A Framework for PKI Implementation: Optimizing Project Management in Ethiopia

Name

Binyam Ayele Haile

Advisior

Henock Mulugeta (PhD)

ADDIS ABABA UNIVERSITY
ADDIS ABABA INSTITUTE OF TECHNOLOGY - AAiT
SCHOOL OF INFORMATION TECHNOLOGY AND ENGINEERING – SiTE

September 2024

ADDIS ABABA UNIVERSITY
ADDIS ABABA INSTITUTE OF TECHNOLOGY - AAiT
SCHOOL OF INFORMATION TECHNOLOGY AND ENGINEERING – SiTE

Binyam Ayele Haile

Advisor: Henock Mulugeta (PhD)

This is to certify that the thesis proposal is prepared by Binyam Ayele titled: "A Framework for PKI Implementation: Optimizing Project Management in Ethiopia". Submit in partial fulfillment of the requirement for the Degree of Master of Science in Cybersecurity(Cyber governance and Management) complies with the regulations and guideline of the university and meets the acceptable standard concerning originality and quality.

Signed by the Examining Committee(SGC):

Name	Signature	Date
1. Advisor: Henock Mulugeta (PhD)	_____	_____
2. Examiner: To be defined	_____	_____
3. Examiner: To be defined	_____	_____

Abstract

In today's increasingly digital world, the security of online communications and transactions is paramount. Public Key Infrastructure (PKI) has emerged as a cornerstone technology for ensuring secure, authenticated, and confidential digital interactions. However, the implementation of PKI projects remains challenging due to its inherent complexities, including certificate management, key distribution, and system integration, National legal framework contradictions & Limitations, lack of interoperability. The lack of a standardized implementation framework further exacerbates these challenges, leading to inconsistent and often flawed deployments that fail to leverage the full potential of PKI.

This study investigates the importance of optimizing a PKI Project implementation framework that support the establishment of a national or organizational PKI project at national or organizational level by developing a comprehensive framework that mitigate PKI project implementation challenges. The study seeks to address the critical need for a comprehensive PKI Project Implementation Framework that can guide organizations in navigating the complexities of PKI deployment. The problem under investigation is the absence of standardized and generic framework and best practices for PKI implementation, which has resulted in varied levels of security and effectiveness across different sectors. The study aims to develop a framework that is adaptable to diverse organizational contexts, ensuring that PKI systems are implemented in a manner that is both secure and scalable.

To achieve this goal, a systematic literature review (SLR) methodology will be employed as the primary research method. The SLR will systematically identify, evaluate, and synthesize existing research on PKI implementation, focusing on the challenges, best practices, and potential solutions proposed in the literature. By analyzing a wide range of studies, the SLR will provide a comprehensive understanding of the current state of PKI implementation and identify gaps that the proposed framework can address. This method will ensure a rigorous and evidence-based approach to the development of the PKI Project Implementation Framework.

This research focused on developing a PKI implementation framework that assist PKI project management. A case study and Key Performance Indictor (KPI) is incorporated to evaluate the proposed framework. As a direct outcome of this study, stakeholders who have plans to implement

PKI within Ethiopia or other country will obtain a proactive understanding of potential implementation considerations that should be taken.

Key words: PKI, PKI framework, Project Management, PKI project implementation

Acknowledgments

My advisor, Dr. Henock Mulugeta (PhD), deserves special recognition because he oversaw my w ork, made the effort to read it, and offered insightful feedback at every stage, beginning with the choice of titles and continuing right up until this point. I would also like to express my gratitude and appreciation to my wife, Bethelehem Motele, as well as my friend, Amanuel Majore, and my brother, Bereket Ayele,a for their encouragement and support, both in terms of their moral and material contributions.

Table of Contents

1 Introduction 1
1.1 Background information 1
1.2 Statement of the problem 3
1.3 Research questions 4
1.4 The objective of the study 4
1.4.1 General objective 4
1.4.2 Specific objective 4
1.5 Contribution of the Thesis study 4
1.5.1 Scientific Contributions 4
1.5.2 Practical Contributions 5
1.5.3 Scope 5
1.6 Structure of the document 5
2 Literature review 6
2.1 Public Key Infrastructure(PKI) 6
2.2 PKI Standards and Legal Frameworks 6
2.3 Threat landscape of PKI ecosystem 9
2.4 Project Management challenges 10
2.5 Related Works 10
2.5.1 Public Key Infrastructure (PKI) in E-Government Systems 10
2.5.2 PKI-Based Secure Infrastructures in Mobile E-Commerce 11
2.5.3 PKI in Educational Institutions 11
2.5.4 Case Studies and Comparative Analysis 11
2.5.5 Comparative Studies and Frameworks 12
2.6 Research gaps 12
3 Methodology 14
3.1 Data Collection 15
3.2 Analysis Method 15
4 Proposed PKI Project Implementation Framework 16
4.1 PKI project implementation phases 18
4.1.1 Analysis: 18
4.1.2 Design: 18

4.1.3 Implementation: 19
4.1.4 Operations & Integration: 19
4.1.5 Continuous Monitoring and Maintenance: 19
4.2 PKI Core Activities in Implementation: 19
4.3 PKI Governance Framework: 19
4.3.1 PKI Deployment Model: 19
4.3.2 PKI Infrastructure and Facility: 19
4.3.3 PKI Training and Awareness: 19
4.3.4 PKI Audit and Certification: 19
4.4 Interdependencies: 20
4.5 PKI Project Implementation Workflow 22
4.6 KPI for success of the Proposed framework 24
4.7 Scenario 25
5 Experiments and Analysis 28
5.1 Experiment 28
5.1.1 Systematic Literature Review 28
5.1.2 Case Study PKI in case of Ethiopia 45
5.1.3 Monitoring and maintenance 52
5.2 Analysis 53
5.2.1 Study Selection Analysis 53
5.2.2 Research Finding's Analysis 55
5.2.3 Case study Interview Analysis 64
6 Results and discussion 67
6.1 Results 67
6.1.1 Overview of PKI Implementation Framework 67
6.1.2 Key Findings 67
6.2 Discussion 69
6.2.1 Effectiveness of the Framework 69
6.2.2 Key Challenges and Mitigations 69
6.2.3 Comparison with Existing Frameworks 70
6.2.4 Impact on Organizational Security Posture 70
6.2.5 Lessons Learned and Future Improvements 70

7 Summary, future work 71
7.1 Summary 71
7.2 Future Work 71
8 References 73
9 Appendix 77
9.1 Appendix A. Description of persons selected for the interview 77
9.2 Appendix C. Assurance 77
9.3 Appendix D. Interview Questions and transcribed Responses 77

List of Figures

Figure 1.PKI and Its Application 1
Figure 2.Kenya PKI Legal Framework 9
Figure 10.The proposed PKI Framework 18
Figure 11. PKI Project detail workflow diagram 21
Figure 3.PRISMA Study Selection process workflow 34
Figure 4. Quality Assessment result 37
Figure 17.Ethiopian National PKI Deployment Model 48
Figure 18.Ethiopian National PKI Infrastructure & Facility 49
Figure 6. PI chart articles selected per source generated through Parsifal 53
Figure 7. bar graph accepted articles selected per source generated through Parsifal 54
Figure 8. The Distribution of the study generated through VOSViewer 55

List of Table

Table 1.PKI Project execution core Activities 16
Table 2. PKI project Phases 16
Table 3. Identified Themes by Phases and Core Activities 17
Table 4.PKI Project participating stakeholder and actors 22
Table 5.PKI Project detail workflow diagram description 24
Table 6.key performance indicator 24
Table 7.PICO Framework 29
Table 8.Research Question 29
Table 9.Research Objective 29
Table 10.digital library sources 30
Table 11.Inclusion and exclusion criteria 30
Table 12.Quality Assessment (QA) checklist 31
Table 13. Data extraction form 31
Table 14. Search strings generated through Parsifal 32
Table 15. Search String results 33
Table 16. Data extraction Summery 42
Table 17. Data synthesis summery table for challenges from studies 45
Table 18.Data synthesis summery table for frameworks from studies 45
Table 19. Ethiopian National PKI Governing Framework 48
Table 20.Liste of selected articles based on publication years 55
Table 21.Greek E-government PKI project implementation methodology 61
Table 22. Cameroon National PKI project execution framework 62
Table 23. eGovernment PKI framework 62
Table 24. Public Key Infrastructure for UAE 62
Table 25. PKI Design for the Real world 63
Table 26: Description of persons selected for the interview 77
Table 27: Assurance methodology used 77
Table 28.Interview Questions and transcribed Responses 81

Abbreviations and acronyms

CA: Certificate Authority

CMP: Certificate Management Protocol

CP: Certificate Policy

CPS: Certificate Practice Statement

EY: Ernest and Young

IEC: International Electrotechnical Commission

IETF: Internet Engineering Task Force

INSA: Information Network Security Administration

ISO: International Organization for Standardization

ITU: International Telecommunications Union

ITU-T: International Telecommunications Union Technology Sector

KPMG: Klynveld Peat Marwick Goerdeler

PDL: Permissioned Distributed Ledger

PKI: Public key Infrastructure

RA: registration authority

RFC: Request for Comment

RQ: Research Question

SLR: Systematic literature review

CHAPTER ONE

1 Introduction

1.1 Background information

A PKI (Public key Infrastructure) is a set of roles, policies, and processes for handling public-key cryptography and digital certificate generation, distribution, use, storage, and revocation. PKI is the most fundamental and essential technology of the past several years, offering online transactions with near-perfect identity, integrity, and non-repudiation. The combination of these technology and legal backing will produce indistinguishable online and offline business environments [1].

PKI is primarily made up of five basic components, which are security policies, certificate authorities (CA), registration authorities (RA), certificate repositories, and PKI-enabled systems. Within the Public Key Infrastructure (PKI), a security policy is often specified by making use of both the CP (Certificate policy) and the CPS (Certificate practice statement), which are both components of the PKI regulatory framework. These policy documents provide a comprehensive operational method that outlines what and how the policy will be enforced and supported in PKI practice [2].

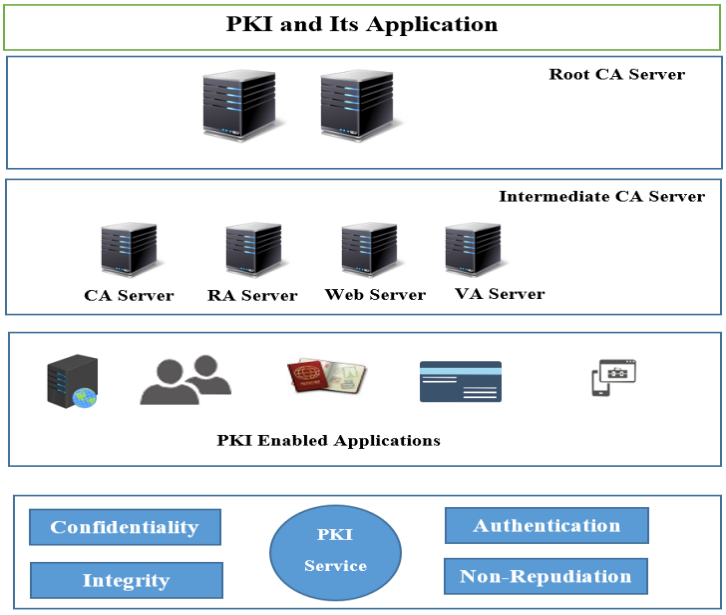


Figure 1.PKI and Its Application

A PKI does not perform a particular business function; rather, it serves as the basis for additional security services. A PKI's primary purpose is to enable the secure and trustworthy distribution and use of public keys certificates. A PKI serves as the foundation for various applications and network security components. Email, different chip card applications, value exchange with e-commerce (e.g., debit and credit cards), home banking, and electronic postal systems frequently require PKI-based security procedures [1].

There have been several published legal documents over the past few years that provide credence to the idea that PKIs should be established within Ethiopia. Electronic Signature Proclamation No. 1072.2018 is the most prominent one. Various initiatives have taken by different government organizations in Ethiopia to establish PKI at national level. Ministry of Innovation and Technology (MICT) formerly known as Ministry of Innovation and Technology (MinT) was the first to take this initiative in 2011, due to change of mandate INSA (Information Network Security Administration) formerly known as the Information Network Security Agency(INSA) have takeover the project in 2013, due to small number subject matter experts exist in the area, lack of defined legal framework and budget constraint the project has forced to delayed for long time.

In 2013, INSA, was given the authority to establish a root certificate authority under Ethiopian law (Proclamation Number 808/2013) [3] . The legal document produced by INSA in 2018 was one of the supporting legal document published to recognize the equivalence of digital signatures and paper-based signatures is the Electronic Signature Proclamation No. 1072.2018 [4]. These and other supporting documents provide the constitutional and statutory framework necessary to implement PKI on a national level in Ethiopia. While the aforementioned legal documents have been developed and published, the implementation of PKI in Ethiopia has not yet taken place until now.

Most projects made on various sector has failed due to various reasons. Project management requires strong leadership and effective management in order to gain the desired goals. Lack of resources, lack of well-established administrative systems and procedures are most prominent issues that are realized most often. Such issues mostly create adverse impact in developing countries when compared to developed countries [5].

When we come to PKI implementation project, one of the reasons behind this challenge is lack of a PKI implementation framework that support PKI project management. The aim of this study is

to design a PKI implementation framework based on review of various standards and literature sources published related to the PKI implementation framework that are conjectured with Project management frameworks.

1.2 Statement of the problem

Most projects made on various sector has failed due to various reasons. Project management requires strong leadership and effective management in order to gain the desired goals. lack of resources, lack of well-established administrative systems and procedures are most prominent issues that are realized most often. Such issues mostly create adverse impact in developing countries when compared to developed countries [4]. PKI project is one of the projects that require strong leadership and effective management.

It is known that PKI has become a cornerstone for securing communications and transactions in various domains, including e-commerce, e-government, and education [6] [7] [8] [9]. Despite its critical role in securing digital environments, the implementation of PKI projects faces numerous challenges that can impact their effectiveness and adoption. Many organizations face significant challenges in its implementation. These challenges include technical complexities, high costs, lack of standardized frameworks, and insufficient expertise among IT professionals [10] [11].

Existing researches on PKI has primarily focused on the technical aspects of cryptography and certificate management [12] [13]. However, there is a gap in the literature regarding the practical application of these technologies in real-world settings, particularly in how organizations can effectively implement PKI systems.

This research aims to address these issues by systematically reviewing existing literature, identifying key challenges & themes and developing a framework used as a practical guideline for effective PKI implementation. By doing so, it seeks to bridge the gap between theoretical knowledge and practical application.

As a direct outcome of this study, stakeholders who have plans to implement PKI within Ethiopia or other country will obtain a proactive understanding of potential implementation considerations that should be taken. In addition, the proposed PKI implementation framework will serve as a guide during the process of putting PKI into action in support of the project management.

1.3 Research questions

- What are the difficulties encountered during the implementation of a PKI project?
- How can a PKI implementation framework support the establishment of a national or organizational PKI implementation project?

1.4 The objective of the study

1.4.1 General objective

The aim of this study is to develop a PKI implementation framework that facilitates the implementation of PKI projects.

1.4.2 Specific objective

This study is intended to achieve the following specific objectives

- Develop a PKI implementation framework that assist PKI project management.
- Develop a KPI and case study and evaluate the Proposed Framework.

1.5 Contribution of the Thesis study

This study on the implementation framework for Public Key Infrastructure provides significant scientific and practical contributions to the field of digital infrastructure management.

1.5.1 Scientific Contributions

1. By developing a comprehensive framework for the establishment of PKI at national or organizational level, the research contributes a framework for the scientific community by drawing on the most effective methods from previous existed studies and industry standards and it seeks to bridge the gap between theoretical knowledge and practical application.
2. This research presents a holistic framework that integrates technical, organizational, governance and project management elements necessary for successful PKI deployment. Unlike existing frameworks that often focus solely on technical aspects, this framework emphasizes the importance of aligning PKI implementation with organizational goals, risk management practices, and regulatory requirements, thus providing a balanced approach that addresses both security and operational efficiency.

3. By synthesizing insights from academic research with practical case studies, the framework bridges the gap between theory and practice in PKI implementation. It offers actionable guidance to practitioners, decision-makers, and security architects, thereby fostering collaboration between academia and industry in the pursuit of more secure and efficient PKI deployments.

1.5.2 Practical Contributions

The framework that is developed will provide an insight to actualize the overall project implementation phases and core activities as well as the expected outcomes from each phase and core activity. As a result,

1. Stakeholders who have plans to implement PKI within Ethiopia or other country will obtain a proactive understanding of potential implementation considerations that should be taken.
2. The Developed PKI implementation framework will serve as a guide during the process of implementing PKI.

In summary, this study's significance lies in its ability to bridge the gap between the theoretical and practical aspects of PKI implementation. For the scientific community, it provides a valuable contribution to the understanding of PKI and their deployment. For practitioners, it offers a practical solution to the challenges of PKI implementation, ultimately enhancing the security and resilience of digital infrastructures.

1.5.3 Scope

This research aims to develop a PKI implementation framework that assists the PKI project execution. Consequently, various literature sources, PKI project technical specification documents and standards will be reviewed and utilized in support of structuring and designing the framework.

1.6 Structure of the document

The remainder of the paper is structured as follows. Chapter 2 provides an overview of PKI technology through literature review. Chapter 3 shows the methodology adopted for the current SLR including all the process utilized. The Proposed solution is presented in the Chapter 4, result and discussion are presented in the Chapter 5. Chapter 6 presents the summary and future work. Chapter 7 the references used for this study. The last section the appendix, the transcribed interview responses are included here.

CHAPTER TWO

2 Literature review

This section presents the literature review conducted on the research topic. For the purpose of the study, it incorporated all the fundamental concepts, project management challenges, related standards utilized for PKI as well as the threats targeting PKI service. Additionally, the literature review incorporated the review legal structure of Ethiopia.

2.1 Public Key Infrastructure(PKI)

A PKI is a set of roles, policies, and processes for handling public-key cryptography and digital certificate generation, distribution, use, storage, and revocation. e-commerce, online banking, and private email are just some of the network activities that benefit from PKI's secure electronic transfer of information [14].

The PKI is primarily made up of five basic components, which are security policies, CA, RA, certificate repositories, and PKI-enabled systems. Within the PKI, a security policy is often specified by making use of both the CP and the CPS, which are both components of the PKI regulatory framework. These policy documents provide a comprehensive operational method that outlines what and how the policy will be enforced and supported in PKI practice [2].

2.2 PKI Standards and Legal Frameworks

As part of the PKI's regulating structure, there are also a number of mandatory standards. Various standard-setting organizations establish and adopt these standards. International Telecommunications Union Technology Sector (ITU-T), Internet Engineering Task Force (IETF), and International Organization for Standardization/ International Electrotechnical Commission(ISO/IEC) are notable standard-setting organizations. Standards have a significant role in managing PKI-related concerns. Among the practices requiring a formal standard are the format of a digital certificate, certificate retrieval, and certificate expiration [15]

PKI relies heavily on adherence to standards. Standard X.509 is one of the well-known standards known as RFC5280, which was originally drafted in 1988 by ITU-T. This standard is intended to address both the format and use of PKI certificates. The other notable standard is RFC3647, which was issued in order to produce a systematic and unified CP and CPS document for the entire world.

The other well-known standard protocol for the administration of digital certificates is Certificate Management Protocol (CMP) with RFC2510 [15].

When we plan to setup a PKI, it is crucial to understand the current legal ground of a country or an organization. This includes understanding the country constitution, regulations, directives that constitutes the legal framework of the country. This enable us to understand the legal mandates with regard to PKI, it also helps us to identify the missing legal documents that needs to be developed [16] [17]. The other major concern that needs to be considered is the PKI governing framework. PKI requires a governing framework to operate and provide the intended service. In the project lifecycle, particularly at initial stage of the requirement analysis, the issue related to legal frameworks needs to be assessed.

