many circumstances when taking distance and time into account. If one assumes that security is a risk to begin with due to the desire for a secret exchange of data in the first place, the exchange of keys becomes further complicated

2.1.2 Public Key Cryptography

In order to solve the key management problem, Whitfield Diffie and Martin Hellman introduced the concept of public-key cryptography in 1976. Public-key cryptosystems have two primary uses, encryption and digital signatures. In their system, each person gets a pair of keys, one called the public key and the other called the private key. The public key is published, while the private key is kept secret. The need for the sender and receiver to share secret information is eliminated; all communications involve only public keys, and no private key is ever transmitted or shared. In this system, it is no longer necessary to trust the security of some means of communications. The only requirement is that public keys be associated with their users in a trusted manner. Anyone can send a confidential message by just using public information, but the message can only be decrypted with a private key, which is in the sole possession of the intended recipient. Furthermore, public-key cryptography can be used not only for privacy, but also for authentication and other various techniques.

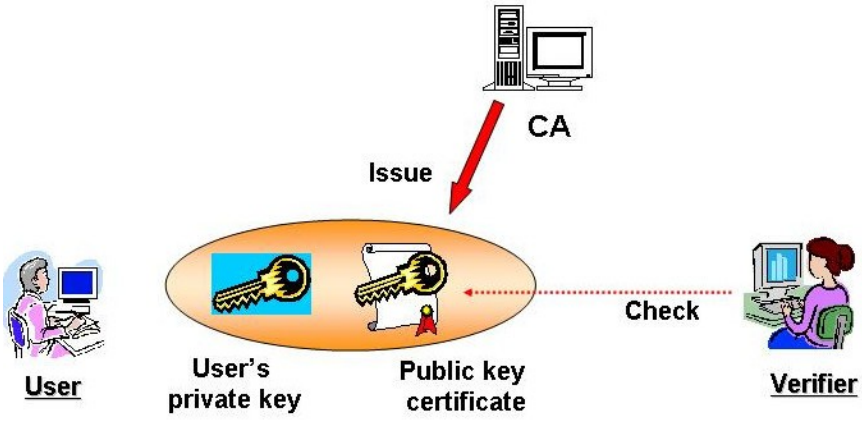
In a public-key cryptosystem, the private key is always linked mathematically to the public key.

Therefore, it is always possible to attack a public-key system by deriving the private key from the public key. Typically, the defence against this is to make the problem of deriving the private key from the public key as difficult as possible. For instance, some public-key cryptosystems are designed such that deriving the private key from the public key requires the attacker to factor a large number; in this case it is computationally infeasible to perform the derivation. This is the idea behind the RSA public-key cryptosystem.

2.1.3 Public Key Infrastructure

A public-key infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. It is therefore an arrangement that binds public keys with respective user identities by means of a certificate authority (CA)

Figure 1: Public Key Infrastructure



2.1.4 Digital Signatures

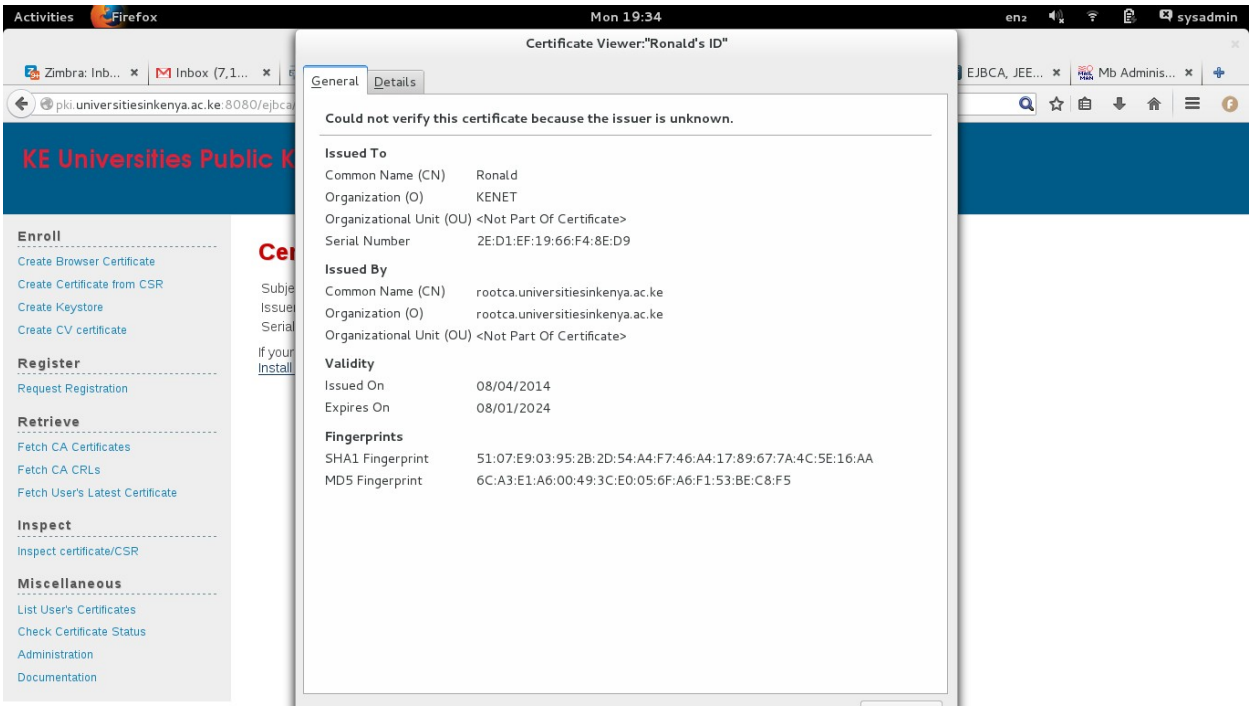
A digital signature is an attachment to an electronic message that includes a mathematical digest of the message created using public key cryptography hence it is specific to both the signer of the message and the message itself. A digital signature can therefore be used as an affirmative identity of both the message sender and the message itself. To sign a message, Alice does a computation involving both her private key and the message itself. The output is called a digital signature and is attached to the message. To verify the signature, Bob does a computation involving the message, the purported signature, and Alice's public key. If the result is correct according to a simple, prescribed mathematical relation, the signature is verified to be genuine;

otherwise, the signature is fraudulent, or the message may have been altered.

2.2.6 Digital Certificates

A digital certificate is an electronic "passport" that allows a person, computer or organization to exchange information securely over the Internet using the public key infrastructure. A digital certificate provides identifying information and it is forgery resistant and can be verified because it was issued by an official, trusted agency. The certificate contains the name of the certificate holder, a serial number, expiration dates, a copy of the certificate holder's public key and the digital signature of the certificate-issuing authority (CA) so that a recipient can verify that the certificate is real. To provide evidence that a certificate is genuine and valid, it is digitally signed by a root certificate belonging to a trusted certificate authority. Operating systems and browsers maintain lists of trusted CA root certificates so they can easily verify certificates that the CAs have issued and signed. When PKI is deployed internally, digital certificates can be self-signed. The diagram below shows a pictorial representation of a certificate obtained from the developed system.

Figure 2: Digital Certificate



2.2 Review of Key Concepts

2.2.1 Evolution of cryptography

Zulkifli (2007) in his paper titled ‘Evolution of cryptography’ describes how cryptography has evolved over time. The paper describes the various fundamentals of cryptography where cryptography is described as the science of secret writing aimed at protecting data so that only the intended recipient may decrypt and read the message. Cryptography is composed of both encryption and decryption. Encryption and decryption keys are the same for Symmetric crypto-system and different for asymmetric crypto-system.

Crypto-analysis is described in the paper as the study of defeating cryptography in the absence of the key(s). The paper also introduces the Shannon’s Theory of Confusion and Diffusion which was published by Claude E. Shannon in 1949 in a paper titled Communication Theory of Secrecy System. Confusion is used to hide the relationship between plaintext and ciphertext while Diffusion aims to spread the statistics over the message to avoid exploits by crypto-analists. Kerchoff’s principle is also introduced in the paper. In 1883, Auguste Kerchoff Von Nieuwenhof stated in the book La Cryptographie Militaire that security of a crypto-system must be totally dependent on the secrecy of the key and not the secrecy of the algorithm.

Three periods of cryptography are presented namely the ancient (until 1918), technical (1919-1975) and finally the paradoxical period (from 1976). In the ancient period, cryptography has been documented to have been used by the Sumeians, the Egyptians and Hebrew scholars some which date as back as 600BC. Some of the technologies employed during this period include the mono-alphabetic substitution cipher and the polyalphabetic substitution cipher.

During the technical period mechanical machines were used to perform encryption. One such machine is the Enigma machine which was used by the German military during the World War II. Codebooks for the machine were published and distributed regularly and the codebooks had to be kept secret by the military. Another technology which emerged during this period and which is described in the paper is the Data encryption Standard (DES). This was prompted by the invention of the computer and digital devices which meant that more operations were being handled electronically. As a result, DES was developed in 1976 and proved to be strong for 20 years.

The final phase described in the paper is the paradoxical period where public key cryptography came into being. For many years, key distribution has been the biggest headache for

cryptography. In 1976, Whitfield Diffie and Martin Hellman in the paper titled ‘ New Direction in Cryptography’ showed a method that allowed two parties to agree on a shared secret key without transmitting the secret key without transmitting the secret key to each other.
The Deffie-Hellman key exchange protocol inspired Rivest, Shamir and Adleman to design the RSA public key cryptography which uses two keys, a public and private key. RSA thus simplified key management. Another technology described in the paper in the paradoxical period is the quantum cryptography which is based on quantum mechanical laws. It is noted that the uptake for quantum cryptography has been low (Zulkifli, 2007).
The paper concludes by noting that the evolution of cryptography has followed the pace of technology and that public key cryptography has raised new concerns such as key and certificate management.

2.2.2: PKI – Advantages and Obstacles

Trust, privacy and security have become a great challenge to electronic communication. Public key infrastructure model tries to solve these issues and make Internet more secure. The paper notes that Internet has revolutionised the way the world communicates and as such it has brought new security problems. It notes that the Internet is a major communication tool in trade, banking, health industry and business.
The paper gives the structure of PKI and defines PKI as a system of digital certificates, certificate authorities and registration authorities that verify and authenticate the validity of each entity involved in an online transaction. It notes that PKI allows the secure exchange of encrypted data between parties over the Internet and it is a combination of hardware, software and policies with the aim of managing digital certificates.
The paper also gives an overview of encryption techniques. Symmetric which uses single key to encrypt and decrypt messages is introduced with DES being given as an example. The major weakness given for symmetric key cryptography is that both the sender and the receiver need to agree about the common secret key and those keys need to be securely stored and transported from the sender to the receiver. Asymmetric key cryptography is described as a solution to the above problem. It uses public/private pair of keys and the example given is RSA. The main disadvantage given for public key cryptography is that much larger keys need to be used to provide same level of security with symmetric key cryptography. As a result symmetric keys are

most used for encryption of data and public key cryptography is used to provide safe transmission of symmetric keys and the creation of digital signatures. Digital signatures are also described as digitally signed data structure that binds identity of a certificate holder to a public key.

The paper also looks at the Australia's PKI trusted hierarchy and identifies three crucial groups within the Australia PKI namely certificate authorities, users and agencies. It notes that different countries around the world have established their own PKI on a government level and also some internal and external vendor PKIs. The major PKI obstacles and challenges discussed in the paper include the fact that software application does not support enough PKI, PKI is too expensive and that it is not well understood. The paper concludes by noting that PKI is a very powerful technology that can offer variety of efficient and trustworthy services over the Internet to all users from all areas of society.

2.2.3: Implementing a PKI for the academic environment

In their paper titled 'Implementing a Public Key Infrastructure for the academic environment, (Manus & Andrei, 2011) present a pilot deployment and implementation of a Public Key Infrastructure within the IT academic environment of the University of Craiova.

The paper begins by describing the importance of a PKI as the need to protect information in transit as universities continuously increase the amount of critical data that is no longer processed on paper. The infrastructure presented on the paper was built, tested and it's currently in operation within the faculty of Automation, Computers and Electronics of the University of Craiova.

The security issues that were identified that led to the PKI deployment included the realization that most of the IT services within the university were authenticated by usernames and passwords. There was no any enforced automatic traceability of individual user responsibility for events taking place from within the university therefore security at an individual level was lacking. In the implementation phase, three tools are analysed that would be used to implement the PKI. They include the DogTag Certificate System (DCS) which is a PKI management software developed by RedHat and that employs Network Security Services. The second tool that was analysed is EJBCA which is a java tool used for deploying PKI and the last tool considered was the OpenCA. OpenCA was chosen because of its simplicity and the fact that it

offers support for essential standards necessary for PKI operations.

The architecture of the developed PKI consist of the Certificate Authority (CA) which is used for creation and revocation of certificates and issuing CRLs, the Registration Authority (RA) that handles the certificate signing requests (CSR) and the LDAP that is used for user management. Also included is a root CA that issues certificates for subordinated top level CAs. The root CA is installed on an offline workstation.

Problems encountered during the PKI implementation include concerns of security since the university does not have fully dedicated perimeter for CA hardware. Additionally, there were software language problems as the system was implemented in Romania. Additionally, due to the complexity of the design, the LDAP module was not implemented.

The paper concludes by noting that without a careful analysis and planning, it is difficulty to alleviate PKI complexity and its impact to the end users and decision makers.

2.3 Conceptual Framework

Kenya has sixty six universities (Commission for University Education, 2014) that are categorised as follows:-

1. Public Chartered Universities
2. Public University Constituent Colleges
3. Chartered Private Universities
4. Private University Constituent Colleges
5. Private Universities with Letter of Interim Authority (LIA)
6. Registered Private Universities

The universities have implemented information systems and are grappling with how to secure these systems. PKI was proposed as one of the ways that universities can increase the security of the systems and electronic communication within the universities.

The concept of the university system is to provide access to university services anywhere at anytime over open networks. This leads to issues of security and privacy in the management of the information systems. Managing such issues in the university environment has different emphases than in the private sector. The broader university approach is socio-technical by nature, involving people and processes as well as technologies.

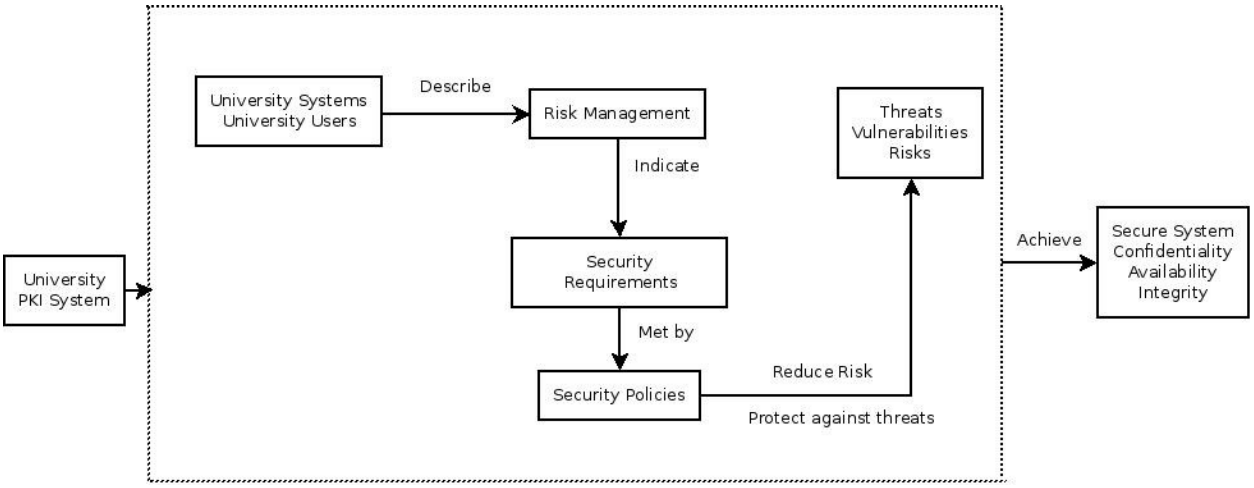
There are several models of information security in the literature that are based on the concept of the socio-technical approach. The Security by Consensus (SBC) model has been suggested by Kowalski (1994). Dhillon (2000) discusses how socio-technical system approaches can be combined with usability engineering in the design of information systems.

Ives et al (1980) model distinguishes between three information system environments (user, IS development, and IS operations environments) and three information system processes (use, development, and operations processes). The environments component defines the resources and constraints that dictate the scope and form of information systems and IS processes.

This research uses the Ives et al (1980) model to appropriately identify the differentiators and requirements needed to be considered by universities in Kenya for effectively maintaining their information security systems. This choice was made due to its comprehensiveness thus the model will enable us to view the information security issues in the context under study.

The framework described below was used for identifying, analysing, evaluating, treating, monitoring and communicating risks relevant to the university systems in Kenya.

Figure 3 : Conceptual Framework



Based on the framework developed above, a questionnaire was developed with questions that sought to understand the threats/vulnerabilities and risks in a university environment in Kenya, the kind of policies that exist and the perception of how PKI system can help achieve overall security in the university environment. See appendix three.

2.4 Conclusion

Public Key Infrastructure is a framework for creating a secure method for exchanging information based on public key cryptography. The foundation of a PKI is the certificate authority (CA), which issues digital certificates that authenticate the identity of organizations and individuals over a public system such as the Internet. The certificates are also used to sign messages, which ensure that messages have not been tampered with.

CHAPTER 3: METHODOLOGY

3.1 Research Design

3.1.0 Introduction

This section describes the research design and specific methodology that was adopted by this study to examine the security of university systems in Kenya. The chapter is presented in different sections including:-

- Methodology used in the study and the rationale for its use
- Details of the participants in the study and the selection criteria used
- Data collection process
- How the data was analysed

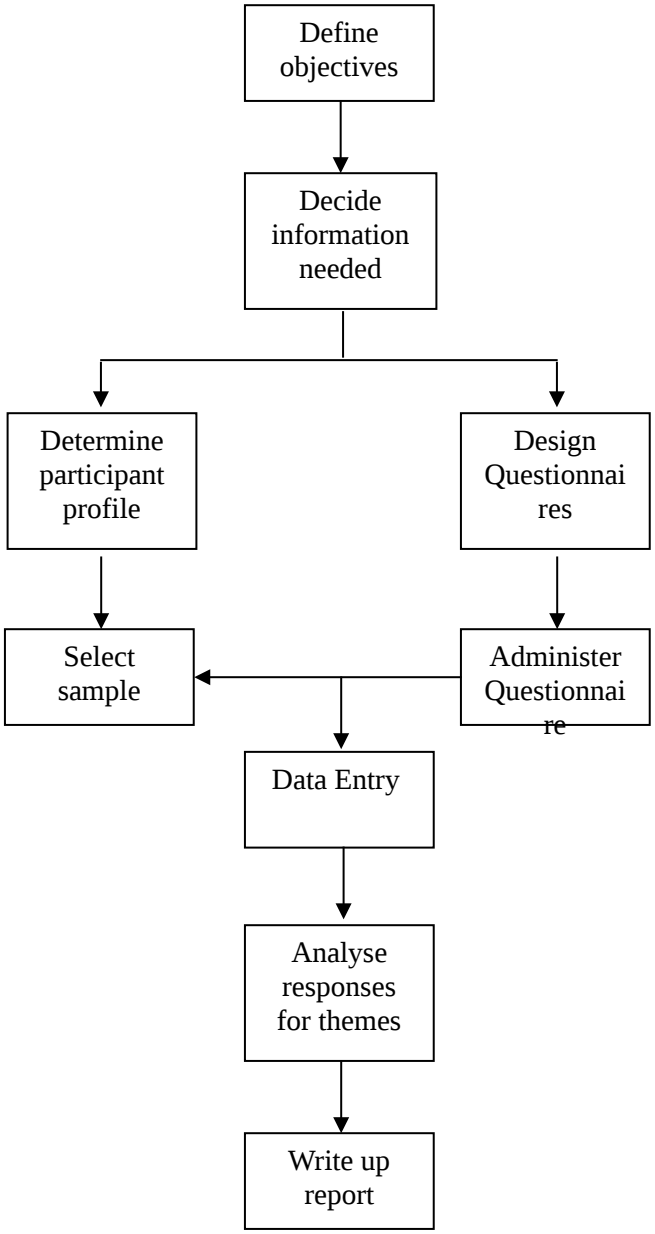
Qualitative approach to research was adopted in order to understand how the university systems users feel and or think of the security employed on the systems. It was also used to identify the security features in the systems that have been deployed by the universities. With concern for the validity, generality and representativeness of the study, the following questions were used as guiding principles in formulating the research design:

1) Data on what? What do these data tell me about and, crucially, what can they not tell me about? The questionnaire sought to understand the current threat facing university systems, the security features that have been implemented on these systems and whether PKI can help improve the security of the systems.
2) Strength of claim. How well do these data tell me this? How convincing are the claims I want to make on the basis of the data?
3) Integration of data? How best can I integrate and make sense of different forms of qualitative data?

