



**Strathmore**  
UNIVERSITY

Strathmore University  
**SU+ @ Strathmore**  
University Library

---

**Electronic Theses and Dissertations**

2018

# 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*

Follow this and additional works at <https://su-plus.strathmore.edu/handle/11071/5993>

## Recommended Citation

Rioba, D. M. (2018). *Design and implementation of a private certificate authority: a case study of Telkom Kenya Limited* (Thesis). Strathmore University. Retrieved from <https://su-plus.strathmore.edu/handle/11071/5993>

This Thesis - Open Access is brought to you for free and open access by DSpace @Strathmore University. It has been accepted for inclusion in Electronic Theses and Dissertations by an authorized administrator of DSpace @Strathmore University. For more information, please contact [librarian@strathmore.edu](mailto:librarian@strathmore.edu)

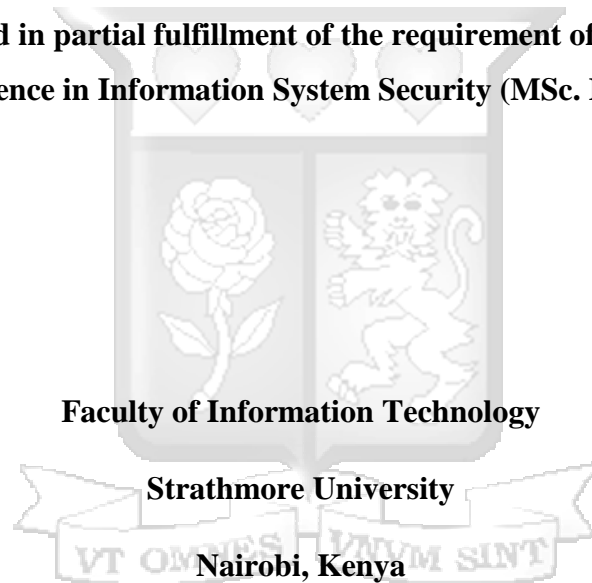
# **DESIGN AND IMPLEMENTATION OF A PRIVATE CERTIFICATE AUTHORITY**

**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)**



**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.....

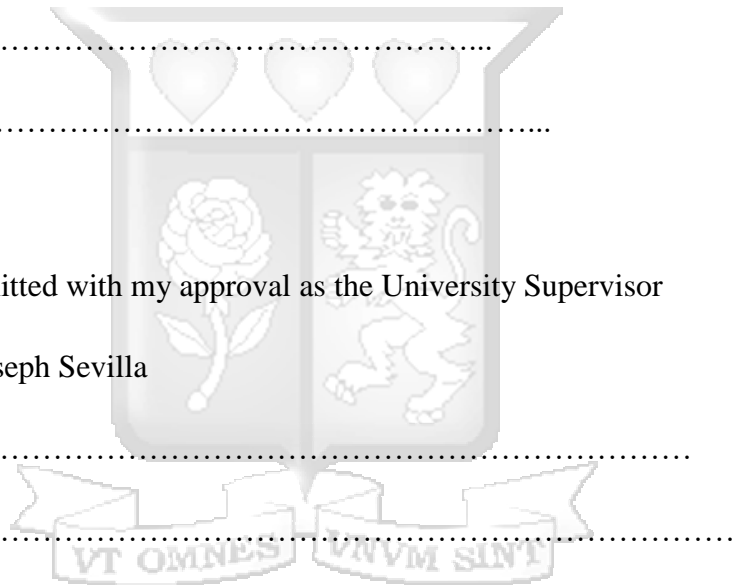
Date: .....