When examining Ethiopia's constitutional framework. Constitution-of-the-FDRE-1994 holds the topmost position in the constitution's hierarchy, followed by Proclamations, Regulations, Policies, and Directives and Standards. The House of Representatives (HPR) is the highest legislative authority. House of People's Representatives (HPR) has the power and authority to ratify various Ethiopian proclamations [18].

Constitutional provisions establish a parliamentary democracy. Two chambers are referred to as the Federal chambers. These are the House of Representatives of the People and the House of Federation (HF). Additionally, the Constitution stipulates a one-house State Council at the state level. The HPR is the highest authority within the Federal Government, while the State Council is the highest authority within the state. The HF, composed of representatives of Nations, Nationalities, and People, is the other representative assembly with specific authority, including the "ultimate" authority to interpret the Constitution [18].

The most important function of the house of people representatives (HPR) is to enact laws on matters assigned to federal jurisdiction and ratify national policy standards. The HPR also exercises other important functions including the appointment of federal judges, the ratification of international agreements and the investigation of the conduct of members of the executive. The most important function of the house of federation (HOF) is interpreting the FDRE Constitution.

It is constitutionally mandated to establish the Council of Constitutional Inquiry to assist it in this task [18].

The Federal Executive in Ethiopian legal system is the Council of Ministers. The Council of Ministers is comprised of the Prime Minister, the Deputy Prime Minister, Ministers and other members as may be determined by law. The Council of Ministers has powers and functions. One of the key roles is to adopt various implementation policies, regulations, directives.

From the aforementioned paragraphs we can conclude that, any adaptation and formulation of the laws of Ethiopian should be passed through any one of the above legislative and executive organs for adaptation and ratification various legal documents country wide. Depending up on the countries legal system there should be a legal framework that support the implementation of PKI and operation as well. In case of Ethiopia Proclamations are ratified by the HPR and regulations are ratified by the council of ministers, while other documents such as policy and directives can be ratified by mandated organization.

For the purpose of the implementation PKI various countries drafted and implemented various legal documents that support the enablement of PKI. Digital signature law is one of the laws that play a key role in realizing and provide a recognition in the equivalence of digital signature with that of the traditional hand written signature. CP and CPS are the other mandatory legal documents that support the implementation and operation of PKI. These two documents should be developed by aligning a documentation framework known as RFC 3647, which defines and states all the requirements and contents that both the CP and CPS should comprises of. While we plan to implement PKI we need to consider the legal frameworks in support of PKI operation. Without the legal frameworks the operation of PKI will be come under question.

The Indian root certificate authority known as Controller of certifying Authority(CCA) can be taken as an instance. The Root CA has published a lots of publications for the purpose of utilizing those publications in operation of the PKI domain. These publications have various purposes, some of these are used as a standard, guideline, policies in the PKI domain and they should be complied by the subordinate CAs in operation of PKI.CP documents, CPS documents, CA site specification

documents, IVG (Identity verification guidelines) and Technical interoperability guideline and standards are some of the important documents that the PKI legal framework should comprises of for smooth operation within the PKI domain.

Various countries have implemented PKI governance framework for the smooth operation and implementation of PKI. Within the continent of Africa there are also countries who have developed and implemented a PKI legal frameworks for the purpose of PKI operation and electronic signature transaction. Kenya one of the prominent one. The highest legislation pertaining to PKI in Kenya is "Kenya Information and Communications Act of 1998 CAP 411A". CCK (Communication Commission of Kenya), who will be taking a role of Root Certificate Authority in Kenya National Public Key Infrastructure, defines license framework for Certificate Service Provider (CSP's) or Certificate Authority that issues certificates through "Technical rollout requirements for Certification Service Provider." The legislative framework for national PKI is depicted as below.

Kenya Information and Communication Act
Kenya Information and Communication Act
Technical Rollout Requirements for Certification Service Providers(CSP's)

Figure 2.Kenya PKI Legal Framework

2.3 Threat landscape of PKI ecosystem

On the online platform, the threat landscape has grown substantially, primarily affecting those who provide security services, such as PKI and certificate authorities (CAs). While implementing PKI at the national or organizational level, we must take into account the threat landscape aimed at PKI services. Quantum computing's emergence has presented the PKI ecosystem with a significant challenge. Various vendors are striving to defend against threats posed by quantum computing. By utilizing VCert and the Venafi Platform, Venafi and Crypto4A have been working together. VCert is an open-source project sponsored by Venafi and Crypto4A. It is a command-line utility designed to generate Quantum-resistant keys using NIST candidate algorithms [13].PKI infrastructure and operations dependent on it are susceptible to cyberattacks. The blog written by Nahla Davies for Globalsign, one of the most prominent providers of digital certificates, discussed the most common attacks against digital certificates. The treats POODLE, DROWN, and HEARTBLEED were the ones that were spoken about in the blog [19].

2.4 Project Management challenges

Projects made on various sector fails due to various reasons. Project management requires strong leadership and effective management in order to gain the desired goals. lack of resources, lack of well-established administrative systems and procedures are most prominent issues that are realized most often. Such issues mostly create adverse impact in developing countries when compared to western countries [1].

In previous years, numerous frameworks for project management have been developed. The purpose of these frameworks is to resolve various project management issues. PMBOK, PRINCE2, and Agile Project Management are the most widely used and well-known frameworks over the past few decades. These frameworks, when comprehended, allow for the successful implementation of a project [20].

PKI project requires a multidisciplinary competency in the area of implementing and establishing PKI at national or organizational level, the aforementioned concepts provide a guidance in selecting the appropriate project management framework that can be utilized in complex projects and that requires the participation of experts in various areas of a project [20]. The PRINCE2 project management framework is regarded as the most valuable asset for facilitating the PKI project implementation procedure and also suggested by this study.

2.5 Related Works

2.5.1 Public Key Infrastructure (PKI) in E-Government Systems

Public Key Infrastructure has become a fundamental component in enhancing the security of e-government systems. Numerous studies have explored its application in various governmental services, aiming to protect data integrity, ensure secure communication, and authenticate users and devices [6] [8] [17]. Notable implementations include the Estonian e-government system, Romanian Schengen Information System, which is often cited as a benchmark for secure digital identity, e-services integration and seamless cross-border transactions [8].The SYZEFXIS-PKI and Cameroon National PKI project represents a crucial step in the Greek government's and Cameroon efforts to secure digital communication and service delivery respectively. They highlights the challenges of scaling PKI infrastructure in a complex, multi-layered governmental

framework and offers insights into addressing interoperability issues between different governmental entities [17] [16].

2.5.2 PKI-Based Secure Infrastructures in Mobile E-Commerce

The rapid growth of mobile commerce has necessitated the development of robust security mechanisms to protect sensitive transactions [7]. PKI is widely recognized as a viable solution due to its ability to provide end-to-end security, including authentication, confidentiality, and non-repudiation. Several frameworks have been proposed, such as the mobile PKI (mPKI) systems in South Korea and Japan, which have set standards for secure mobile transactions [7].

Research has also explored integrating PKI with emerging technologies like blockchain, aiming to further enhance security and trustworthiness in mobile e-commerce platforms. However, the design and implementation of PKI in mobile environments remain challenging due to issues like key management, certificate revocation, and the need for lightweight cryptographic solutions suitable for resource-constrained mobile devices [7].

2.5.3 PKI in Educational Institutions

The integration of PKI into educational systems has gained attention as institutions seek to protect sensitive information and enable secure access to digital resources. Finnish universities, through the FEIDHE project, have been pioneers in adopting PKI to secure student data, authenticate users, and support secure communication channels within academic environments. Other studies have focused on implementing PKI in distance learning and online examination systems, addressing concerns about identity verification and academic integrity. These implementations underscore the importance of a secure infrastructure in supporting the digital transformation of educational institutions [9].

2.5.4 Case Studies and Comparative Analysis

Case studies such as the UAE's national PKI initiative offer valuable lessons on the challenges and successes of deploying PKI at a national level. The UAE’s approach emphasizes the need for a well-defined legal and regulatory framework, comprehensive stakeholder engagement, and continuous monitoring and evaluation of the PKI ecosystem [21]. Comparative analyses of PKI

implementations across different sectors highlight the versatility of PKI and its adaptability to various operational requirements. However, they also reveal common challenges, including the complexity of key management, the need for interoperability across different PKI systems, and the importance of user awareness and education in ensuring the effective use of PKI-enabled services [21].

2.5.5 Comparative Studies and Frameworks

Comparative analyses of PKI implementations across different sectors have provided valuable insights into best practices and challenges. For instance, research by [22] compares the effectiveness of PKI in various e-government projects, identifying common challenges such as interoperability and user adoption. Furthermore, the work of [23] presents a framework for evaluating the security and scalability of PKI systems, which can be adapted to different use cases, including e-government, mobile e-commerce, and education.

These studies collectively highlight the versatility and critical importance of PKI in ensuring secure digital interactions across various sectors. They also provide a foundation for the continued development and refinement of PKI systems to meet the evolving security needs of modern digital infrastructures.

2.6 Research gaps

While there has been considerable progress in deploying PKI in various e-government and educational systems across different countries, several gaps remain in achieving universally secure and efficient implementations. The SYZEFXIS-PKI case highlights the challenges of large-scale PKI deployment in Greece's e-government infrastructure, focusing on security and scalability [16]. Similarly, Finnish Electronic Identification(FEIDHE) explores the integration of PKI in Finnish higher education, revealing difficulties in harmonizing educational protocols with robust security requirements [9]. The research on PKI in Cameroon's public administration emphasizes the challenges of infrastructure deployment in developing countries, particularly concerning resource constraints and policy alignment [17]. Despite these efforts, there is a lack of comparative studies that address the cross-border interoperability of PKI systems, the long-term sustainability of such implementations, and the socio-technical factors that influence their adoption across different sectors. Further research is needed to explore these areas, particularly focusing on creating

adaptable, resilient PKI framework that can be universally applied across various domains and geographies. Detail research gaps, challenges, existing frameworks and their limitations are presented at Chapter three (03) through systematic literature review results.

CHAPTER THREE

3 Methodology

A systematic literature review and a case study is implemented in order to facilitate this research. A Systematic Literature Review (SLR) is a research methodology that employs a systematic approach to gather, identify, and critically evaluate the available research studies (e.g., articles, conference proceedings, books). [24]. Since a SLR informs the reader with current literature about a subject the goal is to review critical points of current knowledge on a topic about research questions [24]. Accordingly, defining an "Initial Idea" in a subject to be studied is the first step before starting the SLR. The systematic literature review basically comprises of seven steps starting from formulating a research question to writing and publishing a report. Through these processes Different tools and frameworks are utilized to facilitate and visualize the systematic literature review process. An online tools called https://parsif.al/ , VOSViewer tools are employed for this research and also PRISM workflow diagram is used to show study selection process. The methodology presented in this paper comprises two main phases: "Planning" and "Conducting" phase as part of SLR [24]. The planning phase of the SLR defined the protocols and research strategies. based on the defined protocol a SLR will be conducted as a second phase [24]. For the purpose of validating the proposed framework a case study and KPI is developed. Additionally, the summary of the limitations of the existed frameworks are incorporated as part of the SLR result. The subsequent section shows the detail planning and conducting phases of the SLR.

This research incorporated a case study on the bases of interview to assess the progress of Ethiopian national PKI establishment. The procedures for data collecting and analysis that were put into practice are broken down into the following subsections for explanation. The data will be gathered from Participants in their normal settings, rather than within the restricted confines of a facility. As a result, the real-world scenario must be included into the data collection strategy [25]. For the purpose of case study purposive method of sampling is selected, the table describes the roles of the interviewers and the rationale for their selection is annexed on Appendix A. This data collection procedure will outline the primary tasks that going to be involved in collecting data for the case study. These consist of:

- Gaining access to the selected interviewee,
- The schedule of the data collection activities,
- Handling unexpected events,
- Protecting human subjects,

3.1 Data Collection

Data collection questions are queries to remind the researcher of the information that needs to be collected [25]. unstructured interview will be used to collect the data for this study. The data collection interview questions are going to be prepared based on the objectives of the assessment. The questions used for the interview are going to be attached in Annex in the future.

3.2 Analysis Method

The analysis method applied for the case study is thematic analysis. Thematic analysis involves systematically identifying, organizing, and offering insight into patterns of meaning (themes) across a data set [26]. It is a way of identifying what is common and makes sense in a talked or written topic. These common patterns need to be important in relation to the particular topic and research objectives. Thematic analysis is selected for this study since it offers a way of coding and analyzing qualitative data systematically, which can then be linked to broader theoretical or conceptual issues in alignment with the objectives of the study.

CHAPTER FOUR

4 Proposed PKI Project Implementation Framework

In order to Develop the Proposed PKI Project implementation Framework, the results found through SLR are referenced. The identified PKI implementation challenges and the proposed frameworks through the SLR are organized by themes. PKI legal framework, PKI deployment model, facility and infrastructure, PKI awareness and training, PKI audit and accreditation activities as core activities of the project execution and Analysis Phase, Design Phase, Implementation Phase, Operation & Integration phase as core phases of the project. Accordingly, the identified phases and core activities are shown below

Core Activities		
No.	**Core Activities**	**Description**
1.	PKI Legal framework	PKI policy development and supporting guideline document preparation.
2.	PKI Deployment model	Design and implementation of PKI model (Hierarchical model and Bridge model)based on the context and objective of PKI initiative.
3.	Facility and infrastructure	Design and implementation Facility and supporting infrastructure utilized for PKI operation, Access controls, Datacenter, Software and hardware.,
4.	PKI awareness and training	Operational trainings that enables proper operation of PKI service. This enables to avoid human errors in the operation of PKI service.
5.	PKI Audit and Accreditation	Process of Accrediting PKI service enables to gain trustworthiness of PKI and helps to gain trust in the service domain.

Table 1.PKI Project execution core Activities

PKI project Phases		
No.	**Phases**	**Description**
1.	Analysis Phase	Analysis of core activities of PKI, assessment of best practices and feasibility assessment on the execution of core activities.
2.	Design Phase	Design and peer review of the core activities enables successful execution of
3.	Implementation Phase	The implementation of core activities based on the defined designs.
4.	Operation & Integration phase	Pilot phase of the project, key generation, operational practices are part of this phase.
5.	Monitoring and maintenance	These phase focuses on monitoring the overall performance of PKI service based on the defined core activities.

Table 2. PKI project Phases

Identified Themes organized by Phases and Core Activities			
No.	Phases	Core Activities	Description
1.	Project management	Project Management Framework with the focus of seven(07) process of PRINCE2.	The Project management framework considered for this study is PRINCE2 project management framework, and the seven phases of PRINCE2 framework are incorporated in the proposed framework.
2.	Analysis	• Legal framework • PKI Deployment model • Facility and infrastructure • PKI awareness and training • PKI Audit and Certification	Analyzing the core activities in PKI project execution. It enables to identify gaps in the execution of PKI project both at national and organizational level. It enables to avoid to contradictions, interoperability, integration issues.
3.	Design	• PKI Legal framework • PKI Deployment model • Facility and infrastructure • PKI awareness and training • PKI Audit and Certification	Information gathered during analysis phase enables smooth design of the intended legal frameworks, architecture, facility and enables to design proper training and audit strategies.
4.	Implementation	• PKI Legal framework • PKI Deployment model • Facility and infrastructure • PKI awareness and training • PKI Audit and Certification	The core activities are implemented in accordance of the designs defined for each core activity. The aforementioned phases provide clear direction through the process. development and testing of the implemented core activities is part of this phases,
5.	Operation and Integration	• PKI Legal framework • PKI Deployment model • Facility and infrastructure • PKI awareness and training • PKI Audit and Certification	After implementation of PKI, the next phase is project pilot, at this stage initial operation is started. Key generation, operational practice are part of the process.
6	Monitoring & maintenance	• PKI Legal framework • PKI Deployment model • Facility and infrastructure • PKI awareness and training • PKI Audit and Certification	These phase focuses on monitoring the overall performance of PKI service based on the defined core activities.

Table 3. Identified Themes by Phases and Core Activities

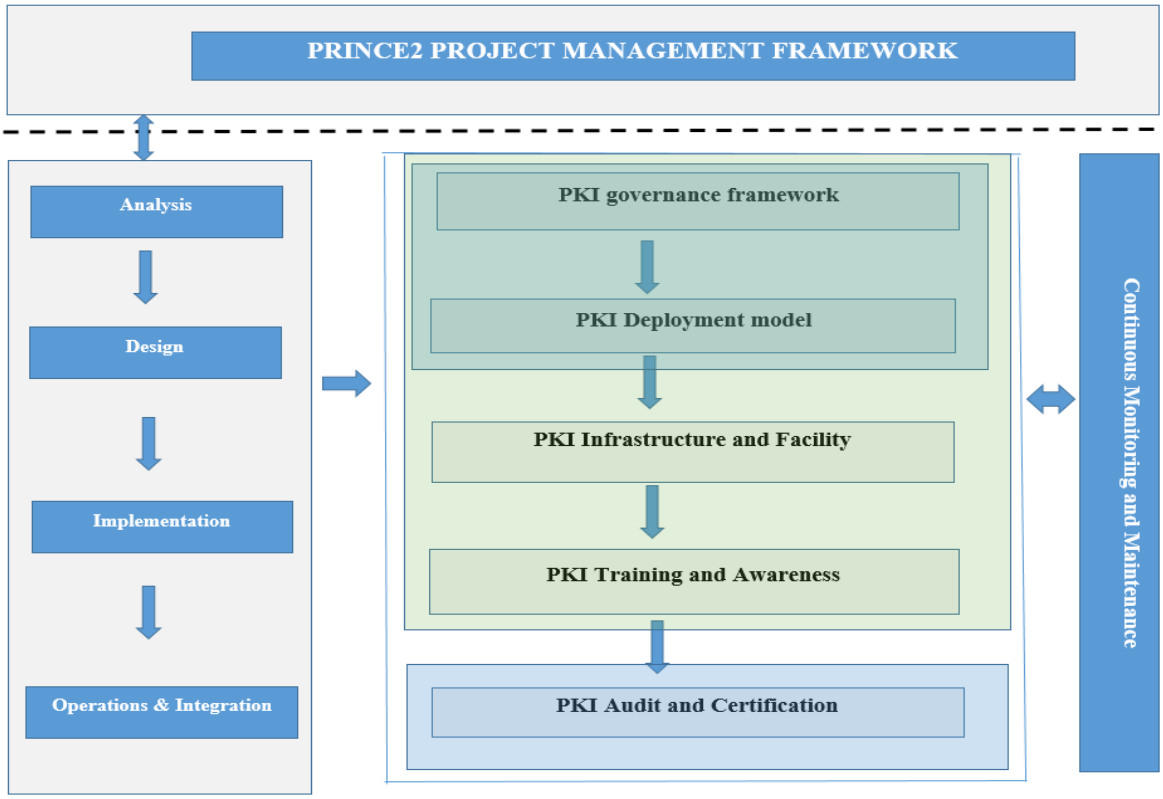


Figure 3.The proposed PKI Framework

The specified central task necessitates the completion of each stage during project implementation. Each fundamental task must be performed autonomously, taking into account the interconnections that exist between the core activities. The description of the proposed framework is explained below.

4.1 PKI project implementation phases

4.1.1 Analysis:

The initial phase where requirements for the PKI implementation are gathered, and a feasibility study is conducted. This phase includes risk assessments, stakeholder identification, and a preliminary plan for the PKI project.

4.1.2 Design:

In this phase, a detailed design of the PKI system is created, covering both logical and physical aspects. It includes the selection of PKI technologies, defining architecture, establishing security policies, and designing workflows.

4.1.3 Implementation:

The PKI components are developed, integrated, and deployed. This phase involves setting up the Certificate Authority (CA), registration authorities, and other required infrastructure.

4.1.4 Operations & Integration:

This phase focuses on the operational aspects, including integrating the PKI system with existing systems and applications, conducting operational tests, and ensuring that all components function as intended.