This approach captured a detailed picture of the participants' experiences, attitudes and perceptions in the universities systems security. The study sought to understand local behaviour and construction of meaning. It also looked for themes that would emerge from the data in order to see if there are commonalities across the case studies.

The following diagram overviews the research process.

Figure 4 : Research Methodology



The purpose of the study was to provide a justification for deployment of PKI at the higher education institutions in Kenya. It sought to prove the theory that implementation of a PKI system in the Kenyan Universities is necessary in order to protect university systems and communication within the university. The study brought an understanding of the complex issue of the security situation at the university environment.

It also exposed the security flaws existing in the University systems hence reinforcing the theory that a PKI infrastructure is required in a university in order to increase security.

3.1.1 Research Design

Qualitative approach to research was adopted in order to understand how the university systems users feel and or think of the security mechanisms employed on the systems. It was also used to identify the security features in the systems and the perceived flaws.

3.1.2. Organization of the Study

Target population

The target population included the entire university community including both the public and private universities with all the teaching staff, IT staff and the students. These are the actual users of the university systems. The teaching staff's interacts with such systems as the examination system and the e-Learning system, the IT staff work on the systems and even manage them such as the email, databases and the online systems while the students interact with email and the student management systems among others. The IT Staff are the actual creators of the systems and are also involved in systems administration.

Study Sample

All the universities in Kenya that are recognized by the commission for university education were identified from the Commission for University Education website and formed the target population.

The table below shows all the universities that formed the study population:-

University Category	**Number**
Public University	22
Public University Constituent college	9
Chartered private university	17
Private university constituent college	5

Private university with letter of Interim Authority	11
Registered private University	2
Total	**66**

Random sampling was used to select the twelve universities that participated in the research. Each individual university in the population had the same chance (or probability) of being selected to be included in the sample. The sample size was arrived at by considering 20% of the total population which was considered to be representative enough to statistically represent the total population.

To select the twelve universities, all the sixty six (66) universities were coded from number one (1) to number sixty six (66). Random number generator, random.org, was used to generate (12) twelve random numbers between one and sixty six. The universities with the corresponding random numbers were then selected to form the study sample. The selected study sample of universities included the following:-

1) University of Nairobi
2) Chuka University
3) Embu University
4) Egerton University
5) Technical University of Kenya
6) Technical University of Mombasa
7) Meru University of Science and Technology
8) Co-operative University of Kenya
9) Daystar University
10) Kabianga University
11) Egerton University
12) Maseno University

The sample size was arrived at by using the finite population correlation constant formulae.

Data Collection

Data was collected by administering questionnaires to the sample population identified above. The reason questionnaires were used is because they are less expensive and easier to administer than personal interviews and they allow confidentiality to be assured. For these reasons a

questionnaire was designed that tried to get the perceptions of the systems users within the university community in Kenya on the effectiveness and the efficiency of the security mechanisms in place. The questionnaire was administered to the ICT Staff since they are the actual creators and maintainers of university systems.

The following questions categories relevant to the objectives of the study were asked:

- Demography
- University systems awareness
- The universities systems security
- PKI awareness

The questionnaires were emailed to the ICT directors/heads of all the identified universities. This was followed by a telephone conversation with the ICT director which acted to explain the relevance of the research questionnaire.

Data Analysis

All the twelve universities returned their questionnaires which sought to provide answers to the following:-

1) Whether universities are running online systems
2) Awareness of security features in the university systems
3) The types of security features at the university systems
4) Some of the threats/Vulnerabilities within the university systems
5) The perception of data and information security
6) PKI awareness
7) Existence of PKI system within the universities

The results of the survey were collected and input onto a spread sheet which was used for analysis. The results are discussed in chapter 4.

3.2 PKI System Analysis and Design

3.2.1 Introduction

This section is divided into two parts. Part one describes the system analysis while part two describes the system design methodology. Dynamic systems development method (DSDM) was used. This is an agile project delivery framework. The reason DSDM was used is because it focuses on the following eight important principles in systems development.

- Focus on the business need
- Delivery of systems on time
- Collaboration with users
- Quality
- Build incrementally from firm foundations
- Develop iteratively
- Communicate continuously and clearly
- Demonstrate control

The DSDM framework consists of three sequential phases, namely the pre-project, project life-cycle and post-project phases. The project life-cycle phase consists of 5 stages that are iterative. The three phases and corresponding stages that were used in the project are explained extensively in the subsequent sections.

3.2.2 DSDM framework

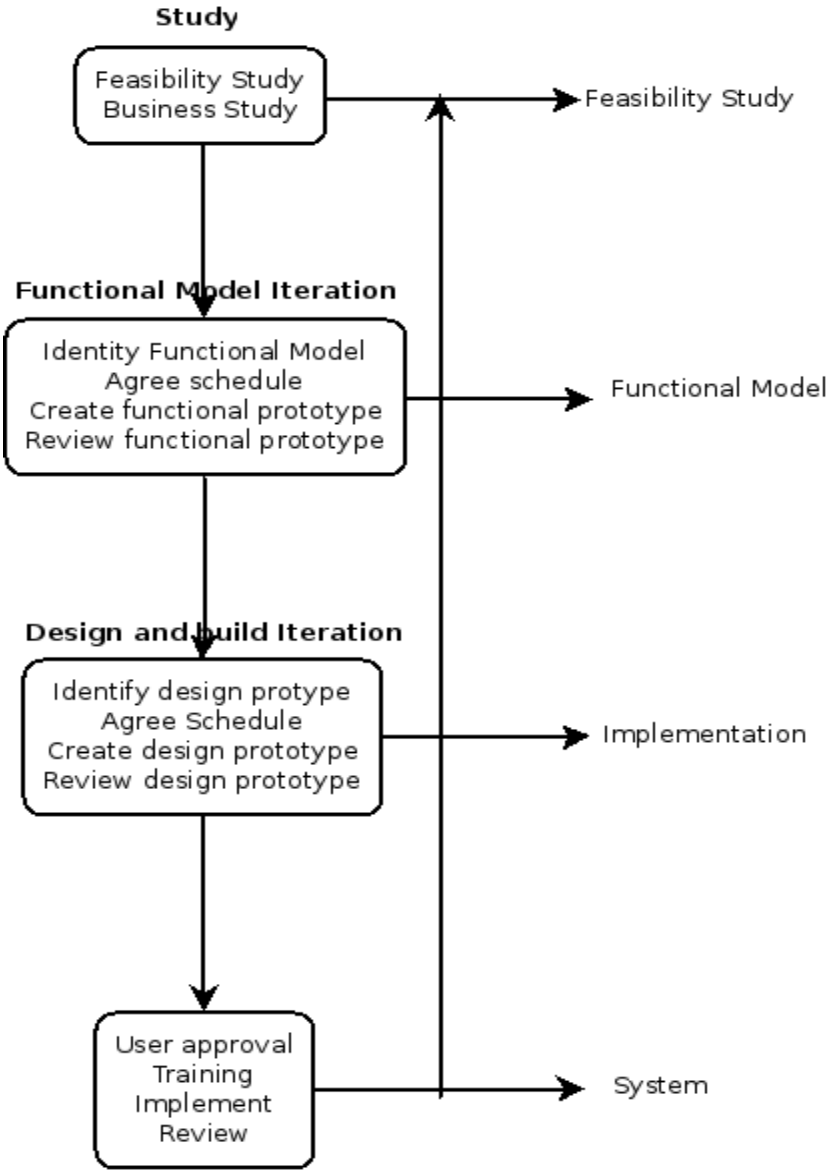
Phase 1 - The Pre-project

In the pre-project phase a proposal was developed and submitted to the panel. The proposal clearly outlined the problem statement, the proposed solution, the objectives, literature review as well as the required resources. The university panel approved the panel and their recommendations were factored in the subsequent phases.

Phase 2 - The Project life-cycle

The actual analysis and design took place at this phase. The diagram below depicts project life-cycle phase of the DSDM development methodology that was used.

Figure 5 : DSDM development methodology


Study
Feasibility Study
Business Study
Feasibility Study
Functional Model Iteration
Identity Functional Model
Agree schedule
Create functional prototype
Review functional prototype
Functional Model
Design and build Iteration
Identify design protype
Agree Schedule
Create design prototype
Review design prototype
Implementation
User approval
Training
Implement
Review
System

3.2.3 System Analysis

System analysis was done in the context of the DSDM agile framework as described in this section. This was mainly done in the phase two of the DSDM methodology.

Study Stage

The study stage had two activities namely:-

Stage 1A: The Feasibility Study

During this stage of the project, the feasibility of using DSDM for the project was examined. The feasibility study aim was to objectively and rationally uncover the strengths and weaknesses of the proposed system, opportunities and threats present in the environment, the resources required to carry through, and ultimately the prospects for success. The two criteria that were used to judge feasibility were the cost required and value to be attained. The feasibility study topics included the following:-

Technology and system feasibility

The project involved development of a public key infrastructure for the university community. There already exist tools and standards for building PKIs. The university setup has the technical capacity to handle a PKI system once completed and with user education, students and faculty can adopt to the developed system. The EJBCA tool was used to develop the project as discussed in the Literature Review.

Legal Feasibility

Legal feasibility was done by checking the laws of Kenya to establish whether any of these laws would be contravened by implementing the system. From the study, it was established that the developed system does not conflict with any known legal requirements.

Operational Feasibility

Operation feasibility was done to establish whether the system can actually work. It was determined that the system was operationally feasible since users were already interacting with online systems within the university. The system only adds an extra level of trust to the systems that are

deployed within the university environment. Furthermore, PKI has been used in other parts of the world hence it is operationally feasible.

Design-dependent parameters such as reliability, maintainability, supportability, usability, reducibility, disposability, sustainability, affordability and others were incorporated into the design.

Economic Feasibility

By securing stored data and data on transit, universities are able to reduce the cost of maintaining systems. This is achieved by the saving made by avoiding litigation costs in case someone sues as a result of exposure of their confidential information, loss of critical data as well as loss of reputation. There have been reported cases of students accessing examination systems and altering their marks in some universities in Kenya. This could have been avoided if the universities had embraced the use of Public Key Infrastructure.

Technical Feasibility

The system runs on two servers with specifications of Minimum 4 GB RAM, 50 GB HDD and 2.4 GHZ Processor. One of the servers serves the public interface while the second one serves the administrator interface. EJBCA tool which is an open source JAVA tool used in the development of Public Key Infrastructure is used in the development.

Linux Operating System and Open source applications were used. This is an intentional approach in order to keep the cost of setup and maintenance as minimal as possible. Specifically the system was deployed on Centos 6.5 Operating system. JBoss Application Server 7.1 was used as the web server for the PKI system.

There are several available encryption algorithms. For the project, 2048-bit RSA with SHA-256 was used. In defining the certificates, the X.509 specification was used. This allows fields such as the following to be included in the certificate:-

i. Version
ii. Serial Number
iii. Certificate Signature Algorithm
iv. Issuer
v. Validity

vi. Subject

vii. Algorithm Identifier

viii. Algorithm Parameters

ix. Extended Key Usage

x. Certificate Key Usage

xi. Authority Information Access

Schedule Feasibility

The project was estimated to take twelve weeks as shown in the table below:-

Table 3: Project Schedule

Week 1-4		
	Week 4-8	
		Week 9-12

Week 1-4

- Design questionnaires
- Conduct Research by administering questionnaires
- Literature Survey
- Research results analysis

Week 4-8

PKI systems development

- Planning
- Analysis
- Design
- Implementation
- Testing

All the deadlines set in the project schedule were found to be feasible.

Stage 1B: The Business Study

The business study extended the feasibility study. After the project had been deemed feasible for the use of DSDM, this stage was used to examine the influenced business processes, user groups involved and their respective needs and wishes. The information from these sessions was combined into a requirements list and a development plan was constructed as a guideline for the rest of the project.

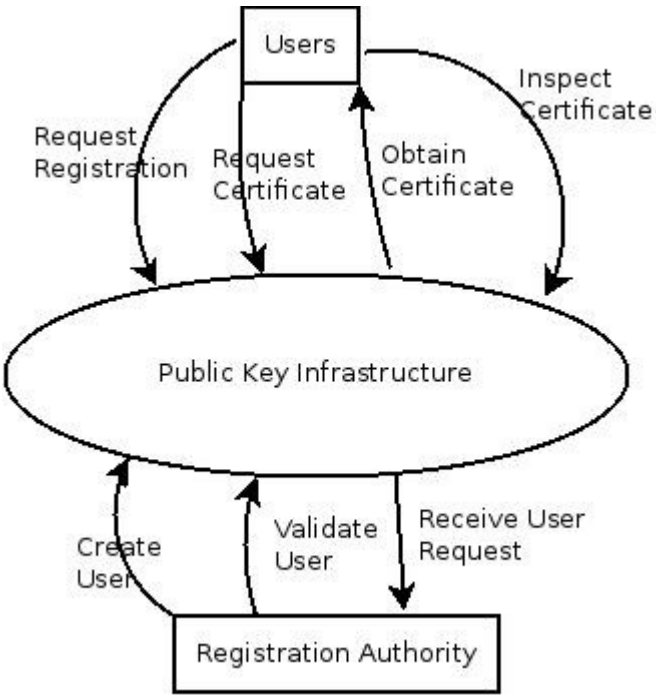
At a top level, a context diagram was used to identify the users and their interactions with the system.

The deliverables for this stage were:-

i. Business area definition that described the context of the project.

   The role of the PKI system is to secure systems and communication between users and systems within the university. Users can use the system to request and retrieve certificates. The certificates requests are in different forms including browser certificates, certificates from CSR or even CV certificates. Users are also able to request for registration and retrieve these certificates once they are ready. Additionally, they are able to inspect certificates received from other users.

Figure 6 : Context Diagram



On their part, Registration Authorities for each of the participating universities receive requests for user registration into the system, validates the users as actual members of the university before approving them to request for a certificate.

The context diagram shown above highlights several important characteristics of the system:-

a) The terminators (external entities with which the system communicates)

b) The data that the system receives from the outside world and that must be processed in some way

c) The data produced by the system and sent to the outside world.

ii. A top level system architecture

The architecture developed from the understanding of the context diagram is shown at page 43. This is a top down architecture where there is a rootCA for the university community in Kenya. Each of the participating universities is a CA and serves its own community. Each of the CAs has one or more Registration Authorities.

Intended Audience

This system will increase systems and electronic online communication within the university community by promoting the use of digital signatures. From the system developed, users can create and download digital certificates that they can use for different purposes. The system will act as the root CA for the university community but also has multiple CAs for different universities.

The users of the PKI system can be categorized as follows:-

a) General users – These are the general users of ICT within the universities. They may use university systems including email. They can create and download certificates from the developed system.
b) Students – For systems where certificate based authentication is enabled and also for signing emails, students can used digital certificates from the developed system.
c) Teaching Staff – Just like students, for systems where certificate based authentication is enabled and also for signing emails, teaching staff can used digital certificates from the developed system
d) ICT staff – These are the actual implementers of systems within the university setup. They will be required to design systems that make use of digital certificates for authentication. They will also maintain the PKI system developed and appoint a Registration Authority.

User Personas and Characteristics

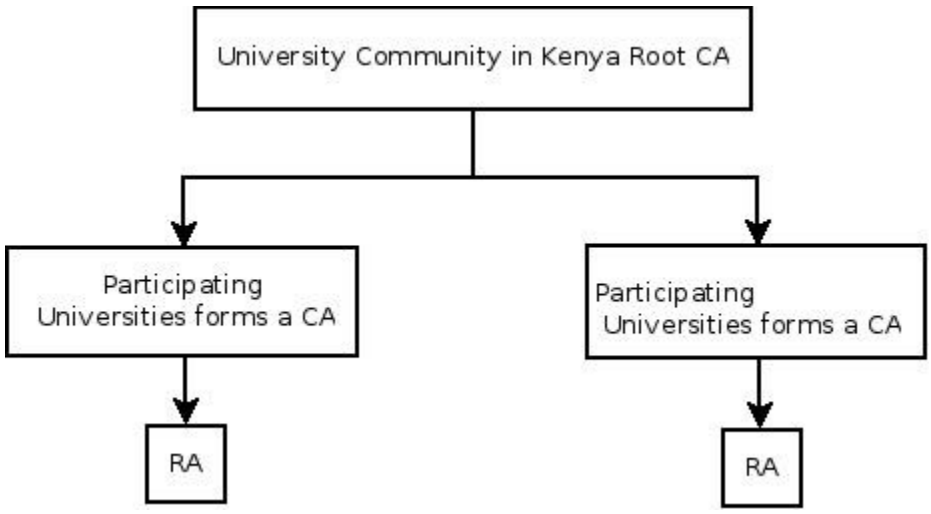
Case 1: A user who is new to PKI and the use of digital certificates in systems development from a system development perspective

Case 2: A user who is new to PKI and the use of digital certificates from a user point of view

Case 3: A user who is competent in PKI and the use of digital certificates in systems development from a system development perspective

Case 4: A user who is competent in PKI and the use of digital certificates from a user point of view

Figure 7 : Top Level Architecture



iii. The following is the requirements list that was generated from the business study:-

Table 4: Requirements List

No	Requirement
1	Users request for registration
2	Registration Authority user approval
3	Certificate Request
4	Certificate Generation
5	Certificate Retrieval
6	Certificate inspection

iv. Risk Log Version 1

Table 5: List Log Version 1

No.	Identified Risk	Description
1.	Users are new to PKI technology	
2	University policy	
3	User behavior	

Several activities were involved in the requirement analysis including:-

i. Eliciting requirements – this involved requirements gathering using questionnaires and prototyping. The questionnaire administered during the research that was done preceding the design enabled an understanding of the security situation at the universities.
ii. Analyzing requirements - determining whether the stated requirements are clear, complete, consistent and unambiguous, and resolving any apparent conflicts. In order to increase clarity and understanding of the requirements, the context diagram shown in the previous page was used.
iii. Recording requirements: this was done using the functional model.