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, GoDaddy, 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































































































## 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.

<b>Test Case Name: System Test</b>				
<b>Date Tested: 5<sup>th</sup> April 2018</b>				
<b>Preconditions</b>				
<b>Post Conditions</b>				
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

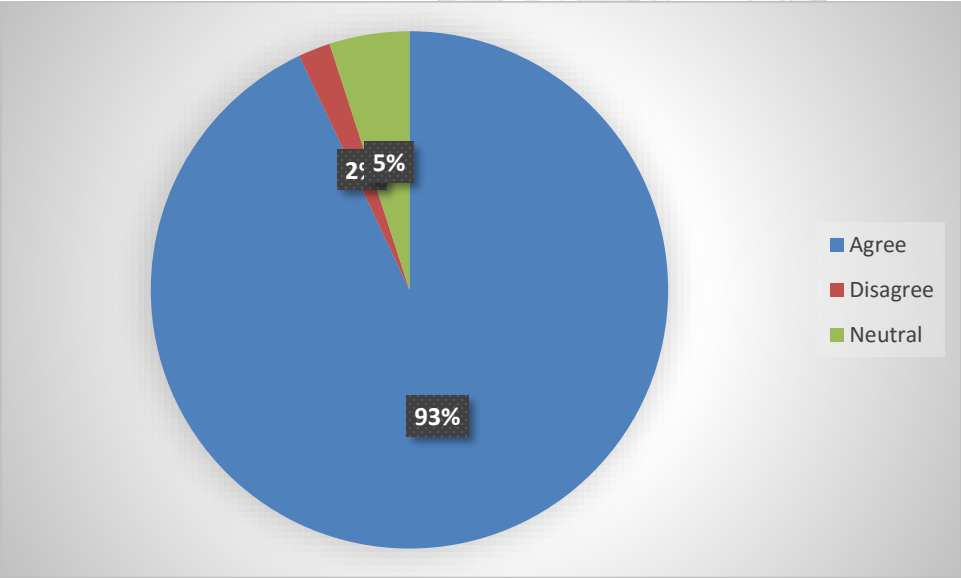
	Agree	Disagree	Other
--	-------	----------	-------

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.

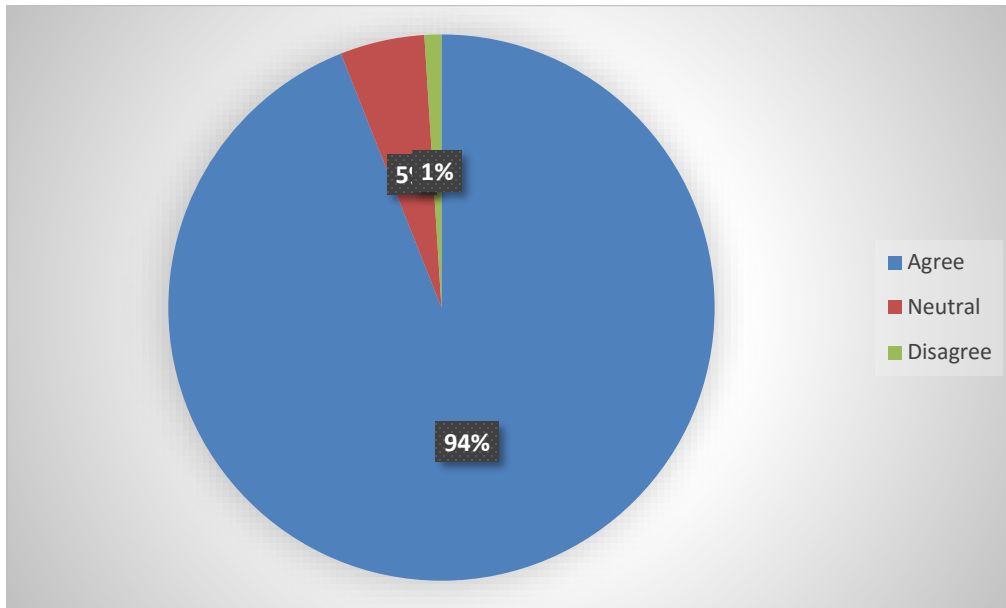
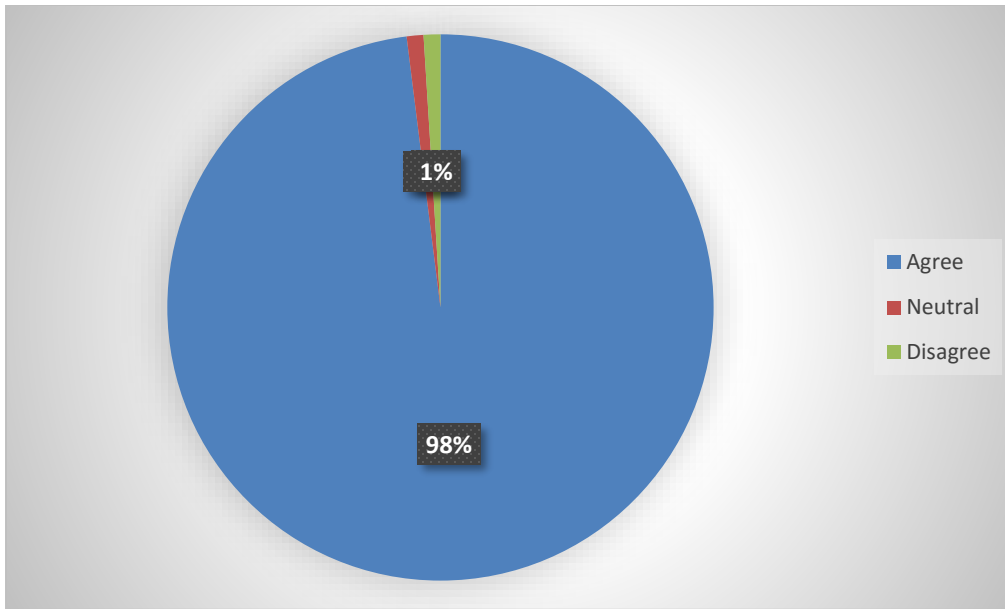


