Government of Malawi

MALAWI PUBLIC KEY INFRASTRUCTURE FRAMEWORK

December 2020

Government of Malawi

MALAWI PUBLIC KEY INFRASTRUCTURE FRAMEWORK

CONTACT INFORMATION

For more information, please contact:

Secretary for Information, Civic Education and Communications Technology
Central Office of Information
Private Bag 310,
Lilongwe 3.
Tel: 01 772 702
Fax: 01 770 650
Email: principal.secretary@information.gov.mw

Acronyms

The following acronyms have been used in this document.

Table 1 - Table of Acronyms

CA	Certification Authority
CCA	Controller of Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DB	Database
DS	Directory Service
DMZ	Demilitarized Zone
DN	Distinguished Name
DNS	Domain Name Service
DR	Disaster Recovery
FIPS	Federal Information Processing Standards
G2G	Government to Government
G2B	Government to Business
B2G	Business to Government
HA	High Availability
HSM	Hardware Security Module
ITU	International Telecommunication Union
ICT	Information Communication and Technology
LDAP	Lightweight Directory Access Protocol
LRA	Local Registration Authority
MIS	Management Information System
NMS	Network Management System
PIN	Personnel Identification Number
OCSP	Online Certificate Status Protocol
OU	Organizational Unit
PA	Policy Authority
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
RA	Registration Authority
RPS	Registration Practice Statement
RFC	Request for Comment
SSL	Secure Socket Layer
SMS	Server Management System (SMS)
SIEM	Security Information and Event Management
TDB	To Be Determined
TLS	Transport Layer Security
TSA	Time Stamping Authority
VPN	Virtual Private Network
WAF	Web Application Firewall

List of Contents

FORWORD

The Malawi Government through the Malawi Digital Strategy in collaboration with other economic strategies such as MGDS, Vision 2020, and SDGs aims to efficiency and accountability in governance. In pursuit of this agenda Government embarked on a digital transformation agenda that has led to the implementation of several digital solutions in key sectors of development such as the AIP, IFMIS, National Registration System, MALTIS, and Msonkho Online for enhanced delivery of service to the public.

The realization of digital transformation, however, requires a digital ecosystem in which digital solutions implemented across different sectors of the economy interoperate. The digital ecosystem requires that digital platforms should be implemented on ICT infrastructure which is not only secure but also digitally trustworthy. The Government, cognizant of the security requirement in digital platforms, enacted the Electronic Transaction and cyber security Act 2016 which provides the legal framework governing the secure implementation and consumption of digital services.

The Government in collaboration with the International Telecommunication Union (ITU), has developed the Malawi Public Key Infrastructure (PKI) Framework. The PKI is a precursor to digital transformation as it provides mechanisms for creation of digital trust and confidence the digital ecosystem at national level.

Preface

The Government of Malawi through the International Telecommunication Union has developed the Malawi Public Key Infrastructure (PKI) Framework line with the Malawi National ICT Master Plan. The PKI Framework provides guidelines for implementation of a successful national PKI system. The PKI system defines roles, policies, and procedures required for creation and management of “Digital Certificates” which are required for implementation of secure electronic transactions and communication systems.

For a long time digital certificates have been outsourced from service providers based outside the country. However the approach does not only drain our limited foreign exchange reserves but it also prolongs the chain of authentication especially when the peers requiring authentication services are locally based. The development of a national PKI framework will therefore foster establishment of an authority responsible for controlling the creation and authentication of digital certificates at domestic level. It is the Government’s expectation that the development of this frameworks should result in effective and affordable digital certificate services available to most consumers at national level

1. Introduction

1.1 General Context

Since 2018, the Government of Malawi has established the "Malawi Digital Government Strategy." The strategy aligns with National priorities such as MGDS, Vision 2020, and SDGs. It will contribute to Malawi's socio-economic development and transform Malawi into a competitive, innovative knowledge society.