The following types of requirements were identified:-

User/Operational Requirements

The Operational requirements were used to define the basic need and, at a minimum, answer the questions posed in the following listing:

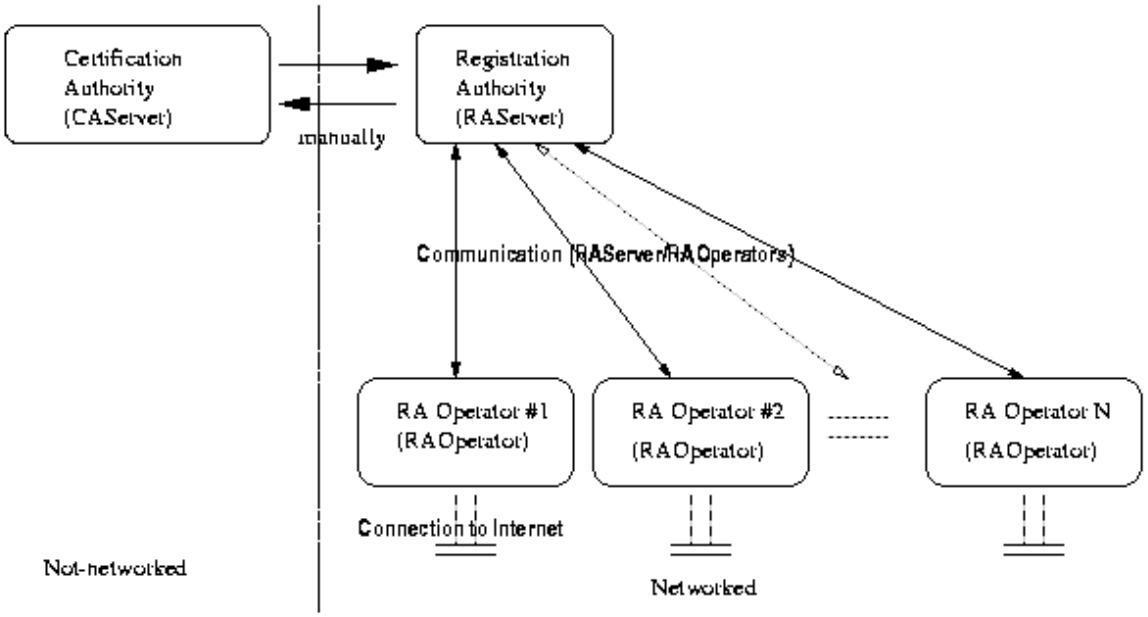
i. Operational distribution or deployment: The system is to be deployed in a centralized location and should be accessible to all universities in Kenya.
ii. Mission profile or scenario: The mission of the system is to secure university systems and online communication within universities in Kenya. This is achieved through the use of digital certificates.
iii. Performance and related parameters: Performance of the system was measured by checking the amount of time it takes for a user to request and receive certificates.

iv. Utilization environments: The system runs two servers, one private and the other is public. The private server carries user certificates and it should be kept in a secure environment.

Architectural Requirements

Architectural requirements were used to explain what has to be done by identifying the necessary systems components of the PKI system as described in a previous section.

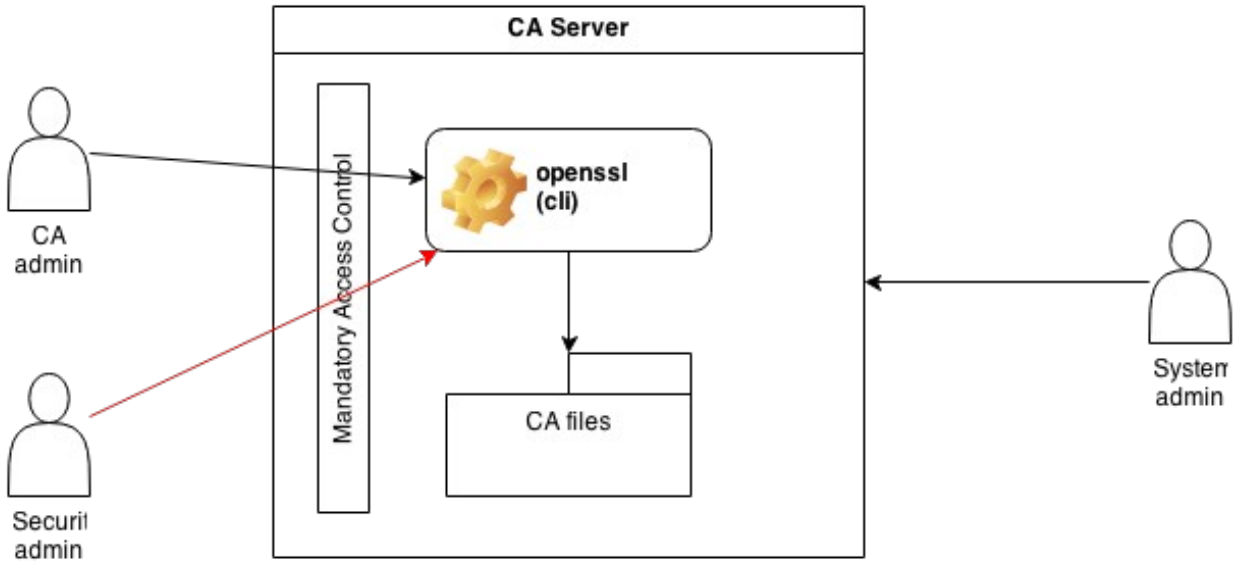
Figure 8: Architectural Requirements



Behavioral Requirements

Behavioral requirements were used to explain what has to be done by identifying the necessary behavior of a system and the expected behavior of the users while interacting with the system.

Figure 9: Functional Requirements



Functional Requirements

Functional requirements were used to explain what has to be done by identifying the necessary task, action or activity that must be accomplished. From the PKI system, users from within the university community will be able to request and generate digital certificates that they can use for secure communication.

Non-functional Requirements

The following non functional requirements were considered:-

Efficiency

The system supports high functionality without significantly increasing hardware and software capabilities.

Usability

The system has the characteristic of being easy to use to the extend that it effectively performs the task for which it is used for. Ease of use was measured by measuring how quickly a task is performed, how many mistakes are made and how quickly the system is learned and how satisfied people are who perform the task.

Accessibility

The system is hosted online on a public server and is web based. This means that users with access to the Internet are able to access the system.

Acceptability

To ensure acceptability, user centered design was employed. Before start of development a study was carried out to the universities. Additionally, prototypes developed were tested by the users.

3.2.4 System Design

This section describes important aspects in the design and implementation of the university community PKI. It forms a continuation to the DSDM methodology. The general priorities during design included:-

i. **Practicability**

   The functionality of the system has to be achieved i.e. it is possible for users to request for and get digital certificates in different forms.

ii. **Aesthetics**

   The inputs and the outputs of the system are compatible to the user look and feel

iii. **Efficiency**

   The system produces results with the existing resources

iv. **Minimizing cost**

   The system is implemented in a Linux operating system with open source tools hence the only cost incurred is the cost of hardware.

v. **Flexibility**

   The system is capable of modification. This is to support repair of bugs, supporting extensibility of software system and support changes in technology. The system is also able to evolve. After the release of version one, more improvements can be done on the PKI system to come up with later versions.

vi. **Security**

   Only authorised persons are allowed to login into the admin interface of the PKI system.

Outline of the DSDM design

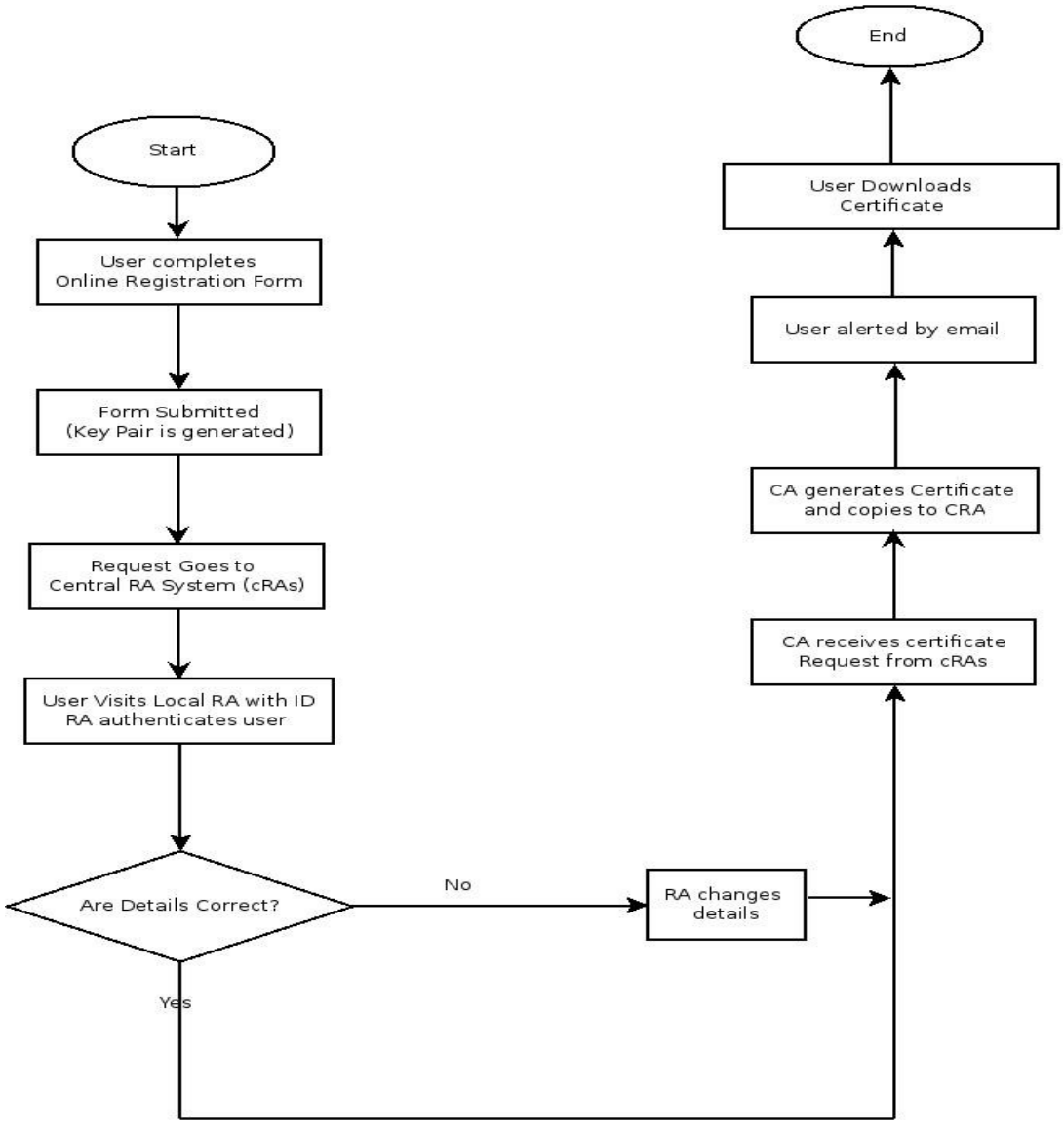
Stage 2: Functional Model Iteration

The requirements that were identified in the previous stages were converted to a functional model. This model consists of both a functioning prototype and models. Prototyping was used to realize good user involvement throughout the project. The developed prototype was reviewed by users.

Functional Model

A structured representation of the activities, actions, processes and operations was modeled in order to discover the needs of the system. The diagram below shows the entire process that users undergo in order to use the system.

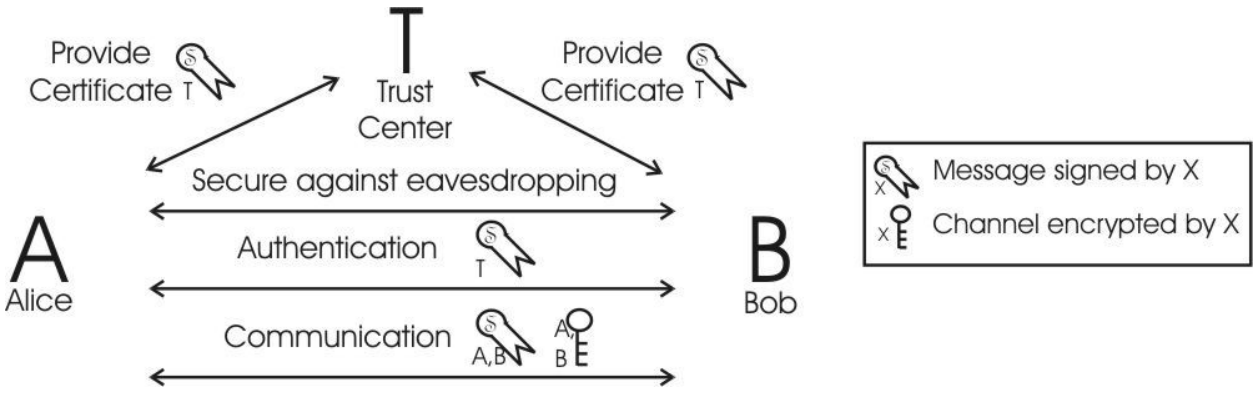
Figure 10 : Functional flow block diagram



Functional Prototype

A prototype of the system capturing the user requirements identified so far was developed. The functional prototype was not only a way to actually see the interactions and user experience of a system in real life; it was also a rough sketch for a final product. It also helped others understand what the solution is all about. A functional model of the same was also developed as shown in the diagram below.

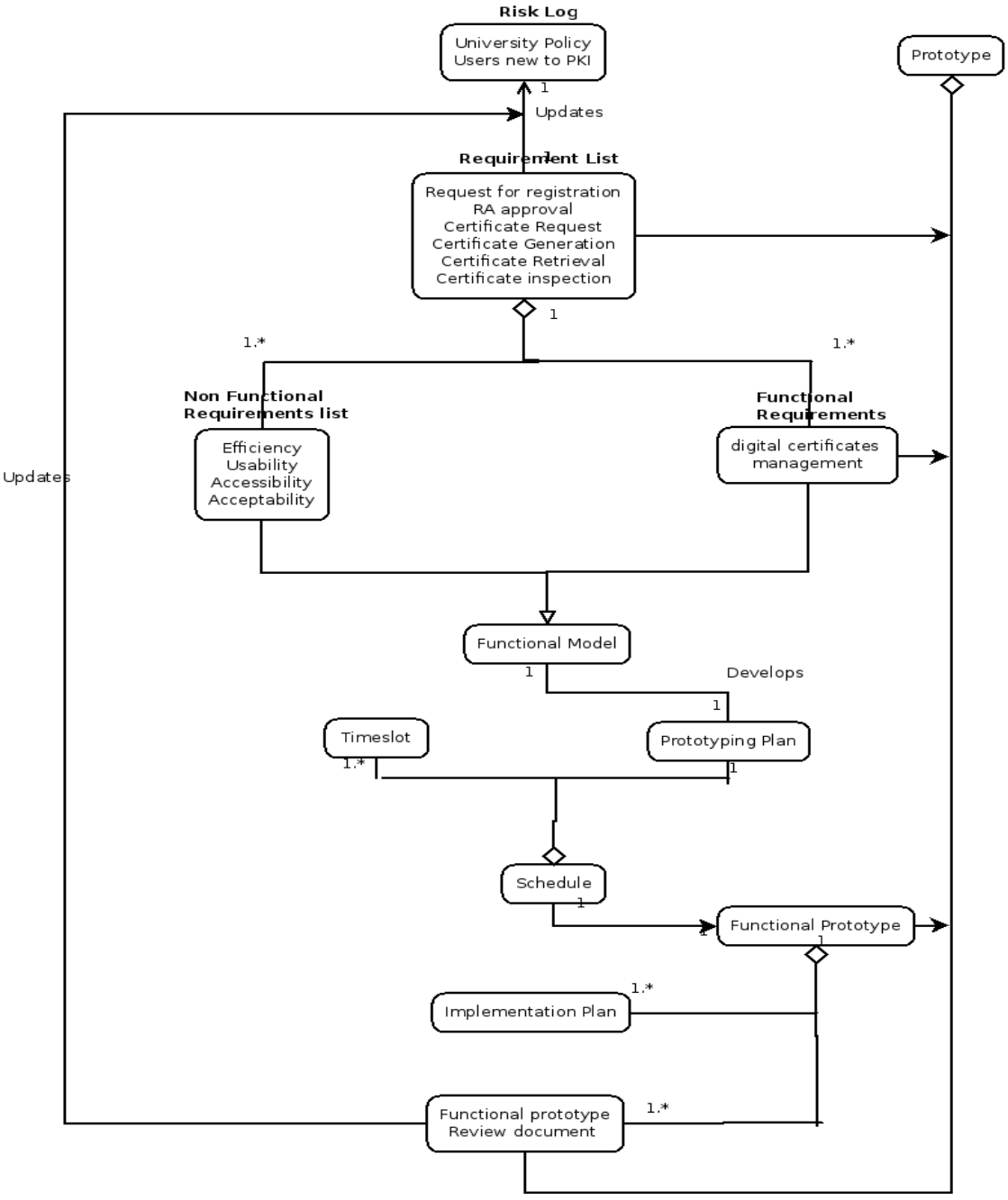
Figure 11: Functional Model



Meta-data model

The associations between concepts of deliverables in Functional Model Iteration stage were depicted in the meta-data model below. This meta-data model was combined with the meta-process diagram of Functional Model Iteration phase in the next part.

Figure 12 : Meta data



Process-data model

This process involved analysis and coding to build a prototype, and the experiences gained from them were used in improving the analysis. The built prototype was not entirely discarded, but gradually steered towards such quality that it was included in the final system. Testing was also done at this stage. Below is the process-data diagram of Functional Model Iteration stage.

Figure 13: Process data Model

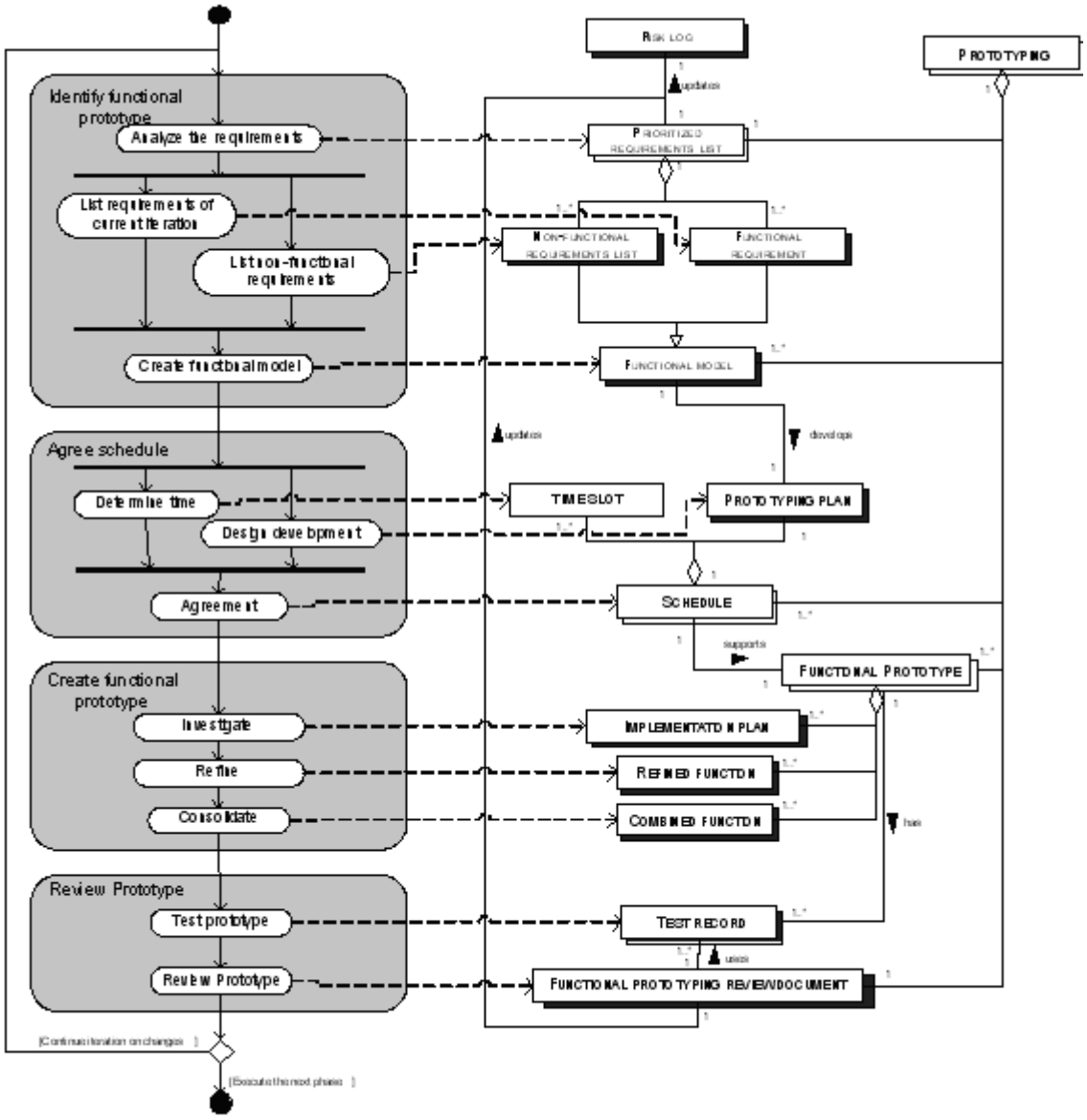


Table 6 : Process data model description

Activity	Sub activity	Description
Identify functional prototype	Analyze the requirements	The requirements of current prototype were analyzed according to the prioritized requirements that were previously developed (in previous phase which is business study phase).