4.1.5 Continuous Monitoring and Maintenance:

This process ensures the ongoing health, security, and performance of the PKI infrastructure. It involves regular updates, monitoring for threats, maintaining operational readiness, and ensuring that the infrastructure aligns with evolving standards and regulatory requirements.

4.2 PKI Core Activities in Implementation:

4.3 PKI Governance Framework:

Establishes the rules, policies, and guidelines for the PKI system, ensuring that the governance aligns with organizational and regulatory requirements.

4.3.1 PKI Deployment Model:

Defines how the PKI infrastructure will be deployed (e.g., centralized, decentralized, or hybrid) and how certificates will be issued, managed, and revoked.

4.3.2 PKI Infrastructure and Facility:

Involves setting up the infrastructure, including hardware security modules (HSMs), secure data centers, network components, and other facilities needed for secure PKI operations.

4.3.3 PKI Training and Awareness:

Provides training for employees, system administrators, and end-users about the use and management of the PKI system. It ensures that all stakeholders are aware of security practices, policies, and procedures.

4.3.4 PKI Audit and Certification:

Regular audits are conducted to ensure compliance with standards and regulations. Certification processes are also established to validate the security and reliability of the PKI infrastructure.

4.4 Interdependencies:

The PKI Governance Framework provides the foundational policies and guidelines for all other components. It directly influences the PKI Deployment Model, ensuring that the deployment aligns with governance policies.

The PKI Deployment Model as well as the legal framework determines the specific requirements for the PKI Infrastructure and Facility setup. The infrastructure's design, capabilities, and security measures depend on the chosen deployment model and legal governing frameworks comprises of alignment in international standards.

PKI Infrastructure and Facility needs to be in place before the PKI Training and Awareness phase begins, as training should be based on the actual infrastructure and operational environment.

PKI Audit and Certification is an ongoing process that relies on continuous Monitoring and Maintenance. It ensures that all phases, from governance to deployment and operations, comply with internal and external standards.

PKI Project detail workflow diagram

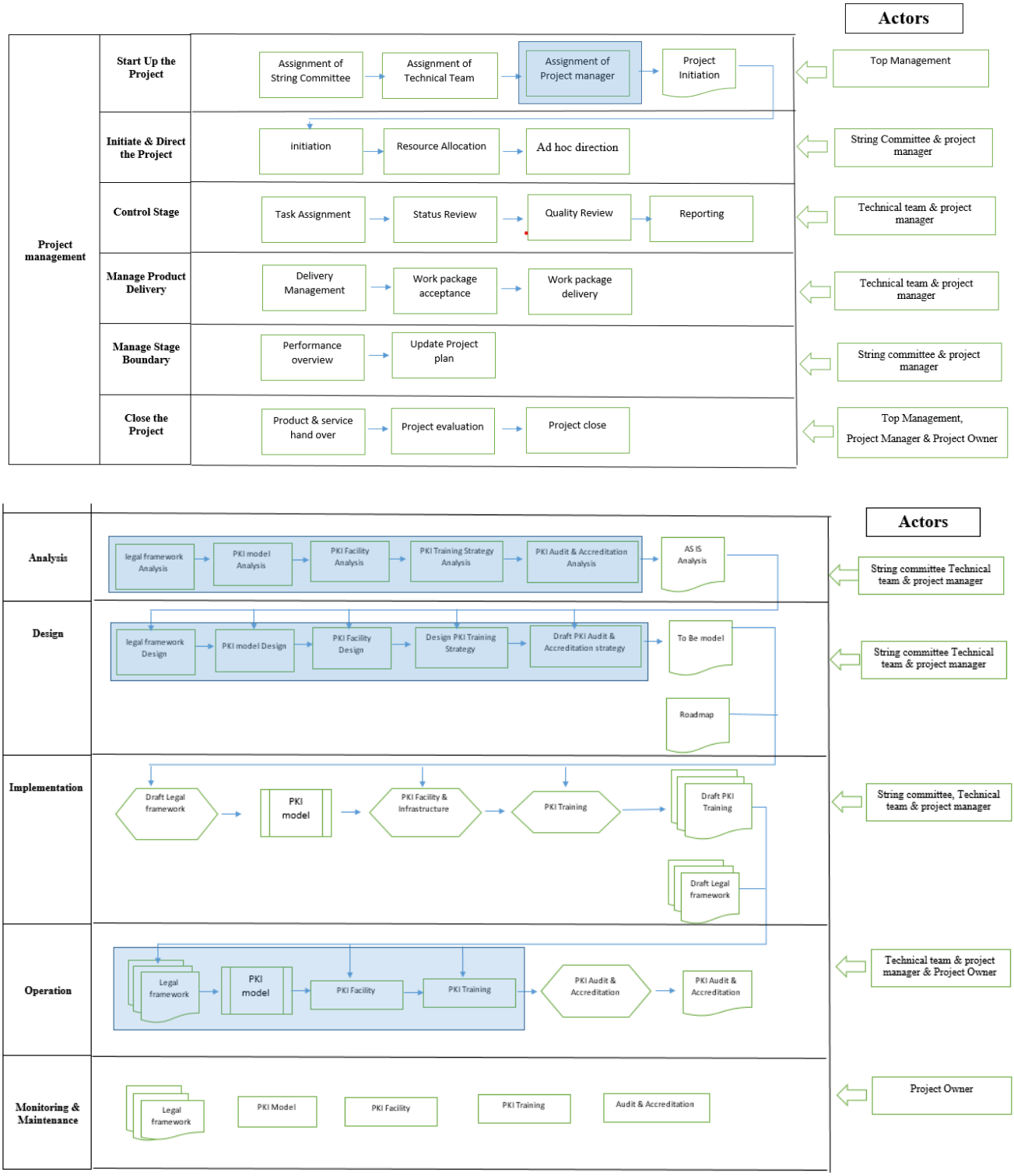


Figure 4. PKI Project detail workflow diagram

4.5 PKI Project Implementation Workflow

This section describes the detail design of the workflow diagram illustrated above. The actors and stakeholders participating in the PKI project execution activity are illustrated below in the table for further clarity. The table shows the participating actors and the project outcome expected in each activity. This table can be used as part of the project charter document developed through the project management phase.

No.	Actors/Participants	Key Responsibility
1.	Top Management	Assign Steering Committee: Establish a steering committee to oversee the project.
2.	Steering Committee	• Assign Technical Team and project manager, allocate technical resources and team members. • Oversite the overall project and provide feedback on challenges that needs discussion.
3.	Legal Team	• Legal Framework Analysis: Analyze the legal requirements and frameworks necessary for the PKI implementation. • Develop Legal Framework: Create the legal documentation and policies.
4.	PKI Team	• PKI Model Analysis: Analyze and design the PKI model. • Execute PKI Model: Implement the designed PKI model. • Develop a training strategy for users and administrators. • Develop Training: Create training materials and conduct training sessions. • Conduct Training: Train users and administrators on the PKI system
5.	Infrastructure Team	• Infrastructure Analysis: Assess and prepare the necessary infrastructure. • Design Framework: Create the high-level and low-level design blueprints. • Datacenter Facility Preparation: Set up the datacenter and related facilities.
6.	Quality Assurance Team	• Plan the audit strategy to ensure ongoing compliance • PKI Audit & Accreditation: Conduct audits and ensure the PKI system meets accreditation standards. • Conduct Initial Audit: Perform initial audits to verify compliance and functionality. • Quality Assurance: Ensure all project deliverables meet quality standards. • Continuous Monitoring & Maintenance: Monitor the PKI system continuously and perform maintenance as needed. • Audit Report: Generate audit reports to document compliance and performance. • Product & Service Evaluation: Evaluate the products and services provided by the PKI system
7.	Project Manager	• Develop Project Mandate: Define the project's objectives and scope. • Resource Allocation: Allocate resources and manage the project plan. • Risk Management Plan: Develop and implement a risk management plan. • Communication Plan: Establish a communication plan for stakeholders. • Final Project Report: Compile a final report summarizing the project outcomes.

Table 4.PKI Project participating stakeholder and actors

NO.	Project Phase	Actors	Tasks	Deliverables
1.	Project Initiation	Top Management,	• Assign Steering Committee • Assign Technical Team • Assign Project Manager	• Project initiation document • Project Charter • Initial Resource Allocation
2.	Project Planning	Steering Committee Project Manager	• Define Objectives and Scope • Allocate Resources • Develop Detailed Project Plan	• Project Plan • Risk Management Plan • Communication Plan
3.	Analysis Phase	Technical Team, Project Manager	• Conduct Legal Framework Analysis • Analysis of Current PKI Model • Analyze PKI Facility and Infrastructure • Analyze PKI Training requirements • Analyze PKI Audit Requirements	**AS-IS document** • Infrastructure requirement • PKI Training requirement • Status of Legal ground • PKI audit requirement • PKI model recommendation
4.	Design Phase	Technical Team, Project Manager	• Design PKI Model • Develop Infrastructure Design • Design Legal Framework • Develop PKI Training Program • Prepare PKI Audit Strategy	**To Be model Document** • PKI Model Design • Infrastructure Blueprint (HLD & LLD) • To be developed Legal Framework • Training Program Outline • Accreditation Strategy Document
5.	Implementation Phase	Technical Team, Project Manager	• Prepare PKI Infrastructure • Deploy PKI Model • Develop Training Programs • Implement Legal Framework • Conduct Initial Audits and Accreditations	• Drafted PKI Legal framework document • PKI Infrastructure & Facility • PKI Model • PKI Training program • PKI Audit program
6.	Operation & integration	Technical Team Project Manager	• Conduct initial operations and test integrations. • Conduct training • Ensure system interoperability and stability. • Manage ongoing certificate issuance and key management.	• Operational PKI legal framework • Operational PKI facility • Audit and evaluation report • Key ceremony report • Training completion Report
7.	Monitoring & Maintenance	Technical Team, Project Owner	• Continuous Monitoring of PKI Service • Regular Maintenance and Updates • Periodic Audits and Accreditations	• Monitoring Reports • Maintenance Logs • Audit and Accreditation Reports
8.	Project Closure	Project Manager, Technical team,	• Conduct Final Project Evaluation • Handover of Product and Services	• Final Project Report • Handover Documentation

NO.	Project Phase	Actors	Tasks	Deliverables
		Top Management Steering Committee	• Close the Project	• Lessons Learned Report

Table 5.PKI Project detail workflow diagram description

4.6 KPI for success of the Proposed framework

This section provides the KPI for the success of applying the proposed framework. For the purpose of evaluating the framework six KPIs are defined in line with the description and measurements.

No.	KPI	Description	Measurement
1.	Project Alignment	ensures that a project's objectives, goals, and outcomes are directly connected to the strategic priorities of the organization, optimizing resources and efforts towards achieving overall business success.	• Project Initiation Document(PID) • AS IS Analysis document • To be model document • Project Plan document
2.	Completeness	Refers to the comprehensive implementation of all necessary components and processes within a Public Key Infrastructure.	• Legal framework • Deployment model • Facility & infrastructure • Training & awareness • Audit and Accreditation
3.	Compliance	Ensures that the PKI system adheres to relevant laws, regulations, and industry standards while establishing clear policies and procedures for managing certificates, authentication, and data protection.	• Legal Framework • Audit findings & report
4.	Interoperability	Ensures secure and reliable digital interactions by allowing entities with different PKI implementations to authenticate, encrypt, and verify digital signatures, thereby enabling broader and more efficient use of secure communication and e-commerce applications	• Legal framework • Facility & infrastructure • PKI Deployment model • Audit & Accreditation
5.	Project Workflow	Utilization of iterative process and decision making process as part of project phase.	• Separation of decision process and technical stage.
6.	Stakeholder Engagement	Involves actively engaging all relevant stakeholders—internal and external—through continuous communication, feedback, and collaboration to ensure their needs and expectations are addressed in the design and implementation of the PKI project.	• Top management • Steering committee • Project manager • Technical team (subject matter experts) • Project Owner (PKI team) • External Auditor

Table 6.key performance indicator

4.7 Scenario

Case Study: Implementing a PKI Project Framework for a Financial Institution

Background

Organization: Organization: XYZ Bank Inc., a mid-sized financial institution specializing in personal and commercial banking services.

Objective: Implement PKI system to enhance security for online transactions, internal communications, and regulatory compliance.

Stakeholders:

- **Top Management**: Initiate the project and assign steering committee.
- **Steering Committee**: Approve and allocate resources, assign technical team.
- **PKI Team**: Assess the requirements to prepare PKI deployment model & PKI training.
- **Legal Team**: Ensures adherence to regulatory requirements.
- **Infrastructure Team:** Assess the requirements to prepare the necessary infrastructure
- **Quality Assurance Team**: Asses requirement to evaluate compliance and security.

Phase 1: Analysis

Activities:

- **Needs Assessment**: Conducted workshops with stakeholders to gather requirements. The IT department identified the need for secure email, digital signatures, and encrypted communications including regulatory review.

KPIs:

- **Stakeholder Engagement Rate**: 90% of identified stakeholders participated in requirements gathering sessions.

Phase 2: Design

Design Elements:

- **Legal Framework**: Drafted policies for certificate issuance, revocation, and lifecycle management.
- **Deployment Model**: Decided on a hybrid PKI model combining internal and external Certificate Authorities (CAs).
- **Infrastructure**: Planned the physical and virtual infrastructure needed for the PKI system, including servers, storage, and network requirements.

- **Training**: Designed training programs for IT staff and end-users, including certification processes.
- **Audit & Accreditation:** PKI infrastructure Audit strategy plan document preparation**.**

KPIs:

- **Policy Adherence**: 95% of PKI policies and Supporting guideline documents were identified and approved by stakeholders.
- **Training Coverage**: Training strategy is designed to cover 85% of IT staff for the initial training program.

Phase 3: Implementation

Activities:

- **System Deployment**: Installed and configured PKI hardware and software, including the CA infrastructure, certificate management systems, and encryption tools.
- **Infrastructure Preparation:** Prepare PKI infrastructure and facility that consider redundancy.
- **Training Preparation**: Preparation of training programs and manuals for end-users and IT staff.

KPIs:

- **Implementation Timeliness**: The project was completed 2 weeks ahead of schedule.
- **System Integration Effectiveness**: 98% of systems integrated successfully without major issues.
- **Training:** Number of training developed based on the training strategy and program.

Phase 4: Operation & Integration

Activities:

- **Ongoing Operations**: Monitored system performance, issued certificates, and managed revocations.
- **Support**: Provided ongoing support and troubleshooting for users.
- **Compliance Monitoring**: Conducted periodic audits to ensure compliance with policies and regulations.
- **User Training**: Rolled out training programs for end-users and IT staff.

KPIs:

- **Operational Efficiency**: Average time to resolve support tickets was 4 hours.

- **Compliance Audit Findings**: Zero critical compliance issues identified in the first audit.
- **Integration**: Integrated PKI with existing systems for secure email, authentication, and transaction signing.

Phase 5: Continuous Monitoring & Maintenance

Activities:

- **Monitoring**: Continuously monitored system performance and security.
- **Maintenance**: Applied updates and patches as needed.
- **Feedback**: Collected feedback from users and stakeholders to identify areas for improvement.

KPIs:

- **Incident Resolution Time**: Average time to resolve security incidents was 2 hours.
- **User Satisfaction**: User satisfaction score was 4.7 out of 5 based on surveys.

Evaluation

Summary: XYZ Bank Inc. successfully implemented its PKI project with a focus on stakeholder engagement, regulatory compliance, and system effectiveness. The framework was evaluated based on KPIs throughout all phases, demonstrating high engagement, adherence to legal requirements, and operational efficiency.

Lessons Learned:

- Early and continuous stakeholder engagement was critical for project success.
- Clear policies and robust training programs were essential for smooth implementation.
- Ongoing monitoring and support ensured the PKI system remained effective and compliant.

CHAPTER FIVE

5 Experiments and Analysis

5.1 Experiment

For the purpose of this study a systematic literature review and a case study is conducted. The systematic literature review is conducted to Identify the major challenges on existing literatures as well as and the proposed frameworks in order to mitigate those challenges identified through the process. The Systematic literature review comprises of the planning phase and the conducting phase.

The case study assesses the current status of the Ethiopian National Root CA(ENRCA). Through the process challenges that are observed through the process of executing National PKI project are discussed and the proposed framework is analyzed against the project execution process.

5.1.1 Systematic Literature Review

5.1.1.1 Planning Phase

Defining the protocol is the first step of an SLR since it describes the procedures involved in the review and acts as a log of the activities to be performed. Obtaining opinions from peers while developing the protocol, is encouraged to ensure the review's consistency and validity, and helps identify when modifications are necessary [24]. One final goal of the protocol is to ensure the replicability of the review.

5.1.1.1.1 Formulate a research question

Defining an "Initial Idea" in a subject to be studied is the first step before starting the SLR. The PICOC (Population, Intervention, Comparison, Outcome, and Context) criteria break down the SLR's objectives into searchable keywords and help formulate research questions [27]. Even if PICOC is widely used in the medical and social sciences fields to encourage researchers to consider the components of the research questions [24], Kitchenham & Charters [6]. compiled the list of PICOC elements and their corresponding terms in computer science.

PICO Framework	PICO key words and Synonyms)
Population	PKI Project Implementation

	PKI project implementation steps, National and Organizational PKI PKI Project management Challenges
Intervention	PKI Project Implementation Framework
Comparison	Absence of PKI Implementation Framework
Outcome	PKI Project Implementation Framework for a PKI project

Table 7.PICO Framework

Clearly defined research question(s) are the key elements which set the focus for study identification and data extraction [21]. This question is formulated based on the PICOC criteria as presented below. (PICOC keywords are underlined).

Research Question	Motivation
RQ-1. What are the difficulties encountered during the implementation of a PKI project?	To identify Major challenges through PKI project execution.
RQ-2. How can a PKI implementation framework support the establishment of a national or organizational PKI implementation project?	To identify Major challenges and proposed frameworks on PKI project execution.

Table 8.Research Question

Once the research question has defined, defining the protocol is the first step of an SLR since it describes the procedures involved in the review and acts as a log of the activities to be performed. A protocol is a document that contains your research plan for the systematic review [24]. Accordingly, the research objective, Selection criteria, Search strategy and the aim of the analysis are defined as follow. The research objective is Rephrase from the research question as an objective. Accordingly, the main objective of the study is presented as follows.

Research Objective
RO. The aim of this study is to develop a PKI implementation framework that facilitates the implementation of PKI projects.

Table 9.Research Objective

5.1.1.1.2 Select digital library sources

The foundation of all academic research activities, regardless of field, consists of expanding previous study and drawing connections to previously acquired information [17]. An effective and

well-conducted review as a research method establishes a solid foundation for advancing knowledge and facilitating the development of theories [17]. for this reason, a systematic literature review is conducted on selected articles. For the purpose of this research two academic research sources are selected Scopus and Science@Direct databases are searched through Parsifal concerning the research objectives defined.

No.	Database	Description	URL
1.	Scopus	From Elsevier. One of the largest databases. Very user-friendly interface.	http://www.scopus.com
2.	Science@Direct	From Elsevier. Focused on engineering literature.	http://www.sciencedirect.com

Table 10.digital library sources

5.1.1.1.3 Inclusion and exclusion criteria

Authors should define the inclusion and exclusion criteria before conducting the review to prevent bias, although these can be adjusted later, if necessary. The selection of primary studies will depend on these criteria. Articles are included or excluded in this first selection based on abstract and primary bibliographic data. Accordingly, the inclusion and exclusion criteria are illustrated in the table below.

No.	Criteria Type	Inclusion Criteria
1.	Inclusion criteria	• Published after 1999 • Published in English language • Reports, policy literature, working papers, Technical document, government documents, • Article in open access • Book and Book sections
2.	Exclusion criteria	• The article only review blockchain technology • Articles not related to research objectives. • Duplicated Studies • Index files

Table 11.Inclusion and exclusion criteria

5.1.1.1.4 Quality Assessment (QA) checklist

Assessing the quality of an article requires an artifact which describes how to perform a detailed assessment. A typical quality assessment is a checklist that contains multiple factors to evaluate. A detailed description of assessment criteria in software engineering, classified into four main aspects of study quality: Reporting, Rigor, Credibility, and Relevance.

