Design and implementation of a private certificate authority: a case study of Telkom Kenya Limited

Deborah M. Rioba
Faculty of Information Technology (FIT)
Strathmore University

DESIGN AND IMPLEMENTATION OF A PRIVATE CERTIFICATE AUTHORITY

A Case Study of Telkom Kenya Limited.

Deborah M. Rioba

Student Number: 54460

A Proposal submitted in partial fulfillment of the requirement of Degree of Masters of Science in Information System Security (MSc. ISS)

Faculty of Information Technology

Strathmore University

Nairobi, Kenya

May, 2018

Declaration

This dissertation as presented is my original work and has not been presented for any award in any other university.

Student Name: Deborah M. Rioba

Student Number: 54460

Signature……...

Date: ……...

This work has been submitted with my approval as the University Supervisor

Supervisor Name: Dr. Joseph Sevilla

Signature……

Date:……

Dedication

This work is dedicated to all those that made it possible for me to successfully do it to completion. These include my lecturers for enriching interactions throughout this study, classmates and family for their trust and encouragement.

Most important, to God, without whom I would not have made it this far.

Acknowledgements

I would like to acknowledge my supervisor Dr. Joseph Sevilla, for his support throughout this research. To, @iLabAfrica and Strathmore University for the opportunity and exposure they have provided during my study period. Thank you to my mother Eunice Rioba for her great sacrifice and immense support. Finally, to Kyle Pillay, Head of IT, Telkom Kenya whose support was key to my accomplishment.

Abstract

Public Key Infrastructure (PKI) provides confidentiality and integrity to an enterprise and its customers. Applications accessed through corporate network needs to be protected when in transit and hence the need for a Certificate Authority (CA). Most enterprises currently purchase digital certificates from other Certificate Authorities, for instance Comodo, Symantec, Digicert, Thwate, GoDadddy, etc. Others purchase through third parties for instance Cloud Productivity Solutions in Kenya who then get their digital certificates from GeoTrust. These certificates are used to guarantee secure communication when accessing services on servers within an organisation. The main challenge of buying of the certificates is the high purchase cost of single or Subject Alternative Name (SAN) certificates. By having their own Certificate Authority, digital certificates would cost less and give an enterprise the means to control large numbers of Digital Certificates for SSL, authentication, document signing, S/MIME (Secure/Multipurpose Internet Mail Extensions) and other usages of digital signatures. This implies that costs would be reduced by generation of enterprise-owned digital certificates instead of purchasing them.

By understanding the current infrastructure in place, a CA was created for generation distribution and revocation of SSL certificates. This would replace purchasing of certificates signed by other public Certificate Authorities.

This dissertation sought to design, develop and implement a comprehensive CA as per the X.509 standard for the purpose of generation of certificates for internal use for corporates and selling of the same to generate revenue so as to cut on costs incurred on purchase of digital certificates. Also a proof of concept of a private CA was used to validate the certificate authority with security of the Certificate Authority being considered.

KEYWORDS: Public Key Infrastructure, Certificate Authority, SSL, Digital Signature

List of Acronyms

CA	Certificate Authority
CAPEX	Capital Expenditure
CIA	Confidentiality, Integrity, Availability
CPS	Certificate Practice Statement
CSR	Certificate Signing Request
KES	Kenya Shillings
LDAP	Lightweight Directory Access Protocol
PKCS	Public Key Cryptographic Systems
PKI	Public Key Infrastructure
HSM	Hardware Security Module
ITU-T	International Telecommunication Union-Telecommunication Section
GUI	Graphical User Interface
S/MIME	Secure/Multipurpose Internet Mail Extensions
SAN	Subject Alternative Name
SSL	Secure Sockets Layer
UML	Unified Modelling Language
OCSP	Online Certificate Status Protocol
ACME	Automated Certificate Management Environment

Table of Contents

List of Figures

List of Tables

Chapter 1: Introduction

1.1 Background of Study

Data stored on a network or transmitted from one user to another must be protected from fraudulent access and misdirection, hence the importance of security. Public Key Infrastructure (PKI) refers to the technical mechanisms, procedures and policies that collectively provide a framework for addressing authentication, confidentiality, integrity and non-repudiation. PKI utilises these two core elements: Public Key Cryptography and Certification Authorities. Binding of digital certificates is established through a process of registration and issuance of certificates at and by Certificate Authority which may be automated or carried out under human supervision.

In public key cryptography, a public key is known to all while the private key is only known to the owner. Since the two keys are mathematically related, whatever is encrypted with a public key may only be decrypted by its corresponding private key in the key pair (Brink, 2002) and whatever is encrypted with a private key is decrypted by its corresponding public key in the key pair.

The use of enterprise-owned Certificate Authority can be an effective way to meet business requirements. The ease of installation, use, maintenance and cost of a Certificate Authority solution can help enterprises determine the solution that best meets their requirements. It is important to review the components of a CA before addressing requirements and solutions.

One of the primary concerns identified by both businesses and consumers in establishing and participating in e-business is the potential loss of assets due to security breaches of commercial transactions and corporate computer systems. A security breach not only erodes confidence in the business but also affects the organisation's reputation capital. Case studies demonstrate risks that include sabotage, vandalism, loss of data confidentiality and integrity, theft of data, fraud and breaches of privacy (Verizon, 2017).

When using the digital certificates to secure servers (for instance web servers), certificates that are generated are used to provide an end-to-end secure flow of communication. A certificate establishes trust between the client, server and issuer of certificates (Certificate Authority), as well as insuring this protection of data in transit (Gigovic, 2014).

1.1.1 X.509 Standard

Since the introduction of this standard for PKI, X.509 standard had been used in generation of digital certificates. This has become a critical part for enterprises, government and consumers. When selecting an X.509 solution, organisations must consider not only the robustness of the technology and the reputation of the provider, but also affordability of the solution and the cost-savings it can provide (Entrust, 2005).

In the original X.509 standard, PKI is referred to as *strong authentication* leveraging a family of cryptographic systems known as Public Key Cryptographic Systems (PKCS). The standard does not necessitate a specific encryption algorithm, but describes itself as a framework applicable to any suitable public key cryptosystem (Melone, 2012).

This standard specifies formats for public key certificates, certificates revocation lists, attribute certificates and certificate path validation algorithm.

1.1.2 Other Applications of Digital Certificates

Digital Signature

This is based on public key cryptography where one can generate two keys that are mathematically linked: one public and another private as a pair. The private key is used to generate a digital signature attached to a message, and the receiver uses the sender's certificate to verify the digital signature (CGI Group Inc, 2004). This gives a recipient reason to believe that the message was created by a known sender (authentication), the sender cannot deny having sent the message (non-repudiation) and that he message was not altered in transit (integrity).

Encryption of Documents

In this, a certificate can be used implicitly for purposes of encryption whereby, the sender of a digital message uses the receiver's certificate to encrypt the message so as to protect the message to protect the confidentiality of the message. Only the receiver can use his/her private key to decrypt the message.

Organisations and people that use computers can describe their needs for information security and trust in systems in terms of three major requirements: confidentiality, integrity and availability. A

Certificate Authority is generally considered to be associated with the four factors, confidentiality, integrity, authentication and non-repudiation.

When an enterprise is responsible for the safe keeping of third party information, the burden of care goes up and the risks go up with it. Certificate Authority enables distribution, management, expiration, rollover, backup and revoking of public/private keys. The owners/users of these keys can be people, devices or applications. There are options of purchasing single certificates and/or multi-domain certificates known as unified communications certificate (UCC) which is multi-domain certificates, whereby they allow one to secure a primary domain, and up to 99 additional Subject Alternative Names (SAN), in a single UCC.

Today in Kenya most enterprises purchase digital certificates to secure transactions for the services accessed by the public through a browser and alternatively use self-signed certificates for the internally accessed services since these have already formed a web of trust among themselves. However, the purchase price of these digital certificates is quite high and hence the need for a cheaper option. Table 1.1 gives a summary of digital certificate prices that are valid for one year from different Certificate Authorities.

Table 1.1 Digital Certificate Prices

Digital Certificate Provider	Product Name	1Year Price	Type	Encryption
Comodo CA	Positive SSL	$49.95	One Domain	128/256 bit
Go Daddy	Standard SSL	$69.99	One Domain	128/256 bit
Comodo CA	Instant SSL	$99.95	One Domain	128/256 bit
Comodo CA	Comodo SSL	$99.95	One Domain	128/256 bit
Go Daddy	Deluxe SSL	$99.99	One Domain	128/256 bit
Thwate	Thwate 123	$149.00	One Domain	128/256 bit
Geotrust	Quick SSL Premium	$149.00	One Domain	128/256 bit
Comodo CA	Positive SSL Wildcard	$149.95	Wildcard	128/256 bit
Comodo CA	Premium SSL	$179.95	One Domain	128/256 bit
Thwate	SSL Webserver Certificate	$199.00	One Domain	128/256 bit

Geotrust	TrueBusiness ID	$199.00	One Domain	128/256 bit
Go Daddy	Premium SSL	$99.99	One Domain	128/256 bit
Global Sign	Domain ServerSign	$249.00	One Domain	128/256 bit
Thwate	Webserver Certificate with EV	$299.00	One Domain	128/256 bit
Geotrust	TrueBusiness ID with EV	$299.00	One Domain	128/256 bit
Go Daddy	Standard SSL Wildcard	$299.99	Wildcard	128/256 bit
Globalsign	Organisation ServerSign	$349.00	One Domain	128/256 bit
Symantec	Secure Site SSL	$399.00	One Domain	128/256 bit
Go Daddy	Deluxe SSL WildCard	$399.00	Wildcard	128/256 bit
Comodo CA	EV SSL Certiticate	$249.00	One Domain	128/256 bit
Comodo CA	Premium SSL Wilcard	$449.95	Wilcard	128/256 bit
Comodo CA	Comodo SSL Wildcard	$449.95	Wildcard	128/256 bit
Thwate	Wildcard SSL Certificate	$559.00	Wildcard	128/256 bit
Geotrust	TrueBusiness ID wildcard	$599.00	Wildcard	128/256 bit
GlobalSign	Domain Serversign Wildcard	$849.00	Wilcard	128/256 bit
GlobalSign	Organisation Serversign Wildcard	$949.00	Wildcard	128/256 bit
Symantec	Secure Site Pro	$995.00	One Domain	128/256 bit
Symantec	Secure Site Pro with EV	$1499.00	One Domain	128/256 bit

The challenge for many organisations is how to bridge the gap from their current IT infrastructure, to enhanced security using a Certificate Authority. A Certificate Authority can be either in-house or managed (outsourced). An in-house one is implemented by operating a private CA which gives maximum level of control. Also, interoperability problems between the CA and the corporate applications are minimised and the issue of Certificate Revocation Lists (CRLs) is greatly simplified. A managed CA solution gives access to digital certificates without the need to buy, establish, operate and protect an in-house CA. On the other hand, external CAs receives certificate requests from individual enterprises and validates the domain through the local registration authority, KENIC (Kenya Network Information Centre) .KE domains. This is possible since KENIC grants license for reselling of .KE domains to other registrars. Once this is done the external CA issues, distributes and stores the certificates and keeps the CRL up-to-date.

The main challenge with not owning a Certificate Authority is the cost involved in buying the certificates. Also, it costs almost nothing to generate digital certificates. The major requirement would be to abide by the law of the land; in this case, it would be The Kenya information and Communications Act 2010 which stipulates the terms and conditions for anything that involves electronic transaction. Let's Encrypt, which is a free and open certificate authority in 2017 had 96.7 % of the 15,270 issued certificates used for phishing sites (Lync, 2017). Also its limited since it can only be used for web servers. This therefore leaves out S/MIME and client certificates as options not taken care of by Let's Encrypt.

In conclusion, implementation of a Certificate Authority requires proper planning in terms of cost, future applications that may need to support with the CA. However, this is not mandatory since applications that the CA may support may not have been conceived yet. This therefore implies that a CA should incorporate a lot of flexibility.

1.1 Problem Statement

The cost of a digital certificate depends on whether it is a single certificate (which translates to more money spent in the long run) or a multi-domain certificate. Based on this, there is need to propose a solution that will allow enterprises to manage their own Certificate Authority for generation of digital certificates at a much lower cost. A wildcard certificate through a third party costs approximately KES. 315,000. Also, for a multi-domain digital certificate which can have a maximum of four digital certificates costs approximates KES. 75,000 through the same third party, both of which are valid for two years.

Based on this, there was need to propose a solution that would allow enterprises to have their Certificate Authority for management of digital certificates. This was proposed for the services used internally by the enterprise and selling solely to the enterprise customers so as to cut down on digital certificate purchase cost.

1.2 Research Objectives

i. To identify challenges in the Public Certificate Authority,
ii. To review Certificate Authority tools,
iii. To design, implement and test a private Certificate Authority by use of a prototype,
iv. To validate the prototype.

1.3 Research Questions

i) What are the challenges experienced with a Public Certificate Authority?

ii) What tools exist for private Certificate Authorities implementation?

iii) How can a Certificate Authority be designed and developed to reduce Certificate costs?

iv) Does the prototype provide a secure and cost effective alternative for private companies?

1.4 Scope of Study

This study entailed conducting a research on the costs implication of having a private Certificate Authority in an enterprise rather than buying of digital certificates. This also involved consideration for selling the certificates solely to their enterprise customers who would be on-boarded on to their network in the process of offering managed security services. This involved designing and implementation of a prototype that could be customized into a full solution based on the needs of any enterprise.

In the building of the prototype, the research sought to create a virtualised system that would be used for the purpose of replicating how the Certificate Authority would be in use in a real environment: by generation, distribution, revocation, use and management of digital certificates using Telkom Kenya Limited as a case study.

1.5 Limitations

The main limitation was getting trust from other Certificate Authorities. It is easy to focus only on Certificate generation, treat it as just another piece of infrastructure, focus on quality of service, uptime and resilience. However, what makes a Certificate Authority special is that it forms the trust anchor for all the systems and applications that rely on the credentials that it issues. Trust is like beauty, it is subjective and contextual- It is in the eyes of the beholder (Moulds, 2016). This is dependent on how certificates are handled (issued, published, archived, revoked and renewed) and is usually defined in the Certification Practice Statement (CPS) (Boeyen, 1997). Building trust involves certificate chains and path validation. One of the ways of building trust in a larger community of trusted certificates involves declaring trust in a group of top level (root) CAs (Haine, 2013). The main challenge in this was gaining trust from other intermediate CAs so as to eliminate 'Untrusted errors'.

1.6 Justification of Research

Most Kenyan enterprises that have the need for digital certificates spend a large amount of money buying certificates every so often. However, implementing a private Certificate authority enables an enterprise to generate their own certificates and thereby reduce the cost of purchase of digital certificates by generating certificates for internal use and selling certificates solely to their enterprise customers. Other than cost benefits, the enterprise gets to control the full Certificate Authority architecture.

1.7 Summary

The Certificate Authority technology has majorly assisted in the accomplishment of integrity, confidentiality, authentication and non-repudiation. In this chapter, the challenge of costs of digital certificates from other Certificate Authorities was looked into, which enabled the problem statement to be outlined inclusive of the objectives of this research. In the next chapter, literature in the Certificate Authority which mainly relies on Public Key Infrastructure, design and implementation was reviewed.

Chapter 2: Literature Review

2.1 Introduction

Completely securing the enterprise today requires more than just purchasing a digital certificate. Picking the right Certificate Authority is not always a straight forward process. Price is a factor as IT budgets continue to feel the squeeze (Flavio, 2015). Most enterprises have in the past concentrated on buying of digital certificates from other Certificate Authorities and have not exploited the need to set up their own Certificate Authority.

2.2 X.509 Standard

Certificate Authority is part of PKI which is governed by the X.509 standard published by International Telecommunication Union (ITU-T). The X.509 is used for public key management, including distributing of digital certificates with a high degree of confidence in binding between the users and their public keys (Chokhani, 1996).

The information included in an X.509 certificate is:

i. Version: This is the version of the certificate
ii. Serial Number: A unique identifier assigned by the CA to the certificate
iii. Signature algorithm: This is the hashing algorithm used for digital signature o the certificate.
iv. Issuer: This is the Certification Authority that issued the certificate
v. Valid from: The date of issuance of the Certificate
vi. Valid to: This is the expiry date of the certificate
vii. Subject: This is the distinguished name of the owner of the certificate
viii. Public Key: This is the public key which is associated with the private key
ix. Thumbprint algorithm: This is the algorithm used to create the certificate hash
x. Thumbprint: The hash of the certificate which is used for positive identification of the certificate

The X.509 certificate allows an extension field that permits any number of additional fields to be added to the certificate. Certificate extensions provide a way of adding information such as alternative subject names and usage restrictions to certificates (Rouse, 2009).

2.3 Design of Systems

The design of systems gives the existing design model of the Certificate Authority and what it entails. This section mainly covers the creation, storage and distribution of digital certificates and processes thereof.

2.3.1 Certificate Authority

This is the entity that digitally signs certificates. It validates requestor's (web servers, users, computers etc.) identity, issues certificates, and maintains certificate status information regarding certificates and issues. It is assumed that a RA (Registration Authority) is part of both the root CA and the Intermediate CA. The role of the RA is to pre-authenticate user identities based on physical world artifacts, and communicate the user identity (consisting) of set attributes to the CA. In reality, the RA can be separate from the CA in which case, additional trust relationships between the CA and the RA are required (Josang, 2013).