	List requirements of current iteration	The functional requirements that would be implemented in the current iteration's prototype were selected.
	List non-functional requirements	List the non-functional requirements of the system was developed
	Create functional model	Analysis model and prototype
Agree schedule	Determine time	Possible timetable to perform the prototyping activities according to the prototyping plan and prototyping strategy was identified.
	Design development	The prototyping plan, including all prototyping activities that were performed on available time slot.
	Agreement	The agreement schedule of when and how the prototyping activities should be performed.
Create functional prototype	Investigate	Investigate the requirements; analyze the functional model that has been built in earlier activity, and set the implementation plan according to the analysis model, that was used to build the prototype in the next sub-activity.
	Refine	Implementation of the functional model and implementation plan to build a functional prototype. This prototype was then refined before being combined to the other functions.
	Consolidate	The refined functional prototype was consolidated with the other prototype of previous iteration.
Review prototype	Test prototype	The test record was used together with users' comments to develop the prototyping review document.
	Review prototype	Based on this functional prototyping review document, the prioritized requirements list and risk log were updated.

Prototyping review document

This document reports on the status of the Final Prototype. During this engineering process, the PKI system was modified to incorporate a number of additional features that made it useful as a prototype and a demonstration of how PKI can work in a university environment. The first prototype provided an understanding of how PKI works and its working procedure. The second prototype implemented the various features of the PKI system and was given to the users to test.

Prioritized requirements list Version 2 then developed as shown below.

Table 7: Requirements List Version 2

No	Requirement
1	Users request for registration
2	Registration Authority user approval
3	Certificate Request
4	Certificate Generation
5	Certificate Retrieval
6	Certificate inspection

Risk Log Version 2

Table 8 : Risk Log Version 2

No.	Identified Risk	Description
1	University policy	

Stage 3: System Design and Build Iteration

The main focus of this iteration was to integrate the functional components from the previous phase into one system that satisfies user needs. It also addressed the non-functional requirements

that have been set. Testing was an important ongoing activity in this stage. This design was based on the architecture already developed for the university PKI.

The deliverables for this stage were:-

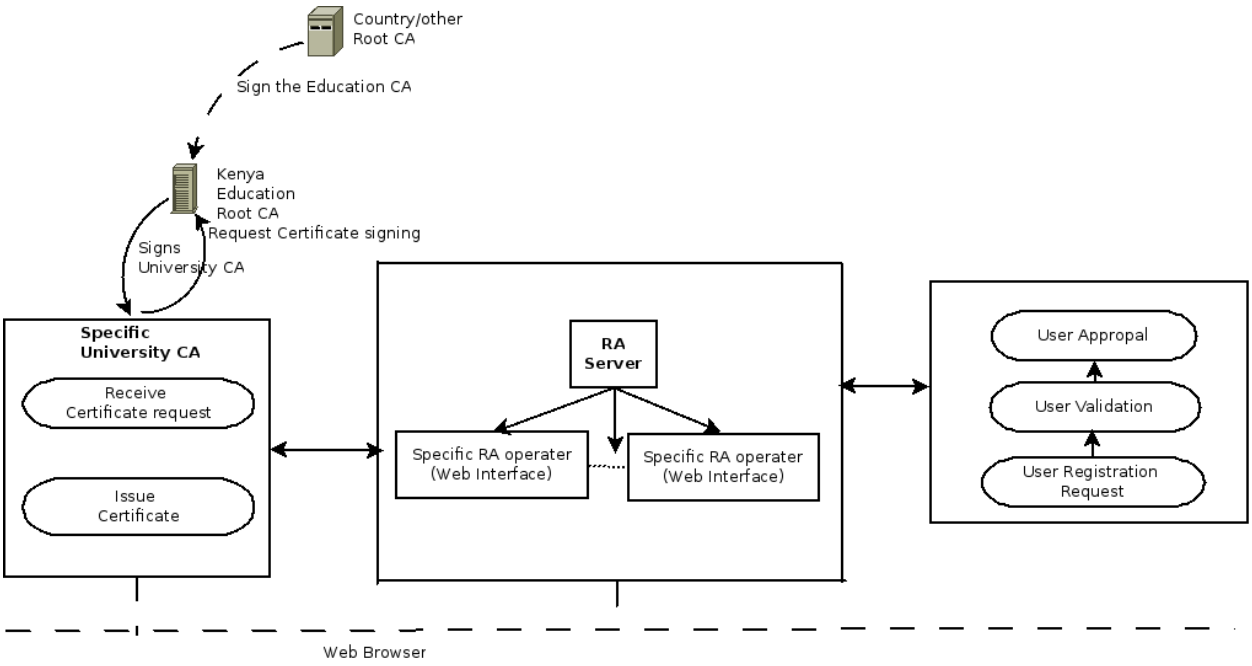
- Design Prototype that end users got to test
- In this stage, the system was mainly built where the design and functions were consolidated and integrated in a prototype.
- User Documentation.

  A documentation of how to use the system was developed and incorporated into the system**.**

System Architecture

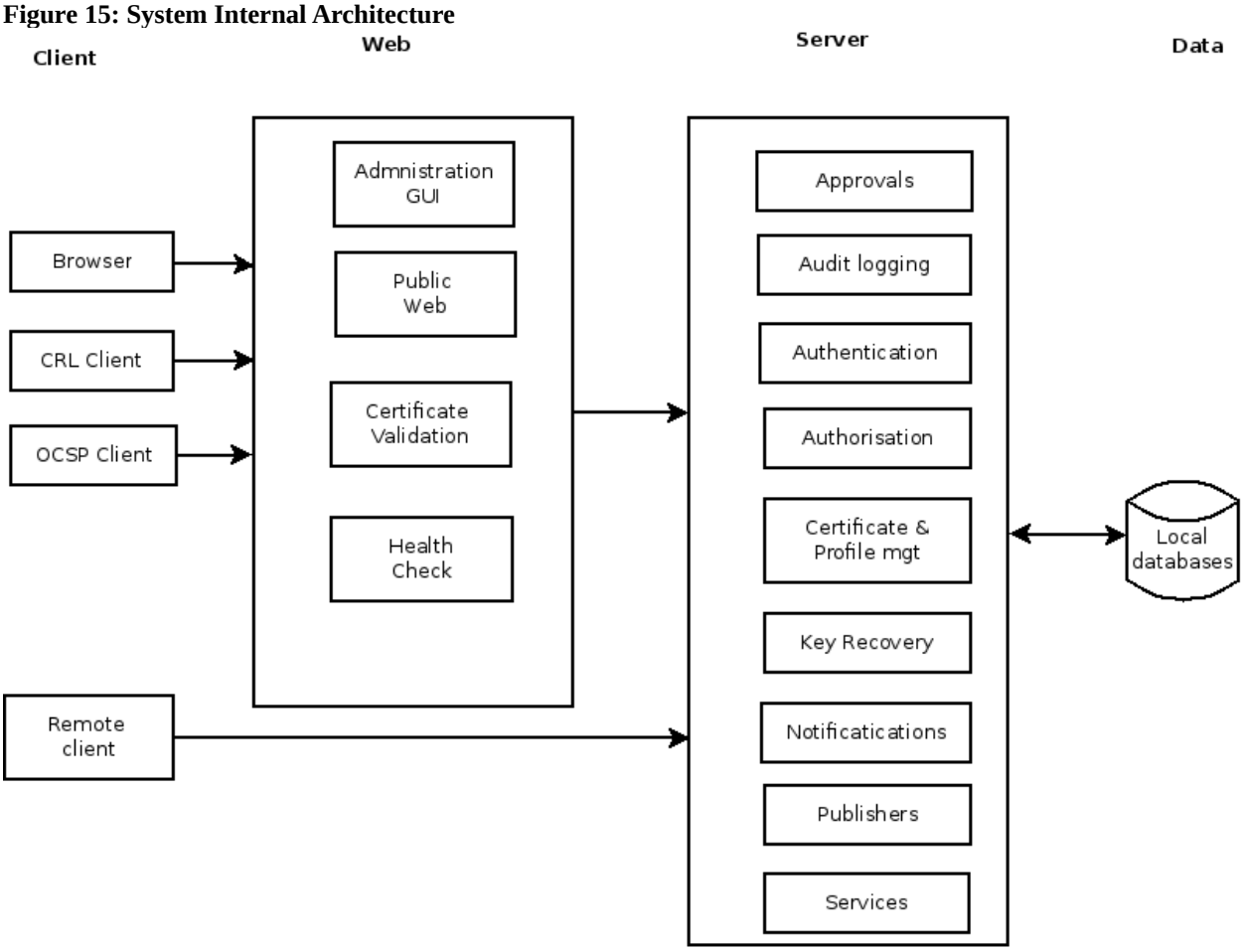
The diagram below shows the final top level and the internal architecture that was designed. The University Community CA will be the root CA for the entire university community. Once PKI infrastructure is fully developed, it will be trusted (signed by) the country root CA. The country root CA is currently being developed by the communication authority of Kenya. Each of the participating universities will be required to appoint a registration authority who will be used to vet user applicants for the system. The universities can choose to have a single registration authority or they can devolve this function to the various departments within the university.

Figure 14: System Architecture



The following diagram shows the internal architecture of the PKI system developed.

Figure 15: System Internal Architecture



Stage 4: Implementation

In the implementation stage, the tested system including user documentation was delivered to the users. The system to be delivered had been reviewed to include the requirements that had been set in the beginning stages of the project. The Implementation was subdivided into three sub-stages:

- User Approval and Guidelines.
- Implement: The tested system was implemented at the location of the end users.
- Review Business: Review the impact of the implemented system on the business was conducted.

The system runs on Linux and openjdk version of java 1.6. Using the tools available in ejbca, a web based PKI for a university environment was developed based on the following X.500 notation:-

- CN = Common Name
- DN = Distinguished Name, which is the CN followed by information about the organization that owns the CA
- OU = Organization, unit
- C = Country, in ISO 3166-1 alpha-2 format (US, KE, etc)

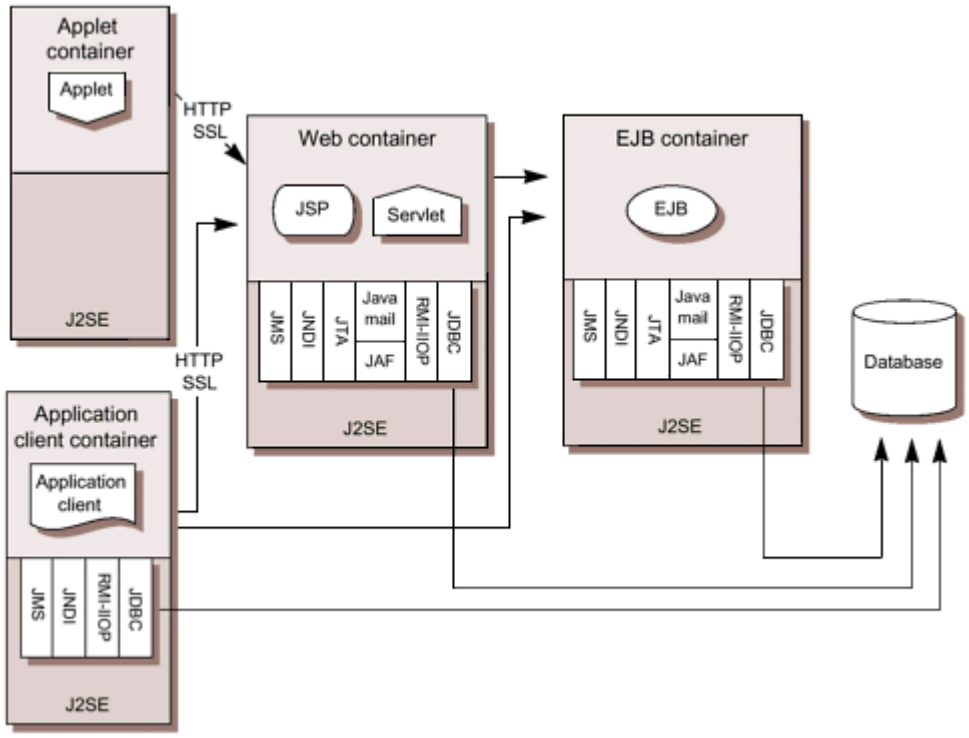
The following are the components that have been implemented for PKI to work:-

- Authentication Code - Each Crypto Token has an associated Authentication Code that is used to encrypt the contents of that particular Crypto Token.
- Certificate - A data structure in X.509 format that typically contains:
    - A public key
    - Information about the owner of the key (in X.500 format)
    - "Certificate Extensions" defining how the certificate is meant to be used
    - The CA certificates that validate the certificate we are examining

    - Certificate Extension - Data field in a Certificate that "suggests" how a certificate is meant to be used. Crypto Token - The logical unit that stores all the public/private keypairs owned by a particular CA held in a MYSQL database.
- Enrollment Code - The password (or other "Token") used to validate a certificate request.
- JKS - Java Key Store. An unencrypted, file-based method of storing encryptions keys.
- Keypair - a Public key and its matching Private key.
- Key Algorithm - The asymmetric cryptographic algorithm used to perform public key encryption.
- Key Alias - A "friendly" name for a Key(pair)
- defaultKey: The key used by default
- certSignKey: The key used for certificate signing. It must comply with the Signature Algorithm defined for the CA using the key.
- keyEncryptKey: The key used for key recovery when reversible encryption is enabled. It must use the RSA algorithm.
- Key Specification -The length of the modulus used by the Key Algorithm. For RSA, it is usually 2048 or 4096 bits long. For Elliptic Curve, it is usually 192, 256, 384, or 512 bits long.
- Keystore - A file used to store certificate information outside of the database. Normally only holds the certificates for the web interface.
- Signature Algorithm -The cryptographic hash algorithm used by a CA to guarantee a certificate's validity.
- Soft Token - A Token (Crypto, or otherwise) held in the database
- Token - A generic term for a secret key. This could be anything from an 8-character ASCII password to an 8192-bit RSA modulus. In the context of an "end entity", ejbca specifically uses this word to refer to the key used to encrypt a certificate issued to that "end entity".

The system consists of MYSQL database, Java and its database connector and Jboss - 7.1.1 component on the backend and a web based user interface.

Figure 16: System Components



The database contains the following tables:-

AdminGroupData

AccessRulesData

AdminEntityData

AdminPreferencesData

ApprovalData

AuditRecordData

AuthorizationTreeUpdateData

Base64CertData

CAData

CertificateData

CertificateProfileData

CertReqHistoryData

CRLData

CryptoTokenData

EndEntityProfileData

GlobalConfigurationData

HardTokenCertificateMap

HardTokenData

HardTokenIssuerData

HardTokenProfileData

HardTokenPropertyData

InternalKeyBindingData

KeyRecoveryData

PeerData

PublisherData

PublisherQueueData

ServiceData

UserData

UserDataSourceData

The system was deployed on jboss 7 server.

Phase 3 - Post-project

The post-project phase ensures the system operates effectively and efficiently. This is realized by maintenance, enhancements and fixes and this will be done once the system is adopted by the universities.

CHAPTER 4: RESULTS

This section describes the results of the study done on the university and presents the system that was developed. The chapter is presented in two sections including:-

i. Study finding
ii. The developed system

Section One

4.1 Study Finding

As described in previous sections, research was conducted on selected universities to understand the security implementations in place and to determine the reediness of the universities in Kenya to adopt public key infrastructure.

The data collected from the universities shows that 100% of all the universities in Kenya use information systems and electronic communication. The systems that run in the universities in Kenya include the following:-

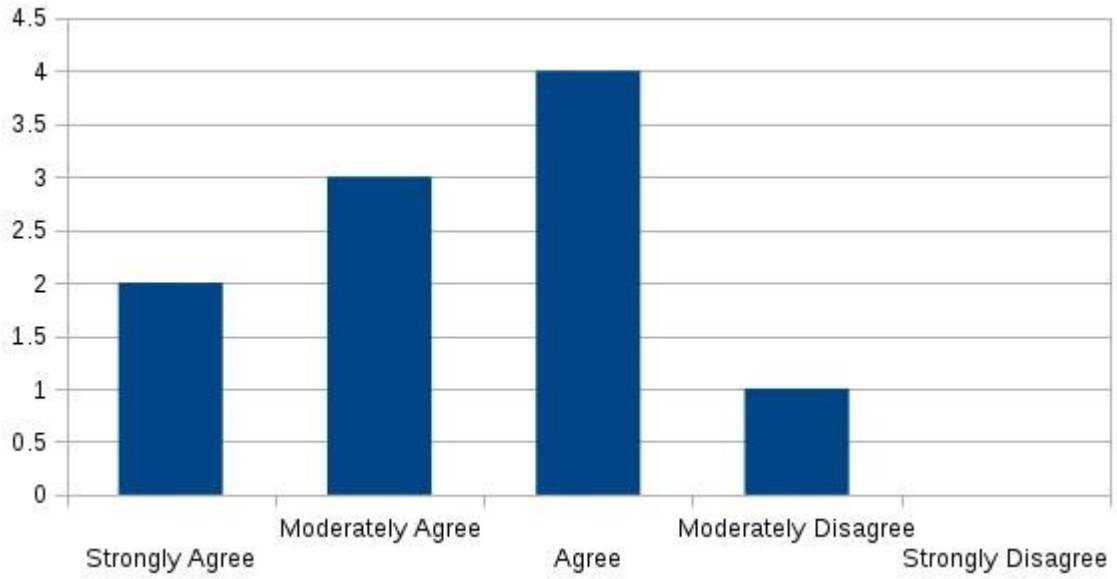
- University ERP systems
- Payroll Systems
- Examinations Processing systems
- Financial Management systems
- Student Management Information Systems
- Automated Quality Management Systems
- Document Management Systems
- Human Resource Management System
- ELearning systems
- Library Information systems
- Document Management Systems
- Ticketing systems
- email
- IP Telephony
- Web portal

In these systems, various security features have been implemented. They include:-

- Group Policy servers for authentication
- Security key for wireless access points
- Firewall
- Use of Passwords
- Physical security e.g. locks, grills
- Use of manpower e.g. Security guard to safeguard Examination room
- Use of staff Identification to allow entry to University and sensitive places"
- Pass-phrase
- Data encryption and decryption
- Smart card access control"
- Biometric
- Logon
- PIN access control

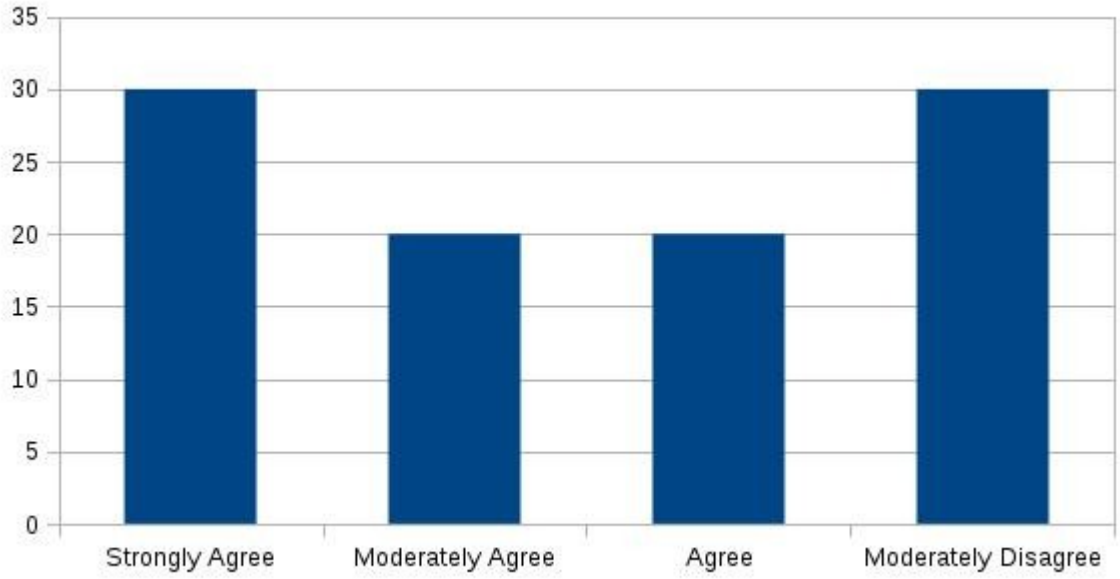
The graph below shows the answers of the respondents when asked about whether they felt secure when using university systems. While many agreed, none strongly agreed that they actually felt secure. This was also the case with how they felt when using email for communication.