No.	Quality Assessment (QA) checklist	Level of Participation
1.	Does the article related to PKI ?	1 -not considered (Score: 0) 2–Partially considered (Score: 0.5) 3 – considered (Score: 1)
2.	Does the article propose a framework or methodology?	1 -not considered (Score: 0) 2–Partially considered (Score: 0.5) 3 – considered (Score: 1)
3.	Does the proposed framework related to PKI implementation framework?	1 -not considered (Score: 0) 2–Partially considered (Score: 0.5) 3 – considered (Score: 1)

Table 12.Quality Assessment (QA) checklist

5.1.1.1.5 Data extraction form

The data extraction form represents the information necessary to answer the research questions established for the review. Synthesizing the articles is a crucial step when conducting research. [24] presented a classification scheme for computer science research, based on topics, research methods, and levels of analysis that can be used to categorize the articles selected.

No.	Data extraction	Description
1.	Main Objective	The solution that the article intended to provide.
2.	Key Findings:	Key findings of the article.
3.	Methodology	The Methodology utilized by the article.
4.	Contribution	The contribution provided by the article for the identified problem.

Table 13. Data extraction form

5.1.1.2 Conducting

After defining the protocol, conducting the review requires following each of the steps previously described. Using tools can help simplify the performance of this task. Standard tools such as Excel or Google sheets allow multiple researchers to work collaboratively [24]. Another online tool specifically designed for performing SLRs is Parsif.al1 [24]. This tool allows researchers, especially in the context of software engineering, to define goals and objectives, import articles using Bibtex files, eliminate duplicates, define selection criteria, and generate reports.

5.1.1.2.1 Build digital library search strings

Search strings are built considering the PICOC elements and synonyms to execute the search in each database library. The PICOC elements are separated with parentheses and the Boolean operator AND.

Base Search strings
("National PKI" **OR** "Organizational PKI" **OR** "PKI Project Implementation Framework" **OR** "PKI Project Management" **OR** "PKI Project Management challenges")
Sub String
("National PKI" **OR** "Organizational PKI" **OR** "PKI Project Implementation Framework" **)**
("National PKI" **OR** "Organizational PKI")
(“PKI project implementation framework”)

Table 14. Search strings generated through Parsifal

5.1.1.2.2 Gather studies

Databases that feature advanced searches enable researchers to perform search queries based on titles, abstracts, and keywords, as well as areas of research. Since most of the databases allow the use of logical operators (i.e., AND, OR) it is utilized to perform the search [24]. Accordingly, the above set of string is searched for the purpose of this study in order to get a defined set of articles that align with the research objective and research question. Accordingly, total of **975** articles are identified with the presented search strategy as shown in the table below.

No.	**Search String**	**Search Results**	
		Scopus	**Science@Direct**

1.	("National PKI" OR "Organizational PKI" OR "PKI Project Implementation Framework" OR "PKI Project Management" OR "PKI Project Management challenges")	19	21
2.	("National PKI" **OR** "Organizational PKI" **OR** "PKI Project Implementation Framework" **)**	24	155
3.	("PKI project implementation framework")	756	0
	TOTAL Search	799	176
			975

Table 15. Search String results

5.1.1.2.3 Study Selection and Refinement

The paper selection process was started with removing duplicates in the first stage. The 141 duplicates were excluded out of 975 documents leaving 834 documents for further investigation. Second, by examining the publication date with regard to inclusion criteria are made and 27 papers are excluded and leaving for title screening. titles with regard to the research topic 553 papers are left for further analysis and finally an abstract section of 553 papers are read and in total, 20 papers are left for further analysis of inclusion by reading the abstract and were included for full-text analysis based on the stated inclusion and exclusion criteria for qualitative synthesis.

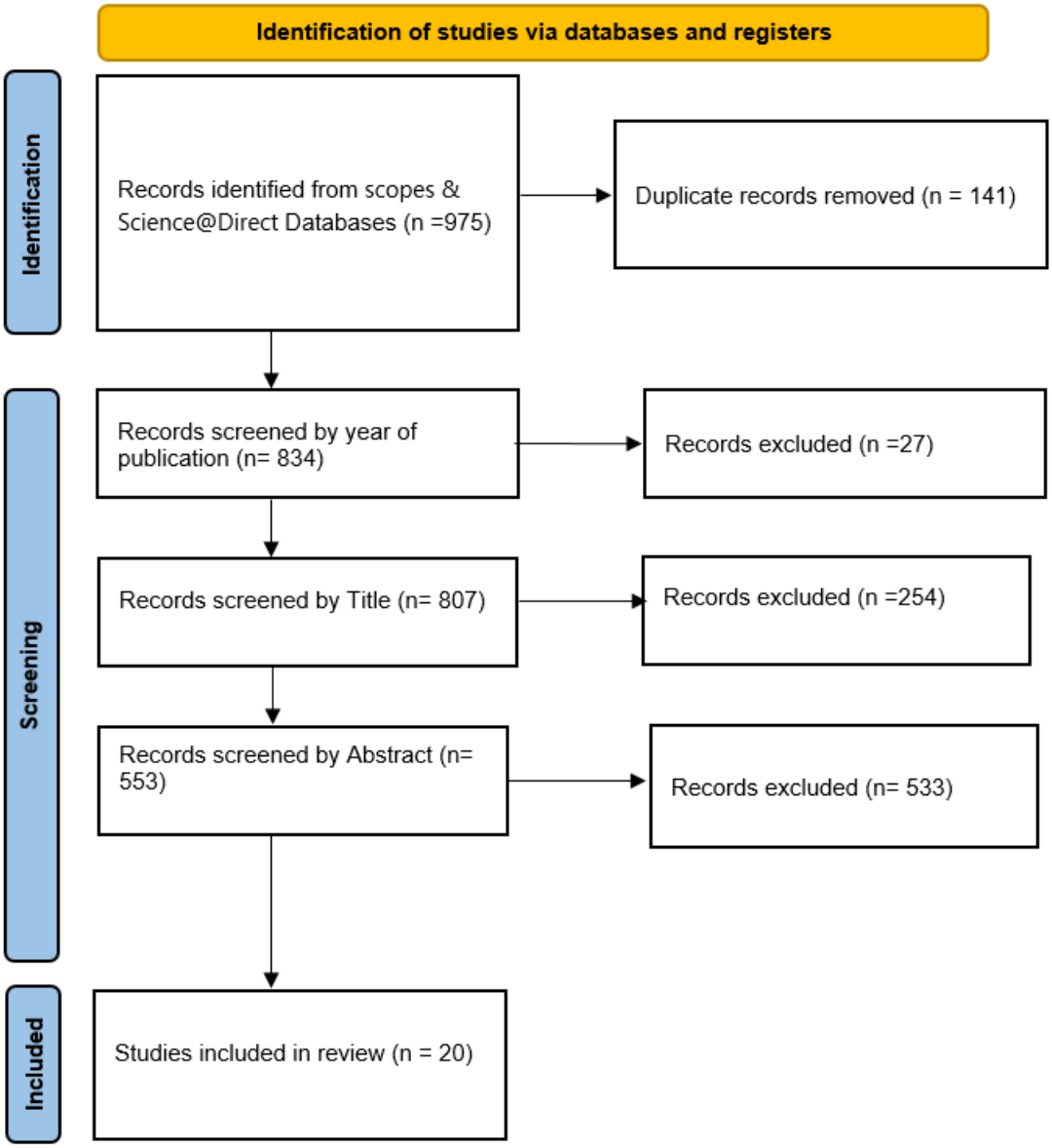


Figure 5.PRISMA Study Selection process workflow

Based on the selection criteria The following research studies are selected. The selected studies are organized by author name and title and illustrated bellow as follows.

No.	Author	Title	Reference
1.	Narendiran, C and Rabara, S Albert and Rajendran, Nishanth	Public key infrastructure for mobile banking security	[27]

2.	Sakane, Eisaku and Aida, Kento and Motoyama, Kazutaka	Design and Implementation of Certificate Authority for High Performance Computing Infrastructure	[28]
3.	Eduardo Jacob and Fidel Liberal and Juanjo Unzilla	PKIX-based certification infrastructure implementation adapted to non-personal end entities	[29]
4.	Gritzalis, Stefanos and Belsis, Petros and Karyda, Maria and Chalaris, Mike and Skourlas, Christos and Chalaris, Ioannis	Designing the Provision of Public Key Infrastructure Services for eGovernment	[10]
5.	Kefallinos, Dionysis and Lambrou, Maria A and Sykas, Efstathios D	Secure PKI-enabled e-government infrastructures implementation: the SYZEFXIS-PKI case	[16]
6.	Carayannis, Elias G and Turner, Eric	Innovation diffusion and technology acceptance: The case of PKI technology	[30]
7.	Tan, Wuzheng and Yang, Maojiang and Ye, Feng and Ren, Wei	A security framework for wireless network based on public key infrastructure	[31]
8.	Akotam, Agangiba W and Kontoh, Millicent S and Ansah, Albert K	E--governance public key infrastructure (PKI) model	[6]
9.	Enaw, Ebot Ebot and Check, Njei	Public Key Infrastructure Deployment in Cameroon's Public Administration	[17]
10.	Hammi, Badis and Monteuuis, Jean-Philippe and Petit, Jonathan	PKIs in C-ITS: Security functions, architectures and projects: A survey	[32]
11.	Hong, Ning	A security framework for the internet of things based on public key infrastructure	[33]
12.	Chan, Dan TF and Hui, Lucas CK	Towards a unified PKI Framework	[34]
13.	Linden, Mikael and Kanner, Janne and Kivilompolo, Mika	FEIDHE-integrating PKI in Finnish higher education	[9]
14.	Chanson, Samuel T and Cheung, Tin-Wo	Design and implementation of a PKI-based end-to-end secure infrastructure for mobile e-commerce	[7]
15.	Hableel, Eman and Byon, Young-Ji and Beak, Joonsang	Public key infrastructure for UAE: A case study	[21]
16.	Kuhn, D Richard and Hu, Vincent C and Polk, W Timothy and Chang, Shu-Jen	Introduction to public key technology and the federal PKI infrastructure	[35]
17.	OU, Chung-Ming and SHAN, Hwai-Ling and HO, Chuan-Te	Government PKI deployment and usage in Taiwan	[36]

18.	Serrano, Nicolas and Hadan, Hilda and Camp, L Jean	A complete study of PKI (PKI's Known Incidents)	[37]
19.	Gutmann, Peter	PKI design for the real world	[38]
20.	Floarea, Adrianand Burdun, Constantinand Florea, Ionutand Togan, Mihai	PKI Implementation for Romanian Schengen Information System	[8]

5.1.1.2.4 Quality Assessment

After the identification of duplicate articles and identifying included articles based on the selection criteria the quality assessment (QA) of the selected research paper is undertaken. QA evaluation in parsif.al, using a simple scale defined in the research protocol. This section illustrates the quality Assessment made on the selected research works. The quality is assessed using the predefined scale. an article QA evaluation in parsif.al, using a simple scale. In this scenario, the scoring procedure is the following Considered = 1, Partially Considered = 0.5, and Not-Considered = 0.

No.	Title	Quality Score
1.	FEIDHE-integrating PKI in Finnish higher education	1.5
2.	Towards a unified PKI Framework	2.0
3.	A security framework for the internet of things based on public key infrastructure	1.0
4.	PKIs in C-ITS: Security functions, architectures and projects: A survey	1.0
5.	Public Key Infrastructure Deployment in Cameroon's Public Administration	3.0
6.	E--governance public key infrastructure (PKI) model	1.5
7.	A security framework for wireless network based on public key infrastructure	2.0
8.	Innovation diffusion and technology acceptance: The case of PKI technology	1.0
9.	Secure PKI-enabled e-government infrastructures implementation: the SYZEFXIS-PKI case	3.0

10.	Designing the Provision of Public Key Infrastructure Services for eGovernment	1.5
11.	PKIX-based certification infrastructure implementation adapted to non-personal end entities	1.0
12.	Design and Implementation of Certificate Authority for High Performance Computing Infrastructure	1.0
13.	Public key infrastructure for mobile banking security	2.0
14.	PKI Implementation for Romanian Schengen Information System	3.0
15.	PKI design for the real world	1.5
16.	A complete study of PKI (PKI's Known Incidents)	1.0
17.	Government PKI deployment and usage in Taiwan	1.0
18.	Introduction to public key technology and the federal PKI infrastructure	2.0
19.	Public key infrastructure for UAE: A case study	2.0
20.	Design and implementation of a PKI-based end-to-end secure infrastructure for mobile e-commerce	2.0

Figure 6. Quality Assessment result

5.1.1.2.5 Data extraction

This section presents a comprehensive analysis of the data extracted regarding the challenges encountered during the implementation of Public Key Infrastructure projects, as well as the frameworks and best practices proposed to address these challenges. The analysis is structured to provide insights into the common barriers to successful PKI deployment and the effectiveness of various strategies in overcoming these challenges.

Data extraction Summery	
Title-1	**A Complete Study of PKI (PKI's Known Incidents**
Main Objective	To analyze known incidents and failures in PKI implementations, highlighting key vulnerabilities and proposing measures to enhance security and reliability.
Key Findings:	• **Incident Classification:** Identifies and categorizes PKI incidents into technical, policy, and human errors. • **Recommendations:** Suggests best practices and strategies to mitigate future PKI-related risks.

Methodology	Qualitative analysis of documented PKI incidents and case studies.
Contribution	Provides critical insights into common pitfalls in PKI systems, serving as a guide for future implementations.
Title-2	**Secure PKI-enabled e-government infrastructures implementation: the SYZEFXIS-PKI case**
Main Objective	To describe the design and implementation of a secure PKI-enabled infrastructure for e-government services, with a focus on the SYZEFXIS-PKI case in Greece.
Key Findings:	• **System Architecture:** Detailed description of the PKI system architecture, including certificate management and security protocols. • **Security Measures:** Focuses on the encryption and authentication mechanisms to protect government data.
Methodology	Case study of SYZEFXIS-PKI, including a security and performance evaluation.
Contribution	Demonstrates the effectiveness of PKI in securing e-government services, providing a reference for other governmental PKI deployments.
Title-3	**Design and Implementation of a PKI-based End-to-End Secure Infrastructure for Mobile E-commerce**
Main Objective	To develop a PKI-based infrastructure that ensures secure end-to-end transactions in mobile e-commerce.
Key Findings:	• **Infrastructure Design:** Proposes a comprehensive PKI infrastructure tailored for mobile e-commerce, including secure communication and authentication. • **User-Centric Approach:** Balances security with user convenience and experience.
Methodology	Experimental implementation and testing in a mobile e-commerce setting.
Contribution	Offers a viable solution for enhancing the security of mobile e-commerce transactions through PKI.
Title-4	**Public Key Infrastructure for UAE: A Case Study**
Main Objective	To analyze the deployment of PKI in the United Arab Emirates, focusing on its applications in both governmental and commercial sectors.
Key Findings:	• **Challenges and Solutions:** Identifies the challenges faced during the PKI implementation and the strategies employed to overcome them. • **Success Metrics:** Measures the impact of PKI on the security and efficiency of services in the UAE.
Methodology	Case study analysis, including stakeholder interviews and document reviews.
Contribution	Provides valuable lessons and best practices from the UAE's PKI deployment that can be applied to similar initiatives globally.
Title-5	**PKI Design for the Real World**
Main Objective	To address the practical challenges of designing and implementing PKI in real-world environments
Key Findings:	• **Design Considerations:** Discusses key design principles that ensure scalability, usability, and security in PKI systems. • **Application Examples:** Illustrates the application of these principles in various industries.
Methodology	Review and analysis of existing PKI systems in different contexts.
Contribution	Provides a practical framework for PKI design, emphasizing adaptability and real-world applicability.

Title-6	**Innovation Diffusion and Technology Acceptance: The Case of PKI Technology**
Main Objective	To explore the factors influencing the adoption and diffusion of PKI technology in organizations.
Key Findings:	• **Adoption Factors:** Identifies key determinants of PKI adoption, including perceived usefulness, ease of use, and trust. • **Diffusion Analysis:** Examines how PKI technology spreads across different sectors.
Methodology	Empirical analysis using surveys and statistical models.
Contribution	Offers a theoretical framework for understanding PKI adoption, providing insights for promoting its acceptance.
Title-7	**E-Governance Public Key Infrastructure (PKI) Model**
Main Objective	To propose a PKI model tailored for e-governance, focusing on security, transparency, and efficiency.
Key Findings:	• **Model Design:** Details a PKI model that supports secure e-governance services, with a focus on key management and certificate processes. • **Impact Assessment:** Evaluates the potential impact of the model on e-governance efficiency.
Methodology	Conceptual development and case studies.
Contribution	Provides a comprehensive PKI model for e-governance, with the potential to enhance public service delivery.
Title-8	**PKI Implementation for Romanian Schengen Information System**
Main Objective	To discuss the implementation of PKI within the Romanian Schengen Information System (SIS) for secure data exchange and communication.
Key Findings:	• **Security Framework:** Outlines the PKI security framework used in the SIS. • **Interoperability:** Focuses on ensuring interoperability with other Schengen member states.
Methodology	Case study analysis with technical details on implementation.
Contribution	Enhances understanding of PKI's role in secure cross-border data exchange within the Schengen area.
Title-9	**Public Key Infrastructure for Mobile Banking Security**
Main Objective	To explore the use of PKI in enhancing security in mobile banking applications.
Key Findings:	• **Security Enhancements:** Describes how PKI can secure mobile banking transactions through encryption and authentication. • **User Experience:** Considers the impact on user experience and adoption.
Methodology	Implementation and testing in a mobile banking environment.
Contribution	Provides a secure framework for mobile banking, demonstrating the critical role of PKI in protecting financial transactions.
Title-10	**Design and Implementation of Certificate Authority for High Performance Computing Infrastructure**
Main Objective	To design and implement a Certificate Authority (CA) for secure access to high-performance computing (HPC) resources.
Key Findings:	• **CA Architecture:** Details the architecture of the CA, including key management and certificate issuance processes.

	• **Security Measures:** Focuses on the security protocols implemented to protect HPC resources.
Methodology	Design and implementation in an HPC environment.
Contribution	Provides a blueprint for integrating PKI into HPC infrastructures, ensuring secure access and communication.
Title-11	**PKIX-based Certification Infrastructure Implementation Adapted to Non-Personal End Entities**
Main Objective	To develop a PKIX-based certification infrastructure tailored for non-personal end entities, such as IoT devices.
Key Findings:	• **Infrastructure Design:** Discusses the unique challenges of certifying non-personal entities and how the infrastructure addresses these challenges. • **Security Protocols:** Emphasizes the security protocols used to ensure reliable certification.
Methodology	Design and case study of implementation.
Contribution	Expands PKI's applicability to non-personal entities, offering solutions for secure device communication in IoT networks.
Title-12	**Designing the Provision of Public Key Infrastructure Services for eGovernment**
Main Objective	To design a PKI service model tailored for eGovernment, focusing on scalability and ease of integration with existing systems.
Key Findings:	• **Service Model:** Proposes a scalable PKI service model for eGovernment applications. • **Integration Strategies:** Discusses strategies for seamless integration with existing governmental IT infrastructures.
Methodology	Conceptual design and analysis of integration case studies.
Contribution	Provides a flexible PKI service model for eGovernment, emphasizing ease of adoption and integration.
Title-13	**A Security Framework for Wireless Network Based on Public Key Infrastructure**
Main Objective	To develop a security framework for wireless networks using PKI, aimed at protecting data integrity and confidentiality.
Key Findings:	• **Framework Design:** Outlines the security framework, focusing on encryption and authentication protocols. • **Performance Analysis:** Assesses the framework's impact on network performance.
Methodology	Design, implementation, and testing in a wireless network environment.
Contribution	Provides a robust security framework for wireless networks, demonstrating the effectiveness of PKI in protecting against common wireless threats.
Title-14	**Government PKI Deployment and Usage in Taiwan**
Main Objective	To examine the deployment and usage of PKI in Taiwan's government, focusing on its applications and challenges.
Key Findings:	• **Deployment Challenges:** Identifies the technical and regulatory challenges faced during PKI deployment. • **Usage Analysis:** Analyzes the usage patterns of PKI across different government sectors.
Methodology	Case study analysis and stakeholder interviews.