Figure 5.10 Ease of Use

## iii) System Responsiveness

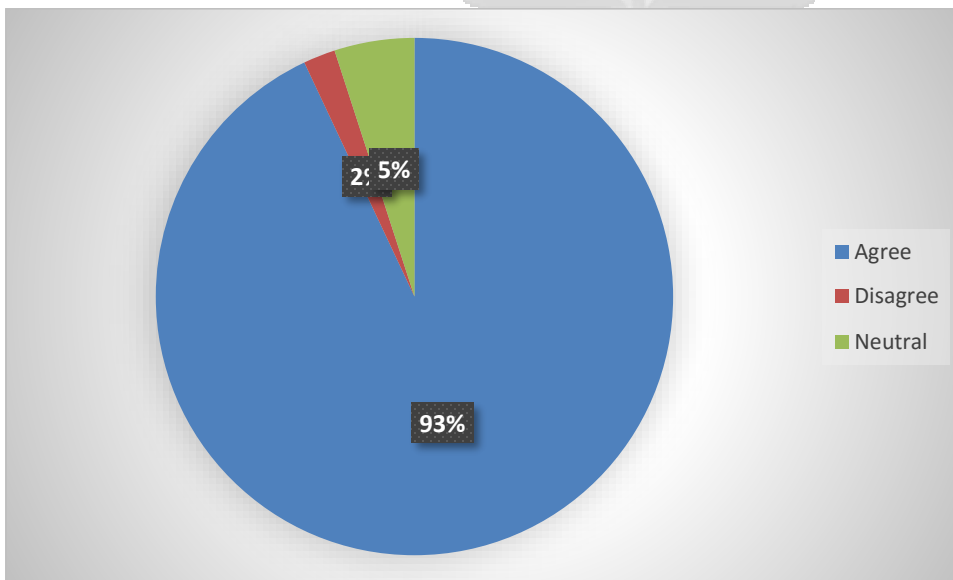
During performance of different transactions, users tested how responsive the system was in terms of giving feedback during various transactions which were mainly, issuance, revocation and request of digital certificates. The results are depicted in Figure 5.9



**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 200 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
<b>Total</b>			<b>1</b>	<b>\$36,800</b>	<b>\$535</b>	<b>1</b>	<b>\$13, 535</b>

**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 mainly 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 paid to the CA admin. The cost implication would be as in Table 5.4.