Figure 17: Satisfaction with security in place at the universities



The graph below shows the level of awareness of PKI within the university community in Kenya.

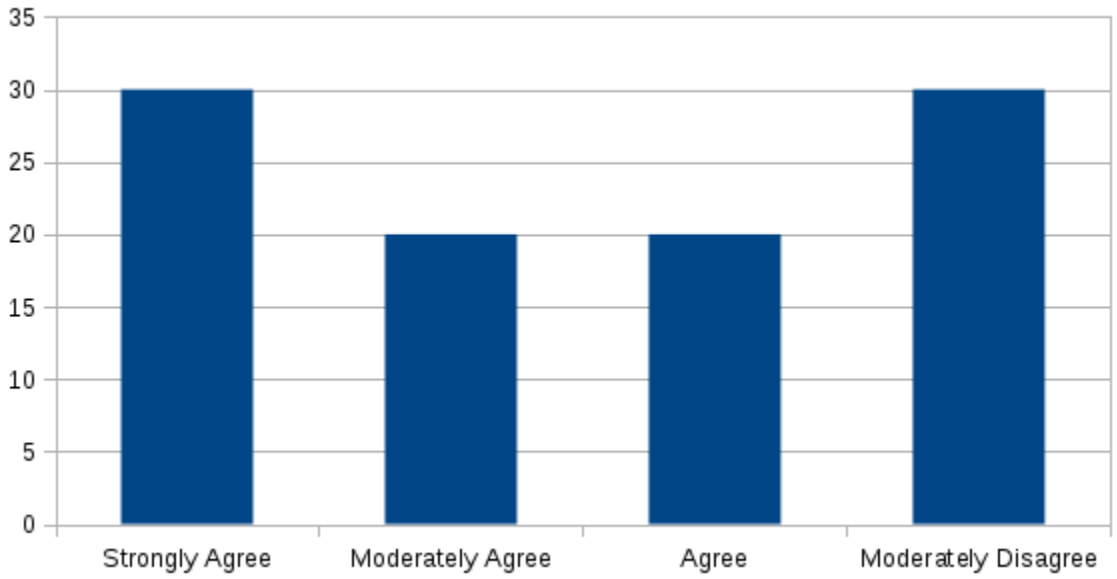
Figure 18: PKI Awareness



The graph shows that there is a split into half between those that are aware of PKI technology and those that are not. Those that are aware of the PKI technology were further asked whether it could help improve the security situation at the university. They were also asked to highlight ways they thought PKI could be used to improve the security situation at their universities and their answers are described in the next section. This means that if PKI is introduced within the university environment, then there is some understanding of how it works hence it would be acceptable.

The graph below shows answers from respondents when asked about whether there have been any successful cyber attacks in the universities.

Figure 19: Successful Cyber attacks

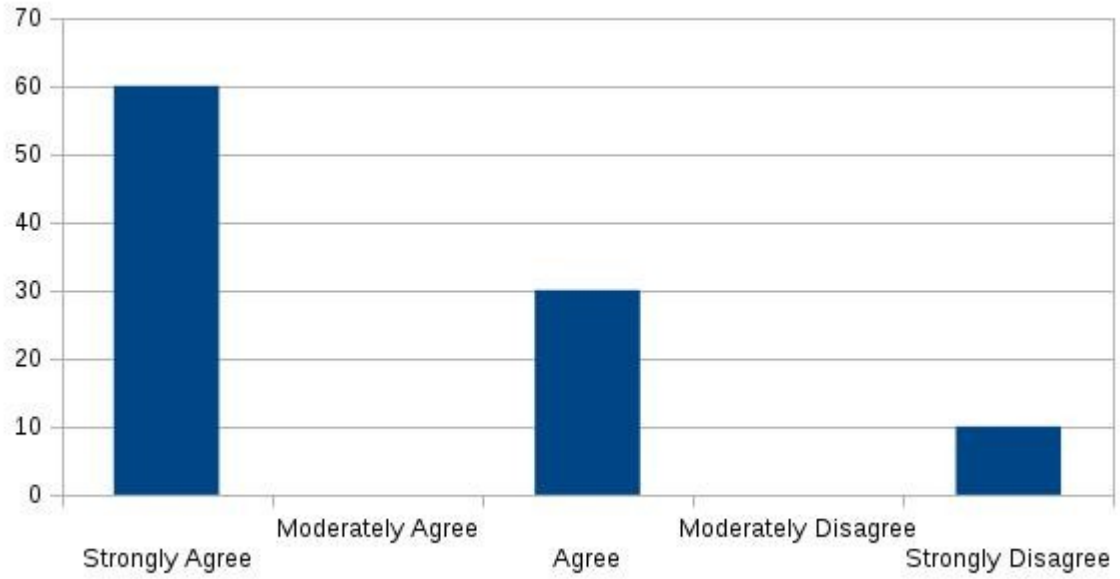


The graph above shows that, 70% of the universities have experienced successful cyber attacks. This is a worrying statistics that needs a solution. 90% of the universities do not have a mechanism or system where interested users can obtain digital certificates. On the other hand, they know the value that PKI would bring to the universities including:-

- Encrypting of data during internetworking, wireless security
- It can enable secure implementation and use of Electronic document management system
- Access to SMIS, secure email, secure online applications
- Used to secure confidential information sent through the network
- Authentication of University staff to the University infrastructure and resources

Although the respondents knew what could be achieved using a University PKI only 10% knew of a platform/place where they could get digital certificates. See the graph below:-

Figure 20 : Access to PKI services



The graph shows that 90% of Universities in Kenya do not have access to PKI services. From the data collected, it is worth noting that universities recognize the need for digital certificates but lack a platform for obtaining these certificates. Backed by this data, PKI for the university that comprised of a university CA and other sub CAs was developed as described in the previous chapter.

Section Two

4.2 The Developed System

The system was successfully deployed on a Linux server running CentOS 6.5 operating system using ant java tool and jboss. Users can request for and receive certificates from the system. This section describes how the system can be used to achieve systems and communication security within the university environment.

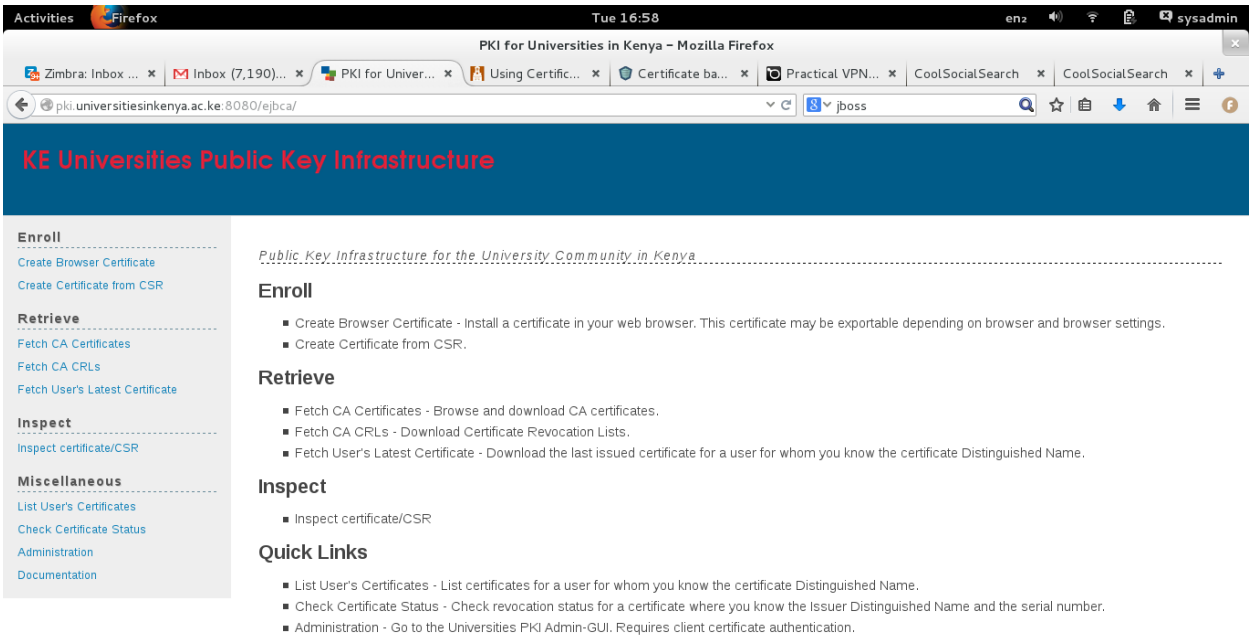
How the system works

The system has two interfaces, one interface that is accessible to the public and the other is only accessible to the administrators. From the public portal, users can request for registration, create browser certificates or even create certificate from CSR. Users can also fetch CA certificates and CRLs and inspect certificates that already exist.

User Interface

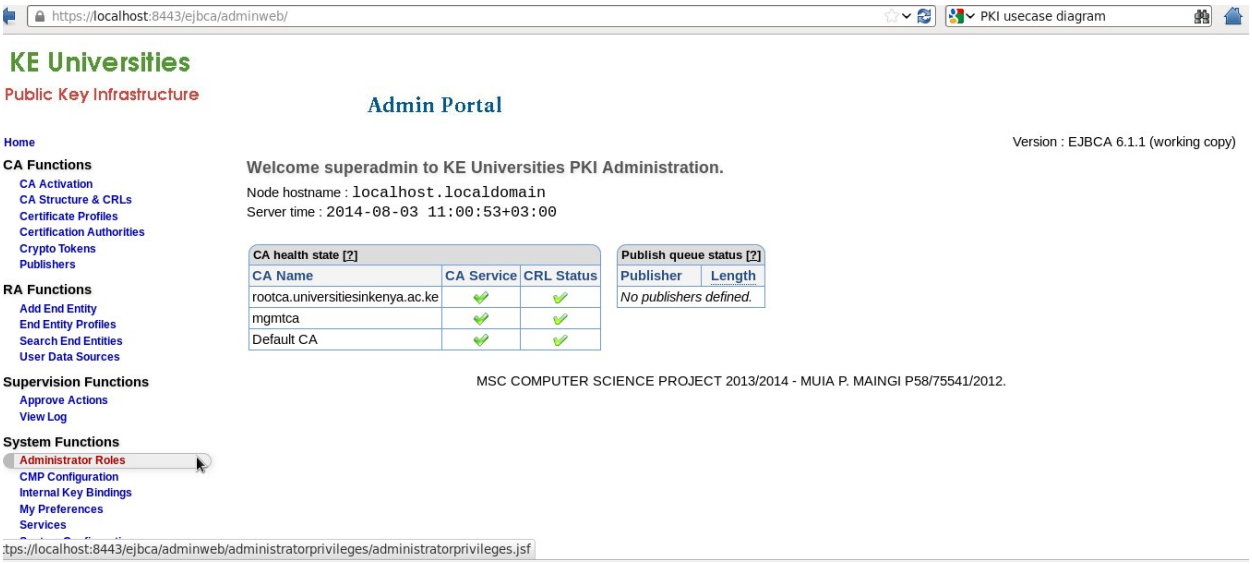
The user interface provides an online platform that can be used to enrol, retrieve and inspect certificates.

Figure 21: PKI User Interface



Administrator Interface

Figure 22: PKI Admin Interface



User Registration

For users to create any certificates from the system, they require a username and some enrolment code. These are created by a Registration Authority upon confirmation that the user is a member of the university. Once users are registered, they are able to perform different tasks some of which are described in the next section.

Obtaining Certificates

There are two ways that a user can obtain a certificate from the portal. This includes:-

1. Create browser certificate
2. Create certificate from a Certificate Signing Request (CSR)

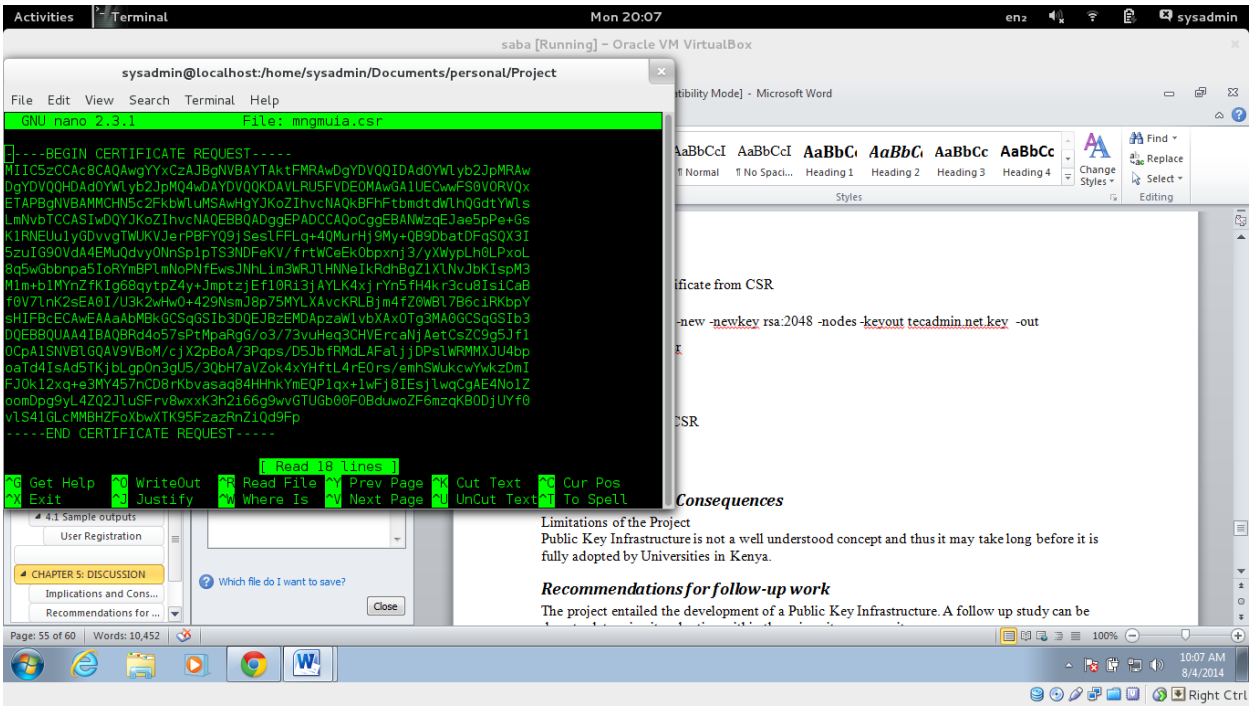
Create Certificate from CSR

To create a CSR from a host machine running Linux, the following command is typed on the terminal

openssl req -new -newkey rsa:2048 -nodes -keyout tecadmin.net.key -out mngmuia.csr

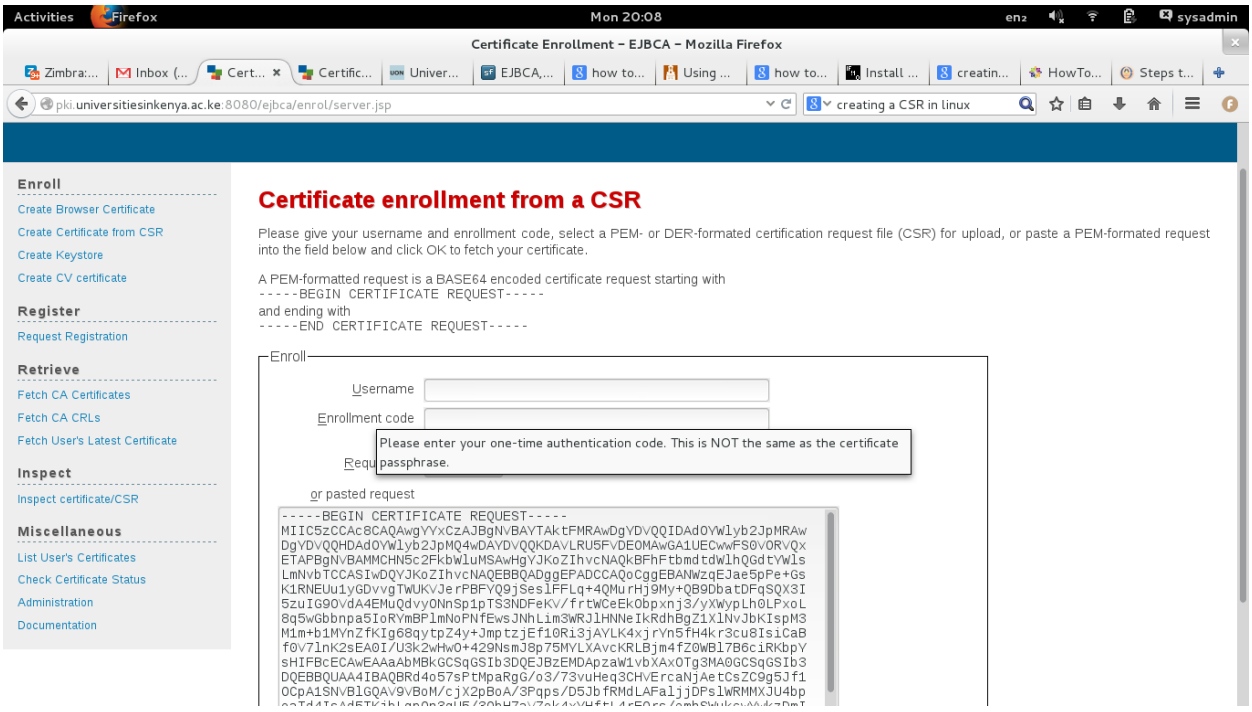
This generates a CSR that looks as shown below:-

Figure 23: Sample CSR

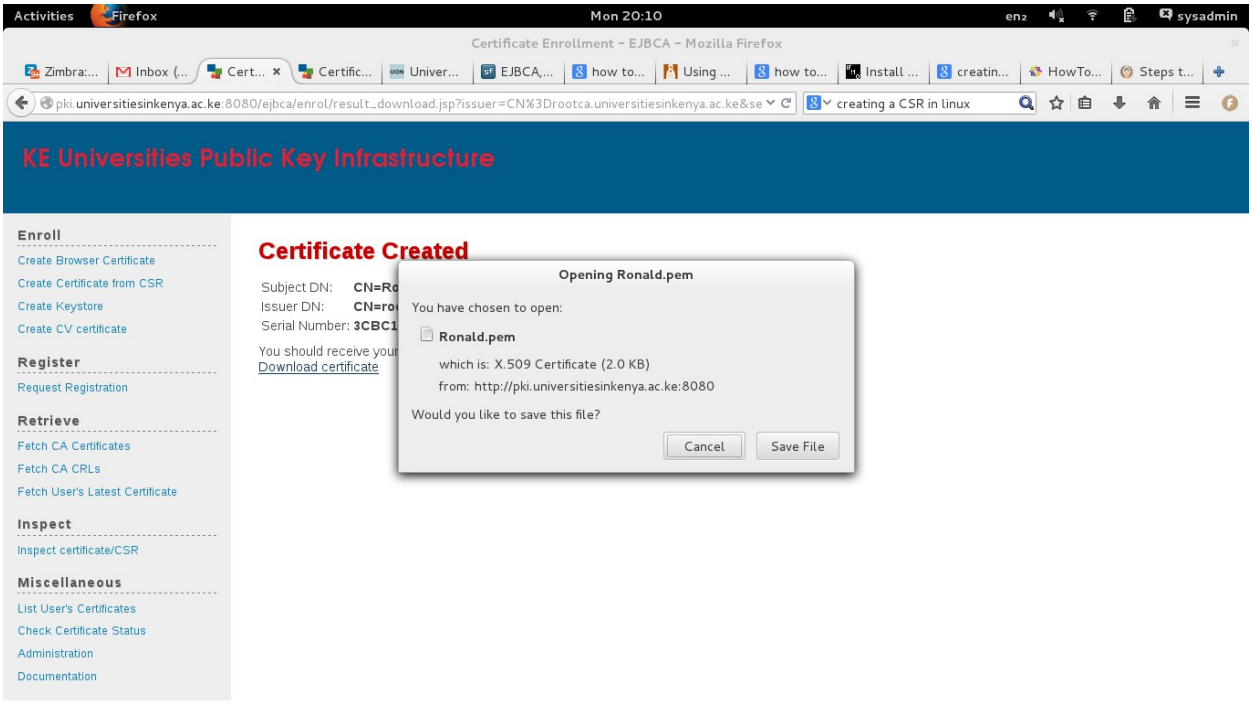


Once the CSR is generated, a user then needs to open the PKI portal and click on create certificate from CSR and paste the CSR on the appropriate field then click submit.