Contribution	Provides insights into the successful deployment and operation of PKI in a governmental context, with lessons for other governments.
Title-15	**Introduction to Public Key Technology and the Federal PKI Infrastructure**
Main Objective	To introduce public key technology and provide an overview of the U.S. federal PKI infrastructure.
Key Findings:	• **Federal PKI Overview:** Provides a comprehensive overview of the U.S. federal PKI, including its architecture and operational components. • **Technology Introduction:** Explains the basic principles of public key technology and its applications.
Methodology	Descriptive analysis of the federal PKI infrastructure.
Contribution	Serves as a foundational resource for understanding the U.S. federal PKI, offering a detailed overview for newcomers to the field.
Title-16	**Public Key Infrastructure Deployment in Cameroon's Public Administration**
Main Objective	To explore the deployment of PKI in Cameroon's public administration, focusing on its impact on governmental operations.
Key Findings:	• **Deployment Strategy:** Describes the deployment strategy, including the challenges faced and the solutions implemented. • **Impact on Operations:** Analyzes the impact of PKI on the efficiency and security of public administration services.
Methodology	Case study of Cameroon's PKI deployment.
Contribution	Provides a detailed account of PKI deployment in a developing country, with practical insights for similar contexts.
Title-17	**PKIs in C-ITS: Security Functions, Architectures, and Projects: A Survey**
Main Objective	To survey the use of PKI in Cooperative Intelligent Transport Systems (C-ITS), focusing on security functions, architectures, and ongoing projects.
Key Findings:	• **Security Functions:** Discusses the security functions provided by PKI in C-ITS. • **Architectures and Projects:** Provides an overview of the PKI architectures used in C-ITS and surveys current projects.
Methodology	Literature review and survey of ongoing C-ITS projects.
Contribution	Offers a comprehensive overview of PKI's role in C-ITS, highlighting its importance in securing intelligent transport systems.
Title-18	**A Security Framework for the Internet of Things Based on Public Key Infrastructure**
Main Objective	To propose a security framework for the Internet of Things (IoT) based on PKI, focusing on securing device communication.
Key Findings:	• **Framework Design:** Details the design of the PKI-based security framework for IoT. • **Scalability and Security:** Addresses the scalability and security challenges of implementing PKI in IoT networks.
Methodology	Design and experimental validation in an IoT environment.
Contribution	Provides a scalable and secure framework for IoT, demonstrating PKI's potential in protecting IoT ecosystems.
Title-19	**Towards a Unified PKI Framework**

Main Objective	To propose a unified PKI framework that can be adapted to various applications, enhancing interoperability and security.
Key Findings:	• **Framework Proposal:** Proposes a unified PKI framework designed to support diverse applications while ensuring security and interoperability. • **Adaptability:** Emphasizes the adaptability of the framework to different use cases.
Methodology	Conceptual development and analysis of existing frameworks.
Contribution	Offers a blueprint for a unified PKI framework, addressing the need for standardization and interoperability in PKI implementations.
Title-20	**FEIDHE - Integrating PKI in Finnish Higher Education**
Main Objective	To integrate PKI into the Finnish higher education system, focusing on securing academic data and communications.
Key Findings:	• **Integration Strategy:** Details the strategy for integrating PKI into higher education, including the challenges and solutions. • **Impact Analysis:** Analyzes the impact of PKI on academic data security and communication efficiency.
Methodology	Case study of PKI integration in Finnish higher education.
Contribution	Demonstrates the successful integration of PKI in an educational context, offering a model for similar institutions.

Table 16. Data extraction Summery

5.1.1.2.6 Data Synthesis

This section presents a synthesis of the data extracted from the 20 studies included in this review. The synthesis is structured around three key themes identified during the review: core PKI activities (legal framework, Deployment models, Facility and infrastructure,), Challenges, mitigation mechanisms applied and proposed frameworks and the respective elements of the proposed frameworks.

5.1.1.3 PKI Project Challenges

Despite the benefits, several challenges to successful PKI implementation were identified across the studies. A recurring theme was the legal governing framework of PKI throughout deployment and management process, cited by 80% of the studies. Studies [16] [17] [8] [6] [21], for instance, emphasized the difficulties faced by organizations as well as countrywide in establishing PKI .Unclear or contradictory laws and regulations, Technical ,procedural & infrastructure complexity which results in maintaining up-to-date revocation lists and managing certificate lifecycles. vulnerabilities such as weak cryptographic algorithms and poor key management practices were frequently mentioned as potential risks as lack of proper operation practices [16] [37].

A significant challenge identified was the low level of user awareness and understanding of PKI, leading to resistance or improper usage [37] [16]. The complexity of ensuring that PKI systems comply with diverse legal and regulatory frameworks, especially in multinational contexts, was highlighted as a major challenge by most studies [8] [16]. Another significant barrier is the high cost associated with PKI infrastructure, mentioned in 2 of the studies. Study [16] noted that smaller government agencies often struggle with the financial burden of PKI, limiting its widespread adoption.

Finally, interoperability issues were highlighted in 70% of the studies, particularly in multi-vendor environments. Studies [8] [16] [37] pointed out the lack of standardization in PKI implementations, leading to difficulties in integrating different systems and platforms.

In response to the identified challenges, the data analysis revealed several frameworks and best practices that have been proposed and implemented across various contexts, most of this solution lies on the technical aspect. To address scalability and interoperability issues, the adoption of hybrid PKI models that combine hierarchical and mesh topologies has been suggested [21]. To improve user adoption, comprehensive training programs that educate users on the importance of PKI and proper usage practices have been proposed [8] [16]. The use of advanced cryptographic algorithms and protocols, such as Elliptic Curve Cryptography (ECC), has been recommended to mitigate security vulnerabilities [32] [37].

5.1.1.4 PKI Project Implementation Framework

The studies reviewed demonstrate a variety of PKI implementation framework within e-government systems and various platforms [7] [8]. Through this study 5 frameworks are identified. Out of the selected studies 30% of them have shown the PKI core activities including legal framework preparation, PKI deployment model, awareness & training. as part of the project. Analysis, design & implementation phases are discussed as part of the project execution phases in study [6] [17] [16]. A study made on e-Government PKI of Greek SYZEFXIS-PKI explained seven phases and four key activities as part of the PKI project implementation, in another cases the Cameroon national PKI implementation incorporated four project phases and highlighted four key processes as part of PKI project implementation framework [17]. E-government PKI model is discussed by the study [6], This study has incorporated three phases including Design,

Implementation, Integration as part of the project phase and only PKI architecture model as part of the core activity in the study. The identified frameworks are further discussed in result section.

The aforementioned studies show that there is inconsistent in executing PKI project based phase and key activities in the execution of PKI as a project. Most of this studies have incorporated analysis and design phase as part of the project and legal framework preparation and PKI deployment models as part of the core activity in PKI project execution. The majority of these employed a hierarchical model, where a single root certification authority (CA) is responsible for the entire system's trust [17] [16]. Other studies favored a mesh model, where trust is distributed across multiple CAs, offering greater flexibility but also increasing complexity [21]. A small number of studies explored hybrid models that combine elements of both hierarchical and bridge architectures. For example, [16] highlights the success of the hierarchical model in the SYZEFXIS-PKI implementation, noting its straightforward management and scalability. Conversely, study [21] illustrates the advantages of a mesh model in the UAE's e-government infrastructure, which allows for regional autonomy in certificate management.

5.1.1.5 Summary of Findings

The synthesis of data suggests that while PKI is a powerful tool for enhancing security, its successful implementation requires careful consideration of various technical, organizational, and regulatory challenges. The proposed frameworks and best practices, such as hybrid PKI models and user education initiatives, have shown promise in addressing these challenges. However, the effectiveness of these solutions often depends on the specific context in which they are applied, highlighting the need for tailored approaches to PKI implementation. The summery of the data synthesis is illustrated below categorizing by challenges and frameworks.

Data Extracted	Study findings	Frequency in percentage	Themes identified	References
Challenges	Contradictory laws	85 % of the selected studies have mentioned: Contradict Laws and Regulations.	Legal Framework	[21] [37] [16]
	Interoperability	75 % of the selected studies have discussed Interoperability as major challenge..	• Legal Framework • Technical interoperability	[33] [32] [27] [36] [16]
	Lack of iterative process of analysis, design and Implementation	10% of the selected studies have discussed Lack of iterative process of analysis, design and Implementation as part of the study.	• Analysis, • Design, • Implementation, • Operation & Integration	[16] [17]

Data Extracted	Study findings	Frequency in percentage	Themes identified	References
	Trustworthiness of a PKI	10% of the selected studies have discussed lack of trustworthiness of PKI System	Audit and Accreditation	[29] [38]
	Lack of scalable PKI model	70% of the selected studies have discussed Lack of scalable PKI model.(hierarchical & bridge CA are defined as recommendation)	PKI deployment models	[34] [7] [21] [16] [17]
	Human error	70% of the selected studies have discussed lack of User awareness & training strategy	Awareness and training	[37] [16]
	infrastructure & Facility complexity	70% of the selected studies have discussed Two factor authentication	Legal Framework Facility & infrastructure	[31] [30]
	Improper security controls	20% of the selected studies have discussed Lack of technical and managerial control.	Facility & infrastructure	[37] [16]
	CPS non-compliance	20% of the selected studies have discussed CPS non-compliance	Monitoring & maintenance	[28] [35]
	Lack of alignment in Planning, effort and coordination	20% of the selected studies have mentioned: Lack of alignment in PKI Execution.	Project management	[16] [8]

Table 17. Data synthesis summery table for challenges from studies

Data Extracted	Study findings	Elements of the Framework	Themes Identified	Reference
Frameworks	E-government of SYZEFXIS-PKI	Organizational, Legal, Technical, Operational, Enterprise	Key Activities	[16]
		Envisioning, Focusing, High level design Detailed Design ,development ,Testing	Phases	
	Cameroon National PKI	Legal framework, Deployment architecture Audit & Accreditation	Key Activities	[17]
		Analysis, Design, Implementation, operation	Phases	
	E-government PKI Model	Deployment architecture	Key Activities	[6]
		Design, Implementation, Integration	Phases	
	UAE's PKI Implementation	Legal framework, Facility & infrastructure User Adoption and Awareness	Key Activities	[21]
		Stakeholder & business Analysis, Implementation, Integration, operation	Phases	
	PKI Design for the Real World	Legal framework, Deployment architecture	Key Activities	[38]
		Need assessment, Design, Integration	Phases	

Table 18.Data synthesis summery table for frameworks from studies

5.1.2 Case Study PKI in case of Ethiopia

5.1.2.1 Background of the Ethiopian National Root CA project

INSA is a government organization that has is established with the Ethiopian proclamation number 808/2013.INSA has given a role and responsibility through this proclamation. INSA has the vision to be a leading national agency in cybersecurity and information security, enhancing the safety and integrity of Ethiopia's digital landscape. mission to protect national information systems, promote cybersecurity awareness, and provide strategic guidance on information security policies and practices. INSA aims to collaborate with various stakeholders, including government agencies,

private sectors, and the public, to build a resilient cybersecurity framework. Article 6 sub article 9 and 10 of this proclamation provides the mandate to INSA to serve as the National root certificate authority of Ethiopia. Accordingly, INSA has an organizational unit that work specific to addressing the role and responsibility given by the proclamation.

The Ethiopian National Root CA project was initiated in the late 2011 by Ministry of Innovation and Technology (MICT) formerly known as Ministry of Innovation and Technology (MinT) .MinT was the first to take this initiative but due to change of mandate INSA (Information Network Security Administration) formerly known as the Information Network Security Agency(INSA) have takeover the project in 2013, due to small number subject matter experts exist in the area, lack of defined legal framework and budget constraint the project has forced to delayed for long time.

In 2017 INSA again initiated the project. The project initiative had two objectives. The first one is to establish a national Root CA that serve as National root CA and country signing CA and a certificate provider that provide a digital certificate to key government organizations. Through the process of project execution, a string committee comprises of Legal department, policy department, Software development department, R&D, Procurement department and finance department. The string committee has obligated to assign a technical team. Due to the discovery of COVID-19 and the government direction to relocate the organization to new building the project has pended for 1year. The legal document produced by INSA in 2018 was one of the supporting legal document published to recognize the equivalence of digital signatures and paper-based signatures which is the Electronic Signature Proclamation No. 1072.2018.

In 2019 The National PKI project has reinitiated with the new building and new management structure. The new management has directed the initiatives made in the late 2017 to proceed and the project activities continued. For the purpose of this case study an interview is conducted and the given responses are appended in Appendix-E. This section shows the narrative from the case study based on an interview response with regard to the Ethiopian national PKI implementation project. The case study discusses the process of the project management, the preparation of PKI

legal framework, design of deployment model, Facility preparation, Training and Audit and certification strategies are discussed.

5.1.2.2 PKI Project Management

The project management utilized for the implementation of Ethiopian national PKI project is PRINCE2.In order to manage the PKI project, a string committee comprises of various stockholders are assigned by the director general of the organization. The representative and members of the string committee are selected from different departments, includes Engineering, PKI, Audit and Evaluation, Law Affairs, Procurement, Project management, Software Development and Research and Development (R & D). Each representatives of the string committee are tasked to choose a technical manager accordingly. The String committee will be going to meet in Fifteen days (15) interval to discuss the overall project progress and to make decisions on issues that require attentions. The string committee is also responsible for allocating resources required for the project.

The technical managers are senior subject matter experts in multi-disciplinary fields that are tasked to oversite the technical implementation of the project. For this reason, the technical managers are required to deliver project implementation roadmap comprises of major deliverables and RACI metrics. The technical managers are also required to report the project progress for the project manager in weekly basis.

The project manager is responsible for organizing meeting agenda for the string committee, follow up project progress with regard to project schedule as well as collaborate project resources. The project manager is responsible for developing project plan by communicating the technical managers.

5.1.2.3 PKI governing framework

The PKI governing framework has passed through all the analysis phase in order to construct the governing framework. Best practices from various countries had reviewed. Indian, Korean, Colombian, Australian, Philippines Root Certificate authority's legal frameworks are reviewed as part of the process. Based on the findings made from the analysis, considering the Ethiopian legal structure a PKI governing framework is designed. Below it shows the Ethiopian national PKI governing framework.

Electronic signature Proclamation	
Regulation	
Certificate Policy	Certificate Practice statement(CPS)
Directives	
Guidelines	
Operational Procedures	

Table 19. Ethiopian National PKI Governing Framework

5.1.2.4 PKI Deployment Model

For the purpose of the design of deployment architecture of National Root CA, various architectures has been reviewed for the purpose of constructing the deployment model. hierarchical deployment model, Bridge CA model and cross certification model where the model that where reviewed as part of designing the deployment model. The Ethiopian legal structure had also reviewed as part of the process. According to the proclamation called reestablishment of INSA proclamation number 808/2013, the mandate to be a National Root CA is given to INSA, based on this proclamation and the review of related practices and suggestion of the consultants the PKI hierarchical deployment model is designed as INSA the anchor of the National PKI domain. The hierarchical deployment model basically comprises of two tire hierarchy, the National Root CA which is INSA and subordinate CA, CAs that provide Digital Certificate Service for various sectors, including Federal government organizations, commercial CA that provide Digital Certificate Service for Financial sectors including Banks and micro finance and Private CA that provide Digital Certificate Service for the private sectors.

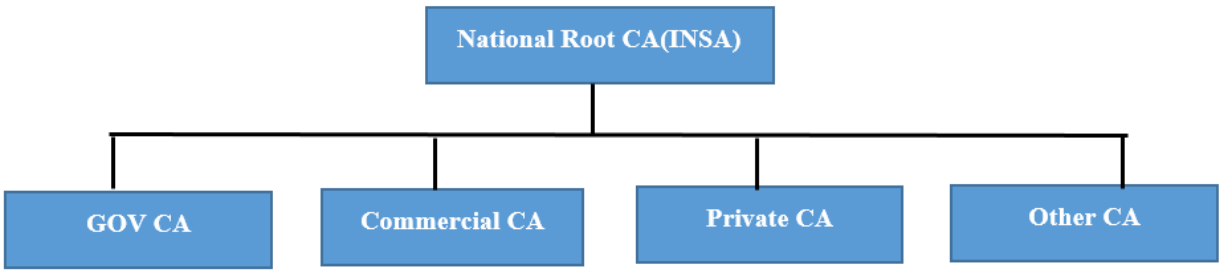


Figure 7.Ethiopian National PKI Deployment Model

During the development of the PKI deployment model all the phases from the proposed framework are employed. During the analysis phase all available deployment models are analyzed and reviewed against the Ethiopian legal structure. Both the Proclamation called reestablishment of

INSA, proclamation number 808/2013 and Electronic signature proclamation 1072/2018 are analyzed as part of the analysis phase. Additionally, international practices from various countries are also analyzed during the analysis phase of project implementation. India Root CA deployment model was one of the models that was analyzed during this phase, since the legal structure of the India considered to be similar to Ethiopian legal structure, at this phase all the studies gained as deliverables are communicated to the project manager through the PKI technical team. During the Design phase of the project implementation the inputs gained from the analysis phase are used to develop the National PKI deployment model, that is hierarchical model as shown on the above image. During the implementation phase of the PKI deployment model the selected model is presented to the string committee and gained approval to make it operational. During all the phases starting from analysis through design and implementation, all the deliverables gained from these phase are reported and communicated to the project manager.

5.1.2.5 PKI Infrastructure and facility

In order to design the PKI datacenter facility, the datacenter standards are reviewed. And also various best practices regarding PKI datacenter are also analyzed. The datacenter design document is peer reviewed by various stakeholders engaging in the implementation of National project.

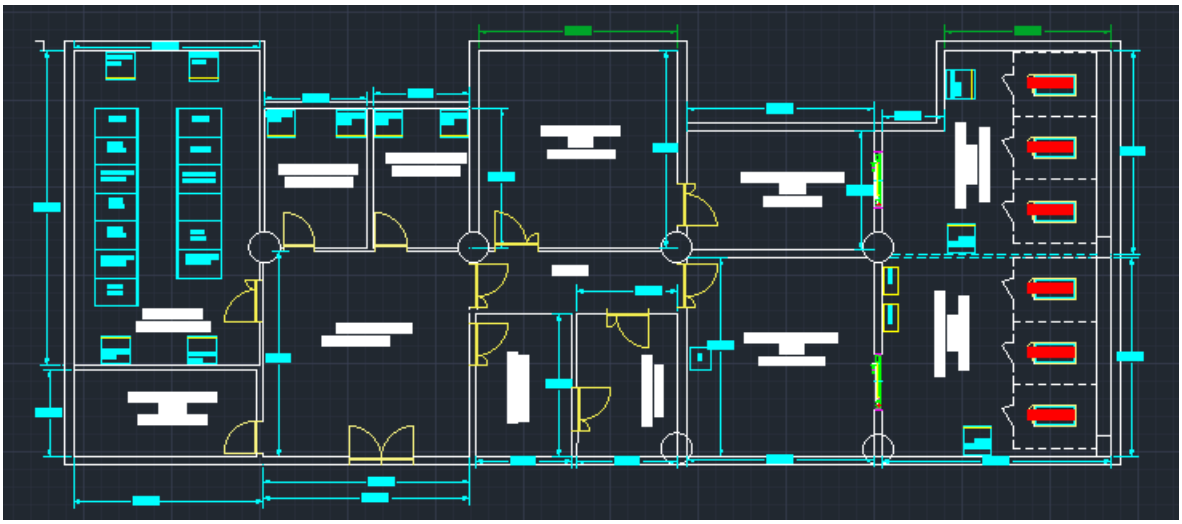


Figure 8.Ethiopian National PKI Infrastructure & Facility

During PKI Infrastructure and facility implementation of the project, all the phases within the proposed framework are employed. During the analysis phase of the PKI infrastructure and facility, International best practices from various countries has been analyzed. India, Egypt, Korean, Philippines, Colombian practices regarding PKI Infrastructure and facility where analyzed. During this phase each functional room of the PKI Data Center, Root CA software

solutions, equipment's, tools and the requirement of site selection criteria for Primary data center and Disaster recovery data center are analyzed. Additionally, various standards related to Data Center design requirements are also revised, which includes Webtrust principles and criteria for certificate authority, Indian PKI Site preparation guideline document and CISSP CBK reference book where three of the main documents that are passed through the document analysis phase. During the analysis phase one of the other thing that was goes through analysis was the Root CA Software solution. For the purpose of the Root CA software solution each functional requirement is identified related to the protection profile document called common criteria for certificate authorities.