2.3.2 Trust Models

Certificate Authority (CA) has a well-structured hierarchical trust model. This is mainly based on path validation, which is the process of verifying the integrity of the certificate chain up to a trusted CA (SANS, 2013)

a. General Trust Model

A public key on a certificate can allow a message encoded with the public key's corresponding private key to be read. Therefore, the public key of the root CA certificates in the browser can be used to read the signature of their child CA issued certificates. This way each certificate issued by the chain can be verified and authenticated, implying the certificate issued to the web server can be verified and the identity of the server can be authenticated (Geraint, 2015).

i) Root Certificate Authority

The root CA's private key sign certificates it issues. The root certificate is a self-signed certificate that identifies the root CA. The most common commercial variety is based on the ITU-T X.509 standard (Trusted Root Certificate, 2012) . A root Certificate is the top-most certificate of the tree, the private key of which is used to sign other certificates, which may include intermediate CAs,

issuing CAs and policy CAs. All certificates immediately below the root certificate inherit the trustworthiness of the root certificate. Root CAs does not issue certificates for users or devices.

To minimize the risk of unauthorised access, the root CA is usually put offline. It is powered off after generation of the root certificate to intermediate CAs and also place in a physically secure place (Microsoft, 2011).

ii) Intermediate CA

This is subordinate to a high-level CA and is designed to issue certificates to other CAs. It is used as a proxy since the root CA must be kept behind layers of security, ensuring its keys are absolutely inaccessible (GoDaddy, 2015).

iii) Issuing CA

This CA issues certificate to users, devices and applications. It may perform the function of a policy CA if one is not above it in the CA hierarchy.

iv) Policy CA

This CA describes the policies and procedures that an organisation implements to ensure processes that validate the identity of certificates holders, and the processes that enforce the procedures that manage certificates are in place. A policy CA issues certificates only to other CAs which upon receiving these certificates must uphold and enforce the policies that the policy CA defined (Lintner, 2002).

It is not mandatory to use policy CAs unless different sectors of an organisation require different issuance policies and procedures. However, if an organisation requires different issuance policies and procedure, a policy CA must be added to hierarchy to define each unique policy (Wiseman, 2012).

2.3.3 CA Hierarchy Options

Single/One-tier Hierarchy

This consists of a single CA, usually consisting of both the root CA and issuing CA. Since the root CA is the trust anchor, any applications, users and/or computers that trust the root CA also trust any certificates issued by the CA

Two-Tier Hierarchy

This consists of an offline root CA which is the root instance of the CA trust chain. The first Active Directory Certificate Service (AD CS) instance installed will need to be the root CA since it establishes the trust hierarchy (Remy, 2016).

It also consists of a subordinate CA which is a child node in the PKI trust chain. This is one level under the root CA.

Three-Tier Hierarchy

This hierarchy model consists of three layers. This has the root, intermediate and issuing CA separately. In this intermediate CAs are also referred to as policy/subordinate CAs. Assuming that the root CA is trusted, the issuing CA validates the intermediate CA, which in turn validates the issuing level. The issuing level CA in turns validates the individuals to whom the CA issues certificates, (Neubauer, 2003). Each level provides a certificate to the level below it and defines policies that govern things for instance certificate use and lifetimes. This therefore forms a certificate chain as shown in Figure 2.1.

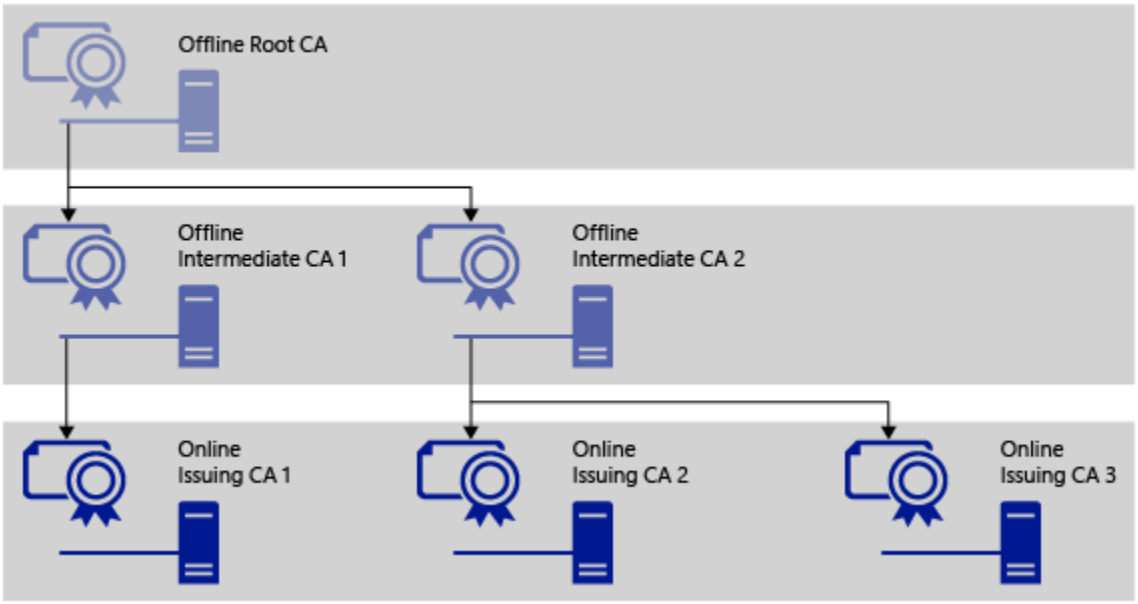


Figure 2.1 CA Hierarchies (Microsoft, 2016)

2.4 Digital Certificate Trust Chain

A Certificate Trust Chain begins with Digital Certificate and each Certificate in the chain is signed by the entity identified by the next certificate in the chain. This chain terminates with the Root CA Certificate which is signed by the Root CA itself. The signatures of all certificates in the chain must be verified up to the Root CA Certificate. Figure 2.2 indicates the trust chain concept.

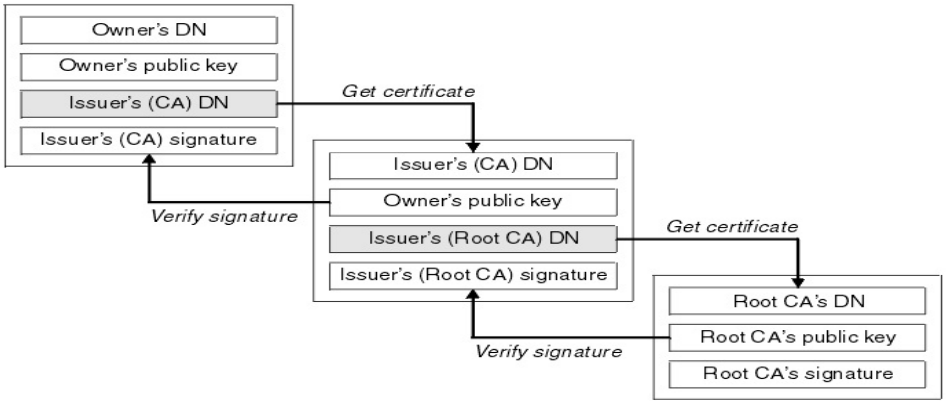


Figure 2.2 Certificate Trust Chain (Symantec, 2017)

Any compromise on the Certificate Authority translates to untrusted Certificates hence the Certificates have to be revoked. Case in point is where Symantec issued one hundred and eight credentials in violation of strict industry guidelines that the organisation agreed to abide by when it made the mistake in 2015 (Hruska, 2017). Nine of the certificates were issued without the permission or knowledge of the affected domain orders, while the other ninety nine were issued to companies with fake data (Goodin, 2017). Also, the number rose from one hundred and twenty-seven to thirty thousand certificates issued over a period spanning several years. Due to this, the Extended Validation (EV) status of all Certificates issued by Symantec-owned CA will no longer be recognised by the Chrome browser for at least a year (starting January 2017) until Symantec fixes its certificate issuance process so that it can be trusted again (Sleevi, 2017). The distrust of all existing Symantec-issued certificates would be gradual requiring that they be replaced over time with new, fully revalidated certificates, compliant with the current Baseline Requirements.

2.5 Let's Encrypt

This is a free, automated and open certificate authority that uses ACME protocol to make it possible to set up an HTTPS server and have it automatically obtain a browser-trusted certificate

(Let's Encrypt, 2016). The main restriction with this is that it only offers certificates for web servers only for HTTPS communication. Also, a risk with this setup is certificate miss-issuance whereby a CA issues a certificate to an unauthorized person. Despite Let's Encrypt complying with industry standards, offering free certificates offered an attractive environment for phishers. In the period between January 1st, 2016 and March 6th, 2017 Let's Encrypt had issued a total of 15,270 SSL certificates containing the word PayPal. Based on a random sample, 96.7% of these certificates were intended for use on phishing sites (Lync, 2017).

2.6 Public Key Infrastructure in Kenya

PKI in Kenya has seen tremendous changes in the near past. The Government of Kenya has a role to promote confidence and trust in the use of ICTs as a key driver of economic development. This is by extension ensuring that online business transactions are more secure. In 2013, there was a plan to implement the National Public Key Infrastructure (NPKI), funded by the World Bank under the Kenya Transparency and Communications Infrastructure Project (KTCIP) which would provide the legal basis for both natural and legal persons (Mbuvi, 2013). With digital signatures, the Government hopes that Kenya will build a significant competitive edge by gaining access to services such as e-government. Therefore one would be able to be issued with their drivers' license through online information systems (Angeng'o, 2013) and for enabling e-Government. PKI creates a safe online environment using electronic signature. Therefore the National PKI will enable and foster the development of various applications incorporating digital signature and hence lead to a trusted environment over open networks, (Communications Authority of Kenya , 2013). So as to achieve some of the goals under ICT this is one of the pillars of Vision 2030.

Concerns have been raised over the security of having to store the root CA for Kenya's PKI at Communications Authority of Kenya (CAK). This is because in the proposed framework, CCK will be both the licensing authority as well as the licensed, operator of the root CA. The conflict of interest is evident and also the end-to-end integrity of a structure that ensures top-down accountability is rendered completely void. The government should consider adopting a 'public-private Partnership' for the implementation of an NPKI to avoid this and also free the Root CA from these issues.

2.7 Financial Return on Investment

Reductions in cost are the most reliable drivers of financial returns for PKI-enabled applications, since they are easy to quantify, hence its popularity. Cost-based financial returns are expressed as a combination of cost saving, cost avoidance, efficiency and effectiveness.

So as to know the financial return on investment, a business case analysis needs to be done which is beyond financial metrics. This may include security needs, business needs, and associated risks and qualitative benefits resulting from investment (Hamilton, Booz Allen &, 2000). Figure 2.3 gives the cost considerations of a CA.

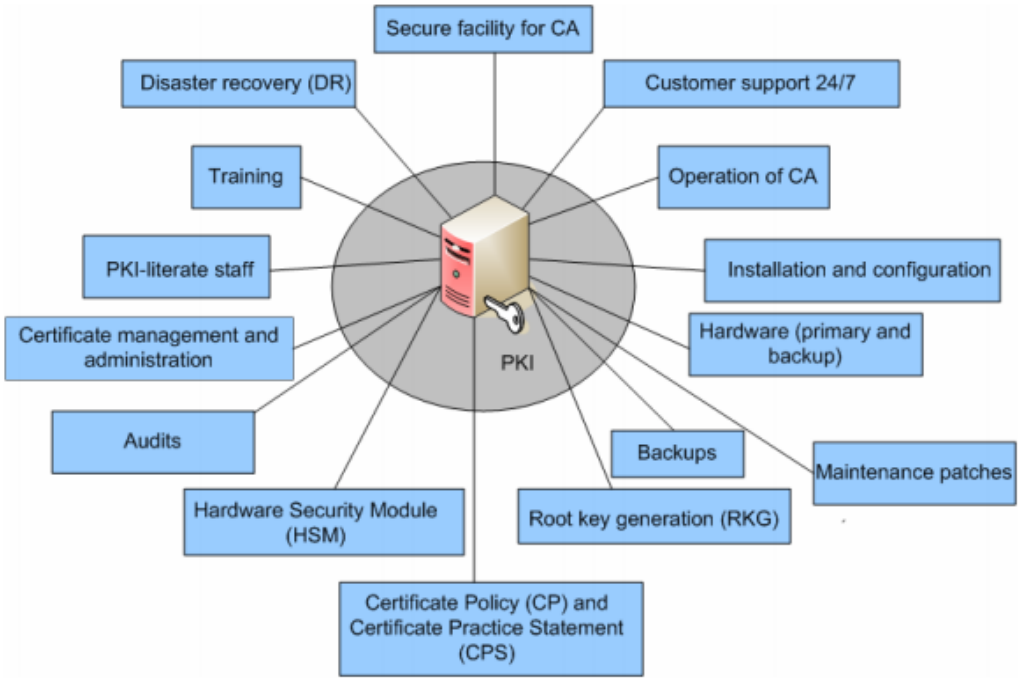


Figure 2.3 Cost Considerations for Private CA (Entrust, 2009)

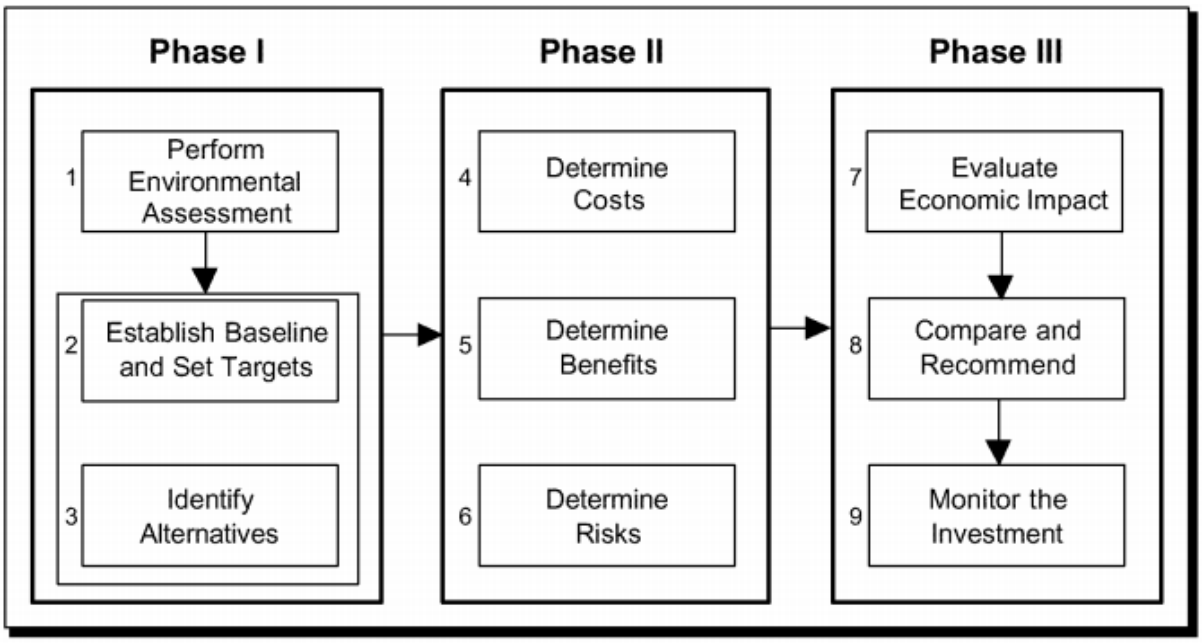


Figure 2.4 Business Case Analysis Methodologies for Certificate Authority (Hamilton, Booz Allen &, 2000)

At its core any business case analysis is founded on comprehensive economic analysis: thus, the business case methodology will examine Certificate Authority in the context of its investment worthiness as well as its technical feasibility as shown in Figure 2.4

2.8 Current Certificate Authority Tools

This section reviews two proposed options for setting up private Certificate Authority. The ease of use and integration with existing environments are the pointers to selecting an appropriate CA setup.

2.8.1 Enterprise Java Beans Certificate Authority

This is CA software built on java technology and is run on Linux as the underlying operating system. It supports browser-based certificate creation and revocation as well as direct interaction with underlying enterprise java beans (EJBs). It stores its certificate in either an SQL database or an LDAP directory (Sunsted, 2002) .

2.8.2 Windows Server 2012 Certificate Authority

This can run several services on a single server. Therefore, the CA would be run within a domain controller for easy distribution of certificates to endpoints within the domain controller. This supports manual and automatic Certificate enrollment and status functions (SANS, 2013).

2.8.3 Linux Based OpenSSL Certificate Authority

This is a CA that will be created using OpenSSL which is a free and open-source cryptographic library that provides several command-line tools for handling digital certificates.

2.9 Conclusions

From the reviewed literature, having an enterprise owned CA would provide a platform through which certificates can be generated for internal use whereby the enterprise would have control over all issued certificates, including renewal and revocation. Since enterprises would be able to generate their own certificates, then the cost of purchasing Digital certificates would be eliminated. Also the most convenient tool to use for implementing a CA would be Windows server 2012 R2 since this is a CA that can be installed, configured and managed that's built on the operating system and also have easy distribution to end hosts since it can be integrated with the domain controller.