The Vision of Malawi Digital Government strategy is: "**A Transformed Government with efficient and accountable administration, which provides seamless Governance by making Public Services convenient and accessible, resulting in social-economic growth of Malawi**." The main objective of this strategy is to promote the digital transformation of Malawi's economy, society, and Government.

The strategy identified three core enablers of digital transformation. Those are the "Digital Ecosystem "that focuses on strengthening the legal, regulatory, and institutional framework; the "Connectivity" that focuses on the development of internet infrastructure intending to provide affordable and high-quality internet access to all citizen; and lastly the "Digital platforms and Services" that focuses on the development of technical capacity and IT infrastructure to deliver services to the citizen.

To implement Malawi's Digital Strategy, the Government has embarked on the development of internet connectivity infrastructure and online services. In this initiative, the Government implemented different digital services such as Ascyuda and Msonkho Online for TAX and Customs, IFMIS, Birth and Death electronic registration, Business electronic registration, eVISA, Personal Property Security Registry, HR Management System, etc.... just to name the few.

The National statistics Office (NSO 2019) report defines that 3.5% of households have a computer and internet access in their home, and 9.9% have internet access in their home, mostly using mobile connectivity.

This Technology development is transforming societies and improving service delivery (G2C, G2B, B2G, etc.…), which contributes to social and economic development. However, it has also introduced new security risks, threats, and unwanted practices such as identity theft, unauthorized access to information, unauthorized modification of electronic information at rest or in transmission, and repudiation of electronic transactions.

Aware of these security threats, The Government of Malawi has opted to protect electronic transactions, communication networks, and computer systems. It started by enacting the Electronic Transaction and cyber security Act 2016, this Act position Malawi with a legal instrument to regulate digital environment development.

To implement this Act, the Government of Malawi (GoM), in collaboration with the International Telecommunication Union (ITU), initiated the development of the Malawi Public

Key Infrastructure (PKI) Framework. The PKI framework defines all components required to implement a successful National PKI system. The setup of the PKI system is in line with the Malawi National ICT Master plan under pillar 1: “ICT Infrastructure Development”; and the Digital Government Strategy. The PKI is an enabler of digital transformation in e-Government, e-Banking and e-Commerce as it increases the TRUST and CONFIDENCE of users in the digital environment, it will allow users of online services to authenticate and sign electronic transactions.

1.2 Risks in the digital environment

On the Internet, interaction takes place through an open network where there is no physical presence. Thus, we do not know the identity of the people with whom we communicate and exchange electronic messages.

Government and Businesses are becoming more and more dependent on digital information and electronic transactions. On the other hand, cybersecurity threats and unwanted practices also increase. For example, the very recent case published on 25 November 2020 was the arrest of 3 cyber gangs in Nigeria that compromised more than 150 countries Government and Private sector companies since 2017, they had stolen identities (usernames and passwords) and infiltrated computer systems by distributing malicious links, more than 50,000 targeted victims have been affected by this attack. Other risks associated with electronic transactions and communication include but are not limited to the unauthorized change of electronic information, unauthorized access to confidential information, and denying fact information transmit.

1.3 Fundamentals of Public Key Infrastructure (PKI)

A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create and manage “Digital Certificates or Digital IDs”. PKI provides the secure electronic transactions and communication including, but not limited to, e-Government, e-Commerce, e-Banking and confidential email or electronic documents.

PKI enables Applications Services Providers (ASP) or Online Service Providers to identify and authenticate users by providing strong authentication with PKI digital certificates, and authentication data integrity and a reasonable basis for non-repudiation through the use of digital signatures, and allows reliable business communications by providing confidentiality through the use of encryption. Below is the description of the four security services and benefits for a PKI system:

- “**Authentication of users**” with a digital certificate, ensures that the recipient of a message and its sender are the ones who have access to the data and have an authenticated electronic identity;

- Authentication "**Data Integrity**" and a reasonable basis for "**Non-repudiation**", through the use of digital signatures, detect any changes that may have taken place accidentally or intentionally while data is stored or transmitted over the Internet and guarantees that the author of a message can in no way deny having originated it;
- and allows reliable business communications by providing "**Confidentiality**" through the use of encryption.