Figure 24: Certificate Enrolment

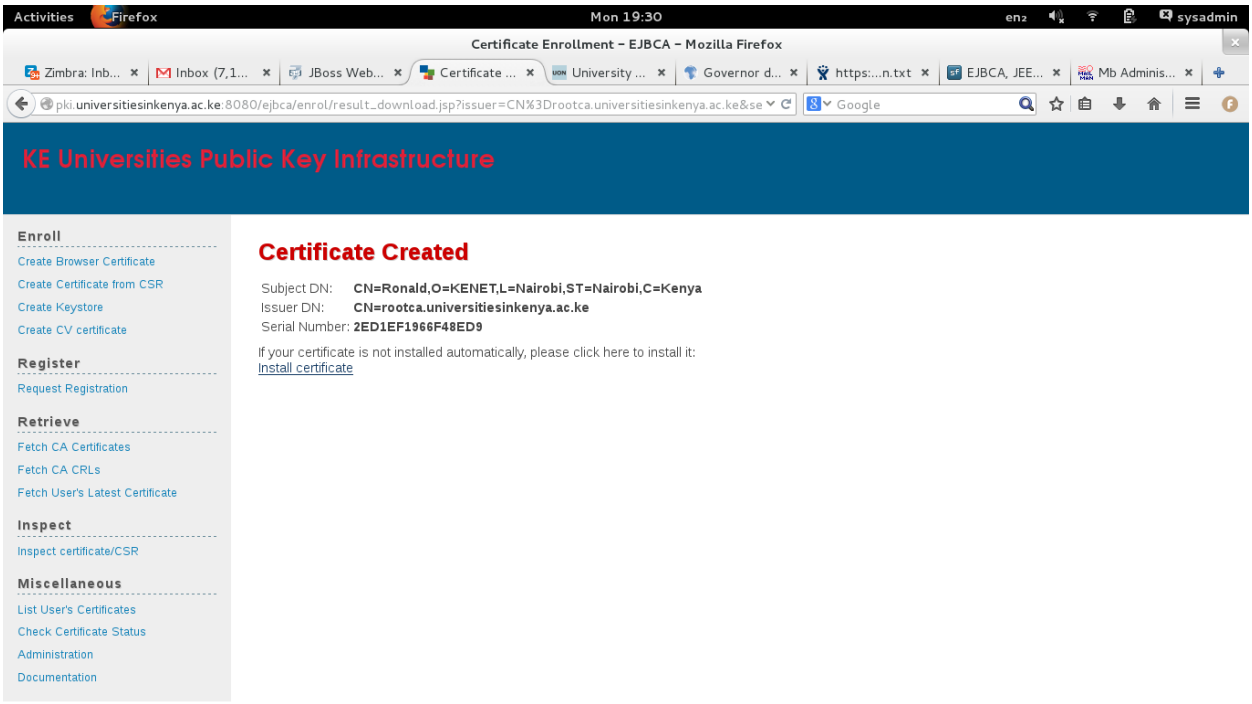


Then follow all the steps until the certificate is created and a prompt for saving the certificate comes up as shown below.



Create browser Certificates

To create browser certificates, users need to go to the PKI portal and click on the create browser certificate menu. They will then be prompted for the enrolment code issued by the Registration Authority during registration after which they are prompted to download or install the certificates.

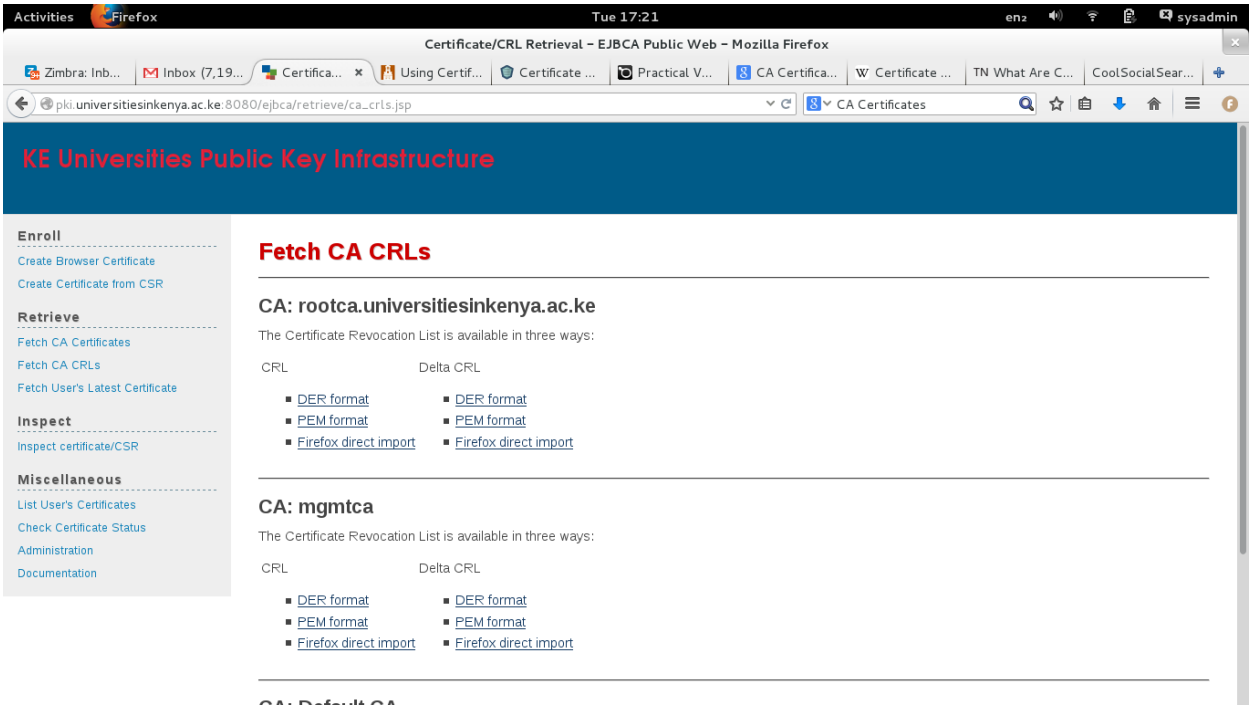


Once the certificate has been installed on the browser, it can be viewed. It can also be backed up for a later use or purpose.

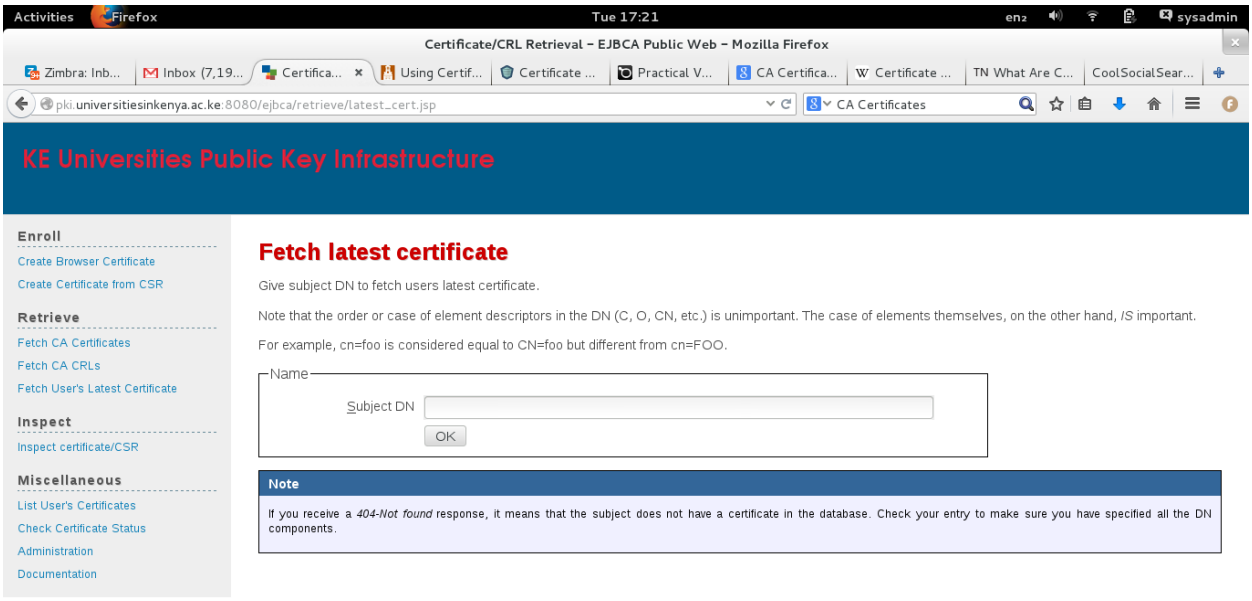
Figure 25: Certificate View

To view certificates an installed certificate in a browser, click view certificates in the browser tools menu.

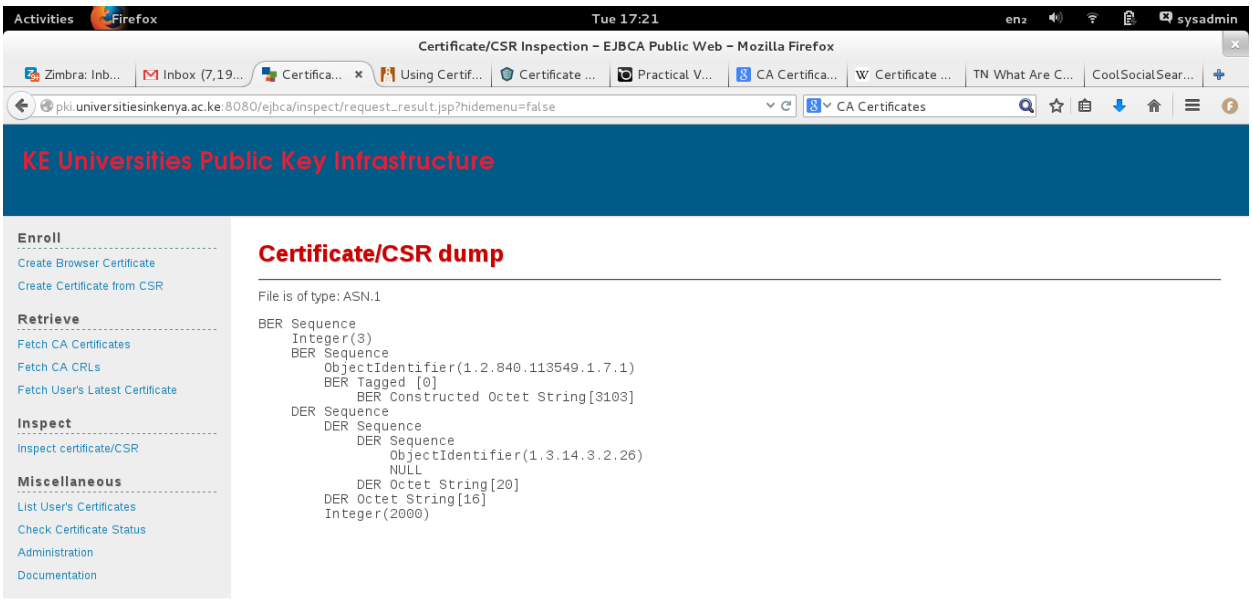
How to fetch CA CRLs



How to fetch latest user certificate



How to Inspect Certificate/CSR



CHAPTER 5: DISCUSSION

5.1 Introduction

PKI enables users of a basically insecure public network such as the Internet to securely and privately exchange data through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates.

5.2 PKI Usage in the university environment in Kenya

The developed system is able to perform the following:-

a) **Securing e-mail from unintended viewers**

This can be done using a mail client. It was tested on thunderbird mail client by following the following steps after the certificate and the key were downloaded.

Step 1: Start Thunderbird

Step 2: Open the Thunderbird certificates manager

Select the Thunderbird→Preferences menu item.

Select the Advanced tab.

Select the Certificates tab

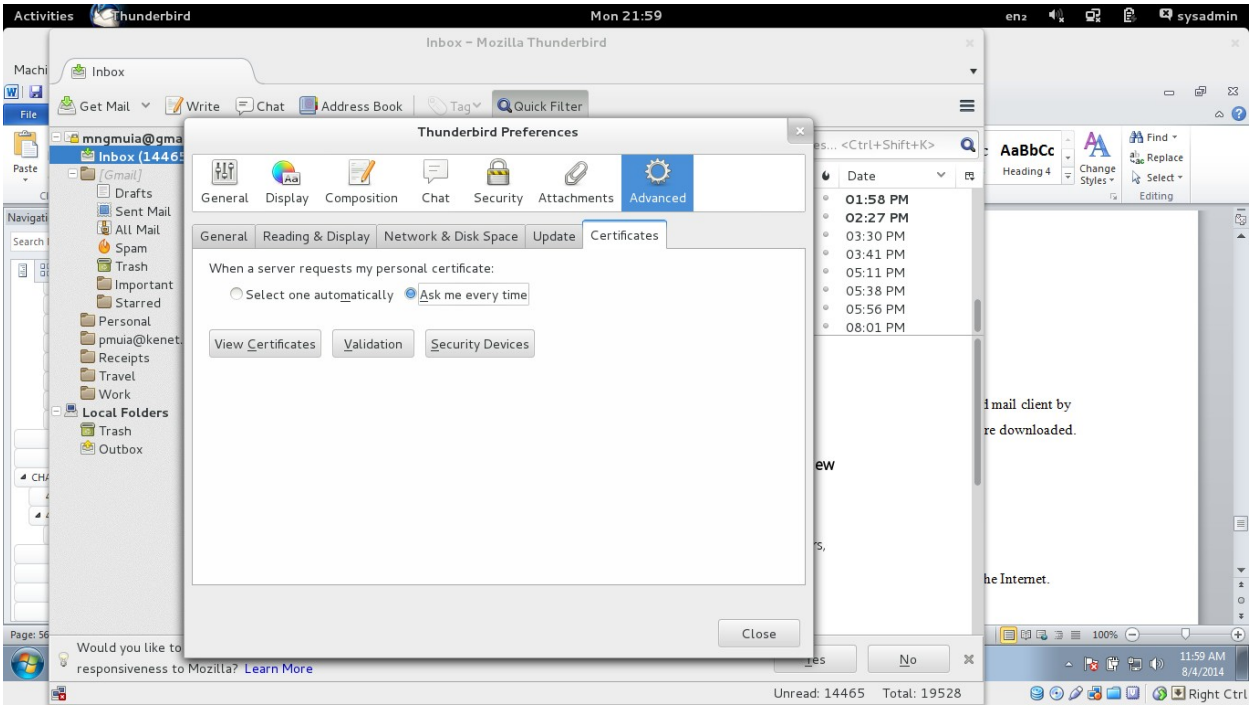
Step 3: Import your private key and certificates

Select the Your Certificates tab.

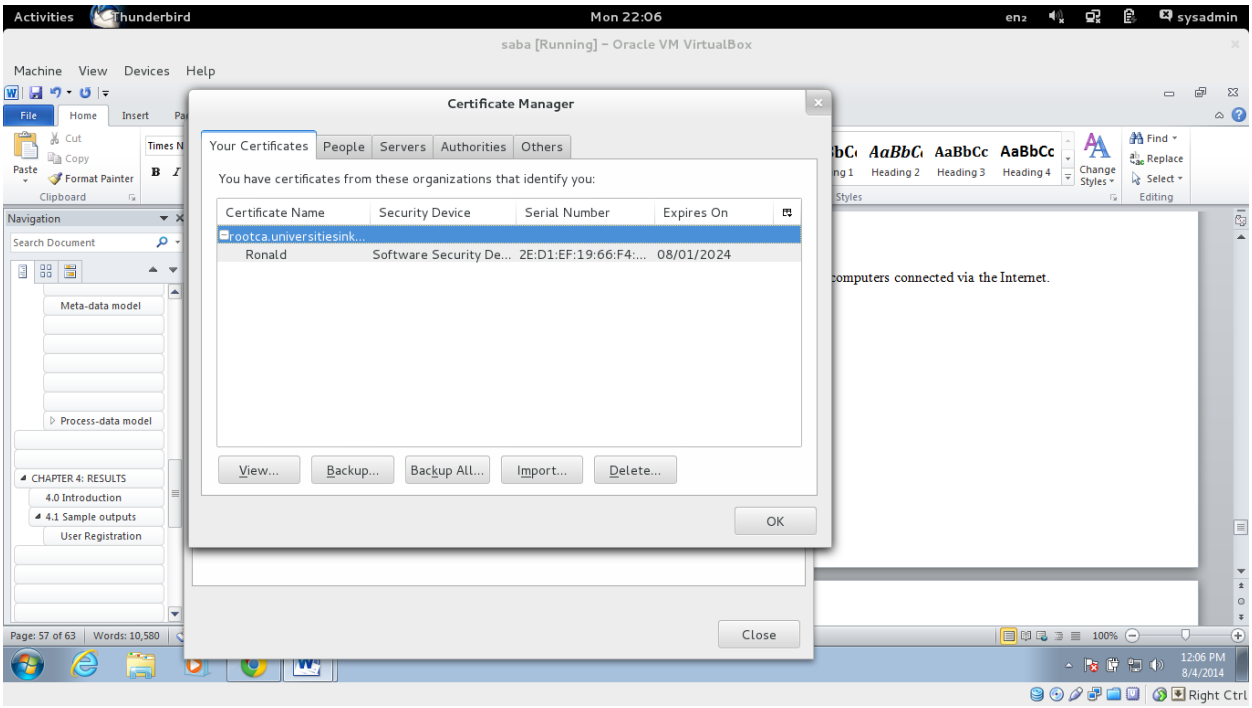
Click on the Import button

Open the PKCS#12 file where your private key and certificates was saved in.

Enter the password for the PKCS#12 file. This is the password you used to create the PKCS#12 file.



The certificate now appears under the list of Your Certificates. The private key is also stored in the certificate manager along with the certificate.