Chapter 3: Research Methodology

3.1 Overview

The research aims at designing and implementing of a private Certificate Authority and how it would save costs for an enterprise. In this chapter the researcher explains the research methodology that was used, the stages in the research and justifies the research framework and the method. It focuses on the research design, types of data, data collection techniques and test design.

3.2 Research Methodology Steps

This research employed the Waterfall methodology which is a linear approach to software development (Lotz, 2013). Since the researcher will be doing a sequential development, the Waterfall methodology will give an exceptional development process. The first step was used to identify challenges in the Public Certificate Authority so as to show cause for the research so as to achieve the first objective. The second step was used to achieve the second objective of reviewing CA tools. The third, fourth and fifth steps were used to achieve the third objective through design, prototyping and testing of the prototype of both the functional and non-functional requirements. The last step was used to validate whether the research addressed the problem statement. This methodology is illustrated in Figure 3.1.

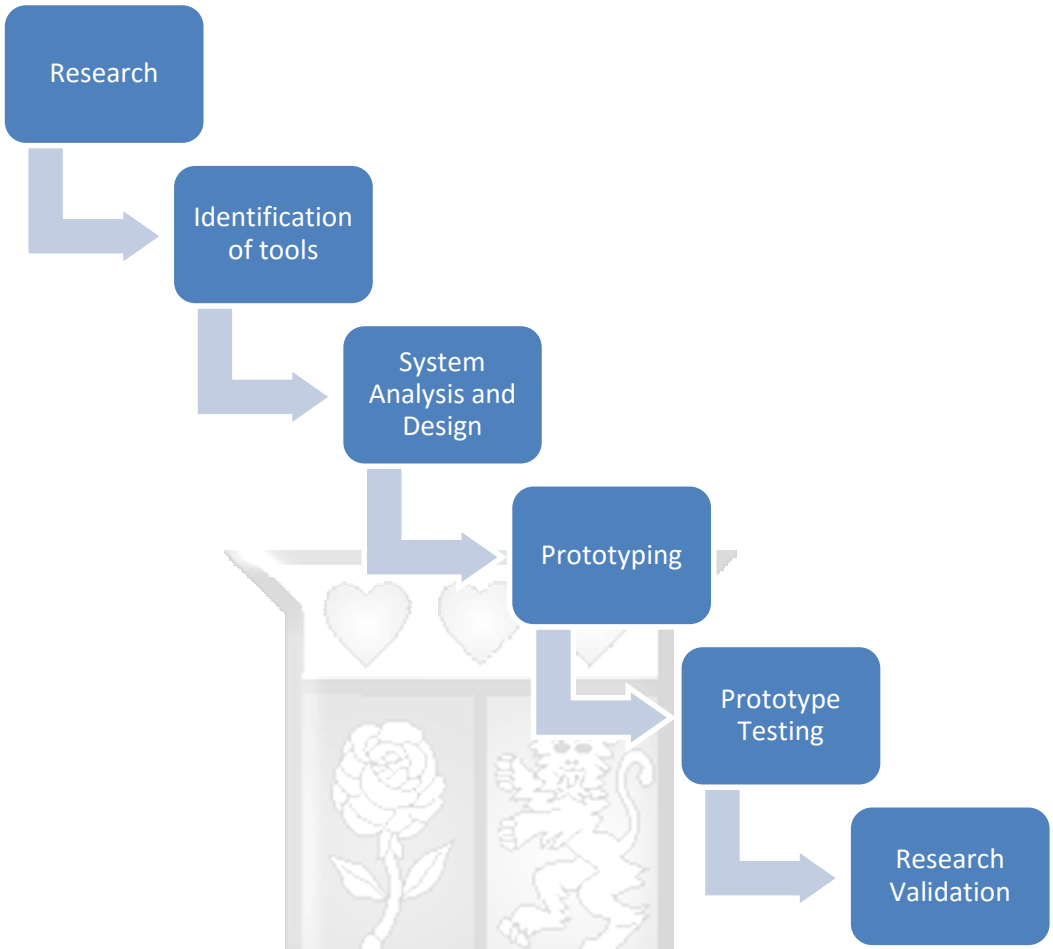


Figure 3.1 Research Methodology Steps (Lotz, 2013)

The research design incorporated mainly quantitative research methods. Quantitative research was used to get a better understanding of current cost implications of buying digital certificates and getting the feedback from users on how user friendly the system was.

3.2.1 Research

System requirements were gathered through document and journal review and analysis of current systems. Personal interviews were conducted so as to get feedback on how the digital certificates are used and cost implication of purchasing digital certificates. The data collected was then analysed which showed the need for the proposed application. Due to the restricted number of the target population, the researcher interviewed system administrators within Telkom Kenya Limited. The researcher used Microsoft office spreadsheets for quantitative data analysis.

3.2.2 Certificate Authority Identification of Tools

This step was used for identification of tools that would most appropriately suit the research which was based on the preliminary requirements identified in the research step. The tools were identified through document and journal review. This enabled the researcher to come up with the suitable tools for the implementation of the prototype.

3.2.3 Prototype Design

The Certificate Authority design was achieved based on collected information on system requirements and detailed analysis of the existing frameworks. Also, in this section, the researcher used workflow diagrams, use case diagrams, sequence diagrams and data flow diagrams (Hahnle & Tinelli, 2007). .

3.2.4 Certificate Authority Prototyping

Prototyping is a technology in which an approximation of a final system is built and tested. Using this approach (Beaudouin, Michel; Mackay, Wendy;, 2002), the study gathered preliminary requirements that were used to build an original version of the solution.

3.2.5 Testing

Upon completion of the implementation, it was important to perform tests to ensure the end product is working logically as expected and that it matched business needs. In this phase the prototype was evaluated to ensure it meets the research objectives.

Also compatibility tests of the SSL certificates with different web browsers was done and also ensured minimum security requirements (Group, 2016) for the Certificate Authority were achieved. This included testing of the digital certificates with different web browsers (Chrome, Firefox and Explorer) with different systems (Windows and Linux) were done of the digital certificates and also with different web browsers. Also the researcher ensured that minimum security requirements are met (Group, 2016). User tests were done to get feedback on the user-friendliness of the system where users interacted with the system and answered a questionnaire for the same.

A usability survey of the Certificate Authority was also done to ensure that the system is user friendly as defined in Appendix II.

3.2.6 Research Validation

In this phase the Certificate Authority was evaluated to ensure it met the research objectives, which was analysis of costs saved when the Certificate Authority is implemented.

3.3 Ethical Measures

The research adhered to the ethical code of conduct by ensuring that all data collected was done at the will of the parties involved and that it was not mandatory to take part in the research. In situations where there was need to obtain permissions the research ensured that all the necessary arrangements had been made to obtain the required permissions to carry out the research.

3.4 Location of Study

The scope of the research was narrowed study was carried out in Nairobi County; targeting government institutions and large enterprises. This is because Nairobi harbors a majority of enterprises within the country which made it easy for the researcher to easily obtain data needed to facilitate the study.

3.5 Conclusions

This chapter assisted in developing a conclusion based on data collected on whether the proposed solution is viable and the possibility of having less costs in enterprises if the solution is implemented.

Chapter 4: System Analysis and Design

4.1 Introduction

This section describes in detail the research design and comprises of feedback of the research findings, analysis of data, analysis of the system implemented and the design of the system. The data collected in this research was from a random sample of documents and was used to develop an analysis of the system which finally led to the design/ architecture chosen for the implementation.

4.2 Research Findings

Data collection was done through self-study, document review and personal interviews defined in Appendix I. The researcher used information provided by one Telecommunication Company (Telkom Kenya Limited) since this information was available upon request.

At the moment, Telkom Kenya Limited does not run a private Certificate Authority. The digital certificates are mainly used for securing web servers and client authentication. This is for both internal Telkom Kenya Limited's web services and other hosted enterprise customers. They used 400 client certificates, 2,050 single certificates and 1 wildcard certificate. Averagely, $13,535 was spent per annum on purchasing of 51 digital certificates. The hosted enterprise customers purchase certificates and have them installed or have Telkom Kenya Limited purchase from other certificate authorities and install the certificate.

Digital Certificate Usage	
E-mail Signing	In the pipeline to implement in 2018
Securing Web Servers and Web Applications	✓
Code Signing	×
Client Authentication	✓

There was also a plan to have 1,500 S/MIME certificates for signing of emails for its 1,500 employees starting September, 2018.

4.2.1 Digital Certificate Cost Findings

The document review and questionnaire in Appendix I was focused on finding out how much was averagely spent on Digital Certificates and the cost incurred in purchasing of the same. The following findings were derived from the document review and questionnaire in Appendix I.

i) Delivery of Service Using Digital Certificates

Most sites that are not internally used and require that they be published to the public domain are considered to be at risk of breach of integrity and confidentiality. To ensure quality of service, whereby data accessed within the public domain is not tampered with, SSL certificates are installed in the hosting servers to enable secure connection between the requestor of information and the hosting server, whether an application service or a web service. Also, client certificates are used as a two-factor authentication method on critical systems where username and password are not adequate as a form of user authentication.

ii) Digital Certificate Purchase Platforms Used

Globally, the most trusted Certificate Authority providers are rated in this order, from the highest in ascending order: Comodo, Digicert, Entrust, Geotrust, GlobalSign, GoDaddy, Symantec and Thwate. Currently, enterprises buy their own certificates directly from Certificate Authorities online. The most common used is GoDaddy due to their relatively low market prices. However, there have been concerns of their trustworthiness on some platforms like the iOS and Safari browser. Also, others use third parties to buy the certificates. Case in Study, Telkom Kenya Limited purchases Digicert through Cloud Productivity Solutions and Entrust Digital Certificates through Lawtrust CA.

iii) Challenges in Current Platforms

The price of Digital Certificates are costly. For Telkom Kenya Limited is Certificates that had one Common Name and two Alternate Names at Ksh. 65,000 as of the year 2017 when bought through a third party (Cloud Productivity Solutions) which were valid for two years. Also, if buying directly from the Certificate Authority providers, the prices are as in Table 4.1.

Table 4.1 SSL Certificates Prices

SSL Provider	Product Name	1Year Price	Type	Encryption
Comodo CA	Positive SSL	$49.95	One Domain	128/256 bit
Go Daddy	Standard SSL	$69.99	One Domain	128/256 bit
Comodo CA	Instant SSL	$99.95	One Domain	128/256 bit
Comodo CA	Comodo SSL	$99.95	One Domain	128/256 bit
Go Daddy	Deluxe SSL	$99.99	One Domain	128/256 bit
Thwate	Thwate 123	$149.00	One Domain	128/256 bit
Geotrust	Quick SSL Premium	$149.00	One Domain	128/256 bit
Comodo CA	Positive SSl Wildcard	$149.95	Wildcard	128/256 bit
Comodo CA	Premium SSL	$179.95	One Domain	128/256 bit
Thwate	SSL Webserver Certificate	$199.00	One Domain	128/256 bit
Geotrust	TrueBusiness ID	$199.00	One Domain	128/256 bit
Go Daddy	Premium SSL	$99.99	One Domain	128/256 bit
Global Sign	Domain ServerSign	$249.00	One Domain	128/256 bit
Thwate	Webserver certificate with EV	$299.00	One Domain	128/256 bit
Geotrust	TrueBusiness ID with EV	$299.00	One Domain	128/256 bit
Go Daddy	Standard SSL Wildcard	$299.99	Wildcard	128/256 bit
Globalsign	Organisation ServerSign	$349.00	One Domain	128/256 bit
Symantec	Secure Site SSL	$399.00	One Domain	128/256 bit
Go Daddy	Deluxe SSL WildCard	$399.00	Wildcard	128/256 bit
Comodo CA	EV SSL Certiticate	$249.00	One Domain	128/256 bit
Comodo CA	Premium SSL Wilcard	$449.95	Wildcard	128/256 bit
Comodo CA	Comodo SSL wildcard	$449.95	Wildcard	128/256 bit
Thwate	Wildcard SSL Certificate	$559.00	Wildcard	128/256 bit
Geotrust	TrueBusiness ID wildcard	$599.00	Wildcard	128/256 bit
GlobalSign	Domain Serversign Wildcard	$849.00	Wildcard	128/256 bit
GlobalSign	Organisation Serversign Wildcard	$949.00	Wildcard	128/256 bit
Symantec	Secure Site Pro	$995.00	One Domain	128/256 bit

Symantec	Secure Site pro with EV	$1499.00	One Domain	128/256 bit

Also, some Certificate Authorities have been compromised in the past, for instance Symantec hence having their Certificates not to be trusted by others.

4.2.2 Research Findings Conclusions

From observation and research done, positive insight was received in how to set up the Certificate Authority. Also functional and non-functional requirements were formulated from this. These were the conclusions made from this process:

i) Most enterprises were buying Digital Certificates from Certificate Authority providers.
ii) There was need to develop a platform that will support generation, issuance and revocation of certificates at lower costs.
iii) The Certificate Authority needs to be secure to avoid compromise of the systems and also the Certificates.

4.3 Certificate Tools Findings

The most appropriate certificate tools to use were Windows servers for both root and subordinate CA since it has in-built certificate authority services that can be configured. Also, it would be easier to integrate an enterprise subordinate CA with an already existing active directory and hence push the certificates to domain users and computers using group policy.

4.4 System Design and Architecture

4.4.1 Introduction

The system design and architecture will cover how the platform was developed and tested. Based on the data collected, the research used UML diagrams as shown in Figures 4.1, 4.2, 4.3, 4.4 and 4.5 to model the systems in order to explain what was obtained from the collected data.

4.4.2 Certificate Authority Analysis

Based on research conducted, the system would need different modules. These are three windows servers (Windows server 2012 R2) and one Windows 10 endpoint. Licenses for Windows Server would be required.

Based on the data collected, functional and non-functional requirements were formulated for the system. The system architecture comprises of two main modules. These modules are the root CA and the subordinate CA.

a) Functional Requirements

i. Certificate Management

The CA is majorly involved in management of certificates. This includes, issuing, revocation, publishing, archiving and renewal of digital certificates.

ii. Validation of Certificate Signing Request

The registration authority (which is also sometimes part of the CA) assures valid and correct registration. It will accept request for digital certificates and authenticate the entity making the request.

iii. Path Validation

Path Validation settings in group policy allows CA administrator to:

a. Manage trusted root certificates-these control which root certification authority certifies and peer trust certificates in the user certificate and root certificate stores can be trusted.
b. Manage trusted publishers- Control which code signing certificates can be accepted for and blocks certificates that are not trusted as per policy.
c. Manage network retrieval and path validation- used to compensate for situations where downloads of a CRL fails because it is too large and network conditions are not optimal.
d. Manage revocation checking policy. These can be set to coordinate use of CRLs and Online Responders during revocation checking.

b) Non-Functional Requirements

a. Performance

The infrastructure was developed on key considerations of performance aspect as processing speeds, throughput and utilisation.

b. Reliability and Recoverability

Developing a CA ensured that it is reliable and that a private key can be recovered by assigning a certificate for a recover agent (i.e. a certificate administrator) and enabling specific certificate template to allow archiving a private key.

c. Security

The CA is secured by having an offline root CA in that it is only powered during issuance and/or reissuance of the root certificate is required. If a root CA is compromised, then all certificates that were issued by that CA are also compromised and could compromise the security of an entire organisational network. Therefore, the root CA is never connected to any network to minimize the risk of the CA private keys becoming compromised.

4.4.3 Certificate Authority Data Processing and Modeling

The system design and architecture will cover how the platform was developed and tested. Based on the collected data the researcher used UML diagrams to model the system so as to explain what was obtained from the data collected. The user(s) in the certificate authority system provide request for certificate generation and generate a certificate and send it to the requester for installation on the specified system, whether within the organisation or an external requester.

i. Process Workflow

This portrays the flow of data and information through the system. This mainly assists in the logical design and defines the actions of defined decisions and information process flow as shown in Figure 4.1.