Other benefits of PKI:

- Increase **productivity** and **efficiency** business processes by reducing errors, cost, and time associated with paper-based business processes;
- Improves "**user satisfaction**" (User Experience) in digital services, enabling communications from anywhere and at any time;
- Reduce "**cost**" related to printing, scanning and transport of outgoing and incoming message;
- "**Environmental protection**" in a paperless work environment.

1.4 Objectives and Scope of the assignment

The objective of this assignment is to develop Malawi Public Key Infrastructure (PKI) Framework that defines components required to establish a successful National PKI system, this include:

- The National PKI Governance structure
- Recommendations of the legal and regulatory aspect related to digital signature;
- PKI Policies framework;
- The architecture design of the national Root CA system;
- The architecture design of the Accredited CA system;
- National PKI Data Center requirements;
- Requirements to establish a successful National PKI system;
- Implementation roadmap of the National PKI system establishment;
- Estimate the cost to implement the National PKI system.

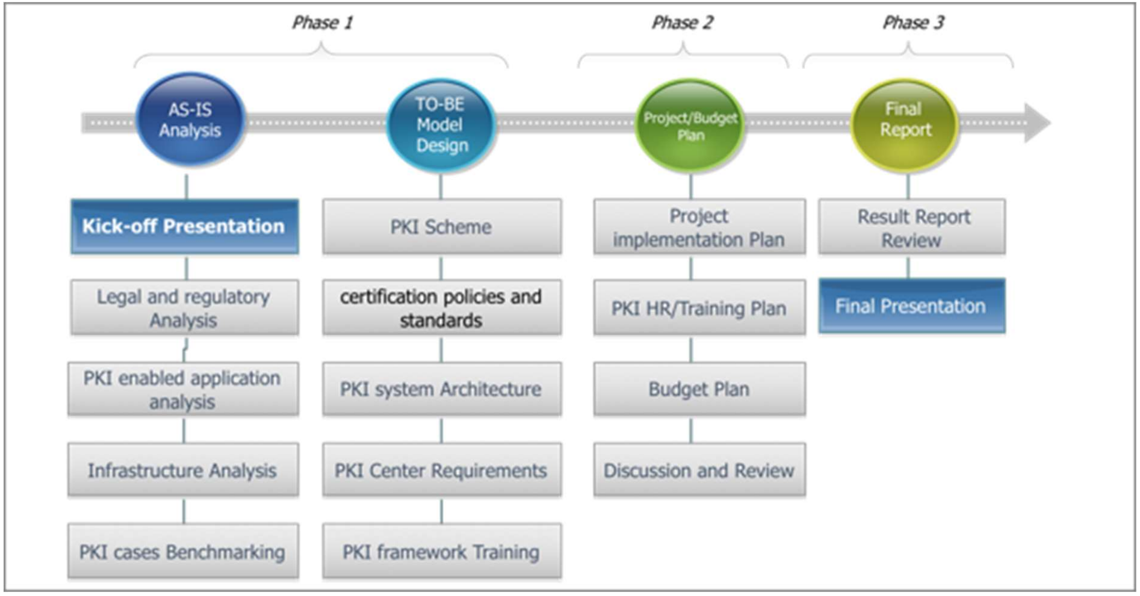
Part I: Current Status Analysis (As-Is)

3. Methodology applied

The development of the PKI framework was managed by MACRA with the support of the International Telecommunication Union and the PKI framework consultant. The project was scheduled into three main phases: Phases I covered the analysis of the current status of PKI in Malawi (As-Is) and the development of the To-Be Model, Phase II focused on Project and Budget Plan whereas Phase III focused on final report review and approval. The PKI framework was conducted in a consultative manner through established working groups (legal, eGovernment and Infrastructure) from key stakeholders, Government Ministries and Agencies, Telecom Operators, and Banks. Key Stakeholders consulted are; MACRA, eGovernment Department, Ministry of Justice, Accountant General, National Registration Bureau, SDNP, MTL, Airtel, and the Central Bank.