Step 4: Send secured emails

Compose a new email by using the Write icon in the toolbar, or use the File→New→Message menu item

Enable digital signing using the Digitally Sign This Message menu item, under the Options menu or under Security item in the toolbar of the write message window. Enable encryption using the Encrypt this Message menu item.

A small icon appears at the bottom right of the write message window when signing, encryption or both is enabled. This icon is looks like an envelope with a red wax seal.

Although the user interface allows one to select any combination of signing and encrypting, when a mail is it will then check whether that combination can be performed. One cannot send an encrypted email unless the certificates for the entire recipient are known to Thunderbird. So initially the first outgoing email messages will have to be sign only, because one does not yet have any certificates for their recipients.

Step 5: Receiving secured emails

When a secured email is received, it is shown with a envelope icon. The red seal indicates that

the signature is valid and the certificate of the signer is trusted by the email program.

b) Web Hosting Security - SSL Certificate on Apache

In order to secure Apache web server, the server needs to have Mod SSL installed and enabled. Request a certificate from the universities PKI system developed and create a folder in the webserver, say ssl

mkdir /etc/httpd/ssl

Edit Apache config file to point to the certificates ie

nano /etc/httpd/conf.d/ssl.conf

Include the following in the apache config file

ServerName example.com:443

SSLEngine on

SSLCertificateFile /etc/httpd/ssl/apache.crt

SSLCertificateKeyFile /etc/httpd/ssl/apache.key

c) Configuring Certificate-Based Authentication

Systems commonly require a username and password to be provided by the user to verify their identity. The SSL/TLS protocol (upon which HTTPS is based) provides a more secure and flexible alternative: certificate-based authentication.

Certificate-based authentication provides several advantages over traditional password-based authentication, but the primary difference is that while password-based authentication relies on secrets defined and managed by the user, certificate-based authentication utilizes secrets issued and managed by the server or, more accurately, the certificate issuer or authority.

Other advantages of certificates include

Certificates automatically expire at a given time. Certificates convey additional information about the holder, such as organizational unit, contact information etc. Certificates can't be

forgotten, as is the case with passwords (although they can be misplaced). The private key contained within a certificate is of high cryptographic strength. This is not generally the case with user-defined passwords, which can often be guessed. Passwords can be defeated using various techniques such as dictionary attacks that cannot be used with certificates.

The main disadvantages of certificates include:

Infrastructure is required to manage the issuing of certificates. Certificates require installation and management. Certificate-based authentication is often more complicated than password-based authentication. Anyone in possession of the certificate's private key is automatically granted access to the server. Certificates should therefore be distributed with care.

Authentication and Authorization

If an HTTPS server is configured to require a certificate then a client application will be unable to connect to the server unless the user can present a certificate that meets the server's requirements. The enforcement of the requirement for a certificate serves two purposes:

i. Only users with a valid certificate (i.e. server-issued proof of identity) can connect to the server.

ii. The user's identity is given by or can be derived from the certificate's contents. Thus certificates can be used for authentication, i.e. verifying (or authenticating) the identity of the user. Additional requirements can be placed on the client certificates to restrict access to those users authorized to access the server. Examples of requirements commonly placed on client certificates include:

- The certificate was issued by a certificate authority known to and trusted by the server.
- The certificate has not expired.
- The organization (or organizational unit) to which the user belongs (as defined by the certificate) is permitted access to the server or repository.

Thus certificates can also be used for authorization, i.e. to verify that the user is authorized to access the server.

d) Communication between servers using SSH and Digital Certificates

Steps

i. Create public and private keys using the developed PKI for universities and store in *~/.ssh*

ii. Copy the public key to remote-host using ssh-copy-id
scp id_rsa.pub <user>@<yourhost>:.ssh/authorized_keys

iii. Login to remote-host without entering the password

Certificates Revocation

The CRL store is used to get a Certificate Revocation List (a signed list of revoked certificates) for the CAs. If you want to revoke a CA you can do so by going to "Edit Certificate Authorities" in the admin GUI. There is a button "Revoke CA". If you revoke a Root CA it will revoke all certificates in the database issued by the root CA, and create a CRL. If you revoke a Sub CA it will revoke all certificates in the database issued by the sub CA, and to the sub CA, and create a CRL. This works automatically if the sub CA and root CA is handled by the same PKI instance.

5.3 Testing and Evaluation

In addition to prototyping development used, the system was given to users for testing and to provide a feedback of the final system. Additionally, an evaluation questionnaire was administered to access the level of satisfaction of the users with the system. The system was tested against an agreed upon performance criteria (See appendix six).

In addition to the questionnaire, the system was subjected to further tests as shown in the next table

Table 9: Prototype testing

No	Description	Expected Results	Observed Results	Comments
1	Throughput – To check whether it can handle multiple requests at the same time. This was done by making several requests from different machines.	To be able to handle several requests	Was able to handle multiple requests	Throughput level is acceptable

2	Response time – This test was carried out to check whether the time taken when a request is made to the system and the time it takes to reply was at an acceptable level. This was done using a stop watch.	Response time of less than 30 seconds	Average response time 15 seconds	Response time is acceptable
3.	Reliability – This was used to test whether the results of the system were consistent	System Reliable	System Reliable	Good
4.	Availability – Test carried out to check whether the system is always available when users need to use it.	System always available	System always available	Good

From the tests conducted, the system was found to be usable and acceptable hence can can be adopted by the university community in Kenya.

CHAPTER 6: CONCLUSION

The project entailed a study of the systems security of the university community in Kenya. Further, a Public Key Infrastructure for the university community was also developed. Architecture for developing PKI for a university environment was also developed. From the study done, cyber security is a serious threat and any technology that would help in mitigating this threat is highly welcome. It also showed that university ICT staff are aware of how they could use the infrastructure in their respective universities.

The Architecture developed included a root certification authority that with each of the universities running a certification authority signed by the root certification authority. The universities also act as registration authorities.

Using the system developed, users are able to request and obtain digital certificates that can be used for securing email, servers, web security and checking the validity of other certificates. Additionally, the certificates can be used for systems authentication whenever this capability in enabled.

A follow up study can be done to determine its adoption within the university community in Kenya and what can be done to increase this adoption.

6.1 Relationship to previous work

From the literature survey conducted, university of Croivea (Marius, 2011) has implemented a university PKI using OpenCA tool. This project developed a rootCA for the university community in Kenya using EJBCA. It relied on the concept developed by Rivest, Shamir, and Adleman in 1978 on public key cryptography.

6.2 Practical and theoretical implications

If adopted within the university community in Kenya, the developed PKI system will lead to improved security and trust when users interact with the systems within the university. Specifically a digital certificate and the infrastructure under which the digital certificate is issued will provide the information and structure needed to:

- minimise fraud by authenticating the identity of people via the Internet
- provide privacy of messages by minimising the risk that they can be read in transit, or by

anyone, other than the intended recipient

- assure the integrity of electronic communications by minimising the risk of them being altered or tampered with in transit without the recipient being aware
- Provide non-repudiation of transactions so that people cannot deny involvement in a valid electronic transaction.

From the study that was carried out in the universities in Kenya, the above formed some of the threats that the universities were experiencing hence the developed system will go along way in increasing security of systems and electronic communication within the universities in Kenya.

6.3 Achievements

The PKI system that was developed has been tested to be fully functional and users are able to perform the following:-

i. Request for certificates
ii. Inspect Certificates
iii. Download Certificates
iv. Enrol Certificates in a browser

The certificates generated can be used on browsers, servers or even on email in order to achieve the security goals of Confidentiality, Integrity and Non Repudiation within the universities.

6.4 Constraints

The Project only entailed the development of a PKI system. Universities will therefore need to come up with policies that can be used to govern the PKI in place. In addition, system developers within the university community will need to start incorporating the use of digital signatures in their systems design.

False Sense of Security - No matter how safe a public key cryptography system is, it only protects what it's designed to protect. Transfer of data is protected by a mixture of public and private key encryption and is extremely safe. However, once data is received, if a user leaves a computer with access to a server out in the open, someone could sit down at the keyboard, download all of the securely transferred data and steal it. Public key encryption won't protect against that and, as such, it's only a part of an overall security system.

6.4 Statement of Conclusion

Most systems in the universities in Kenya are now online and various technologies have been deployed to protect data in these systems. Universities are aware and are ready to adopt the use of PKI to increase the level of security in these services especially for online transactions and online communication. This would also reduce the cost of paper and the bulkiness currently involved in official communications.

The architecture used to develop the system was designed in a user centred approach using the DSDM Agile methodology. The system was later tested with twelve universities and thus can be adopted by the rest of the university community in Kenya.

There is need to protect both the information systems and electronic communication within the university environment. There are many factors that affect systems security in a university environment. Threats are getting sophisticated by the day and universities need to employ defence in depth strategy in order to reduce chances of successful attacks and also to protect user data. The developed PKI system can be used to provide an extra layer of security to the already existing security mechanisms within the university community

References

1 A. Jancic, M.J.Warren, Miss, 2004. PKI - *Advantages and Obstacles. Post Graduate*. United States: We-B Centre & Edith Cowan University.

2 Commission for University Education - Home. 2014. *Commission for University Education - Home*. [ONLINE] Available at: http://cue.or.ke/. [Accessed 09 June 2014].

3 Dhillon, A. (2000). *Group Dynamics Meet Cognition: applying socio-technical concepts in the design of information systems*. London: Springer, p119-125.

4 Ives B., Hamilton S., Davis, G. (1980); *A Framework for Research in Computer-Based Management Information Systems*; Management Science, Vol. 26, No. 9 (pp. 910- 934)

5 Kowalski S. (2003). *Do Computer Security Models Model Computer Crime: An Emperical Study*. Canadian Computer Security Symposium. 5 (1), p2-6.

6 Marius, Mr., 2011. *Implementing a Public Key Infrastructure for the Academic Environment*, 12, 1-6.

7 Meoli Kashorda, Timothy Waema, Prof., (2014). *E-Readiness Survey Report*. In E-Readiness Survey. Nairobi, 1st May 2014. 1st May 2014: KENET. 1-100.

8 SERIANU, TEAM, 2012. *Kenya Cyber Security Report 2012*. Kenya Cyber Security Report, [Online]. 1, 1-28. Available at: http://www.serianu.com/ [Accessed 08 July 2014].

9 White, J.W. & Kowalski, R. (1994). *Security by Consensus*. In Security Models, 1994. .

10 Zulkifli, Mr., (2007). *Evolution of Cryptography*. In Cryptography. New York, 17 January 2007. New York: Mohd Zaid . 1-6.

APPENDICES

Appendix One: Sample code

Start mail.properties ###.

mail.jndi-name=java:/EjbcaMail
mail.user=mngmuia
mail.password=XXXXX
mail.smtp.host=localhost
mail.smtp.port=25
mail.from=mngmuia@gmail.com
mail.contentencoding=UTF-8

database.properties

Start database.properties

---------- Database configuration ----------

#This variable is used in our standalone.xml <datasource> stanza
datasource.jndi-name=EjbcaDS

# This is the TYPE of db, not the NAME OF the db
database.name=mysql

# Be sure to use utf-8
database.url=jdbc:mysql://127.0.0.1:3306/ejbcadb?characterEncoding=UTF-8
database.driver=com.mysql.jdbc.Driver

database.username=ejbcadbuser

```
# Change this to your mysql user password:
database.password=XXXXX

### End database.properties ###


<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
<%@ taglib uri="http://java.sun.com/jsp/jstl/core" prefix="c" %>
<%@ page pageEncoding="ISO-8859-1"%>
<% response.setContentType("text/html;
charset="+org.ejbca.config.WebConfiguration.getWebContentEncoding()); %>
<%@page errorPage="/errorpage.jsp" import="
org.ejbca.config.GlobalConfiguration,
org.ejbca.ui.web.RequestHelper,
org.ejbca.ui.web.admin.configuration.EjbcaJSFHelper,
org.ejbca.core.model.authorization.AccessRulesConstants
"%>
<jsp:useBean id="ejbcawebbean" scope="session"
class="org.ejbca.ui.web.admin.configuration.EjbcaWebBean" />
<jsp:setProperty name="ejbcawebbean" property="*" />
<%  // Initialize environment
        GlobalConfiguration globalconfiguration = ejbcawebbean.initialize(request,
AccessRulesConstants.ROLE_ADMINISTRATOR,
AccessRulesConstants.REGULAR_ACTIVATECA);
        EjbcaJSFHelper.getBean().setEjbcaWebBean(ejbcawebbean);
%>
<html>
<head>
  <title><c:out value="<%= globalconfiguration.getEjbcaTitle() %>" /></title>
```

```
  <base href="<%= ejbcawebbean.getBaseUrl() %>" />
  <link rel="stylesheet" type="text/css" href="<%= ejbcawebbean.getCssFile() %>" />
  <meta http-equiv="Content-Type" content="text/html; charset=<%=
org.ejbca.config.WebConfiguration.getWebContentEncoding() %>" />
</head>

<f:view>
<body>
        <h1><h:outputText value="#{web.text.ACTIVATECAS}"/></h1>
        <div class="message"><h:messages layout="table" errorClass="alert"/></div>
        <h:form>
        <h:dataTable value="#{cAActivationMBean.authorizedTokensAndCas}"
var="tokenAndCa" styleClass="actCas" footerClass="actCasFooter"
headerClass="actCasHeader">
                <h:column>
                        <f:facet name="header"><h:panelGroup><h:outputText
value="#{web.text.CRYPTOTOKEN}"/><br/><h:outputText
value="#{web.text.ACTIVATECAS_NAME}"/></h:panelGroup></f:facet>
                        <h:outputLink rendered="#{tokenAndCa.first &&
tokenAndCa.cryptoToken.existing}" value="adminweb/cryptotoken/cryptotoken.jsf?
cryptoTokenId=#{tokenAndCa.cryptoToken.cryptoTokenId}&ref=caactivation">
                                <h:outputText
value="#{tokenAndCa.cryptoToken.cryptoTokenName}"/>
                        </h:outputLink>
                        <h:outputText rendered="#{!tokenAndCa.first}"
value="#{tokenAndCa.cryptoToken.cryptoTokenName}"/>
                        <h:outputText rendered="#{!tokenAndCa.cryptoToken.existing}"
style="font-style: italic;" value="#{web.text.ACTIVATECAS_NA}"/>
                </h:column>
                <h:column>
                        <f:facet name="header"><h:panelGroup><h:outputText
```

```
value="#{web.text.CRYPTOTOKEN}"/><br/><h:outputText
value="#{web.text.ACTIVATECAS_STATE}*"/></h:panelGroup></f:facet>
                    <h:panelGroup rendered="#{tokenAndCa.first}">
                        <h:graphicImage
rendered="#{tokenAndCa.cryptoToken.cryptoTokenActive}" url="adminweb/images/status-ca-
active.png" height="12" width="12" style="border-width:0"/>
                        <h:graphicImage rendered="#{!
tokenAndCa.cryptoToken.cryptoTokenActive}" url="adminweb/images/status-ca-offline.png"
height="12" width="12" style="border-width:0"/>
                        <h:outputText value=" #{web.text.ACTIVE}"
rendered="#{tokenAndCa.cryptoToken.cryptoTokenActive}"/>
                        <h:outputText value=" #{web.text.OFFLINE}" rendered="#{!
tokenAndCa.cryptoToken.cryptoTokenActive}"/>
                    </h:panelGroup>
                    <h:outputText rendered="#{!tokenAndCa.first}" escape="false" value="
&#12291;"/>
                </h:column>
                <h:column>
                    <f:facet name="header"><h:panelGroup><h:outputText
value="#{web.text.CRYPTOTOKEN}"/><br/><h:outputText
value="#{web.text.ACTIVATECAS_ACTION}"/></h:panelGroup></f:facet>
                    <h:panelGroup rendered="#{tokenAndCa.first}">
                        <h:selectBooleanCheckbox
value="#{tokenAndCa.cryptoToken.cryptoTokenNewState}"
disabled="#{tokenAndCa.cryptoToken.stateChangeDisabled}"/>
                        <h:outputText value=" #{web.text.ACTIVATECAS_KEEPACT}"
rendered="#{tokenAndCa.cryptoToken.cryptoTokenActive}"/>
                        <h:outputText value=" #{web.text.ACTIVATE}" rendered="#{!
tokenAndCa.cryptoToken.cryptoTokenActive}"/>
                    </h:panelGroup>
                    <h:outputText rendered="#{!tokenAndCa.first}" escape="false" value="
```

```
&#12291;"/>
                </h:column>
                <h:column>
                        <f:facet name="header"><h:panelGroup><h:outputText
value="#{web.text.CA}"/><br/><h:outputText
value="#{web.text.ACTIVATECAS_NAME}"/></h:panelGroup></f:facet>
                        <h:outputText value="#{tokenAndCa.ca.name}"/>
                </h:column>
                <h:column>
                        <f:facet name="header"><h:panelGroup><h:outputText
value="#{web.text.CA}"/><br/><h:outputText
value="#{web.text.ACTIVATECAS_SSTATE}"/></h:panelGroup></f:facet>
                        <h:graphicImage rendered="#{tokenAndCa.ca.active}"
url="adminweb/images/status-ca-active.png" height="12" width="12" style="border-width:0"/>
                        <h:graphicImage rendered="#{!tokenAndCa.ca.active}"
url="adminweb/images/status-ca-offline.png" height="12" width="12" style="border-width:0"/>
                        <h:outputText value="#{web.text.ACTIVE}"
rendered="#{tokenAndCa.ca.active}"/>
                        <h:outputText value="#{web.text.EXPIRED}"
rendered="#{tokenAndCa.ca.expired}"/>
                        <h:outputText value="#{web.text.REVOKED}"
rendered="#{tokenAndCa.ca.revoked}"/>
                        <h:outputText value="#{web.text.OFFLINE}" rendered="#{!
tokenAndCa.ca.active && !tokenAndCa.ca.expired && !tokenAndCa.ca.revoked}"/>
                </h:column>
                <h:column>
                        <f:facet name="header"><h:panelGroup><h:outputText
value="#{web.text.CA}"/><br/><h:outputText
value="#{web.text.ACTIVATECAS_SACTION}"/></h:panelGroup></f:facet>
                        <h:selectBooleanCheckbox value="#{tokenAndCa.ca.newState}"
disabled="#{tokenAndCa.ca.unableToChangeState}"/>
```

```
                    <h:outputText value=" #{web.text.ACTIVATECAS_KEEPACT}"
rendered="#{tokenAndCa.ca.active}"/>
                    <h:outputText value=" #{web.text.ACTIVATE}" rendered="#{!
tokenAndCa.ca.active}"/>
                </h:column>
                <h:column>
                    <f:facet name="header"><h:panelGroup><h:outputText
value="#{web.text.CA}"/><br/><h:outputText
value="#{web.text.ACTIVATECAS_MONITORED}"/></h:panelGroup></f:facet>
                    <h:selectBooleanCheckbox
value="#{tokenAndCa.ca.monitoredNewState}" disabled="#{!
tokenAndCa.cryptoToken.existing}"/>
                    <h:outputText value="#{web.text.ACTIVATECAS_HCHECK}"/>
                </h:column>
                <f:facet name="footer">
                    <h:outputText value="* #{web.text.ACTIVATECAS_FOOTNOTE}
(#{web.ejbcaWebBean.hostName})."/>
                </f:facet>
            </h:dataTable>
            <h:panelGrid columns="3">
                <h:outputLabel rendered="#{cAActivationMBean.activationCodeShown}"
for="authCode" value="#{web.text.ACTIVATECAS_ACTCODE}:"/>
                <h:inputSecret rendered="#{cAActivationMBean.activationCodeShown}"
id="authCode" value="#{cAActivationMBean.authenticationCode}"/>
                <h:commandButton action="#{cAActivationMBean.applyChanges}"
value="#{web.text.APPLY}"/>
            </h:panelGrid>
        </h:form>

        <%/* Include footer */%>
        <jsp:include page="<%= globalconfiguration.getFootBanner() %>" />
```

```
</body>
</f:view>
</html>

<%@taglib uri="http://java.sun.com/jsp/jstl/core" prefix="c"%>
<%@page pageEncoding="ISO-8859-1" errorPage="errorpage.jsp"%>
<%@page import="org.ejbca.config.GlobalConfiguration"%>
<%@page import="org.ejbca.config.WebConfiguration"%>
<%@page import="org.ejbca.core.model.authorization.AccessRulesConstants"%>
<%@page import="org.ejbca.ui.web.RequestHelper"%>
<% response.setContentType("text/html;
charset="+WebConfiguration.getWebContentEncoding()); %>
<html>
<jsp:useBean id="ejbcawebbean" scope="session"
class="org.ejbca.ui.web.admin.configuration.EjbcaWebBean" />
<jsp:setProperty name="ejbcawebbean" property="*" />
<%   // Initialize environment
  GlobalConfiguration globalconfiguration = ejbcawebbean.initialize(request,
AccessRulesConstants.ROLE_ADMINISTRATOR);
%>
<head>
  <title><c:out value="<%= globalconfiguration.getEjbcaTitle() %>" /></title>
  <base href="<%= ejbcawebbean.getBaseUrl() %>" />
  <link rel="shortcut icon" href="<%=ejbcawebbean.getImagefileInfix("favicon.png")%>"
type="image/png" />
  <link rel="stylesheet" type="text/css" href="<%= ejbcawebbean.getCssFile() %>" />
  <meta http-equiv="Content-Type" content="text/html; charset=<%=
WebConfiguration.getWebContentEncoding() %>" />
</head>

<frameset rows="100,*" cols="*" frameborder="NO" border="0" framespacing="0">
```

```
  <frame name="<%= globalconfiguration.HEADERFRAME %>" scrolling="NO" noresize
src="<%= globalconfiguration.getHeadBanner() %>" >
  <frameset cols="250,*" frameborder="NO" border="0" framespacing="0" rows="*">
    <frame name="<%= globalconfiguration.MENUFRAME %>" noresize scrolling="NO"
src="<%= globalconfiguration.getAdminWebPath() +
                                                    globalconfiguration.getMenuFilename()
%>">
    <frame name="<%= globalconfiguration.MAINFRAME %>" src="<%=
globalconfiguration.getAdminWebPath() + globalconfiguration.getMainFilename() %>">
  </frameset>
</frameset>
<noframes>
<body>
  <h1><%= ejbcawebbean.getText("ERRORNOBROWSER") %></h1>
</body>
</noframes>
</html>
```