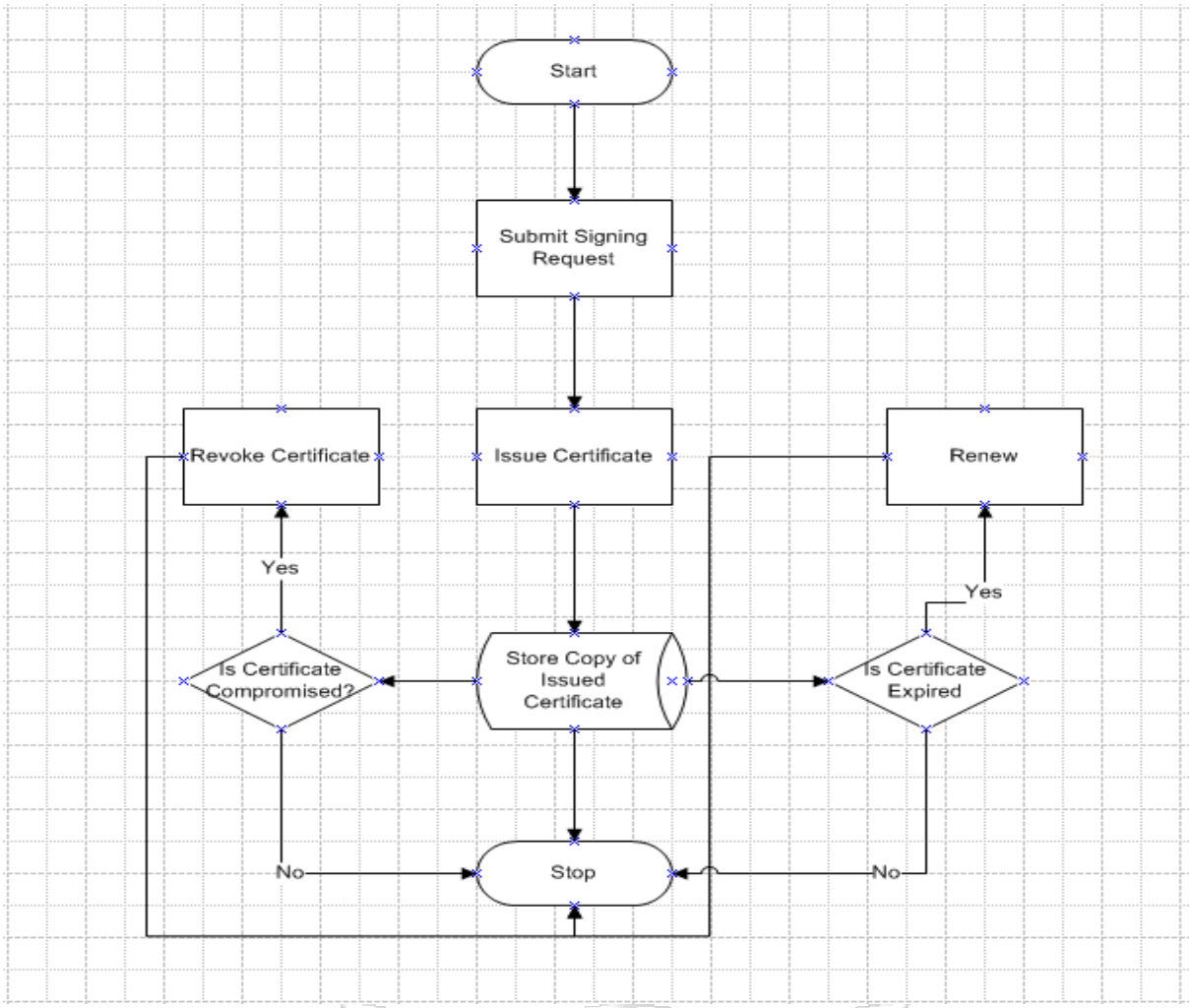


Figure 4.1 Process Workflow Diagram

ii) Use Case Modelling

The use cases discussed below have been used to depict the processes in the system and their interactions. The actor is the CA administrator who generates certificate from CSR generated from a system that needs certificate installed.

a. Use Case Diagram

Figure 4.2 depicts the various functionalities of the certificate authority and the relationship between the functions and system user.

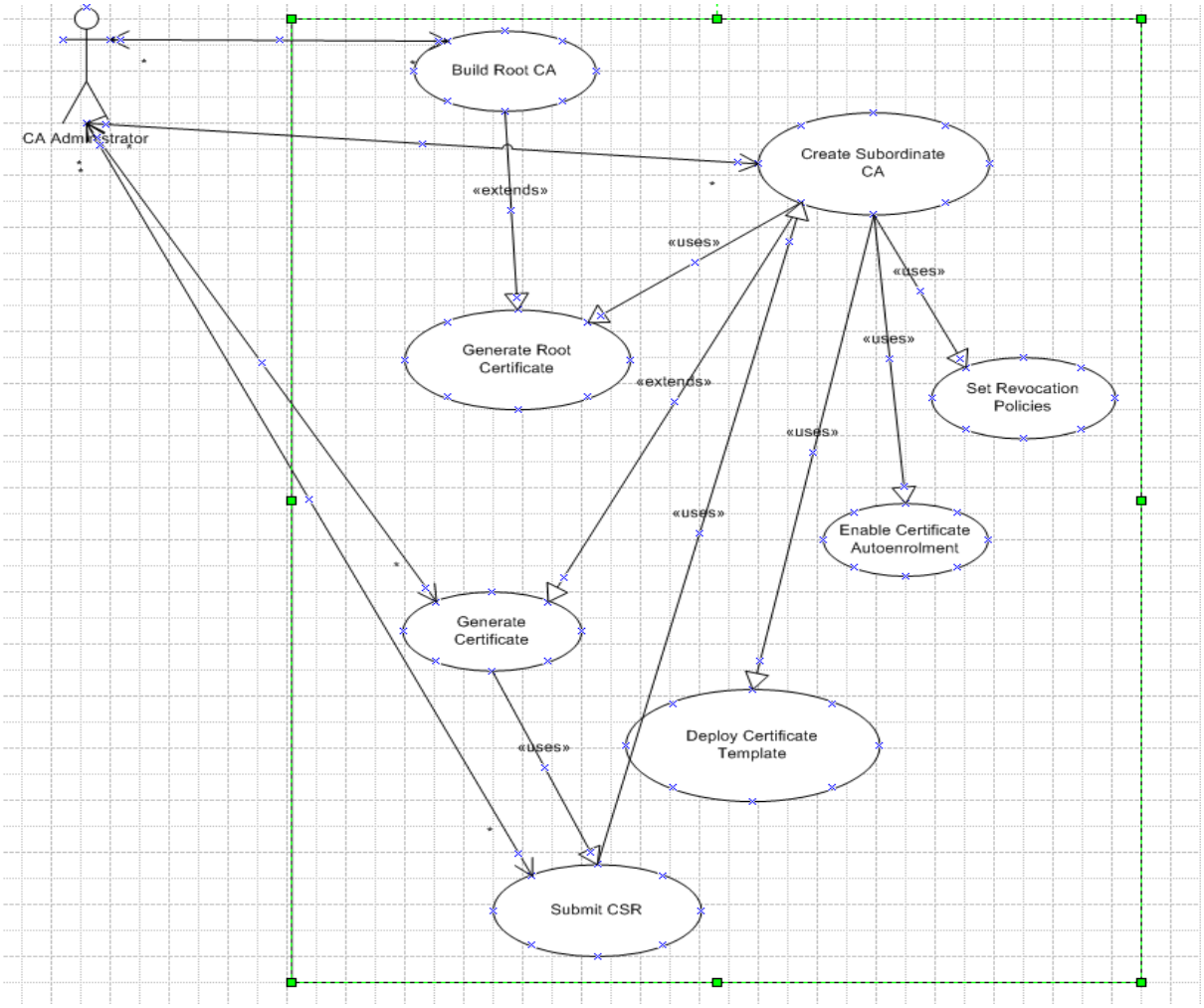


Figure 4.2 Use Case Diagram

b. Use Case Description

The main use cases that will be considered for description from the use case diagram are the build root CA, create subordinate CA, and generate certificate as they are the most critical processes of the application. Table 4.2 describes how a root CA is created. This is important since the root CA will be offline and the generated root Certificate used in implementing a subordinate CA.

Table 4.2 Build Root CA

Use Case	Build Root CA
Actor	CA Administrator.
Purpose	To configure the root Certificate Authority.
Overview	This is the initial stage of setting up a CA where the root CA is built and the Root Certificate generated.
Cross Reference	Generate root certificate use case.
Pre-Conditions	Administrator must be logged in to the platform.
Post Conditions	The Root Certificate is stored in the local database of the root CA.

The subordinate CA is used in signing of CSR and this hence forms the backbone of the Certificate authority as shown in Table 4.3.

Table 4.3 Create Subordinate CA

Use Case	Create subordinate CA
Actor	CA Administrator.
Purpose	To install and configure the subordinate Certificate Authority.
Overview	The use case stars with using the root certificate to set up the subordinate CA. This is then used to sign certificate signing request to generate SSL Certificate.
Cross Reference	Generate root certificate use case, Submit CSR use case, Deploy Certificate Template use case, enable auto-enrolment use case and set revocation policies use case.
Pre-Conditions	Administrator must be logged in to the platform, have the root Certificate from root CA.
Post Conditions	The Root Certificate is stored in the local database of the root CA.

After all this is set up, a certificate is then generated and this is represented by the Generate certificate use case as described in the Table 4.4.

Table 4.4 Generate Certificate

Use Case	Create Certificate

Actor	CA Administrator.
Purpose	To generate Certificate from submitted CSR.
Overview	The subordinate CA signs the CSR submitted by the CA administrator and hence a Certificate is generated.
Cross Reference	Create subordinate CA use case and Submit CSR use case.
Pre-Conditions	Administrator must be logged in to the platform, subordinate CA must have been set up and a CSR generated from an external system requiring the certificate.
Post Conditions	A copy of the certificate is stored in the local database of the subordinate CA.

ii) Sequence Diagram

The sequence diagram in Figure 4.3 shows the flow of events within the certificate authority system during implementation and the process of certificate generation.

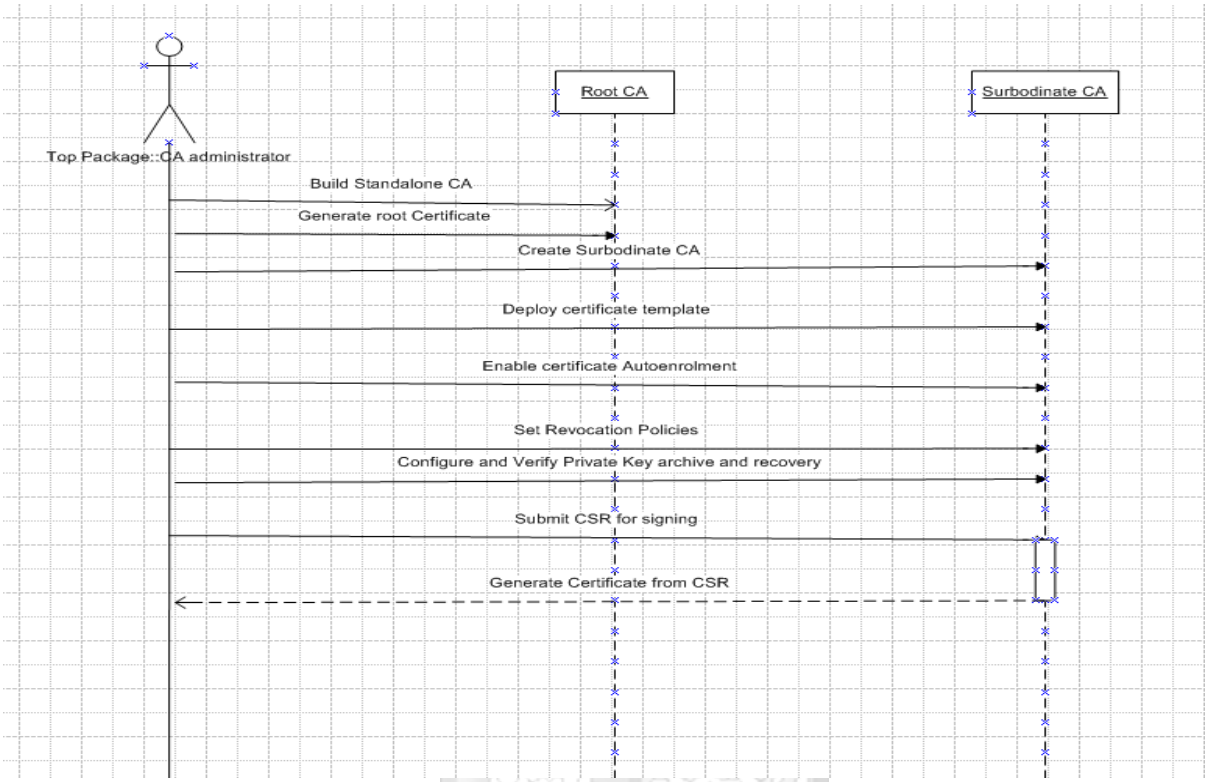


Figure 4.3 Sequence Diagram

iv) Data Flow Diagrams

These indicate flow of data from users to the different processes in the Certificate Authority system and their interactions with the process. Figure 4.4 shows level 0 diagram (context diagram) which is the high level diagram.

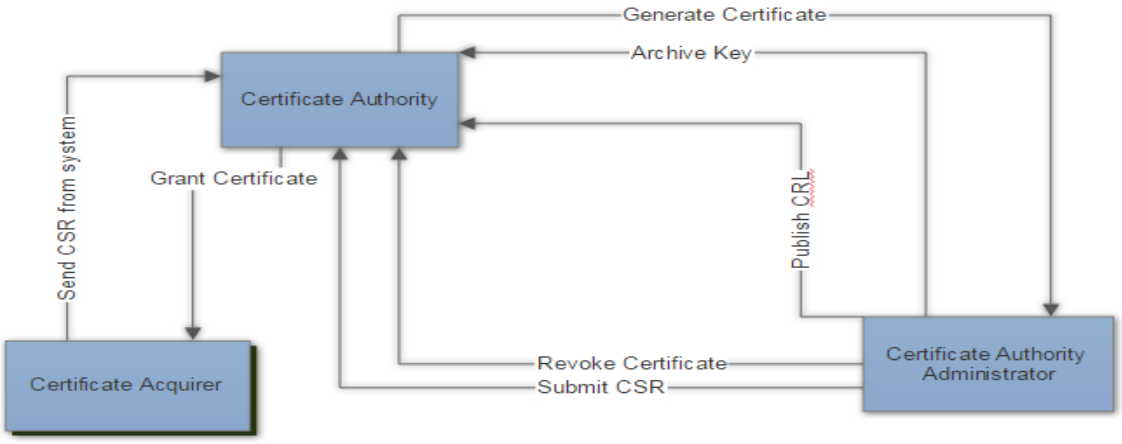


Figure 4.4 Level 0 Data Flow Diagram

Level 1 diagram in Figure 4.5 is a more detailed context data flow diagram. The context diagram has been broken down to give the details of the processes of certificate request, issuance and revocation.

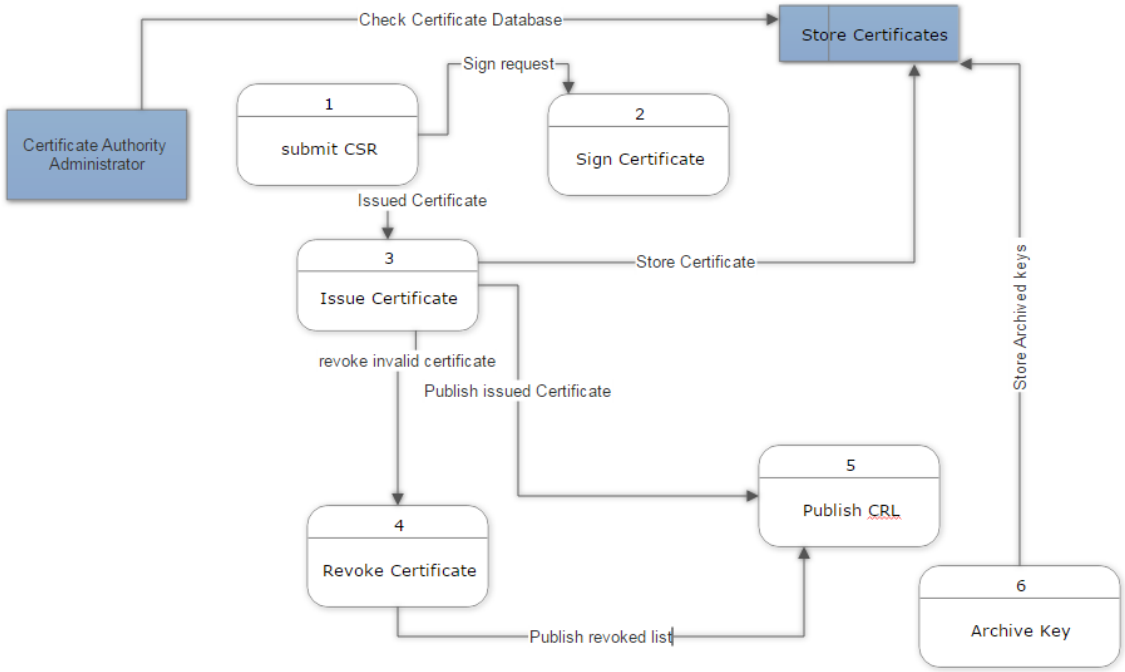


Figure 4.5 Level 1 Data Flow Diagram

4.3.4 Database and Data Security

The platform will handle certificates, certificate keys certificate revocation lists. Both the root CA and the subordinate CA will store their own certificate keys. The private keys for both were set at 4096-bit key length using the hash algorithm SHA1 for signing certificates issued by the respective Certificate Authorities before they are stored locally in the system. The public keys for both the root and subordinate CA were also set to be 4096-bit key length and use SHA256 hashing algorithm

Also, the root Certificate Authority was offline after extraction of the root Certificate to ensure that the private key of the root certificate is not compromised.

Chapter 5: Prototyping and Prototype Testing

5.1 Introduction

Based on the designs developed in Chapter 4, the system designs were developed and the prototype tested to ensure that the system functionalities were met. In this section the system implementation is discussed.

5.2 Development Environment

This was set up so as to facilitate the certificate authority implementation as per plan. This is elaborated in Table 5.1.