During the design phase of the National PKI project implementation an input gain from the analysis phase is utilized. During this phase PKI Data Center Architecture is designed as a high level document(HLD) considering the identified functional rooms identified on the analysis phase. The number of Servers required, the power systems, AC Systems and the required access control were designed accordingly as a Low level document(LLD).

During the design phase the other thing that was done is design of Software requirement which is Root CA Software requirement based on the input gained from the analysis Phase. Both the HLD and LLD design documents that shows the PKI software deployment architecture and the software and hardware requirement including a context diagram is designed is designed at this phase.

During the implementation Phase of the National PKI project, civil work of the infrastructure is implemented based on the defined HLD and LLD design document in the Design phase. For the purpose of the civil work a required Devices and Equipment's that are identified in the analysis phase and design phase are purchased accordingly aligned with the Civil work. During the implementation phase regarding the PKI software solution the development of Root CA software Is implemented based on the defined LLD design document defined at the Design phase of project implementation. The functional requirements are tested against the requirement of the common criteria for CA document to gain a common criteria(CC) certification. During all the phases starting from analysis through design to implementation, all the deliverables gained from these phase are reported and communicated to the project manager.

5.1.2.6 PKI Software Solution Development

During the Analysis Phase of PKI Software Solution Development, Various options are analyzed based on the project scope. Accordingly, three options are analyzed and made ready for discussion

by the string committee for a decision. The three options were, option-1: Develop a software from scratch, option-2, Develop a software from open source solutions and the 3rd option was to purchase a software solution that meet the organization need. These three options do have both their own benefit and drawbacks. Option one has benefit to own the technology but it consumes a reasonable time, while the second option has provided a starting point to develop a software solution but it has disadvantage if the software is considered to have a Common Criteria(CC) with the sole owner of the organization. The third option has time benefit, if we consider to have technology ownership it is difficult to own the software based on this option the String committee has decided to develop the software with the help of consultants that have experience in the PKI software solution development.

Based on the decision made by the string committee, the Design phase is continued. During the design phase The software development team has developed a software requirement Specification (SRS) that shows all the functional requirements in a way that comply international standards. Some of the functional requirements were the system required to generate a key pair with RSA 4096 key length and the system required to issue a digital certificate for certificate providers(CAs) in a way that comply the international practice and other additional requirements are included within the document. During the implementation phase of the project, with the help of consultants the software is developed in a way that comply with common criteria(CC) certification. At the time of writing the software is under final test.

5.1.2.7 PKI Training and Awareness

The critical and required trainings are identified through analysis of best practices from various previously done technical documents as well as the consultants engaged in the implementation of National PKI Projects that enables the smooth operation of PKI.policy document preparation training, Secure software development and maintenance training, operational training, Compliance training, Audit criteria and requirements training are some of the trainings that are identified through analysis of various technical documents with regard to PKI infrastructure. Technical trainings related to various security devices that are utilized within the operation of PKI are also identified. HSM training, Firewall training, Networking training, power system maintenance training, datacenter infrastructure and facility training are some of the trainings identified by the project technical teams. For the purpose of the overall training the number of personnel's have identified in order to take the required training. The selection approach used for the training is

based on the defined kills and disciplines as well as experience. Since these trainees will engage in the operation of the national PKI and the area requires higher security clearance. Those trainees will undergo the organization security clearance process.

5.1.2.8 PKI Audit and Certification

The Ethiopian national PKI implementation project aimed to gain both Webtrust certification for the PKI datacenter facility and Common criteria (CC) certification for the Root certificate software that is developed internally. For the purpose of audit and certification analysis of various technical documents and various known audit firm's documents have been reviewed by INSA technical team. The requirements for audit and certification are defined based on the analysis and review of those documents. Webtrust principles and criteria for certificate authorities, which discusses and set criteria's the overall requirement against the PKI facility. The other document reviewed by the INSA technical team regarding PKI audit and certification is European Telecommunications Standards Institute (ETSI) standards, which set the requirements against Secure implementation of PKI. The other critical document reviewed by the INSA technical team regarding PKI audit and certification is the Protection Profile for Certification Authorities version2.1. This Protection Profile (PP) describing security requirements for a Certification Authority is intended to provide a minimal, baseline set of requirements that are targeted at mitigating well defined and described threats.For the purpose of the certification processes recommendation from consultants has been given and based on the recommendation given by the consultants a required document that are planned to developed are identified. Security target document to be developed according to Protection Profile for Certification Authorities and Webtrust checklist document that is going to be developed in accordance with the criteria set by Webtrust principles and criteria for certificate authorities document were the identified documents that are planned to be developed.

5.1.3 Monitoring and maintenance

The activity monitoring and maintenance of the PKI infrastructure is done after the national project is stablished and start providing the service. During these activities the overall operation and supporting infrastructure are planned to be monitored in 24/7 manner. For the purpose of these activities an organizational structure that comprises of an expert in the field of various discipline are organized. PKI solution continuous development team, PKI governing document development and maintenance team, PKI operation team, PKI facility administration team are the teams that are engaged in the overall operation of the National PKI establishment and operation. The inputs and

reports gained from the defined team will be going through maintenance process according to the defined procedures set by the future PKI governing documents.

5.2 Analysis

5.2.1 Study Selection Analysis

The main source of information chosen for this study was the Scopus and Science@Direct databases. Scopus and Science@Direct is a multi-disciplinary database with easy features to refine the search results by year, document types, authors and affiliations. It is the largest abstract and citation database of peer-reviewed papers with relatively large coverage in comparison with other databases such as Web of Science and Google Scholar [39].Accordingly, the articles through the selected databases 15.5% of the articles were retrieved from Science@Direct and 84.5% of the articles were retrieved from Scopus. For further reference the report generated by Parsifal is illustrated below.

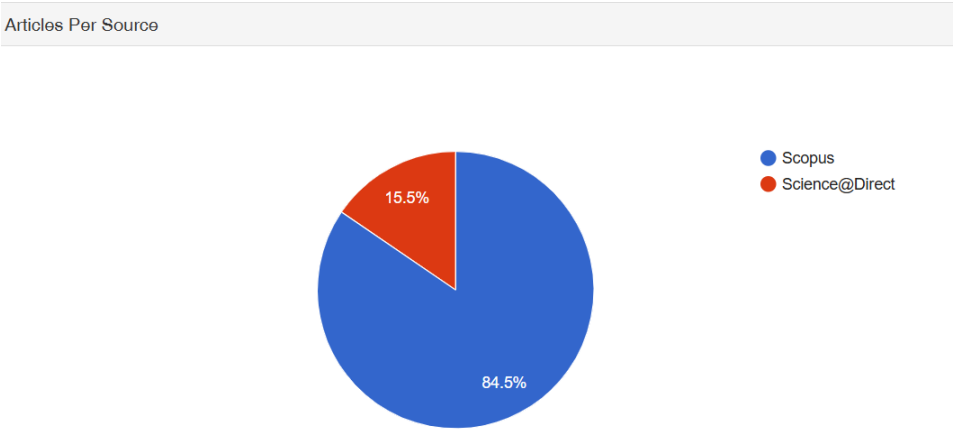


Figure 9. PI chart articles selected per source generated through Parsifal

Total of 975 Research works are identified through the search strings generated by Parsifal. These research papers are imported to Parsifal for study selection process (. bib, bibtex format). 140 duplicate research works were excluded. Out of this duplicated research works 103 research papers were excluded from Scopus and 38 papers are excluded from Science@Direct database search. 814 research works are excluded based on the selection criteria defined. These includes years of publication (Prior to 2000), unrelated Titles, abstract and paper contents with regard to the research objective and language (Not English). Accordingly,104 papers from Science@Direct are excluded

based on the selection criteria defined and 710 research papers from Scopus are excluded based on the selection criteria defined. Finally, For the purpose of this research 20 research works are identified with regard to the research question and objective of the study. 11 research papers were accepted from Scopes search database and 9 research works where accepted from Science@Direct database were accepted for further analysis based on the defined research objective. The graph blow illustrates the aforementioned idea and is generated through Parsifal.

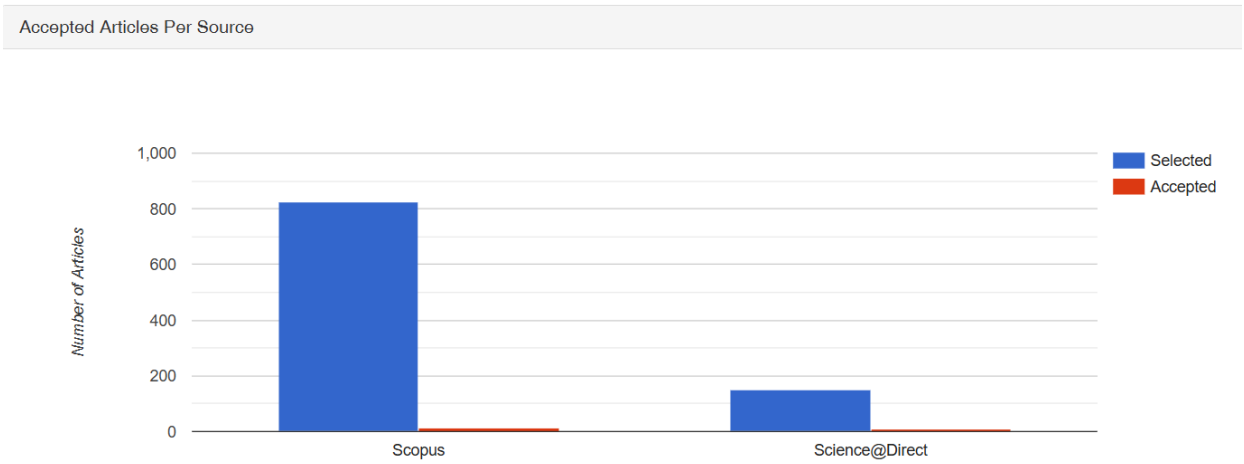


Figure 10. bar graph accepted articles selected per source generated through Parsifal

For the purpose of this research a total of 20 research papers are filtered. The research papers are organized by Author, Title, by publication Years. Most recent research works searched through the search string focuses on Block chain technology and the application of blockchain technology in various digital platforms. This shows the current focus of the research. The table and the graph shown below illustrates the selected papers by year of publication and the frequency.

,No.	**Year**	**Number of papers**
1.	2001	3 articles
2.	2003	1 article
3.	2004	1 article
4.	2005	1 article
5.	2006	3 articles
6.	2009	2 articles
7.	2011	1 article
8.	2013	4 articles
9.	2014	2 articles

,No.	Year	Number of papers
10.	2019	1 article
11.	2022	1 article

Table 20.Liste of selected articles based on publication years

Over the past 8 years, the majority of research efforts have been dedicated to studying blockchain technology and its implementation across different digital platforms. This indicates the present area of focus in the research. Several scholarly papers have been published in recent years that specifically examine PKI technology, its application, and its integration in diverse sectors. The dissemination of research work is depicted below using the VOSViewer tool.

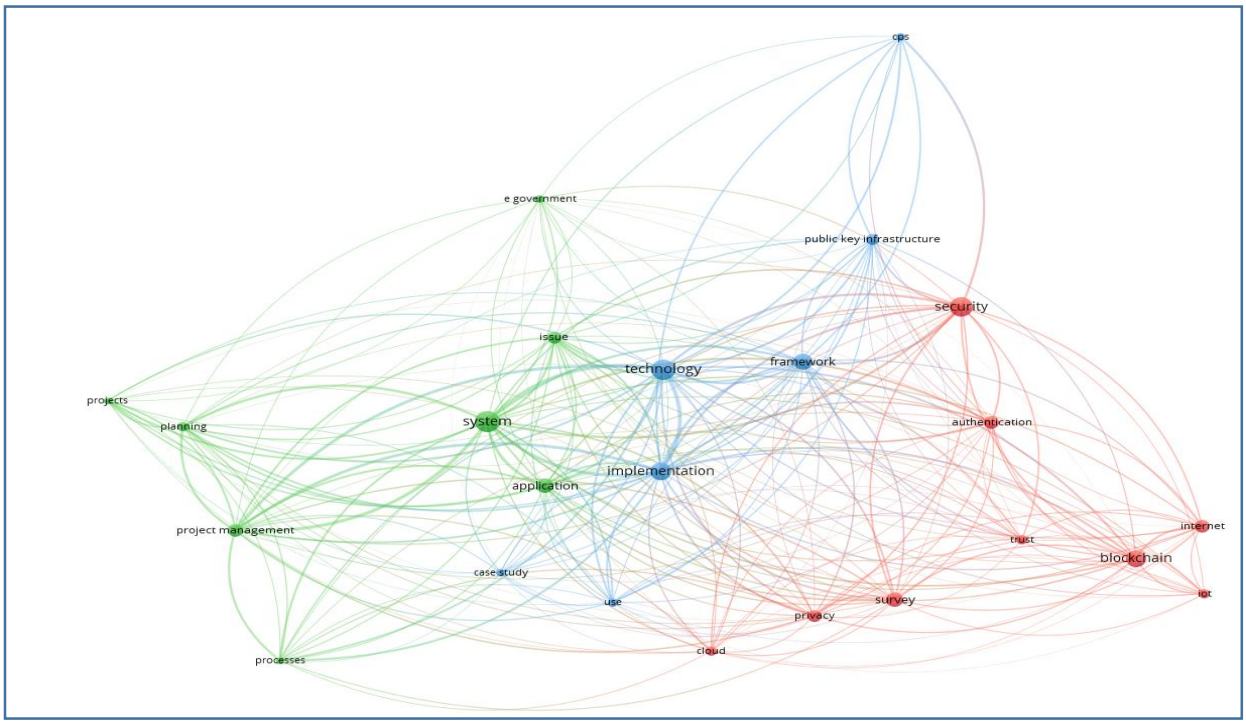


Figure 11. The Distribution of the study generated through VOSViewer

5.2.2 Research Finding's Analysis

RQ-1 What are the difficulties encountered during the implementation of a PKI project?

PKI Plays a major role in the digital world. Various countries have implemented PKI to enable various service in various sector. Border control, e-government services , e-commerce services and financial services such as Internet banking are some of the services enabled by PKI [7] [36].Even though PKI Plays a key role in ensuring digitalization, establishment of PKI at national or organizational level always challenging. There are various reasons for this, a number of research

works have discussed these challenges in various methods. Survey and case study are the most prominent ones [12]. This section briefly discusses the major PKI project implementation challenges that are identified through SLR and the proposed frameworks utilized through PKI project execution.

5.2.2.1 Project management framework

One of the major setbacks can be a commonly witnessed through PKI Project execution is lack of alignment between the affected organizational units' goals and the PKI project implementation needs. Also, lack of planning, effort, coordination [16]. This is due lack of proper management of PKI project. Various project management frameworks existed. The purpose of these existing frameworks is to resolve various project management issues. PMBOK, PRINCE2, and Agile Project Management are the most widely used and well-known frameworks over the past few decades. These frameworks, allow for the successful implementation of a project in various project scenario's [6]. In PKI project execution, the involvement of various subject matter expert is required, which makes it challenging in organizing and identifying proper deliverables, which creates a burden in the task of the project manager [8] [16]. Out of these frameworks PRINCE2 has greater advantage in such projects due to the separation between the project management Stages and technical Stages, which alleviates the burdens of project managers who lack expertise in the project's domain [20].

The other one that needs to be considered in project execution is adaptation factor organizations planning to establish PKI should consider and assess the Organizational capabilities, Organizational task and characteristics and security technology characteristics prior to the project execution [30].As summary 20% of the selected studies have mentioned: Lack of alignment in PKI Execution.

5.2.2.2 PKI Project implementation Phase

Lack of iterative process of analysis, design and Implementation and Design considerations central in an effort to build a good understanding of problems, solutions, alternatives, costs and risks. In particular, investment analysis and a dedicated business case study can provide invaluable guidance for the success of the project. Contextualizing PKI technology and its process solutions is critical for success [16]. PKI project Implementation at national or organizational level should consider a legal framework, Deployment Architecture, Facility and infrastructure, Awareness and

Training, and Audit and Accreditation as core activates, and these core activities required to be executed through careful Analysis, design, implementation and operational phases.

5.2.2.3 PKI Governing Legal Framework

Unclear or contradictory laws and regulations among the executive, legislative and judicial branches or negative norms and behavior can constrain efforts to use PKI technology [16] [17]. Most of the studies highlight the lack of proper legal framework across the country has a major setback for most of the challenges [37] [30]. One of the major reasons is the interdependency that exist with other core activities such as the dependency of PKI legal framework on datacenter preparation and the dependency of training on datacenter preparation. Design of deployment model, Design and implementation of facility and supporting infrastructure are the most prominent once. For this reason, the preparation of PKI legal framework takes the initial stage in project execution activity.

5.2.2.4 Scalable PKI Deployment Model

The selection of the PKI deployment model depends on the main objective of the establishment of PKI.PKI deployment model must ensure scalability and at the same time it must ensure interoperability. various research works have discussed different models on how to ensure scalability and interoperability. Hierarchical model and bridge models are the most prominent models discussed through various research works in order to ensure scalability and interoperability [6] [16] [21]. Lack of scalable PKI Architecture creates a challenge in the application of PKI in various services specially in implementation of boarder control across states [8].

5.2.2.5 PKI Facility and Infrastructure

Due to the technical and procedural and infrastructure complexity that security technologies (and in particular a PKI solution) impose, as well as the novelty that these technologies and respective work practices present, not only at the end-user level but also at the designer/implementer level, it is imperative to ensure strong technical and managerial skills for the key members of the project [10]. Also, it is well advised to anticipate possible shortages of qualified technical staff and an incremental approach can help in dealing with this problem [16].

5.2.2.6 PKI Awareness and Training

Extended and persistent efforts for raising user awareness, training, involvement and solution acceptance is mandatory. End-users' attitudes and perception of the system's ease of use and

reliability must be reviewed to ensure successful implementation and use/operation of the infrastructure [21] [16]. Likewise, user (in particular public servant) privacy and confidential concerns, as well as a sense of autonomy and required responsibility-accountability are challenges that must be adequately addressed in an e-government PKI initiative.

5.2.2.7 PKI Audit and Accreditation

Lack of a concise and thorough risk assessment activity and resultant controls may undermine the trustworthiness of a PKI infrastructure and lack of a formal validation of CA practices and of an accreditation of the service's CPS [17]. challenges related to a more general institutional framework and policy environment in which governmental organizations pursuing e-security efforts operate. In this context, institutions have not only laws and regulations, but also norms, actions or behavior that people accept as good or take for granted. Additionally, external pressures such as policy agendas and politics may affect the results of security initiatives [16].