Appendix Two: Sample Screen displays

Figure 26 : User registration

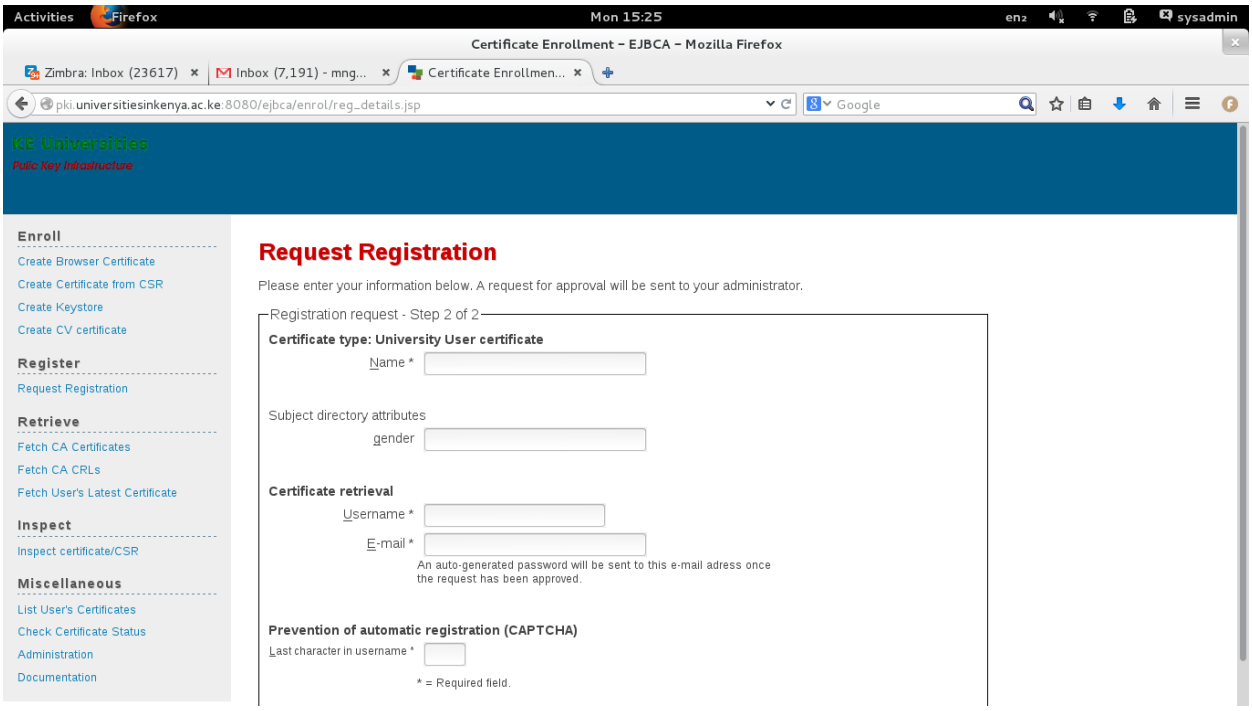


Figure 27 : Fetching CA CRLs

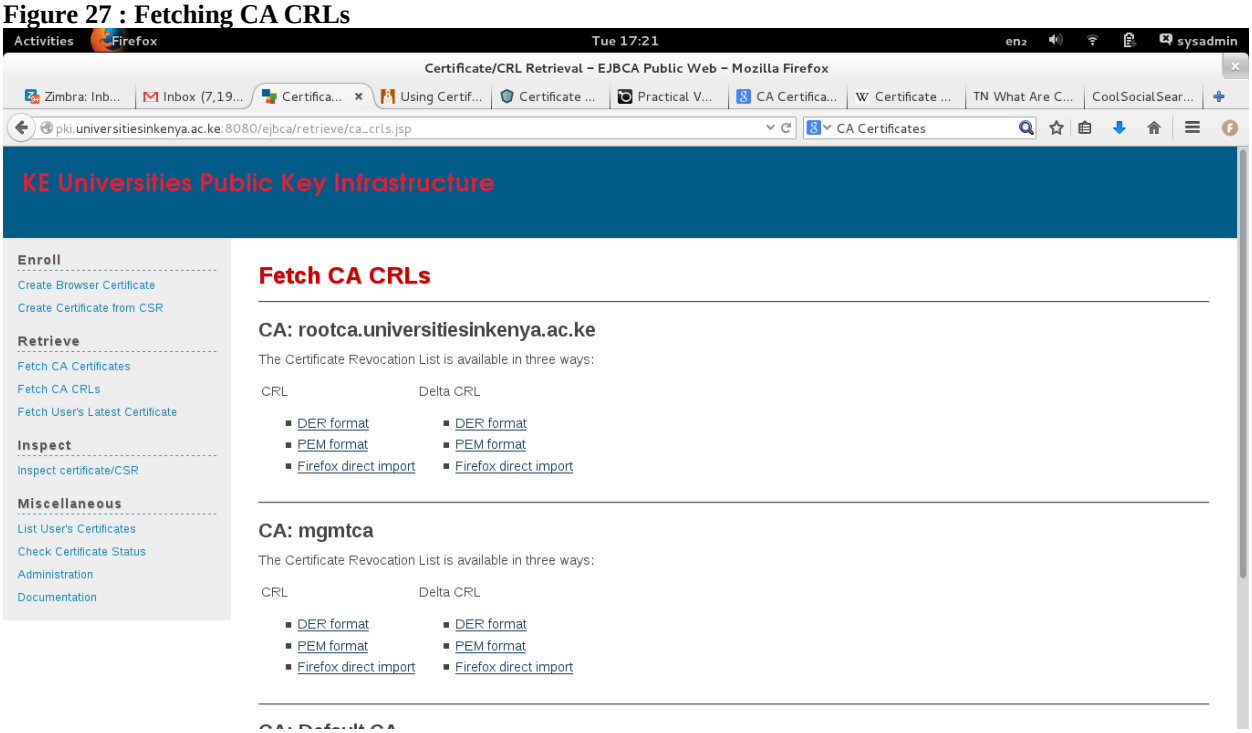
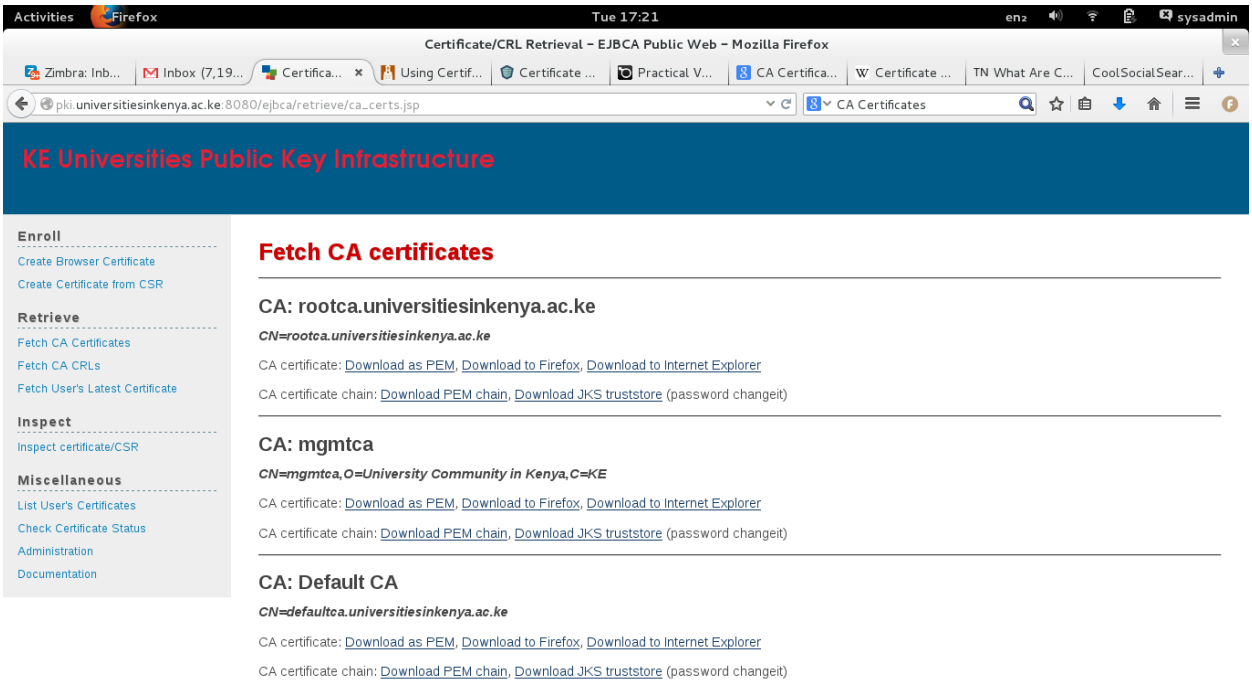


Figure 28 : Fetching CA certificates


Activities
Firefox
Tue 17:21
en2
sysadmin
Certificate/CRL Retrieval – EJBCA Public Web – Mozilla Firefox
Zimbra: Inb...
Inbox (7,19...
Certifica...
Using Certif...
Certificate ...
Practical V...
CA Certifica...
Certificate ...
TN What Are C...
CoolSocialSear...
pki.universitiesinkenya.ac.ke:8080/ejbca/retrieve/ca_certs.jsp
CA Certificates
KE Universities Public Key Infrastructure
Enroll
Create Browser Certificate
Create Certificate from CSR
Retrieve
Fetch CA Certificates
Fetch CA CRLs
Fetch User's Latest Certificate
Inspect
Inspect certificate/CSR
Miscellaneous
List User's Certificates
Check Certificate Status
Administration
Documentation
Fetch CA certificates
CA: rootca.universitiesinkenya.ac.ke
CN=rootca.universitiesinkenya.ac.ke
CA certificate: Download as PEM, Download to Firefox, Download to Internet Explorer
CA certificate chain: Download PEM chain, Download JKS truststore (password changeit)
CA: mgmtca
CN=mgmtca,O=University Community in Kenya,C=KE
CA certificate: Download as PEM, Download to Firefox, Download to Internet Explorer
CA certificate chain: Download PEM chain, Download JKS truststore (password changeit)
CA: Default CA
CN=defaultca.universitiesinkenya.ac.ke
CA certificate: Download as PEM, Download to Firefox, Download to Internet Explorer
CA certificate chain: Download PEM chain, Download JKS truststore (password changeit)

Appendix Three: ICT Staff Questionnaire

UNIVERSITY OF NAIROBI

SCHOOL OF COMPUTING & INFORMATICS

MSC PROJECT

A Public Key Infrastructure (PKI) for the Higher Education Institutions in Kenya

A survey of the current systems security in the higher education community in Kenya: Questionnaire for ICT staff.

Kindly answer the following questions. The answers given will be treated as private and confidential and will only be used for the purpose of developing theory for the project.

13) Section One: Demography

Date …….

University Name ……

Designation ……

14) Section Two: University Systems Awareness

Does your university use information systems and electronic communication? *(Tick where appropriate)*Yes …… No ……

Kindly name four systems that your university has implemented?

……

……

……

……

……

……

15) Section Three: University Systems Security

Kindly highlight some of the threats/Vulnerabilities experienced by the university systems……

……

……

……
……

Are you aware of security features employed on the university systems?

(Tick where appropriate) Yes …….No. ……

Kindly name four systems security features used by the university e.g. passwords, biometrics etc.

……
……
……
……
……

8. Kindly tick where appropriate

	Strongly disagree		Agree		Strongly Agree
	1	2	3	4	5
I feel secure using the university systems					
I feel secure using the university email					
I am aware of PKI technology					
I feel users private data stored in the university systems is secure					
I feel university servers are secure					
There has been successful cyber attacks in the university systems before					

Users are happy with the security deployed at the university application					
Sensitive and confidential documents are sent via email					
Sensitive and confidential documents sent via email in the university are secure					
I feel digital certificated can be used to secure university systems and electronic data communication					
There is no system in the university where students can register to request for digital certificates					

9. Kindly explain how you think PKI can be used to increase the security situation at the university

.....
.....
.....
.....
.....

10. Do you have an ICT policy within your university? YESS …….NO…….

What does the policy say about

PKI?.....
.....

.....

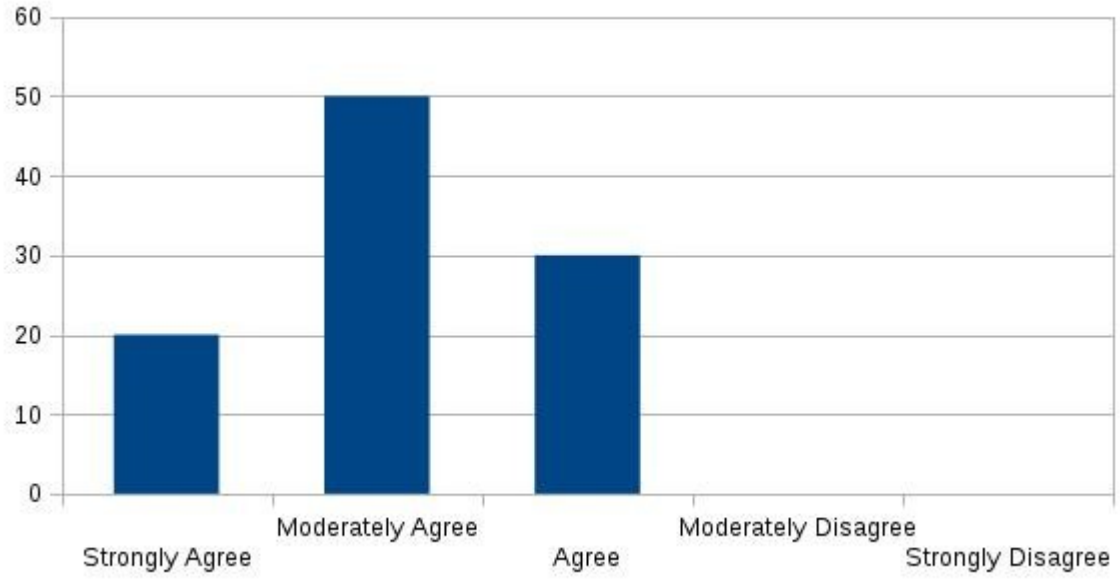
Thank you

Appendix Five: Sample Collected data

Table 10 : Perception of security while using email

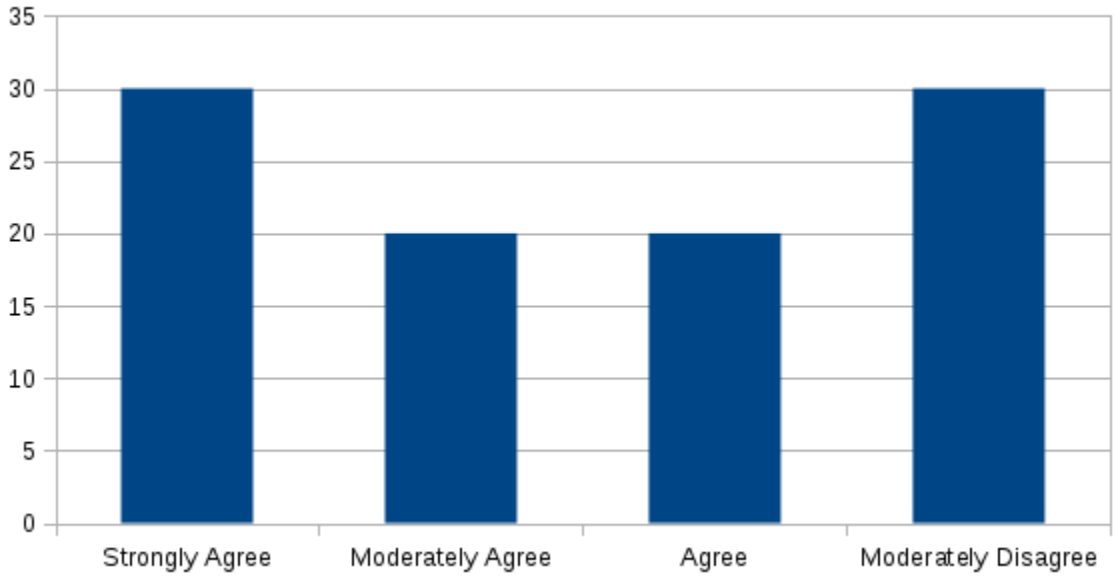
Answer	Percentage
Strongly Agree	20
Moderately Agree	50
Agree	30
Moderately Disagree	0
Disagree	0

Figure 29: Perception of security while using email



Successful attacks in the universities

Answer	Percentage
Strongly Agree	30
Moderately Agree	20
Agree	20
Moderately Disagree	30
Disagree	0



ci

Appendix Six: Testing questionnaire

1. Do you think the prototype is easy to use?

Yes -90% No – 10%

2. If yes, what did you find easiest to do?

Sample answers

User registration

Certificate request

Certificate downloading

3. Why is it easy to use

Sample answers

Easy navigation

Users are led very well

4. If no, what do you think made the interface not easy to use

Sample answers

No proper documentation

5. Is the interface appealing

Yes - 90% No -10%

6. What is the most appealing in the system?

Sample answers

Good user experience

The way information is packaged

The system can be used anytime

7. What would you want to remove from the interface to make it better for you?

Answers

Nothing

8. Do you think this application is useful to you?

Yes - 95% No – 5 %

If it is do you think you would use it frequently?

Yes - 100% No – 0%

9. Is there anything about this system that you think is useless

Yes – 0% No – 0%