Virtual Machine Name	Role	Configuration
root_CA	Root Certificate Authority	Server with Windows Server 2012 R2
sub_CA	Domain Controller, DNS Server, Subordinate CA	Server with Windows Server 2012 R2
server1	Internet Information Services	Server with Windows Server 2012 R2
rioba-PC	Client Endpoint	Windows 10

Table 5.1 Software Requirements

5.3 Certificate Authority Set-up

Both the root CA and the subordinate CA were built on Windows platform based on findings that most organisations used Windows for their Servers and end-user machines. The CA was built to issue certificates to computers connected to the Domain Controller through a group policy in the Active Directory.

5.3.1 Root Certificate Authority

This was set up and the root Certificate generated for use of signing for any certificate signing requests made to the root Certificate. Figure 5.1 shows the root configuration which includes the hashing algorithm and root certificate key length.

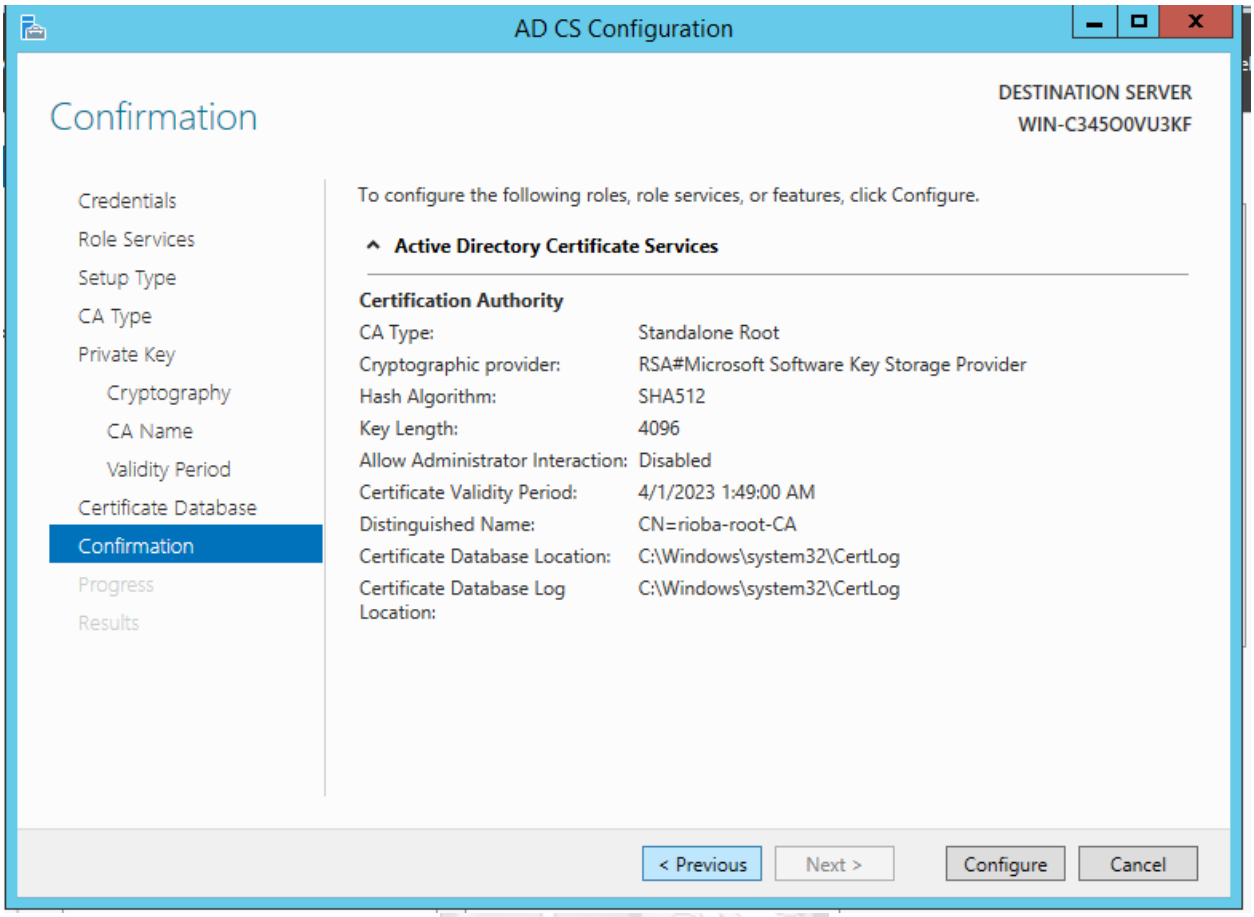


Figure 5.1 Root CA Setup

5.3.2 Subordinate CA CSR signing

When the Subordinate CA is set up a trust chain has to be established with the root CA. Therefore, a CSR is generated from the Subordinate CA and submitted to the root CA for signing.

The CA window in Figure 5.2 shows the folders where the certificates are stored according to their category. Certificate with request ID 2 is a pending certificate signing request.

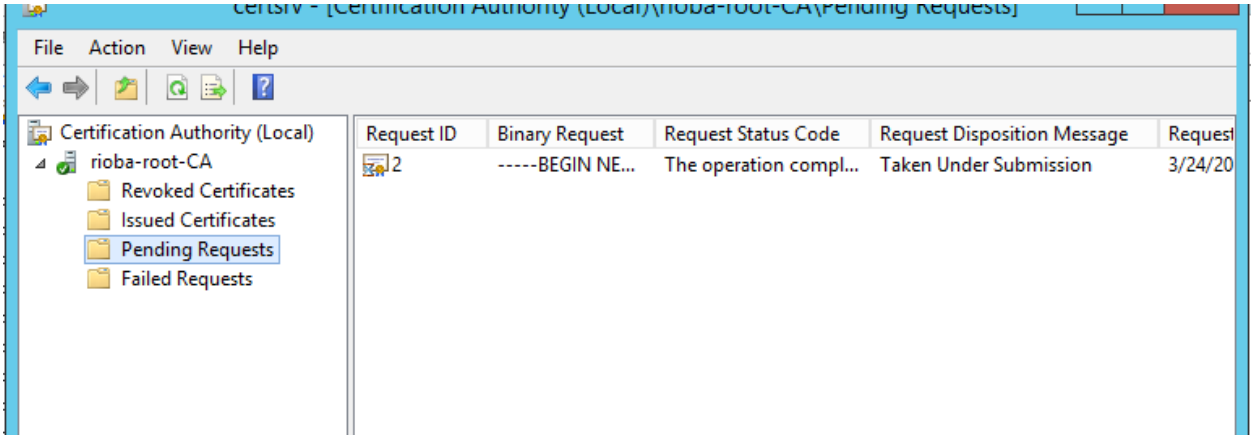


Figure 5.2 Submitted Request from Subordinate CA

Once the certificate request is signed, it is moved to the issued folder as shown in Figure 5.3 at which point it can be exported and used for the intended purpose.

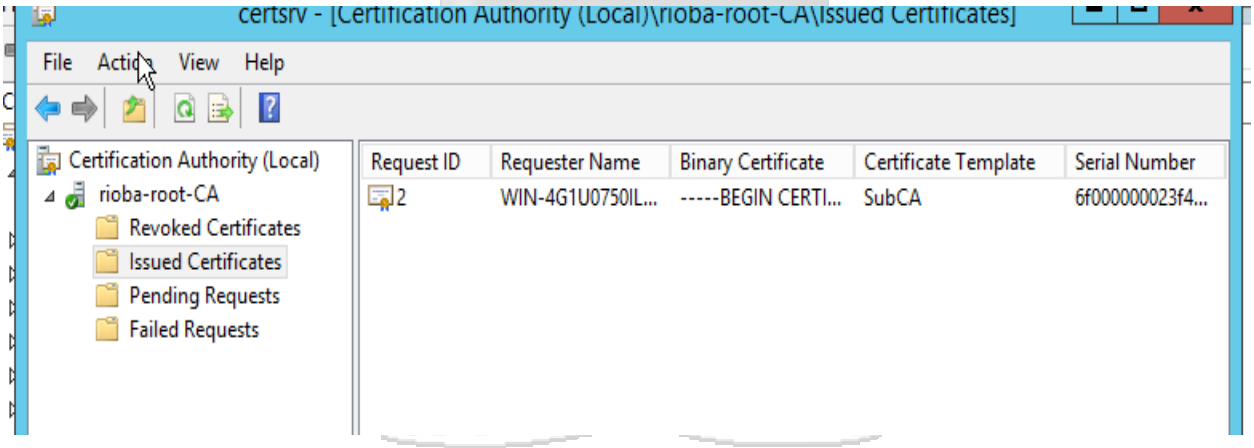


Figure 5.3 Issued Certificate from Root CA

5.3.3 Certificate List

The Certificate trust chain is now established as shown on Figure 5.4. The root CA Certificate is placed in the Trusted Root CA and the subordinate CA certificate placed in the Intermediate CA folder respectively. This therefore forms the chain of trust.

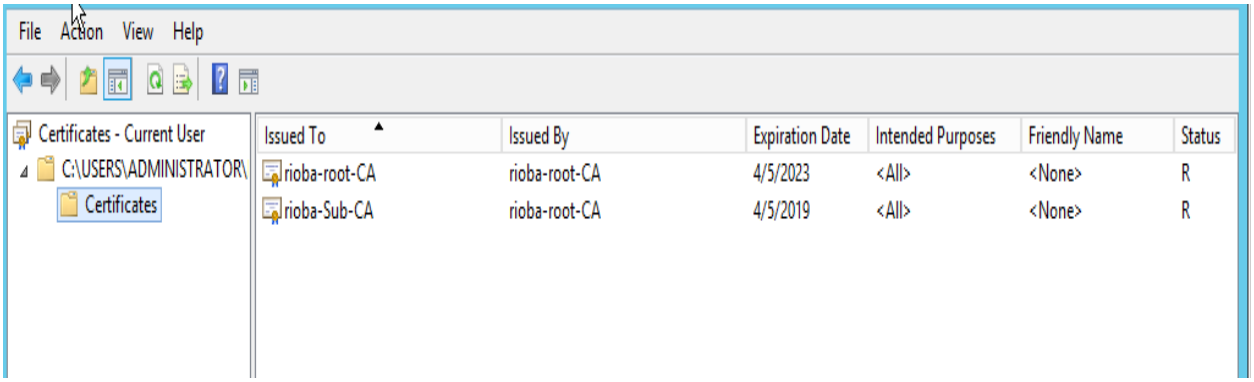


Figure 5.4 Root and Subordinate CA Certificate Chain

For any other certificate issued by this CA will include this chain of trust as illustrated in the Figure 5.5.

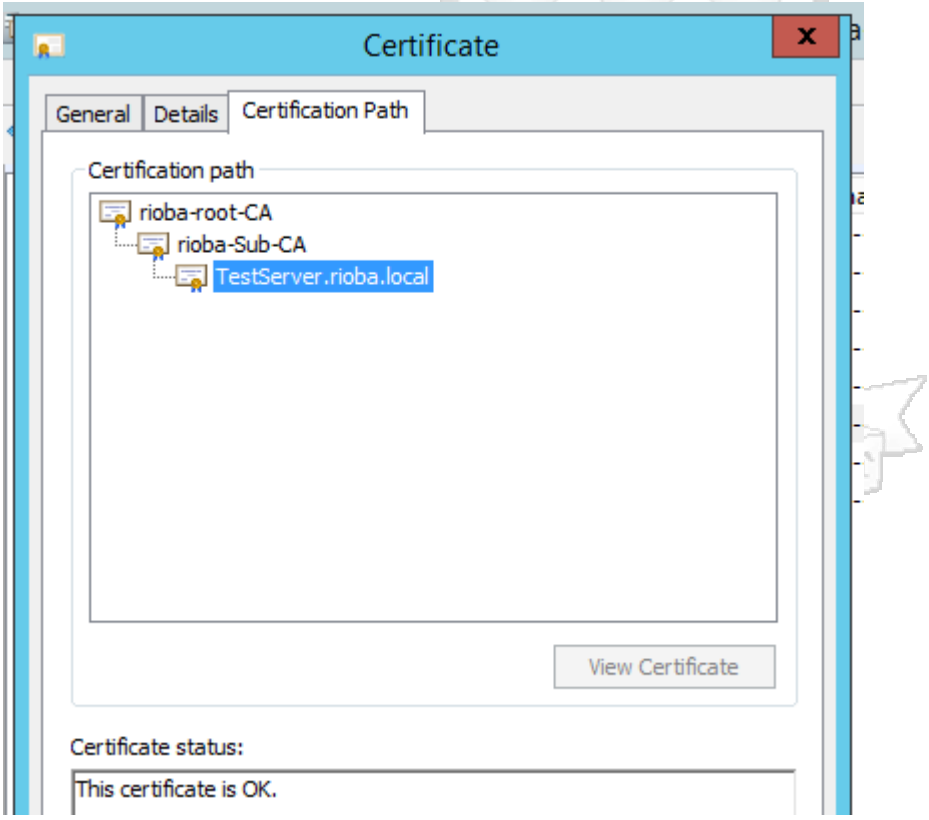


Figure 5.5 Certificate Trust Chain

5.3.4 Certificate Revocation

Any certificates that have expired are listed in this folder. This includes those that have automatically expired and those that have manually been revoked due to other reasons like compromise of the issued certificates.

5.3.5 Certificate Auto-enrollment

Figure 5.4 shows the Certificate automatic enrollment which is set up via group policy in the domain controller which allows distribution of certificates without the awareness of the client.

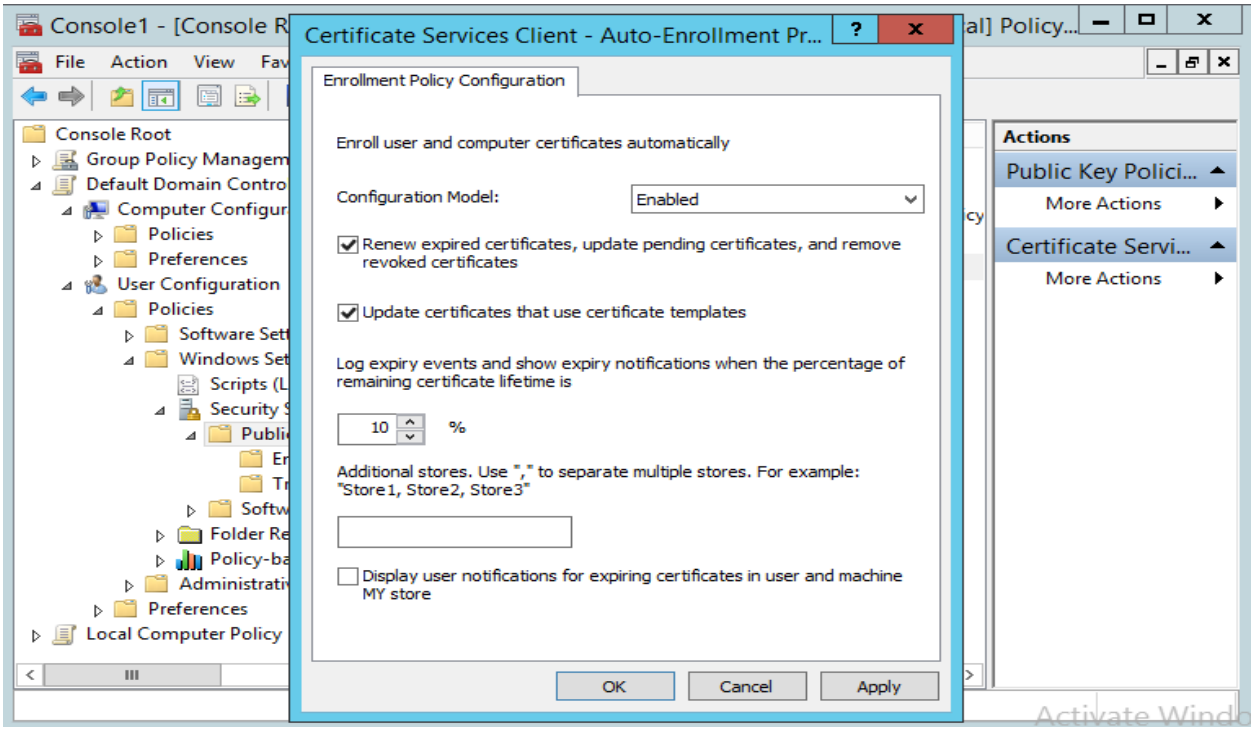


Figure 5.6 Enabling Auto-Enrollment

5.3.6 OCSP Responder

This checks for the certificate status and revocation status which is in two categories: when it expires after issuance or when it is revoked before expiry due to multiple reasons such as key compromise or suspension. Figure 5.5 shows the status for the setup CA.