		Private CA Cost (Year 1)			2 <sup>nd</sup> 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
<b>Total Cost</b>				<b>\$113,600</b>			<b>\$48,600</b>
Certificate issuing price	Single Certificates	\$35	2,000	\$70,000	\$35	2,000	\$70,000
	Wildcard Certificates	\$100	0	0	\$100	0	0
<b>Total cost Difference</b>				<b>-\$43,600</b>			<b>\$21,400</b>

**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.

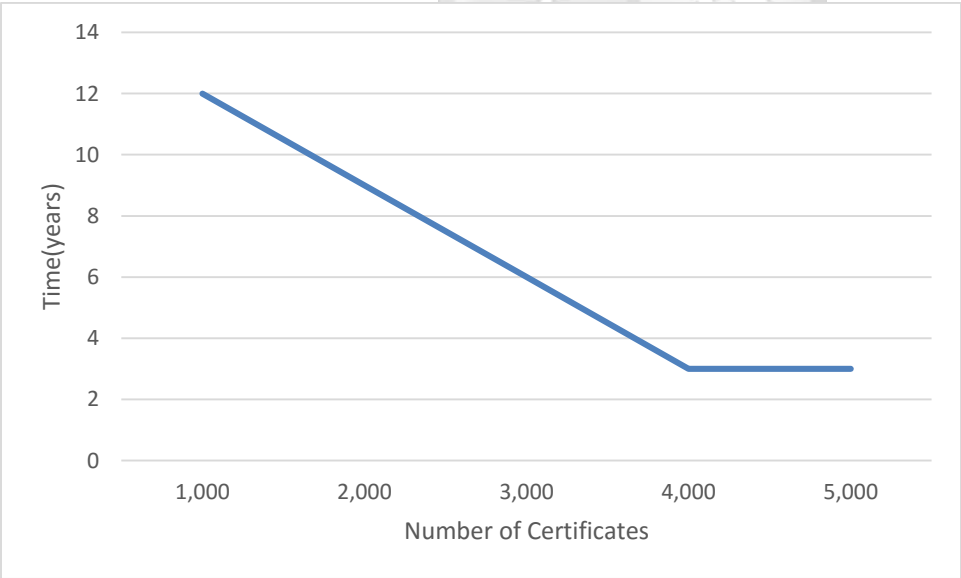
Also, the researcher user different selling prices ranges; \$20, \$30 and \$40.

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 6<sup>th</sup> year and in the 3<sup>rd</sup> year if selling 4000 or 5000 digital certificates. This is shown in Table 5.7

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

**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**

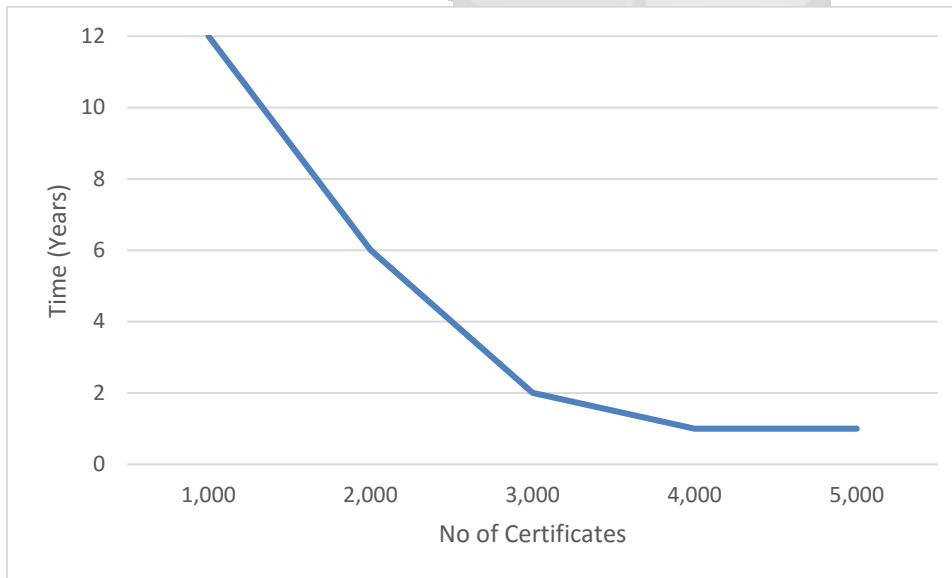
When digital certificates are sold at \$30, continuous losses are made when selling 1,000 certificates or less. The breakeven point is achieved during year six and second year when selling