5.2.2.8 PKI Interoperability

The PKI must be interoperable between the different organizations involved. Security solutions utilized between PKI participants within the PKI domain needs to be insured [30] [8]. Countries implementing PKI at national level requires Interoperability [21] [17]. Interoperability is the cornerstone of an expandable and functional PKI infrastructure is the possibility to be able to interoperate among the different CAs [6]. The application of PKI in Border control system is an instance that forces interoperability to exist within the PKI domain. Interoperability among legal governing documents such as CP, interoperability between certificate profile are some of the things that needs to be considered [8]. In most cases PKI interoperability is aimed to study the possible ways to enhance and facilitate the use of electronic signatures across borders [8]. Three of the key aspects in this scenario are the legal recognition of electronic signatures, trustworthiness of PKC and technical interoperability's [16] [38] [34]. Legal recognition of electronic signatures which are the main application of public key cryptography, should be recognized in law with the same legal effect as equivalent to handwritten signatures. When necessary, an electronic signature should be admissible to courts [6] [38]. Trustworthiness of public key cryptography Relying parties are generally hard to determine the quality of certification services and trustworthiness of foreign PKI. In order to improve on this, we suggest establishing the role of trusted third-party (TTP) in the local country to assess the public key cryptography technical interoperability. Electronic signatures have a long history of development in cryptography. Security of electronic signatures should hold

the properties of authenticity and nonrepudiation. Electronic signature technology should be reliable, but it should not be favor to a particular technology for PKI interoperability.

5.2.2.9 PKI Project Implementation Frameworks

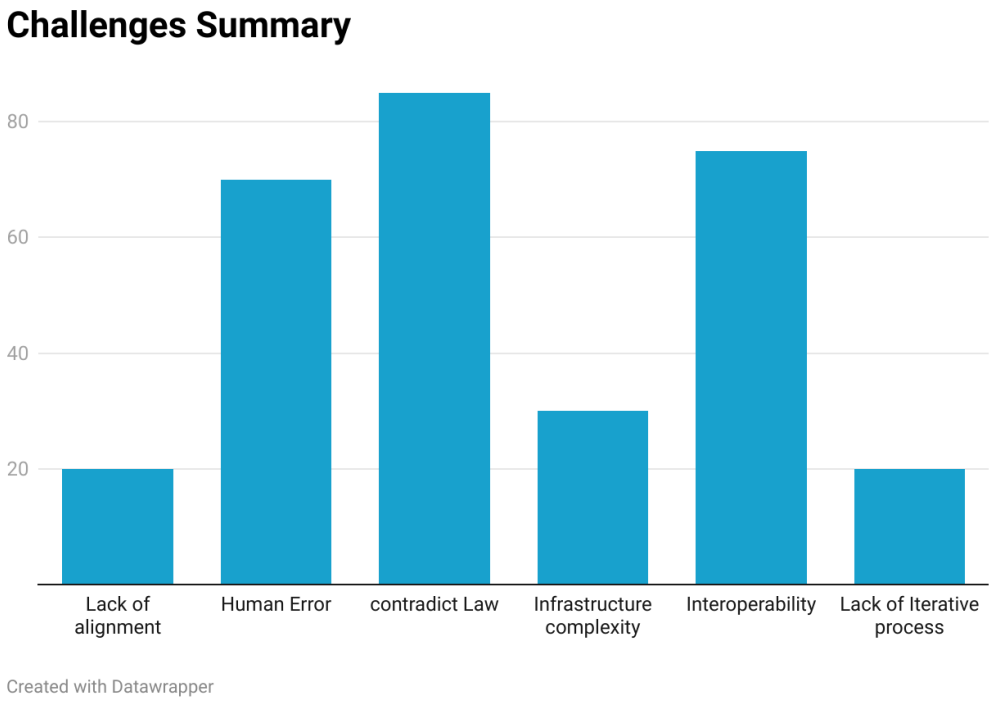
Various research works have discussed different frameworks in implementation and integration of PKI in various Digital platforms. Since most of these studies focuses on the implementation of various services on already established PKI infrastructure, they have limitation on discussing PKI at project level. The application of PKI in education system to enable smart card authentication [9], The application of PKI to enable mobile e-commerce [7], the application of PKI in high performance computing environment [28], these are some of the research works that can be seen as an instance.

A few research works discussed PKI implementation in various sectors at national and organizational level. An article made on the implementation of PKI in Cameroon's public administration is one instance, this article shows the process of the implementation of PKI to address the risk of forgery, theft, or abuse of identification credentials and promote the implementation of e-government and e-commerce services at national level. The article has discussed PKI implementation project considering the following throughout project execution. Analysis, Design, Implementation and Operation. And key Activities are done. Legal framework, Design consideration (Flexibility, Scalability, Interoperability), PKI deployment model (Hierarchical model, Cross-certification) [17].

Most of the selected papers have discussed PKI project implementation challenges in the project execution. lack of proper legal governing framework, interoperability, lack of well-structured project management framework, lack of operational training, technical, procedural & infrastructure complexity, lack of iterative process of analysis, design and Implementation and Operation in project execution, lack of scalable PKI models and trustworthiness of a PKI infrastructure are some of the common challenges that are discussed in most of the selected studies.

In order to overcome these challenges different studies, have proposed different solutions. Some scholars recommend design considerations elements (Scalability, Interoperability and Flexibility) as part of the design phase of the project execution [17]. One of the major challenge identified through the research studies is contradictory laws and regulations (lack of proper legal framework). To overcome this challenge various solutions are proposed. The first one is pre risk assessment

and analysis which is also called readiness assessment [17]. The second one mandatary recommendation given by various scholar prior to project execution is the recognition electronic signature as a part of the country law [8]. In order to overcome operational issues various research studies have recommended best practices including establishment of voluntary accreditation scheme, classification of certificate types, determining the certificate lifetime, develop of CPS [34] [37] [16]. Most of these recommended practices lies on proper management of legal frameworks and the sub sequent guideline documents. To address lack of scalable PKI models different scholars have suggested the utilization of hierarchical PKI model and bridge CA models [17]. To overcome lack of iterative process of analysis, design and implementation and operation in project execution a few scholars have incorporated design and implementation phases as part project execution [6] [10] [16].



RQ-2 How can a PKI implementation framework support the establishment of a national or organizational PKI implementation project?

Various Studies have proposed frameworks for PKI project execution in order to overcome issues discussed though project execution. Five frameworks are identified through the SLR process. The study [16] has defined a PKI project implementation as part of the case study for Greece PKI (SYZEFXIS-PKI) to implement e-Government services. The project execution methodology

comprises of 7 phases (envisioning, focusing, high level design, detailed design, development, testing) and 5 core activities (organizational, legal, technical, operational, enterprise).

The study has not discussed the framework in a way that shows detail activity aligned with the defined project phases as well as the major deliverables expected from each core activity and phase. The other major challenge noticed through this framework is the interdependencies that exist between those core activities not shown. The figure below shows the defined architecture illustrated by the study.

No.	Framework	Phases	Core Activity
1.	Greek PKI	Envisioning Focusing HLD LLD Development & Testing Deployment Evaluation,revision,strengthning	• Enterprise • Organizational • Legal • Technical • Operational

Table 21.Greek E-government PKI project implementation methodology

The second framework is the framework utilized for Cameroon National PKI project execution [17]. Three fundamental activities have been identified by the study: Audit & Accreditation, Deployment architecture, and Legal framework. Furthermore, it has outlined four phases for project execution: Analysis, Design, Implementation, and Operation. The research has concentrated on the design and analysis process during the project phase, as well as the development of a legal framework and deployment architecture, which are essential components of the core activity. The study suggested the implementation of a hierarchical deployment architecture with a bridge CA. Furthermore, the investigation identified three legal regulatory frameworks for PKI as part of the legal framework's preparation. The following topics are of interest: the law pertaining to cybersecurity and cyber criminality, the assessment and accreditation document for PKI, and the CP and CPS [17]. The study has also identified readiness assessment and audit & accreditation as components of the process. The framework component is summarized in the table below.

No.	Framework	Phases	Core Activity
1.	Cameroon National PKI	Analysis Design Implementation	• Legal framework • Deployment architecture • Audit & Accreditation

Table 22. Cameroon National PKI project execution framework

The third framework is a study made on e-government PKI model [6]. The study centers on the design, implementation, and integration aspects during the project period. The implementation phase of the project focuses on executing the PKI deployment model and integration scenarios. The framework aims to address how PKI is integrated with different e-government services, with integration being a central activity within the framework. The study suggested incorporating a hierarchical model into the fundamental activity of the deployment architecture. The following table provides a concise summary of the framework component.

No.	Framework	Phases	Core Activity identified
1.	eGovernment PKI model	Design Implementation Integration	• Legal framework • Deployment architecture

Table 23. eGovernment PKI framework

The fourth framework identified through the SLR is the PKI implementation survey made on UAE [21]. The study has demonstrated the procedures that were implemented during the execution of the PKI project. The study highlights the significance of user adoption and awareness, as well as the preparation of a legal framework, in the execution of a PKI project to address the challenge of interoperability. In the project execution overview, the study has integrated two core activities (Legal framework, User Adoption and Awareness) and four core phases (Analysis, Implementation, Integration, operation). The study underscores the importance of conducting a stakeholder and business analysis prior to the execution of the project. The framework component is summarized in the table below.

No.	Framework	Phases	Core Activity
1.	Public Key Infrastructure for UAE	Analysis Design Implementation Integration	• Legal framework • User Awareness & Training

Table 24. Public Key Infrastructure for UAE

The fifth framework identified through the SLR is a study made on PKI Design for the Real world [38]. The study endeavors to address the potential for PKI systems to be designed to accommodate a variety of user sizes and numbers (Scalability), adapt to the needs of various organizations and technological advancements (Flexibility), and ensure interoperability between various PKI systems and standards (Interoperability). The study suggested that a need assessment be conducted

prior to the execution of the project. The study suggested a framework that includes two main activities (Deployment architecture, Legal framework) and three phases (Need assessment, Design, Integration) as part of the project execution. The framework component is summarized in the table below.

No.	Framework	Phases	Core Activity
1.	PKI Design for the Real world	Need assessment(Analysis) Design Integration	• Legal framework • Deployment architecture

Table 25. PKI Design for the Real world

The aforementioned PKI project frameworks show inconsistent core activity and phase through project execution. PKI requires facility and infrastructure comprises of Functional rooms to operate [14]. In the majority of the selected papers, this fundamental activity is not addressed as part of project execution and is not included in the proposed frameworks and project execution phases. The technical, procedural, and infrastructure complexity, as well as the absence of appropriate access control, are the primary obstacles to the successful execution of PKI projects, as identified in numerous studies [37]. Facility and infrastructure should be regarded as essential activities in the execution of PKI projects in order to address those obstacles. The other issue is user awareness and training. A variety of studies have addressed the challenge of human error in the operation of PKI services [37] [8] [16]. In order to overcome the challenges, these activities should be considered indispensable in the implementation of PKI initiatives.

Even if the studies have incorporated operation as part of project phase they do lack core activity to be incorporated as PKI project execution framework. Facility and infrastructure, Awareness and training are some of the core activities that can be raised as an example. Generally speaking, the SLR shows that there is inconsistence or no generic and universally accepted framework that is used as a guide for PKI project execution. In order to overcome the aforementioned challenges and limitations exist in existing frameworks a framework needs to be developed. For this reason, the proposed frameworks in the next section has designed based on the challenges and limitation expressed in the aforementioned section. Summary of the analysis of existing framework limitations are described in the table below.

Data Extracted	Study findings	Limitation
Frameworks	E-government of SYZEFXIS-PKI	• The study lacks clarity in addressing expected deliverables from each core activity and phase. • The study does not incorporate project management framework as part of the project execution methodology. • The study provide Project execution methodology as part of the case study.
	Cameroon National PKI	• The study does not incorporate facility and infrastructure, User awareness & training as part of the core activity of the project. As a result, it lacks to address technical interoperability and human error issues throughout the project execution and service operation. • The study does not incorporate project management framework as part of the project.
	E-government PKI Model	• The study does not incorporate facility and infrastructure, User awareness & training as part of the core activity of the project. • The study does not integrate project management framework as part of the project.
	UAE's PKI Implementation	• The study does not incorporate facility and infrastructure, User awareness & training as part of the core activity of the project. • The study does not integrate project management framework as part of the project. • The study focuses on survey of existing service.
	PKI Design for the Real World	• The study does not incorporate facility and infrastructure, User awareness & training as part of the core activity of the project. • The study does not integrate project management framework as part of the framework.

5.2.3 Case study Interview Analysis

This section analyzes the interview based case study analysis of the Ethiopian National Root CA project implementation. The major activities and challenges that are Phased during the execution of PKI.

5.2.3.1 Project Management Framework

The organization utilizes the PRINCE2 framework, a structured project management methodology often applied in technology-driven environments. Key processes included visibility analysis, steering committee establishment, and project charter development. PRINCE2 aids in defining clear roles for technical managers from various departments, enhancing deliverable-focused management. A challenge identified was stakeholder commitment, underscoring the necessity of cohesive teamwork and communication.

5.2.3.2 Audit and Certification

The project aims to create a trustworthy PKI for secure digital services. Emphasis is placed on obtaining certifications like WebTrust for service reliability and Common Criteria (CC) for the Root CA software. Standards such as ISO and ETSI were reviewed to ensure the project aligns with international best practices. These certifications enhance credibility and compliance with global security standards.

5.2.3.3 Deployment Architecture

The deployment design was influenced by reviewing international legal frameworks from countries like India, Australia, and South Korea. This comparative approach provides insight into structuring both the legal and technical facets of the National PKI, accommodating regulatory and functional requirements tailored to the project's scope.

5.2.3.4 Training Requirements

Proper administration and operation of PKI systems necessitate specialized skills. The project's training plan includes certifications in security, network management, and hardware security, such as COMPTIA Security+, CISSP, and HSM certifications. This indicates a strong focus on equipping the team with necessary technical competencies for sustainable PKI management.

5.2.3.5 Datacenter Infrastructure

The PKI datacenter's unique security demands are acknowledged, involving high-level standards and specific materials like Faraday cages for physical protection. Collaboration between engineers and security consultants ensured compliance with these standards, emphasizing secure operation environments essential for PKI functionality.

5.2.3.5.1 Challenges in Implementation

Stakeholder understanding of PKI's complexity, resource allocation, and interdependency management were notable hurdles. Project delays and budget constraints also disrupted the initial timeline, leading to project termination. However, these challenges were addressed, allowing the project to progress. This history highlights the need for comprehensive planning and resource alignment in large-scale PKI projects.

5.2.3.6 Continuous Monitoring and Operation

The PKI operation requires ongoing oversight, including hardware monitoring, network data flow, and system health checks. The planned deployment of log mechanisms and asset registry supports this, ensuring continuous, secure, and reliable service delivery.

5.2.3.7 Conclusion

The interviews reveal a structured, multi-faceted approach to implementing a National PKI project, with significant attention to project management, certification standards, training, and infrastructure. The challenges encountered underscore the importance of early stakeholder education, resource management, and thorough planning for project sustainability and success.

CHAPTER SIX

6 Results and discussion

6.1 Results

6.1.1 Overview of PKI Implementation Framework

The proposed PKI project implementation framework was successfully developed to address the unique requirements of secure digital infrastructure for example e-government, mobile e-commerce, etc. The framework encompasses several phases: Project Initiation, Planning, Analysis, Design, Implementation, Monitoring, and Closure. Each phase includes clearly defined tasks, roles, deliverables, and performance metrics to ensure systematic deployment.

6.1.2 Key Findings

- **Effective Role Definition and Assignment**:

  Interview Insights: The implementation demonstrated that clearly defining roles and responsibilities for each stakeholder—Top Management, Steering Committee, Project Manager, Technical Team, and Project Owner—was critical for effective project governance. The structured allocation of roles reduced ambiguity and improved coordination among teams.

  Literature Finding: Effective communication throughout the project execution enables the participating parties to understand the role and responsibility in the project execution as a result it enhances stakeholder engagement.

- **Improved Resource Allocation and Risk Management**:

  Interview Insights: The Planning Phase's focus on detailed resource allocation and risk management led to optimized use of resources.

  Literature Findings: lack of phased approach implementation of PKI enables the proper allocation of resources. Since PKI requires some amount of initial cost**.** The predefined risk management strategies ensured that potential issues were identified early, and mitigation strategies were in place, thereby minimizing disruptions.

- **Seamless Integration of PKI Components**

  Interview Insights: In order to design the architecture, we reviewed various technical documents developed for PKI implementation. We are also try to review legal structure of different countries who has implemented PKI at national level. Around 30 countries legal structure are reviewed on the course of the review process. India, Philippines, Australia, Kenya, South-Korea are some of well-known countries that where under review. Accordingly, the reviews that are made on these countries provided as an input to design and structure both the legal framework as well as the deployment architecture of the PKI model.

  Literature Findings: The Analysis and Design phases facilitated a thorough understanding of existing systems and the development of a tailored PKI model. The integration of PKI components—such as digital certificates, Certificate Authorities (CAs), and secure communication protocols—was completed without significant technical challenges, highlighting the robustness of the design framework.

- **Successful Implementation and Deployment**:

  Interview Insights: A plenty of datacenter projects have undertaken by INSA in the previous years. PKI data center is special because it requires greater security as well as it requires to follow a set of standards and a defined criterion.For the purpose of implementing a datacenter, the first task was reviewing the required PKI standards and best practices made on the PKI Datacenter. Based on the input gained from the review we are planning to select an appropriate site for the operation of the PKI service.

  Literature Findings: The Implementation Phase achieved its primary goals, including the deployment of PKI infrastructure, execution of training programs, and initial audits for accreditation. All key performance indicators (KPIs), such as stakeholder engagement, completeness, and compliance with legal frameworks, were met or exceeded.

- **Continuous Monitoring and Maintenance**:

  Interview Insights: PKI Contains a set of components that require continuous monitoring and maintenance. Accordingly, during the course of the operation a set of system

components are identified in the continuous monitoring and maintenance. Legal framework documents, systems and devices that require license are some of the components that require continuous monitoring and maintenance. For the purpose of monitoring it is planned to deploy log mechanisms and asset registry.

Literature Findings: The Monitoring and Maintenance Phase established a comprehensive process for ongoing monitoring, including automated system checks and regular audits. This continuous feedback loop ensured system reliability and compliance with evolving security standards.

6.2 Discussion

6.2.1 Effectiveness of the Framework

The results indicate that the PKI project implementation framework is effective in providing a structured and phased approach to deploying secure PKI-enabled infrastructures. The clear outlining of stages—from initiation to closure—ensured that each phase was executed with a focus on quality, security, and compliance. By dividing the project into manageable phases, the framework minimized risks and enabled better control over the implementation process.

6.2.2 Key Challenges and Mitigations

While the framework proved effective, several challenges were encountered:

- **Coordination Among Stakeholders**: Ensuring seamless coordination between diverse stakeholders (e.g., technical teams, legal advisors, and top management) was challenging. This was mitigated through regular communication and status update meetings, which facilitated real-time issue resolution and enhanced stakeholder engagement.
- **Adaptation to Evolving Security Standards**: PKI implementation must align with constantly evolving security standards and regulations. This required adaptive planning and frequent updates to the project plan, ensuring that the system remained compliant with new laws and security protocols.
- **Resource Constraints**: Limited technical expertise and financial resources posed constraints during the implementation phase. To mitigate these, the project adopted a phased resource allocation strategy, prioritizing critical tasks and optimizing the use of available resources.

6.2.3 Comparison with Existing Frameworks

When compared to existing PKI implementation methodologies, such as e.g., SYZEFXIS-PKI, the proposed framework offers a more comprehensive approach by integrating legal compliance, continuous training, and audit processes into the project lifecycle. The inclusion of training and audit components ensures long-term sustainability and compliance, which is often overlooked in other models.

6.2.4 Impact on Organizational Security Posture

The implementation of the PKI framework significantly enhanced the organization's security posture by enabling secure communications, digital signatures, and data integrity checks. The adoption of a PKI-based system reduced the likelihood of data breaches, improved trust in electronic transactions, and facilitated compliance with industry regulations.