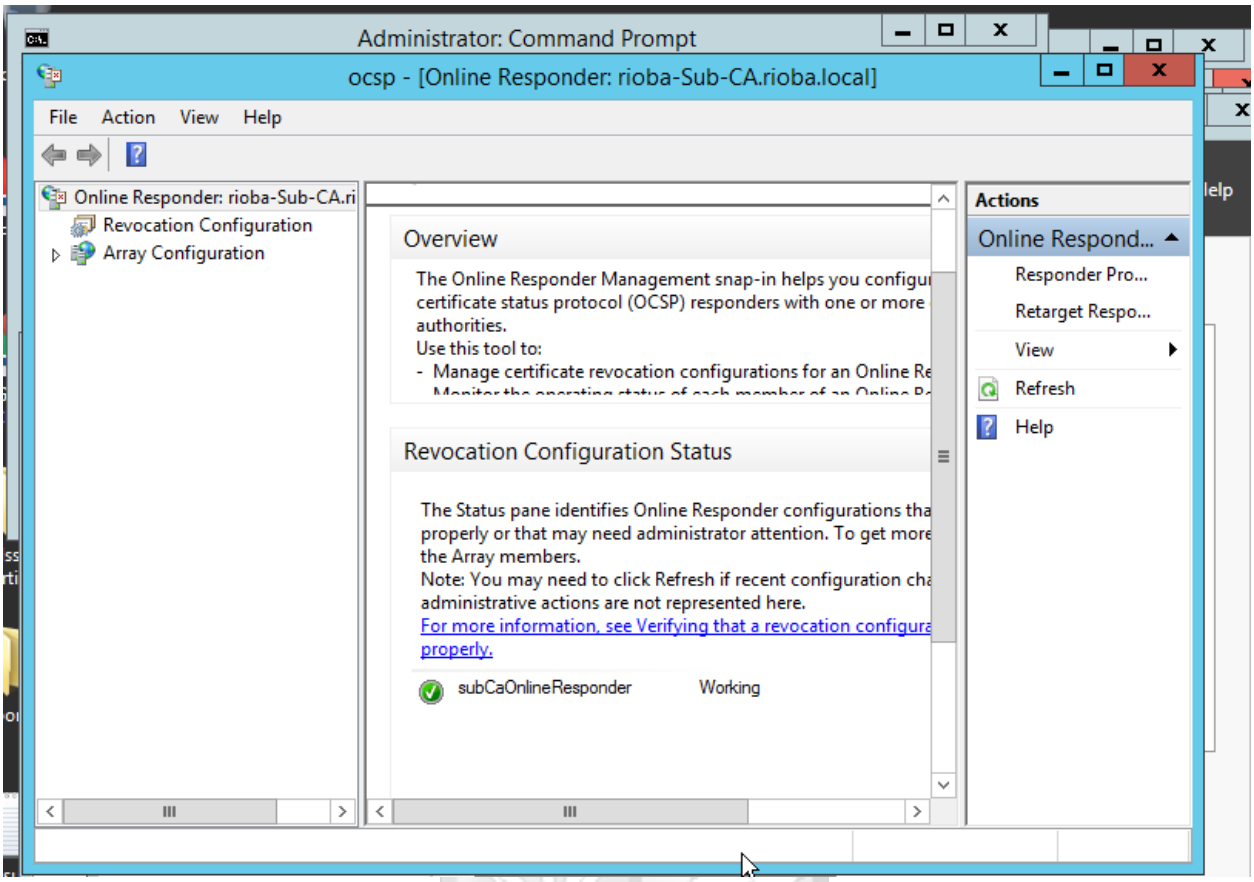


Figure 5.7 OCSP Responder

5.3.7 Certificate Auto-enrollment

This enables the authenticated users to upload their certificate signing requests based on the available templates. These are promptly signed and issued and downloaded. Also the certificate chain may be downloaded. This includes both the root and subordinate certificates.

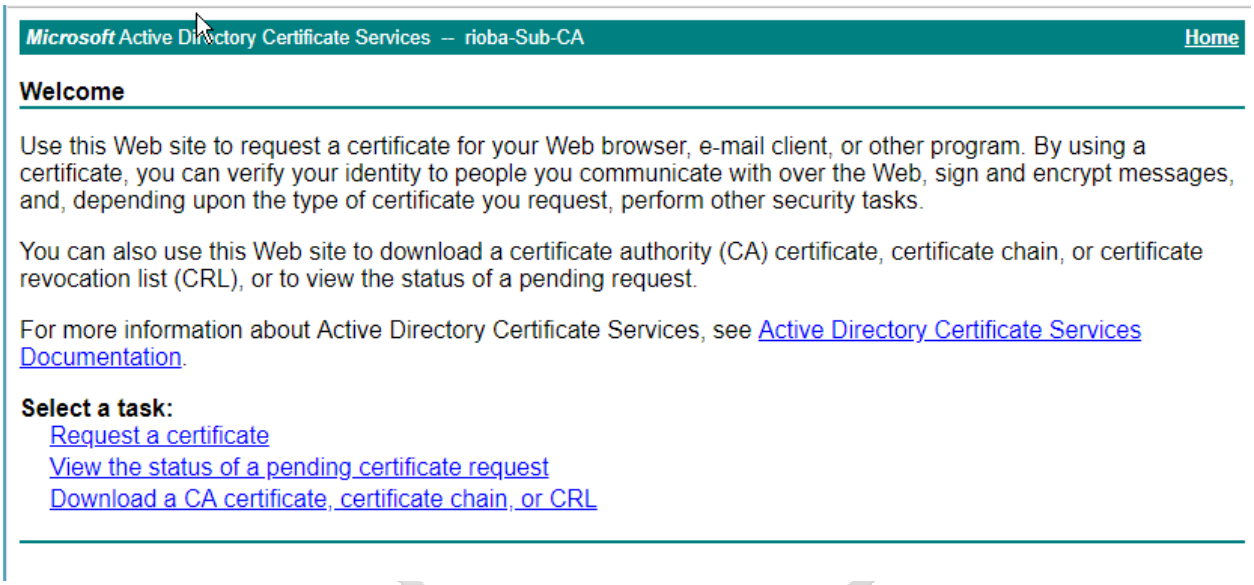


Figure 5.8 Certificate Auto Enrollment Platform

5.4 Certificate Issuance Process

The user within the domain will receive the certificates on their certificate folders when they are deployed using group policy from the subordinates CA which run on the same server as the active directory. For the users not in the domain, they have to submit certificate requests either via email as a text file or on the CA's web auto enrollment platform. If on email, the CA administrator will load it in the request folder, have the CA issue the certificate and export it to a local folder within the CA. This is then shared with the user. If done via auto-enrollment, the certificate will automatically be loaded in the request folder and the administrator goes through the same process to issue. The requestor can check the status of the submitted signing request on the same platform.

The CA administrator then shares the certificate with the requestor. For auto-enrollment, the certificate signing request will contain an email address which will be used to share the certificate. The process of domain validation has been eliminated since the domains used are dummy non-registered domains.

The certificate chain (root and subordinate CA certificates can be downloaded on the auto enrollment web platform.

5.5 Prototype Testing

The prototype testing included unit testing, integration testing with different browsers, functional testing to ensure the specified functionalities were fulfilled, usability testing.

Test Case Name:	**System Test**			
Date Tested:	**5th April 2018**			
Preconditions				
Post Conditions				
Steps	Action	Expected Response	Result	Comment
1	Check if certificate is shown on different browsers.	Certificate should show on the browser certificate store	Pass	Installation Successful after pushing through group policy via active directory. However https runs only on Explorer and Edge browsers
2	Check if application runs correctly.	Both the root CA and subordinate CA should show active after setup	Pass	Functions worked and the appropriate layouts are displayed with the trust chain displayed within the certificate.
3	Ease of Usability	Show Pending requests, revoked certificates, issued certificates, failed requests.	Pass	This is shown as a list and easy to use since its GUI for both root and subordinate CA

Table 5.2 Test Cases

5.5.1 User Tests

A system usability survey was conducted and results obtained are shown in Table 5.3

	Agree	Disagree	Other

Is the system user friendly	95%	5%	0%
Ease of use of the system	94%	5%	1%
Was the system responding fast enough?	98%	1%	1%
I am willing to use this system for certificate management	89%	3%	8%

Table 5.3 Test Cases

i) Ease of Use

The study sought to find out the ease of use of the prototype which was analyzed by different users. A questionnaire was sent to the users and the response was analyzed. After the application was set up, the first impression of users on the application design, looks and color combinations was shown in Figure 5.9. 93% agreed that the system was user friendly and appealing, 2% disagreed and 5% were neutral

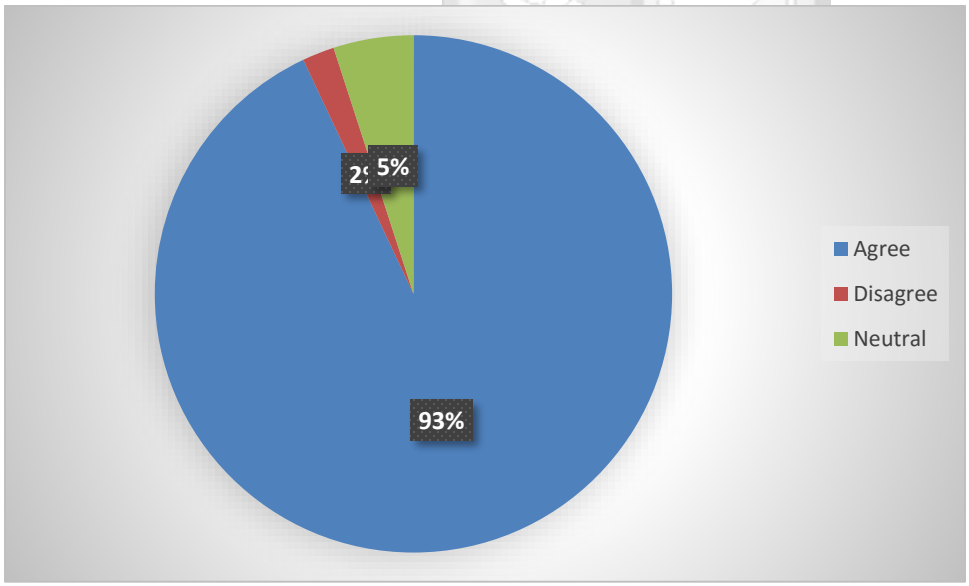


Figure 5.9 User Friendliness

ii) Core Functionalities

The core functionalities were then checked by the users on how easy it was to find them and navigate through as shown in Figure 5.8. 94% agreed that it was easy to use, 5% were neutral and 1% disagreed since in their day to day they mainly use Linux systems.

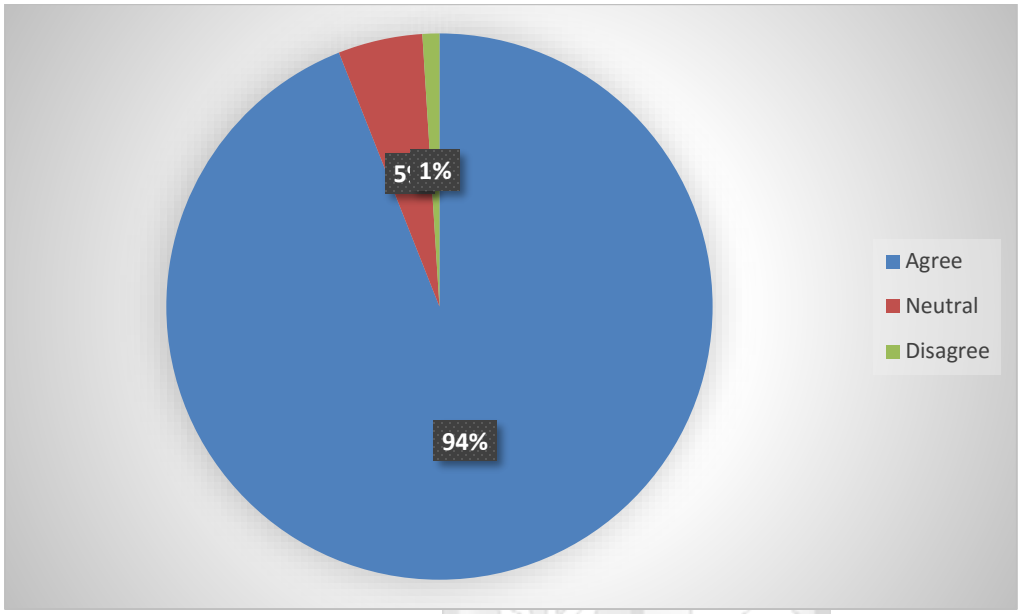


Figure 5.10 Ease of Use

iii) System Responsiveness

During performance of different transactions, users tested how responsive the system was in terms of giving feedback during various transactions which were mainly, issuance, revocation and request of digital certificates. The results are depicted in Figure 5.9

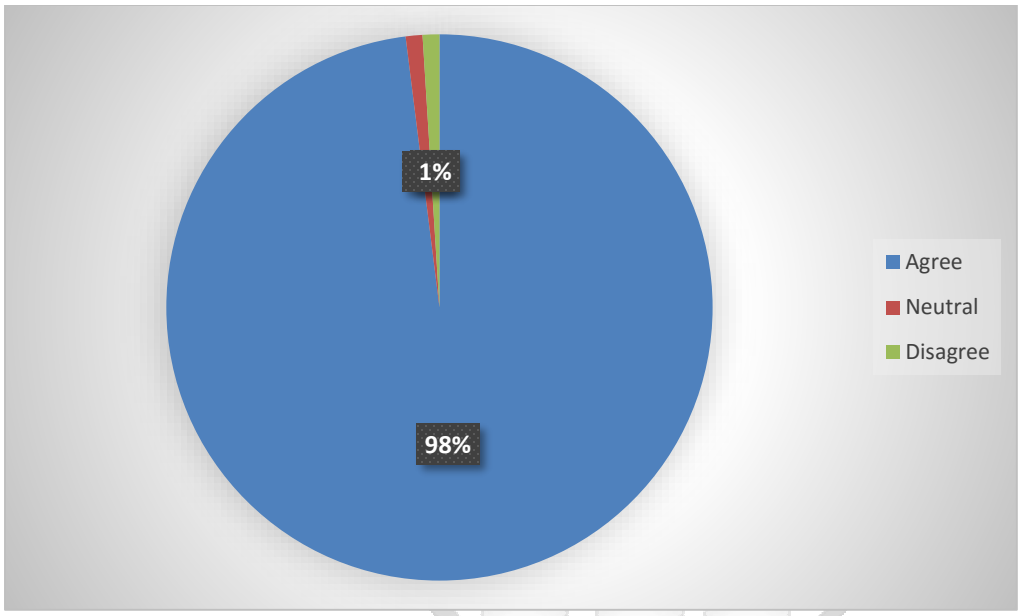


Figure 5.11 System Responsiveness

iii) System Usage

93% of the users interviewed agreed that the prototype was effective since it gave them control over the digital certificates that are required. Also, in the event of compromise, the digital certificate can be immediately revoked and another one issued. 5% were neutral and 2% disagreed.

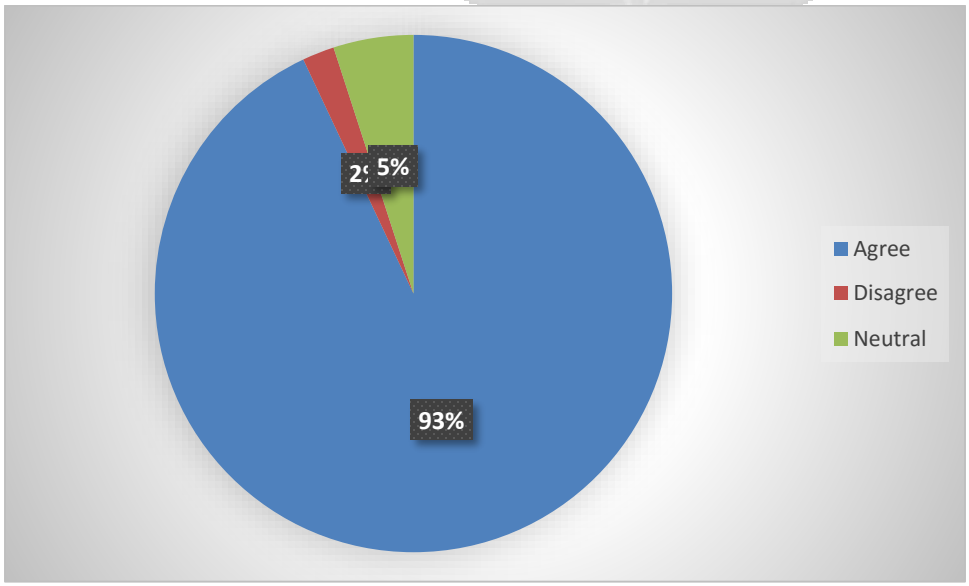


Figure 5.12 System Usage

5.6 Cost of Setting Up and Running a Private CA

The cost that was looked at in this study was CA initial costs, operational costs and maintenance costs over a period of two years since SSL/TLS certificates are required to be valid for a maximum of two years. For the purposes of this research, validity of a certificate was one year. This therefore was used across board for both code signing certificates and client certificates.

Only one wildcard certificate was used since it can be used to secure 99 domains. Also, Entrust public CA was used since a quotation was available for other services such as managed PKI services.

The researcher considered 50 multi-domain certificates; these have one common name and three alternative names at a cost of $278 and any extra name comes at an extra cost of $54 up to 250 domains. However, for this case, we used the option of having only four domains per certificate so as to minimize exposure of the number of domains put to risk in the event that the private key of the certificate is compromised. This therefore meant a total of 299 domains would be considered. Table 5.3 shows the cost of having a private CA versus buying digital certificates.

This is only for certificates that would be used internally since the certificate would not be trusted in the public domain. Also it is with the assumption that the infrastructure is in place.