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	<b>113,600</b>	<b>48,600</b>	<b>48,600</b>	<b>48,600</b>	<b>48,600</b>	<b>48,600</b>	
Revenue	30,000	30,000	30,000	30,000	30,000	30,000	1,000
Cumulative Profit Made	<b>-83,600</b>	<b>-102,200</b>	<b>-120,800</b>	<b>-139,400</b>	<b>-158,000</b>	<b>-176,600</b>	Certificates
Revenue	60,000	60,000	60,000	60,000	60,000	60,000	2,000
Cumulative Profit Made	<b>-53,600</b>	<b>-42,200</b>	<b>-30,800</b>	<b>-19,400</b>	<b>-8,000</b>	<b>3,400</b>	Certificates
Revenue	90,000	90,000	90,000	90,000	90,000	90,000	3,000
Cumulative Profit Made	<b>-23,600</b>	<b>17,800</b>	<b>59,200</b>	<b>100,600</b>	<b>142,000</b>	<b>183,400</b>	Certificates
Revenue	120,000	120,000	120,000	120,000	120,000	120,000	4,000
Cumulative Profit Made	<b>6,400</b>	<b>77,800</b>	<b>149,200</b>	<b>220,600</b>	<b>292,000</b>	<b>363,400</b>	Certificates
Revenue	150,000	150,000	150,000	150,000	150,000	150,000	5,000
Cumulative Profit Made	<b>36,400</b>	<b>137,800</b>	<b>239,200</b>	<b>340,600</b>	<b>442,000</b>	<b>543,400</b>	Certificates

**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.



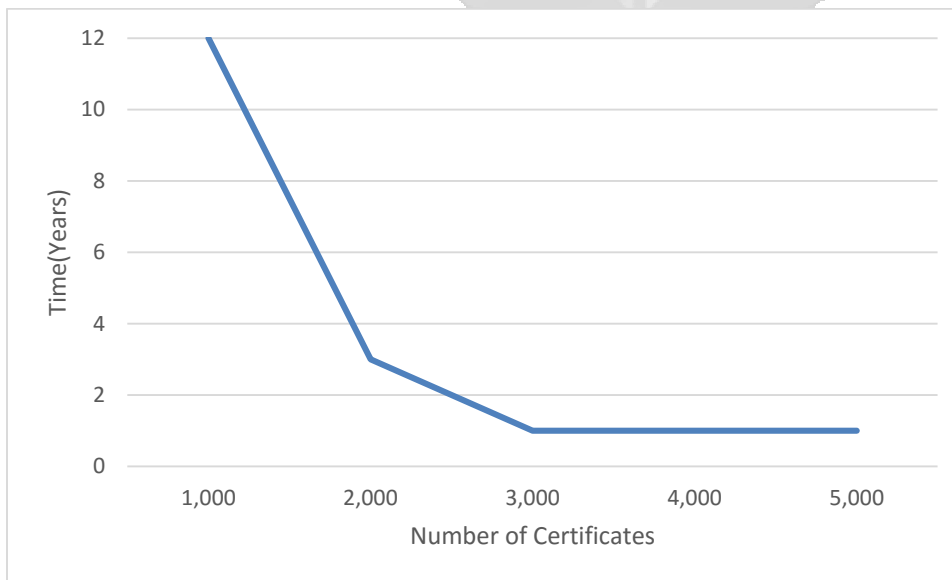
**Figure 5.14 Breakeven Point when Selling at \$30**

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	<b>113,600</b>	<b>48,600</b>	<b>48,600</b>	<b>48,600</b>	<b>48,600</b>	<b>48,600</b>	
Revenue	40,000	40,000	40,000	40,000	40,000	40,000	1,000
Cumulative Profit Made	<b>-73,600</b>	<b>-82,200</b>	<b>-90,800</b>	<b>-99,400</b>	<b>-108,000</b>	<b>-116,600</b>	Certificates
Revenue	80,000	80,000	80,000	80,000	80,000	80,000	2,000
Cumulative Profit Made	<b>-33,600</b>	<b>-2,200</b>	<b>29,200</b>	<b>60,600</b>	<b>92,000</b>	<b>123,400</b>	Certificates
Revenue	120,000	120,000	120,000	120,000	120,000	120,000	3,000
Cumulative Profit Made	<b>6,400</b>	<b>77,800</b>	<b>149,200</b>	<b>220,600</b>	<b>292,000</b>	<b>363,400</b>	Certificates
Revenue	160,000	160,000	160,000	160,000	160,000	160,000	4,000
Cumulative Profit Made	<b>46,400</b>	<b>157,800</b>	<b>269,200</b>	<b>380,600</b>	<b>492,000</b>	<b>603,400</b>	Certificates
Revenue	200,000	200,000	200,000	200,000	200,000	200,000	5,000
Cumulative Profit Made	<b>86,400</b>	<b>237,800</b>	<b>389,200</b>	<b>540,600</b>	<b>692,000</b>	<b>843,400</b>	certificates