6.2.5 Lessons Learned and Future Improvements

Key lessons learned during the implementation include the importance of stakeholder engagement, the need for continuous training and updates, and the value of a flexible project plan that can adapt to new security challenges. Future improvements may involve enhancing automation in monitoring processes, integrating more sophisticated analytics for threat detection, and expanding the framework to support emerging technologies such as IoT and blockchain.

CHAPTER SEVEN

7 Summary, future work

7.1 Summary

This research developed a comprehensive PKI Project Implementation Framework by conducting a systematic literature review (SLR) of existing studies and frameworks in public key infrastructure (PKI). The framework was designed to address the common challenges associated with implementing PKI projects, such as interoperability, scalability, security, and cost-effectiveness. It provides a structured approach for organizations to follow, covering key components including policy formulation, stakeholder engagement, technology selection, risk management, and governance. The proposed framework aims to guide practitioners in successfully implementing PKI projects while ensuring compliance with international standards and best practices.

By synthesizing the insights from various case studies and research papers, the framework incorporates practical guidelines and step-by-step processes to mitigate potential risks and enhance the overall effectiveness of PKI deployment. The findings highlight the importance of a holistic approach that includes both technical and organizational perspectives. Furthermore, the framework serves as a valuable resource for decision-makers, security architects, and IT professionals involved in PKI implementation across various sectors, including government, finance, healthcare, and education.

7.2 Future Work

While the proposed PKI Project Implementation Framework provides a robust foundation for guiding PKI deployments, there are several areas for future research and development. First, empirical validation of the framework through case studies and real-world implementations in different organizational settings would help refine and enhance its applicability. Future studies could explore the framework's effectiveness in various domains, such as smart cities, IoT ecosystems, and 5G networks, where PKI is expected to play a critical role in securing communications.

Additionally, research could focus on integrating emerging technologies, such as blockchain and quantum-resistant cryptography, within the PKI framework to address evolving security challenges. As PKI adoption continues to grow globally, there is also a need to explore the socio-economic impacts of PKI deployment, including cost-benefit analysis and policy implications. Further work could investigate automated tools and methodologies for monitoring and managing PKI systems to ensure continuous compliance and operational efficiency.

Finally, the framework could benefit from a more detailed exploration of user-centric approaches, such as enhancing user experience and addressing privacy concerns, to increase adoption rates and trust in PKI solutions. By addressing these areas, future research can contribute to the continuous evolution of the PKI Project Implementation Framework, ensuring it remains relevant and effective in a rapidly changing technological landscape.

CHAPTER EIGHT

8 References

[1] JoelWeise, "Public Key Infrastructure Overview," *Sun Microsystems, Inc,* p. 29, August 2001.

[2] R. Hunt, "Technology infrastracture for PKI and Digital certificate," *Elsevier,* p. 12, 2000.

[3] E. h. o. p. representatives(HPR), Information Network Security Agency Re-establishment Proclamation, Addis Ababa: Federal Negarit Gazette, 2013.

[4] E. H. o. p. representatives(HPR), Electronic Signature Proclamation, Addis Ababa: Federal Negarit Gazette, 2018.

[5] W. Yanwen, "The Study on Complex Project Management in Developing country," *Elsevier,* p. 6, 2012.

[6] A. W. a. K. M. S. a. A. A. K. Akotam, "E--governance public key infrastructure (PKI) model," *International Journal of Electronic Governance,* vol. 6, pp. 133--142, 2013.

[7] S. T. a. C. T.-W. Chanson, "Design and implementation of a PKI-based end-to-end secure infrastructure for mobile e-commerce," *World Wide Web,* vol. 4, pp. 235--253, 2001.

[8] A. a. B. C. a. F. I. a. T. M. Floarea, "PKI Implementation for Romanian Schengen Information System," in *ISSE 2011 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2011 Conference*, 2011.

[9] M. a. K. J. a. K. M. Linden, "FEIDHE-integrating PKI in Finnish higher education," *Inform atic,* p. 211, 2001.

[10] S. a. B. P. a. K. M. a. C. M. a. S. C. a. C. I. Gritzalis, "Designing the Provision of Public Key Infrastructure Services for eGovernment," Citeseer.

[11] D. a. L. M. A. a. S. E. D. Kefallinos, "Secure PKI-enabled e-government infrastructures implementation: the SYZEFXIS-PKI case," *Electronic Government, an International Journal,* vol. 3, pp. 20--438, 2006.

[12] R. L. B. B. W. C. Ahmad Samer Wazan, "PKI interoperability: Still an issue? A solution in the X.509 realm," p. 15.

[13] M. Brown, "PKI and Quantum: How to Prepare Your Public Key Infrastructure for Quantum Computing," Venafi, August 9, 2022.

[14] C. Canada, "WEBTRUST® FOR CERTIFICATION AUTHORITIES," in *WEBTRUST PRINCIPLES AND CRITERIA FOR CERTIFICATION* , CPA Canada, 2020, p. 87.

[15] C. Mitchell, "PKI standards," *University of London,,* p. 17, 2000.

[16] D. a. L. M. A. a. S. E. D. Kefallinos, "Secure PKI-enabled e-government infrastructures implementation: the SYZEFXIS-PKI case," *Electronic Government, an International Journal,* vol. 4, no. 3, pp. 420--438, 2006.

[17] E. E. a. C. N. Enaw, "Public Key Infrastructure Deployment in Cameroon's Public Administration," in *Proceedings of the 2014 Conference on Electronic Governance and Open Society: Challenges in Eurasia*, 2014.

[18] T. Twibell, "Ethiopian Constitutional Law: The Structure of the Ethiopian and Comparative Law Review," *Loyola of Los Angeles International ,* vol. 21, Ethiopian Constitutional Law: The Structure of the Ethiopian .

[19] N. Davies, "Recent SSL/TLS Certificate Attacks Show the Importance of Updating Your Encryption Protocols," GlobalSign, February 22, 2021.

[20] R. Al-Maghraby, "Project Management Frameworks: Comparative Analysis," *IPMA 2010 World Congress,* p. 4, 2010.

[21] E. a. B. Y.-J. a. B. J. Hableel, "Public key infrastructure for UAE: A case study," in *Proceedings of the 6th international conference on security of information and networks*, 2013.

[22] S. a. K. H. C. a. S. D.-i. Lee, "Privacy-preserving PKI design based on group signature," in *secau Security Research Centre*, Edith Cowan University, Perth, Western Australia, 2011.

[23] Z. e. al, "A Framework for Evaluating the Security and Scalability of PKI Systems," *Computer Networks,* vol. 57, pp. 2266-2279, 2013.

[24] W. O. L. L. Angela C., "How-to conduct a systematic litrature review:A quick guide for computer scince research," *MethodsX,* vol. 9, p. 101895, 2022.

[25] R. K. Yin, Case study research and applications : design and methods, vol. 1, SAGE Publications, 2018, p. 4.

[26] V. B. V. a. H. N. Clarke, hematic analysis. Qualitative psychology: A practical guide to research methods, 2015.

[27] C. a. R. S. A. a. R. N. Narendiran, "Public key infrastructure for mobile banking security,IEEE," *2009 Global Mobile Congress,* pp. 1--6, 2009.

[28] E. a. A. K. a. M. K. Sakane, "Design and Implementation of Certificate Authority for High Performance Computing Infrastructure," vol. 2013, 2013.

[29] E. a. L. F. a. U. J. Jacob, "PKIX-based certification infrastructure implementation adapted to non-personal end entities," *Future Generation Computer Systems,* vol. 19, pp. 263--275, 2003.

[30] E. G. a. T. E. Carayannis, "Innovation diffusion and technology acceptance: The case of PKI technology," *Technovation,* vol. 26, pp. 847--855, 2006.

[31] W. a. Y. M. a. Y. F. a. R. W. Tan, "A security framework for wireless network based on public key infrastructure," in *2009 ISECS International Colloquium on Computing, Communication, Control, and Management*, IEEE, 2009, pp. 567--570.

[32] B. a. M. J.-P. a. P. J. Hammi, "PKIs in C-ITS: Security functions, architectures and projects: A survey," *Vehicular Communications,* vol. 38, p. 100531, 2022.

[33] N. Hong, "A security framework for the internet of things based on public key infrastructure," *Advanced Materials Research,* vol. 671, pp. 3223--3226, 2013.

[34] D. T. a. H. L. C. Chan, "Towards a unified PKI Framework," in *2014 International Symposium on Technology Management and Emerging Technologies*, IEEE, 2014, pp. 113--118.

[35] D. R. a. H. V. C. a. P. W. T. a. C. S.-J. Kuhn, Introduction to public key technology and the federal PKI infrastructure, Citeseer, 2001.

[36] C.-M. a. S. H.-L. a. H. C.-T. OU, "Government PKI deployment and usage in Taiwan," *Information and security: an international journal,* vol. 15, pp. 39--54, 2004.

[37] N. a. H. H. a. C. L. J. Serrano, "Incidents), A complete study of PKI (PKI's Known," in *PRC47: The 47th Research Conference on Communication, Information and Internet Policy*, 2019.

[38] P. Gutmann, "PKI design for the real world," in *Proceedings of the 2006 workshop on New security paradigms*, 2006.

[39] R. a. M. A. a. T. H. a. J. P. Kebede, "Circular economy in the built environment: a framework for implementing digital product passports with knowledge graphs," in *EC3 Conference 2023*, European Council on Computing in Construction, 2023, pp. 0--0.

[40] F. K. A. U. a. D. E. Clemens Brunner, "A Comparison of Blockchain-based PKI Implementations," *Scitepress,* p. 8, 2022.

[41] R. Perlman, "An overview of PKI trust model," *IEEE Network,* p. 6, 1999.

[42] R. E.-H. a. N. H. Mohamad Osmani, "Blockchain for next generation services in banking and finance:cost, benefit, risk and opportunity analysis," *Journal of Enterprise Information,* p. 16, 2020.

[43] Y. K. ,. S. T. a. P. K. Lukas König, "Comparing Blockchain Standards and Recommendations," *Future Internet,* p. 17, 2020.

[44] M. S. S. Ashiq Anjum, "Blockchain Standards for Compliance and Trust," *IEEE COMPUTER SOCIET Y,* p. 7, 2017.

[45] P. &. M. C. Jarupunphol, "PKI implementation issues in B2B e-commerce," *EICAR Conference,* p. 14, 2003.

[46] M. o. I. a. Technology(MinT), Digital Ethiopia 2025 – Summary, Addis Ababa: Ministry of Innovation and Technology(MinT), 2022.

[47] N. N. a. M. v. Oosten, "Real-world Application of Public Key Infrastructures Deployment Methodology," *Compact,* p. 9, 2001.

[48] P. H Klopper and iVIBA, "The qualitative research proposal," *Curationis,School of Nursing Science, North-West University (Potchefstroom Campus), South Afnca,* p. 12, December,2008.

[49] O. y. &. L. Stewin, "Reliability and validity misnorms for qualitative research," *The canadian Journal of nursing research,* p. 7, 1988.

[50] H. Snyder, "Literature review as a research methodology: An overview and guidelines," *Elsevier,* p. 7, 2019.

[51] O. a. T. Gough, "Systematic Literature Review: An Introduction," *Sage Publications Ltd,* 2017.

[52] L. N. L. Debajyoti Pati, "How to Write a Systematic Review of the Literature," *journals.sagepub.com,* p. 16, 2017.

[53] Swift, "How much do you pay for your PKI solution?," SWIFT.

[54] S. Mazaher, "A Survey of State of the Art in Public Key Infrastructure," *Norsk Regnesentral,* p. 35, 2003.

[55] R. Al-Maghraby, "Project Management Frameworks: Comparative Analysis," *IPMA 2010 World Congress,* p. 4, Nov ,2010.

CHAPTER NINE

9 Appendix

9.1 Appendix A. Description of persons selected for the interview

No.	Organization	Position of the participant	Mode of participation	Reason for selection
			Interview	
1	INSA	Information security Consultant	✓	Expected to have full view of PKI technology Implementation.
2	INSA	PKI Experts	✓	Expected to have full view of PKI technology Implementation.
3	INSA	PKI Project manager	✓	Expected to have overall view of PKI project Implementation

Table 26: Description of persons selected for the interview

9.2 Appendix C. Assurance

No.	Epistemological standards	Strategies	Criteria
1.	Truth value	Credibility	Member checking Triangulation(Methods, Participants)
2.	Applicability	Transferability	Selection of sources
3.	Consistency	Dependability	Triangulation(Methods, Participants)
4.	Confirmability	Confirmability	Triangulation(Methods, Participants)

Table 27: Assurance methodology used

9.3 Appendix D. Interview Questions and transcribed Responses

No.	Interview Question
1.	What project management framework utilized for National PKI project & What process where undertaken?
	Responses from project Manager
	• Our organization utilizes PRINCE2 project management framework and methodology for most of the projects that are undertaken by INSA. Since our organization mainly work on technology sector and most works are performed by groups of technical teams and the main task of project manager is managing the overall deliverables based on the defined project plan and milestone, utilizing PRINCE2 project management framework is the first option to use on most projects.

	• Using a PRINCE2 project management framework requires commitment of every stakeholder, most of the time the major challenge in implementing such framework. Such challenges are also realized in National PKI Project implementation. • PRINCE2 project management framework by itself helps in decreasing the burden of Project manager because it helps the project manager to focuses on managing the overall project plan and subsequent deliverable. • To give an insight on the process that we go through, During the course of PKI Implementation Project, a visibility analysis was first made and findings from the analysis where communicated and presented for the top management. Based on the direction given by the top management of INSA, a steering committee from various departments were chosen most of the members of the steering committee where Department Heads. Engineering Department Head, PKI Department Heads, Development Department Heads, Project management Department Heads, R&D Department Heads, Governance Department Heads and Audit Department Heads where the members of the steering committee that are appointed by the Director General.to lead the steering committee a Deputy Director General was appointed. Accordingly, Deputy Director General has directed the members of the steering committee to appoint technical manager from each department. The project management head then appointed and direct a project manager to develop a project charter and lead the project and manage the expected deliverable. The project charter was basically containing the objectives of the project and key responsibilities of each technical manager appointed by each members of the steering committee. The project Charter were communicated with the top management as well as the steering committee to provide an input. The Project charter also contain a communication plan that recommends a meeting once in 15 days and in each meeting to have a report on the progress of the project. Based on PRINCE2 project management framework and the direction given by the Deputy Director General The main responsibility of members of the steering committee were, to appoint a technical manager and mobilize resources for the project. The technical managers appointed by each member of the steering committee where expected to deliver a Roadmap to the project manager. Accordingly, the project manager required to present the provided Roadmap to the top management. After the Roadmap provided by the technical manager, the project manager task was to compile each deliverable from each technical manager and present the project status to the top management in a 15 days' basis.
2.	Does the National PKI project consider audit and certification?
	Responses from project Manager and Security Consultant
	Project manager: The main objective of National PKI project as it is defined in the project management roadmap, establishing a National PKI that is trusted on various internet based platforms. *Security Consultant:* Such infrastructure and services require truest for this reason considering service certification is mandatory. For the purpose of establishing National PKI we are considering Webtrust Certification for the overall service

	provided by the infrastructure and common criteria(CC) certification for the Root CA software that is used to generate a digital certificate for Certificate providers (Issuing CAs).While choosing these certifications we have done a lots of reviews to understand the relevance of such certifications.Webtrust,ISO,ETSI where the some of the standards that are reviewed in detail for the purpose of PKI certification.
3.	What deployment architecture does National PKI project plan to utilize?
	Responses from Security Consultant and PKI operation Head
	Security Consultant: In order to design the architecture, we reviewed various technical documents developed for PKI implementation. We are also try to review legal structure of different countries who has implemented PKI at national level. Around 30 countries legal structure are reviewed on the course of the review process. India, Philippines, Australia, Kenya, South-Korea are some of well-known countries that where under review. Accordingly, the reviews that are made on these countries provided as an input to design and structure both the legal framework as well as the deployment architecture of the PKI model.
4.	Does the National PKI project consider Training?
	Responses from Security consultant
	Security Consultant: PKI requires proper service provision and administration to comply with international standards as well as to provide secure service. For these reason reviewing and analyzing the required training for service provision becomes mandatory. During the course of review various certifications that provide general understanding of the PKI domain are considered as part of the training. COMPTIA Security +, COMPTIA Linux +, CISSP, CISM, Firewall certifications, Network Certifications, Server administration certifications and HSM related certifications where some of the certifications considered to be taken as part of the training plan. We considered such certifications because we believe such certifications provide the required basic skill as well as knowledge to operate and administrate the service.
5.	What is a PKI Datacenter infrastructure and what makes it different from other similar Datacenter infrastructures?
	Responses from Data center engineer, Security consultant
	Data center engineer: A plenty of datacenter projects have undertaken by INSA in the previous years.PKI data center is special because it requires greater security as well as it requires to follow a set of standards and a defined criterion. For the purpose of implementing a datacenter, the first task was reviewing the required PKI standards and best practices made on the PKI Datacenter. Based on the input gained from the review we are planning to select an appropriate site for the operation of the PKI service. Accordingly, the engineering team has designed a datacenter including high-level and low-level design in compliance with the standard as well as the chosen site for the operation of PKI service. During the design a number of functional rooms required for the service and the set of equipment's needed for the datacenter facility are discussed in depth with various stakeholders based on defined PKI standards. Additionally, based on the defined standard deferent set of materials are

	selected for the civil work. shield metal and faraday cage are some of the materials that needs to be installed within the facility. *Security consultant:* PKI requires secure facility in order to provide the service, in order to design the datacenter facility in collaboration with datacenter team we have reviewed various standards and best practices to comply.
6.	What challenges are faced in implementing National PKI project?
	Responses from Security consultant, Project manager, Data center engineer
	Security consultant： Understanding the PKI domain by the project stakeholder was by itself was a challenge. It requires a greater effort to create a full insight on the project implementation. Since PKI requires some amount of budget and resource, acquiring these resource was the other major challenge. Subject matter experts on the PKI Domain was also challenging, since the awareness and importance of PKI is not communicated well this created a challenge in the process of implementing PKI at national level. *Project manager:* PKI project requires the engagement of different stakeholders and commitment. during the course of the implementation of the project commitment was one of the major challenge. Late delivery of project deliverables was one of the challenge in the project execution. In the late 2012 Ethiopian calendar the project was initiated and failed one of the major reason for the unsuccessfulness was understanding of the interdependencies that exist between tasks identified by the technical team.as a result without selecting and preparing an appropriate site and legal framework a procurement has executed. Even if the devices required for the PKI facility are procured because of the interdependences exist we can deploy those devices. Due to a lack of initial budget and together with the aforementioned issues the project forced to be terminated at that time. But currently these issues were resolved and we are on the verge of finalizing the project. *Data center engineer:* PKI Datacenter is different from other related datacenter projects.it requires basic understanding of the PKI domain, understanding of the required standard and the required access controls utilized for the facility was also a challenge during the implementation of the project. Understanding of each functional room of the facility and the required access control needed to secure each functional room was new in the domain of datacenter implementation. The other major challenge that was realized during the course of project implementation was choosing an appropriate site for the datacenter civil work based on the standard defined.
7.	What is considered in National PKI continuous monitoring and operation?
	Responses from Security consultant, PKI facility Administration Head
	PKI facility Administration Head: The department was established to monitor day to day activity with regard to PKI operation. Monitoring how the network operate, monitoring the data flow through those networks and the security of those data flows through the network, Monitoring the health of the hardware servers, monitor how the CCTV cameras are working, monitor how AC systems and power systems are operating, are some of the activities that require

	continuous monitoring and maintenance. Since such services require a 24/7 service provision this equipment's and Devices require continuous monitoring for smooth operation of the service. *Security consultant：* PKI Contains a set of components that require continuous monitoring and maintenance. Accordingly, during the course of the operation a set of system components are identified in the continuous monitoring and maintenance. Legal framework documents, systems and devices that require license are some of the components that require continuous monitoring and maintenance. For the purpose of monitoring it is planned to deploy log mechanisms and asset registry.

Table 28.Interview Questions and transcribed Responses