		Private CA Cost			**Public CA Cost**		
Cost Category	**Product/Process**	**Unit Cost**	**Quantity**	**Total Cost**	**Unit Cost**	**Quantity**	**Total Cost**
Licenses	Microsoft Windows Licenses	$1,000	2	$2000	0	0	0
Operational	Salaries for CA admin (monthly)	$3,000	12	$36,000	0	0	0
Maintenance	Disaster Recovery Test	$120	1	$120	0	0	0
	Preventive Maintenance	$120	4	$480	0	0	0
Compliance	Yearly Audits		1		0	0	
Certificate Production Cost	Single Certificate	0	50	0	$278	50	$13, 000

	Wildcard Certificate	0	1	0	$5350	1	$535
Total			**1**	**$36,800**	**$535**	**1**	**$13, 535**

Table 5.4 Cost Comparison

Also so as to make economic sense the researcher used a maximum value of 100 digital certificates for each category; SSL certificate, S/MIME certificates, Client Certificates.

Another scenario was having the certificate authority issue certificates to non-domain users. The case study was manly done for Telkom Kenya Limited who at the time of this research had 2,000 web hosted enterprise customers. This therefore implied that other than the approximated 299 certificates, an extra 2,000 certificates would be issued but at a cost. The cost would not be prohibitive so as to allow customers to choose the company's CA certificates instead of buying from another public CA. This however introduced a challenge where users would get disclaimers that the site is not trusted. The viable solution to this would be to have a trusted root certificate sign the subordinate CA. For a public CA to sign another subordinate, the controls have to be checked and a thorough audit done so as to ensure that the subordinate CA complies with best practice and also the policies and standards set by the signing root CA. However, the researcher considered the option of having the root certificate included in browsers which would cost an initial $75,000 and subsequent annual fee of $10,000. The selling price for each certificate would be $50 for single certificates. The cost for wildcard certificates would be $100. However, since the customers are different this was not relevant to the research. If the certificates would not be sold, the running cost would be $36, 800 versus $535 for purchasing certificates.

The internal certificates were not charged therefore only 2,050 single certificates and one wildcard would be produced but only 2,000 single certificates sold. Preventive maintenance is mainly for patching of the enterprise CA which would require restarts of the server and hence has to be done during a scheduled change window. The only cost would be overtime dues payed to the CA admin. The cost implication would be as in Table 5.4.

		Private CA Cost (Year 1)			2nd year		
Cost Category	**Product/Process**	**Unit Cost**	**Quantity**	**Total Cost**	**Unit Cost**	**Quantity**	**Total Cost**
Licenses	Microsoft Windows Licenses	$1,000	2	$2,000	$1,000	2	$2,000
Operational	Salaries for CA admin (monthly)	$3,000	12	$36,000	$3,000	12	$36,000
Maintenance	Disaster Recovery Tests	$120	1	$120	$120	1	$120
	Preventive Maintenance	$120	4	$480	$120	4	$480
Compliance	Annual Security Audits	$75,000	1	$75,000	$10,000	1	$10,000
Certificate production cost	Single Certificates	0	2,050	0	0	2,051	0
	Wildcard Certificates	0	1	0	0	1	0
Total Cost				**$113,600**			**$48,600**
Certificate issuing price	Single Certificates	$35	2,000	$70,000	$35	2,000	$70,000
	Wildcard Certificates	$100	0	0	$100	0	0
Total cost Difference				**-$43,600**			**$21,400**

Table 5.5 Cost Comparison over Two Years

Year one: $113,600 to run the CA and sell certificates worth $70,000. Loss made would be $43,600

Year two: $48,600 to run the CA and sell certificates worth 70,000. Profit made would be $21,400. This is also inclusive of the subsequent years since the initial audit cost is expensive. After the initial, the subsequent cost is a constant $10,000.

The costs not included are backup costs, load balancing, virtualization software licenses and hardware, firewalls, and archival. This is because in the enterprise, these are already in place for both primary site and disaster recovery site.

5.7 Cost Analysis

i) When Setting up CA without Selling CA without Selling Certificates

Table 5.5 indicates the cost that will be incurred yearly for running a CA without selling digital certificates. From this, purchasing certificates would be cheaper than building a CA. The cost incurred if a CA is set up would be $23,265 more than if digital certificates were bought.

	Private CA	Purchasing Certificates	Cost Difference
Running Costs	$36,800	$0	
Purchase Costs	$0	$13,535	
Price Difference			$23,265

Table 5.6 Cost Analysis I

i) When Setting Up CA and Selling Solely Enterprise Customers

Table 5.7 shows the costs over a period of six years with the cumulative profit made over that period. The assumption made is that the customer base will be constant and neither diminish or grow.

Also, the researcher user different selling prices ranges; $20, $30 and $40.

When certificates are sold at $20, a continuous loss would be experience if the number of certificates sold is 1,000 or 2,000. When selling 3,000 certificates, the breakeven point is experienced in the 6th year and in the 3rd year if selling 4000 or 5000 digital certificates. This is shown in Table 5.7

Selling Price @$20							
	Year1	Year2	Year3	Year4	Year5	Year6	Certificate Number
Running Cost	**113,600**	**48,600**	**48,600**	**48,600**	**48,600**	**48,600**	
Revenue	20,000	20,000	20,000	20,000	20,000	20,000	1,000 Certificates
Cumulative Profit Made	***-93,600***	**-122,200**	**-150,800**	**-179,400**	**-208,000**	**-236,600**	
Revenue	40,000	40,000	40,000	40,000	40,000	40,000	2,000 Certificates
Cumulative Profit Made	***-73,600***	***-82,200***	***-90,800***	***-99,400***	***-108,000***	***-116,600***	
Revenue	60,000	60,000	60,000	60,000	60,000	60,000	3,0000 certificates
Cumulative Profit Made	***-53,600***	***-42,200***	***-30,800***	***-19,400***	***-8,000***	***3,400***	
Revenue	80,000	80,000	80,000	80,000	80,000	80,000	4,000 Certificates
Cumulative Profit Made	***-33,600***	***-2,200***	***29,200***	***60,600***	***92,000***	***123,400***	
Revenue	100,000	100,000	100,000	100,000	100,000	100,000	5,000 Certificates
Cumulative Profit Made	***-13,600***	***-37,800***	***89,200***	***140,600***	***192,000***	***243,400***	

Table 5.7 Cost Analysis II

Figure 5.13 indicates when the breakeven point will be achieved when selling different number of certificates at $20.

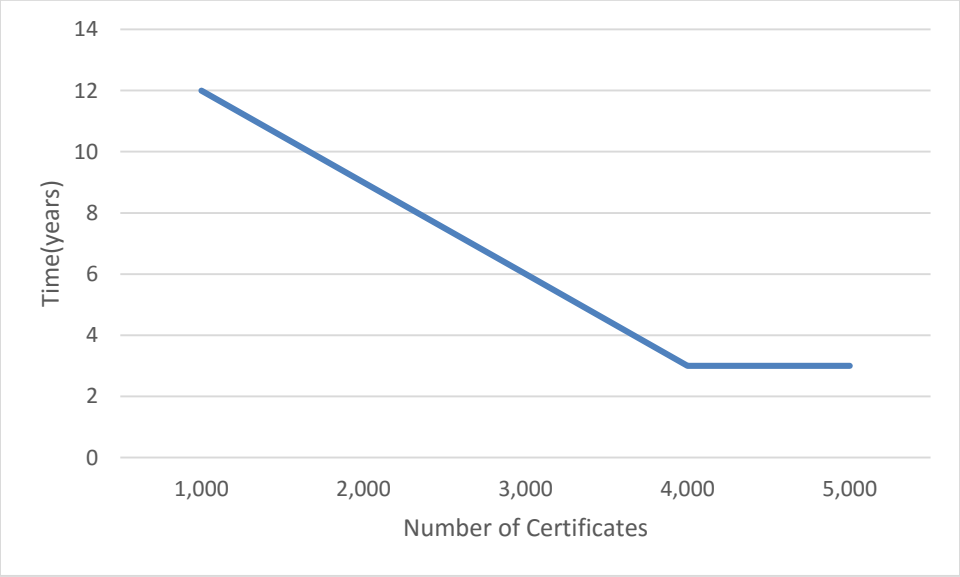


Figure 5.13 Breakeven Point when Selling at $20

When digital certificates are sold at $30, continuous losses are made when selling 1,000 certificates or less. The breakeven point is achieved during year six and second year when selling

2,000 and 3,000 certificates respectively. When selling 5,000 certificates, the breakeven point is achieved in the first year as in Table 5.8

Selling Price @$30							
	Year1	Year2	Year3	Year4	Year5	Year6	Certificate Number
Running Cost	**113,600**	**48,600**	**48,600**	**48,600**	**48,600**	**48,600**	
Revenue	30,000	30,000	30,000	30,000	30,000	30,000	1,000 Certificates
Cumulative Profit Made	***-83,600***	***-102,200***	***-120,800***	***-139,400***	***-158,000***	***-176,600***	
Revenue	60,000	60,000	60,000	60,000	60,000	60,000	2,000 Certificates
Cumulative Profit Made	***-53,600***	***-42,200***	***-30,800***	***-19,400***	***-8,000***	***3,400***	
Revenue	90,000	90,000	90,000	90,000	90,000	90,000	3,0000 Certificates
Cumulative Profit Made	***-23,600***	***17,800***	***59,200***	***100,600***	***142,000***	***183,400***	
Revenue	120,000	120,000	120,000	120,000	120,000	120,000	4,000 Certificates
Cumulative Profit Made	***6,400***	***77,800***	***149,200***	***220,600***	***292,000***	***363,400***	
Revenue	150,000	150,000	150,000	150,000	150,000	150,000	5,000 Certificates
Cumulative Profit Made	***36,400***	***137,800***	***239,200***	***340,600***	***442,000***	***543,400***	

Table 5.8 Cost Analysis III

Figure 5.14 indicates when the breakeven point will be achieved when selling different number of certificates at $30.

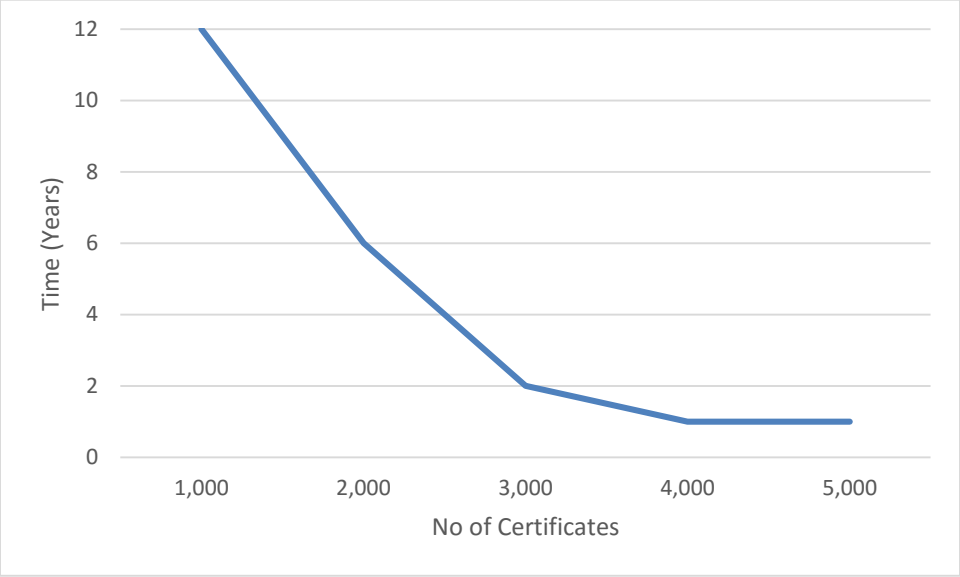


Figure 5.14 Breakeven Point when Selling at $30

When digital certificates are sold at $40, continuous losses are made when selling 1,000 certificates. When Selling 3,000, 4,000 and 5,000 certificates the breakeven point is achieved in the first year as in Table 5.8

Selling Price @$40							
	Year1	Year2	Year3	Year4	Year5	Year6	
Running Cost	**113,600**	**48,600**	**48,600**	**48,600**	**48,600**	**48,600**	
Revenue	40,000	40,000	40,000	40,000	40,000	40,000	1,000 Certificates
Cumulative Profit Made	***-73,600***	***-82,200***	***-90,800***	***-99,400***	***-108,000***	***-116,600***	
Revenue	80,000	80,000	80,000	80,000	80,000	80,000	2,000 Certificates
Cumulative Profit Made	***-33,600***	***-2,200***	***29,200***	***60,600***	***92,000***	***123,400***	
Revenue	120,000	120,000	120,000	120,000	120,000	120,000	3,0000 Certificates
Cumulative Profit Made	***6,400***	***77,800***	***149,200***	***220,600***	***292,000***	***363,400***	
Revenue	160,000	160,000	160,000	160,000	160,000	160,000	4,000 Certificates
Cumulative Profit Made	***46,400***	***157,800***	***269,200***	***380,600***	***492,000***	***603,400***	
Revenue	200,000	200,000	200,000	200,000	200,000	200,000	5,000 certificates
Cumulative Profit Made	***86,400***	***237,800***	***389,200***	***540,600***	***692,000***	***843,400***	

Table 5.9 Cost Analysis IV

Figure 5.15 indicates when the breakeven point will be achieved when selling different number of certificates at $40.

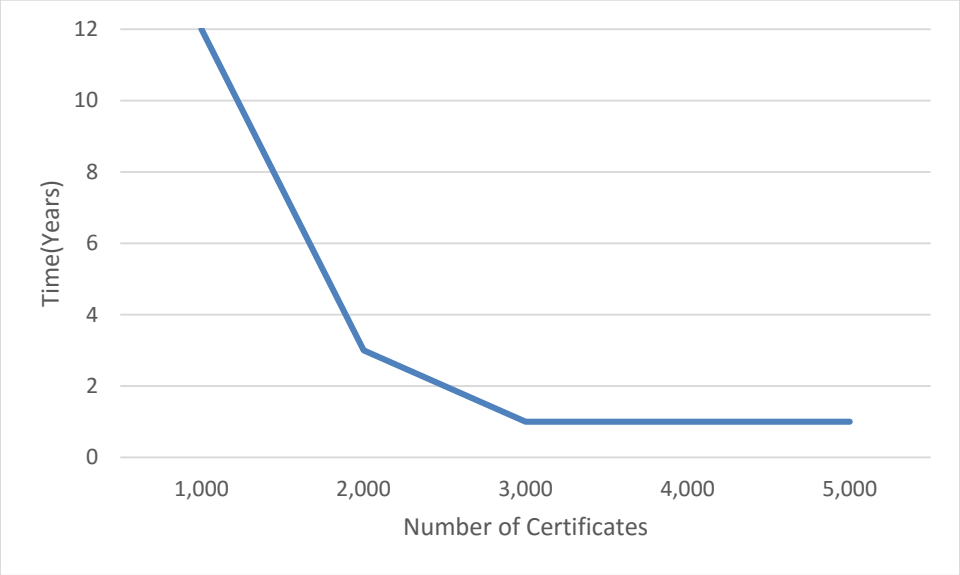


Figure 5.15 Breakeven Point when Selling at $40

From the cost analysis above, it would cheaper if certificates were sold solely to enterprise customers. To break even, at $20, the certificates need to be over 3,000 certificates; at $30 and $40, equal to or greater than 2,000 certificates;

5.8 Prototype Validation

The prototype built did address the problem statement of cost saving whereby the enterprise will need to sell digital certificates to its enterprise customers so as to save costs. However, there needed to be a threshold to be reached. From the cost analysis done in section 5.7, the certificates to be sold to enterprise customers each at $20 need to be 3,000 yearly so as to reach the breakeven point in the sixth year; at $30, customer need to be over 2,000 or more. If customers are 2,000 the breakeven point will be reached in the sixth year. If sold at $40, the minimum customers need to be 2,000 so as to have a breakeven point at the third year. This therefore implies that the breakeven point is dependent on the price of the digital certificate.

5.9 Conclusions

The architecture of choice made it possible for an efficient implementation of the Certificate Authority. Waterfall methodology gave an opportunity for the implementation to be done in a systematic manner, from feasibility study through to conclusion and recommendation.

Chapter. 6: Discussions of Results

6.1 Introduction

After the design, implementation and testing process, the study pursued to find out if the set objectives for the research were accomplished and how the developed solution relates with current systems so as to identify the strengths that would make it preferred option based against the current existing systems.

6.2 Explanation of Findings

The researcher worked together with IT personnel and also extracted information from already documented work to identify how to minimize costs of SSL Certificates. From the mentioned source, the researcher concluded that a different approach can be used other than the one already in place. The data collected was tailored to assist in answering and meeting the objectives of the research. The discussion below explains how the research objectives were met.

6.3 Discussions

The first objective in Section 1.3 was to identify challenges in the SSL Certificate Management. The study identified that most Enterprises spend a great deal of money on purchasing of SSL Certificates. Also some of the Certificate Authorities have been breached in the past due to lack of validation of the requestors information of who they claim to be. This has hence led to the actual Certificates being distrusted until they follow due process set by regulators. The second objective was to review the gap in the current Certificate Authority in terms of cost optimisation. The main challenge identified in the research was the relatively high cost of Certificates when bought from a public Certificate Authority service provider. This is dependent on the type of Certificate to be purchased and the validity period.