**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**

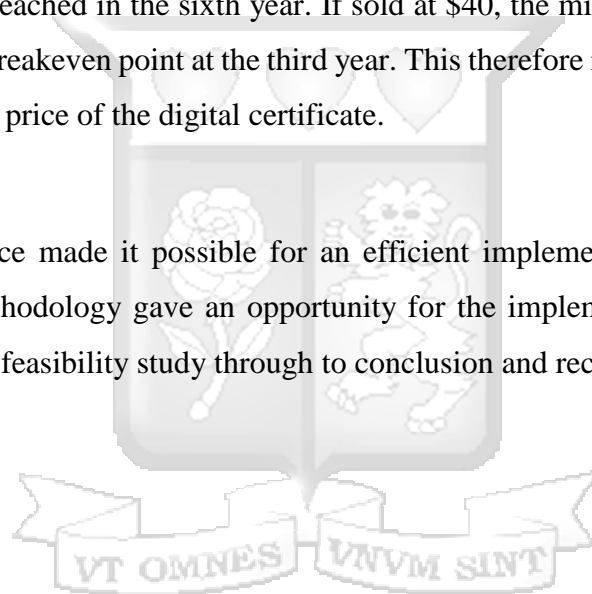
From the cost analysis above, it would be cheaper if certificates were sold solely to enterprise customers. To break even, at \$20, the certificates need to be over 3,000 certificates; at \$30 and \$40, equal to or greater than 2,000 certificates;

### **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**

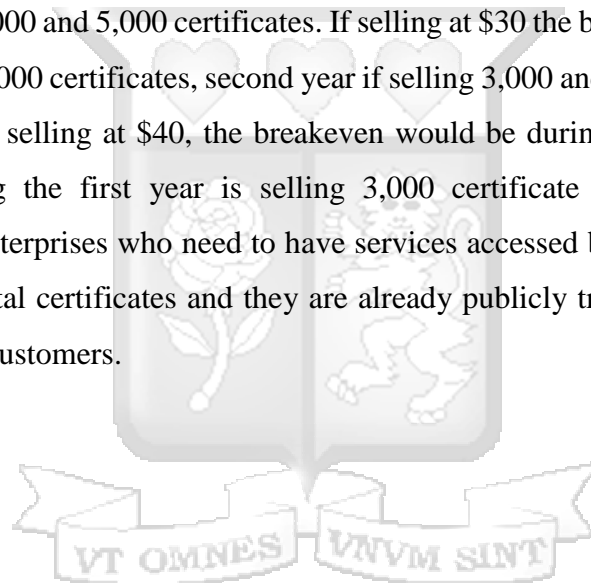
Certificates from a private CA will not be trusted unless it is added to the browser’s root list. This requires rigorous auditing and there is no single definition of what it means to be trusted, since each application is free to define their trust and use their own root certificates. The cost is not

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 Commissions 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](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](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 Prevalant than Previously 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/](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](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.
- Slevi, R. (2017, March 23). *Intent to Deprecate and Remove: Trust in existing Symantec-issued Certificates*. Retrieved from Google Groups: [https://groups.google.com/a/chromium.org/forum/#!msg/blink-dev/eUAKwjihhBs/\\_IALqHtKCQAJ](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 November 12, 2016, from Network Steve: [http://www.networksteve.com/forum/topic.php/Why\\_POLICY\\_CAs/?TopicId=33996&Posts=6](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%**

SIMILARITY INDEX

**16%**

INTERNET SOURCES

**4%**

PUBLICATIONS

**9%**

STUDENT PAPERS

#### PRIMARY SOURCES

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