The third objective was to design and implement a private Certificate Authority Infrastructure by use of a prototype. Section 4.3 System Design and Architecture describe how the design of the Certificate Authority was done in accordance to the system requirements. Chapter 5 describes the development process of the Certificate Authority as per the designs that had been developed. When building a Certificate Authority, the main cost would be the initial cost which includes hardware costs and periodic costs which includes purchase of software licenses and internal staffing cost for managing of the CA. The Researcher performed different tests and documented the results for the

test in section 5.5. After successful testing, it was concluded that the Certificate Authority met the required functionalities. The final objective was to validate the built prototype and it was concluded that for costs to be saved, the CA would need to sell certificates to its enterprise customers at yearly. The certificate price and the amount of certificates determined the different breakeven points as depicted in Table 6.1.

	Certificate Number				
	1,000	2,000	3,000	4,000	5,000
Price					
$20	-	-	Year6	Year3	Year3
$30	-	Year6	Year2	Year1	Year1
$40	-	Year3	Year1	Year1	Year1

Table 6.1 Breakeven Points for Different Scenarios

6.4 Advantages of the Private Certificate Authority versus Purchasing of Certificates.

The developed Certificate Authority has the following advantages over purchased Digital Certificates.

i) The process of issuing Certificates is faster since for internal requests, verifications are not required

ii) The certificate can be trusted within a private network and loaded in the trusted root folders and intermediate CA and hence still usable even with the 'untrusted disclaimer' on browsers.

iii) It is easy to revoke an issued certificate and the certificates can be given short validity period which reduces the scope of data compromised if server vulnerability is uncovered.

6.5 Disadvantages of the Private Certificate Authority Prototype

Certificates from a private CA will not be trusted unless it is added to the browser's root list. This requires rigorous auditing and there is no single definition of what it means to be trusted, since each application is free to define their trust and use their own root certificates. The cost is not

necessarily cheaper since this is dependent of the amount of certificate being issued. This also does not make economic sense if the enterprise is a small one.

6.6 Conclusions

From the feedback received during the user test, the developed prototype received positive feedback. A private CA would be advantageous if the enterprise already has an equipped primary site and a disaster recovery site. For those that offer managed services like web service hosting, it would still require that the certificates are included in web browsers and this is done at an extra cost.

To break even if selling at $20 the breakeven would be during the sixth year for 1,000 certificates and third year for both 4,000 and 5,000 certificates. If selling at $30 the breakeven would be during the sixth year if selling 2,000 certificates, second year if selling 3,000 and first year if selling 4,000 and 5,000 certificates. If selling at $40, the breakeven would be during the third year if selling 2,000 certificates during the first year is selling 3,000 certificate or more. It is therefore recommended that for enterprises who need to have services accessed by non-domain users, it is cheaper to purchase digital certificates and they are already publicly trusted if they do not have any potential enterprise customers.

Chapter 7: Conclusions, Recommendations and Future Work

7.1 Conclusions

From the research, it was concluded that the feasibility of running a cost effective private certificate authority depends on the type of business. It is cost effective for enterprises that already have infrastructure in place for their core business so that the CA services can ride on this infrastructure. These include backup costs, load balancing, virtualisation software licenses and hardware, firewalls, and archival.

The users survey conducted users found the Microsoft based CA appealing and easy to use with minimal latency.

From Chapter 6, it was evidently clear that there is a point below which a private CA would cost more to run than purchasing of digital certificates.

7.2 Recommendations

From the feedback received during the user test, the developed prototype received positive feedback. A private CA would be advantageous if the enterprise already has infrastructure set up on both the primary and disaster recovery sites.

The breakeven points for different prices and different number of customers is given in Table 7.1

	Certificate Number				
	1,000	2,000	3,000	4,000	5,000
Price					
$20	-	-	Year6	Year3	Year3
$30	-	Year6	Year2	Year1	Year1
$40	-	Year3	Year1	Year1	Year1

Table 7.1 Breakeven Points for Different Scenarios Summary

Also for those that offer managed services like web service hosting, it would still require that the digital certificates are included in web browsers and this is done at an extra cost after a satisfactory audit process.

The cost of the certificates needs to be considerably affordable so as to be attractive to the customer who is being on boarded. Also it should be included in the contract and service level agreement document so that it is viewed as a value addition rather than an extra cost as much as it could be negligible.

7.3 Future Work

The researcher focused this study on a single case study which is a telecommunication company and offers managed services to its clients. The researcher recommended that a cost comparison be done using other trusted root certificate authorities for cross signing so as to have the CA issue trusted certificates.

References

Angeng'o, C. (2013, March). *Techweez*. Retrieved November 17, 2016, from Kenyan Government Commisions National Public Key Infrastructure (PKI): http://www.techweez.com/2013/03/20/government-commission-national-public-key-infrastructure/

Beaudouin, Michel; Mackay, Wendy;. (2002). *Prototyping Tools and Techniques.* Retrieved from https://www.kth.se/social/upload/52ef5ee4f2765445a466a28a/mackay-lafon-prototypes-52-HCI.pdf

Boeyen, S. (1997). *Certificate Policies and Certification Practise Statements.* Retrieved from http://www.entrust.com/wp-content/uploads/2013/05/cps.pdf

Brink, D. (2002, August). *PKI and Financial Return on Investment.* Retrieved from Oasis PKI: http://www.oasis-pki.org/pdfs/Financial_Return_on_Investment.pdf

CGI Group Inc. (2004). Public Key Encryption and Digital Signature: How do they work? *CGI*.

Chokhani, S. (1996). A Security Flaw in the X.509 Standard. *CygnaCom Solutions, Inc* .

Clark, D. D., Borbert, E. W., & Gerhart, S. (1991). *Computers at Risk Safe Computing in the Information Age.* National Academy Press.

Communications Authority of Kenya . (2013). The Establishmet of Kenya National Public Key Infrastructure (PKI).

Entrust. (2005). *x.509 PKI Certificates Drive Enterprise Security*. Retrieved from Entrust: https://www.entrust.com/resources-downloads/x509/

Entrust. (2009). *PKI best Cost Value.* Retrieved from https://www.entrust.com/wp-content/uploads/2013/05/Entrust-Managed-Services-PKI_TCO.pdf

Flavio, M. (2015). *Enterprise SSL Certificate Management: What You Need to Know*. Retrieved November 2, 2016, from digicert: https://blog.digicert.com/managedpki-is-the-right-solution-for-enterprise-certificate-management/

Geraint, W. (2015, February 20). *Trust within the PKI*. Retrieved from GeraintW Online Blog: http://geraintw.blogspot.co.ke/2015/02/trust-within-pki.html

Gigovic, B. (2014). Fundamentals of the PKI Infrastructure. *Global Knowledge Training LLC*.

GoDaddy. (2015). *What is an intermediate certifiacate*. Retrieved from Go Daddy: https://uk.godaddy.com/help/what-is-an-intermediate-certificate-868

Goodin, D. (2017, January 21). *Already on probation, Symantec issues more illegit HTTPS certicates* . Retrieved April 4, 2017, from Ars Technica: https://arstechnica.com/security/2017/01/already-on-probation-symantec-issues-more-illegit-https-certificates/

Group, C. S. (2016, September). Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates.

Hahnle, R., & Tinelli, C. (2007, August). *Introduction to UML.* Retrieved from The University of Iowa: http://homepage.divms.uiowa.edu/~tinelli/classes/181/Spring08/Notes/04-UML-intro.pdf

Haine, B. (2013). PKI Models: Whom do you trust? *SANS*.

Hamilton, Booz Allen &. (2000). Approach for business case analysis of using PKI on Smart Cards for Governmentwide Applications.

Hruska, J. (2017, January 23). *Symantec caught once again improperly issuing illegitimate HTTPS certificates*. Retrieved April 4, 2017, from ExtremeTech: https://www.extremetech.com/internet/243202-symantec-caught-improperly-issuing-illegitimate-https-certificates

Josang, A. (2013). PKI Trust Models. *IGI Global*, 4-15.

Let's Encrypt. (2016, April). *How It Works* . Retrieved from Let's Encrypt: https://letsencrypt.org/how-it-works/

Lintner, J. (2002). The Place and roles of the Certificate Authority. *Narodna Banka Slovenska*.

Lotz, M. (2013, July 5). *Segue Technologies* . Retrieved February 18, 2017, from Waterfall vs Agile: Which is the Right Development Methodology for your Project?: http://www.seguetech.com/waterfall-vs-agile-methodology/

Lync, V. (2017, March 20). *PayPal Certificate Far More Prevelant than Prevously Thought*. Retrieved from SSLStore: https://www.thesslstore.com/blog/lets-encrypt-phishing/

Mbuvi, D. (2013, March 21). *CIO/ East Africa*. Retrieved from Kenya's PKI likely to catalyse e-Business growth: http://www.cio.co.ke/news/main-stories/kenya's-pki-likely-to-catalyse-e-business-growth

Melone, M. (2012, April 9). *Microsoft Technet*. Retrieved from PKI Certificates and the X.509 Standard: https://blogs.technet.microsoft.com/option_explicit/2012/04/09/pki-certificates-and-the-x-509-standard/

Microsoft. (2011, April 15). Retrieved November 7, 2016, from Offline Root CA: https://social.technet.microsoft.com/wiki/contents/articles/2900.offline-root-certification-authority-ca.aspx

Microsoft. (2016). *Securing PKI: Planning a CA Hierarchy*. Retrieved from Technet: https://technet.microsoft.com/en-us/library/dn786436(v=ws.11).aspx

Moulds, R. (2016, February 15). *Building Trust into a PKI- Part 4*. Retrieved from Key Management and Payments Security Blog- Thales e-Security: https://www.thales-esecurity.com/blogs/2013/june/building-trust-into-a-pki

Neubauer, J. (2003, June 15). *Building a 3-Tier CA Hierarchy*. Retrieved November 14, 2016, from ITPro Windows: http://windowsitpro.com/security/building-3-tier-ca-hierarchy

Remy, A. (2016, March 11). *Installing a Two Tier PKI Hierarchy in Windows Server 2016*. Retrieved November 12, 2016, from My IT World: http://arthurremy.com/index.php/107-tutorials/342-installing-a-two-tier-pki-hierarchy-in-windows-server-2016

Rouse, M. (2009). *TechTarget*. Retrieved November 2, 2016, from x.509 Certificate: http://searchsecurity.techtarget.com/definition/X509-certificate

SANS. (2013, July 28). *PKI Trust Models.* Retrieved from https://www.sans.org/reading-room/whitepapers/vpns/pki-trust-models-trust-36112

Shanks, W. (2013). Building and Managing a PKI solution for small and medium size business. *SANS*.

Sleevi, R. (2017, March 23). *Intent to Deprecate and Remove: Trust in existing Symantec-isssued Certificates.* Retrieved from Google Groups: https://groups.google.com/a/chromium.org/forum/#!msg/blink-dev/eUAKwjihhBs/_IALqHtKCQAJ

Sunsted, T. (2002, May 24). *IT World*. Retrieved February 2, 2017, from EJBCA: An Open Source, Java-based Certificate Authority: http://www.itworld.com/article/2785524/development/ejbca--an-open-source--java-based-certificate-authority.html

Symantec. (2017). *How Certificate Chains Work*. Retrieved from Symantec: https://knowledge.symantec.com/support/ssl-certificates-support/index?page=content&actp=CROSSLINK&id=SO16297

Trusted Root Certificate. (2012, May nd). *Certificate Authorities and Trust Hierarchies*. Retrieved from Global Sign: https://www.globalsign.com/en/ssl-information-center/certificate-authority-root/

Verizon. (2017, April 20). *Data Breach Investigations.* Retrieved from https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf

Wiseman, S. (2012, July 23). *Why Policy CAs?* Retrieved Novmber 12, 2016, from Network Steve: http://www.networksteve.com/forum/topic.php/Why_POLICY_CAs/?TopicId=33996&Posts=6

APPENDIX I: Digital Certificates Interview Questions

Pre-Prototyping

This Interview was designed to get feedback on the cost implication of purchasing of digital certificates so to help to in finding out whether running a private certificate authority would be a cheaper option.

1. Do you run a private certificate authority?
   () Yes
   () No
2. What do you use digital certificates for?
   () E-mail signing
   () Securing Web Servers
   () Code Signing
   () Client Authentication
3. If any other is used, kindly list them.

_____

4. How much on average do you spend on purchasing the digital certificates yearly?

APPENDIX II: User Experience Feedback

Post-Prototyping

This questionnaire was designed to get feedback on the CA prototype and help improve or address any features of concern. Please ascertain if you are able to view load a certificate signing request, issue a certificate, revoke it and push certificates to endpoints using group policy.

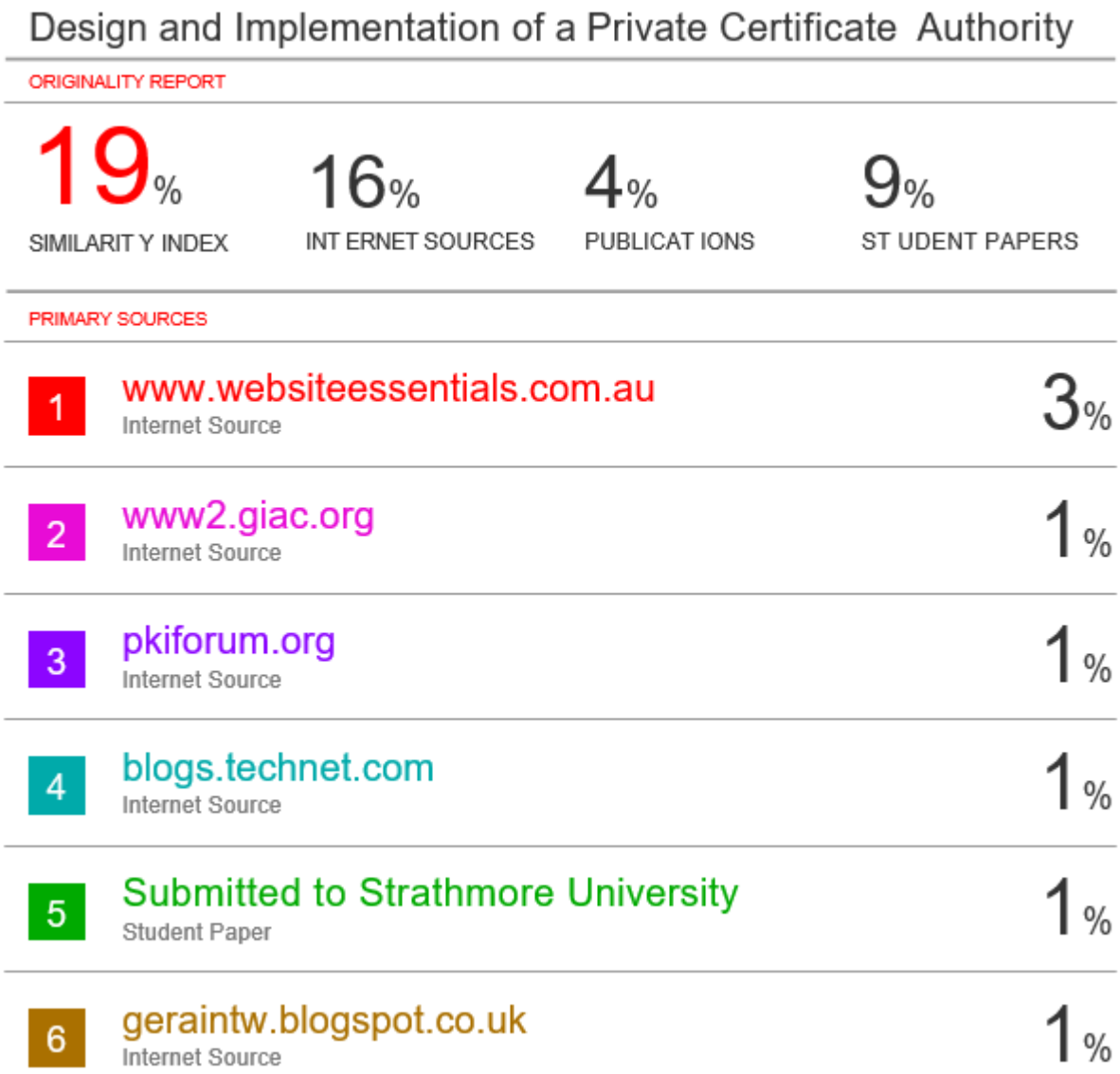
1. The prototype was appealing
   () Agree
   () Disagree
2. If you disagree, kindly give your reason

_____

3. Core functionalities were easy to find.
   () Agree
   () Neutral
   () Disagree
4. The application was responsive when interacting with and performing background tasks.
   () Agree
   () Neutral
   () Disagree
5. Would you consider the application more effective as compared to the current system?
   () Yes
   () No

APPENDIX III: Turnitin Similarity Index Report

*



Design and Implementation of a Private Certificate Authority

ORIGINALITY REPORT

19%	16%	4%	9%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.websiteessentials.com.au Internet Source	3%
2	www2.giac.org Internet Source	1%
3	pkiforum.org Internet Source	1%
4	blogs.technet.com Internet Source	1%
5	Submitted to Strathmore University Student Paper	1%
6	geraintw.blogspot.co.uk Internet Source	1%