As inputs to the PKI framework, the consulting team gathered information through interview questionnaires, workshops, review of relevant documentation (electronic transaction and Cyber Security Act 2016, Malawi Digital Government strategy, communication regulation, ICT policy, and the National ICT master plan), analysis of the eGovernment services, Infrastructure analysis and an in-depth discussion with working groups, comparison with best practices (benchmarking). Based on the collected information, a tailored PKI framework to establish a successful Malawi National PKI system was developed.

Figure 1: Phases of the PKI framework project.



4. Analysis of the current PKI status

4.1 Electronic Transaction and Cyber Security Act of 2016

The analysis of Malawi Electronic Transaction and Cybersecurity Act of 2016 provides information on the need to establish regulations to develop and promote the use of digital signature in electronic transactions, as well as to establish the Governance structure of certification services in Malawi.

The Malawi Electronic Transaction and Cybersecurity Act of 2016, define important aspects related to Public key infrastructure (PKI), electronic signature, digital signature certificate, and certification authority (CA). However, some important legal aspects related to electronic identification, electronic stamp or e-Seal, Electronic Time Stamp, authentication of internet sites, CA accreditation criteria, Accreditation process and auditing procedure are not clearly defined in the Electronic Transaction and Cybersecurity Act of 2016.

4.1.1 Electronic Signature

The Electronic Transaction and cyber security Act of 2016, section 8 (1 - 3), set the requirem ents for electronic signature. It shall be authentic if:

(a) the means of creating the electronic signature is- within the context in which it is used- linked to the signatory and not to any other person;

(b) the electronic signature creation means was at the time of signing under the control of the signatory and not any other person, and done without duress and undue influence; and

(c) any alteration made to the electronic signature after signing is detectable.

Recommendation 1: In addition to the above, the consulting team recommends that an electronic signature that it is based on a "Digital signature certificate" issued by an Accredited Certification Authority (CA) recognized in or outside Malawi should be accepted as a signature in the same way as a "Handwritten Signature."

Recommendation 2: In addition to electronic signature, the consulting team recommends to define the requirements for other trusted services provided by Certification Authorities (CA), and these are:

(i) Electronic identification;

(ii) Electronic stamp (e-Seal);

(iii) Electronic time stamping;

(iv) Authentication of internet site;

(v) Electronic archiving.

4.1.2 Digital certificate

The Electronic Transaction and cyber security Act of 2016, section 12 (1- 5) “Recognition of digital signature certificates and digital signatures”, states that the Authority shall ensure that digital certificates comply with international best practices and standards.

Recommendation: The requirements for a digital signature certificate should be defined in the Certification Policy and Certification Policy Statement (CPS) of the Root CA and Accredited CA. The following elements should be considered while defining the requirements for a digital certificate in the CP and CPS:

(a) The registration process and the requirements to issue a certificate to subscribers;

(b) Certification authority and subscribers’ certificates profiles;

(c) Protection of private CA and subscribers’ keys.

4.1.3 Encryption

The Electronic Transaction and Cybersecurity Act of 2016, section 52 (1- 5) “Encryption”, states that the Minister, in consultation with the Authority, shall issue regulations.

Recommendation: Encryption is one of the security services of the Accredited CA, but in case it is not used and managed properly it can deny or prevent access to information when needed. The consulting team recommends to establish a commission in charge of controlling and regulating the development and the use of encryption in Malawi. Accredited CA providing Encryption service must establish a mechanism to recover the encryption keys in case of lost or when the certificate has expired.

4.1.4 Trustworthy system

The Electronic Transaction and Cybersecurity Act of 2016, section 52 (1- 4) “Trustworthy system”, states that the Minister in consultation with the Authority shall issue regulations in respect of the use, importation, and exportation of inscription programs and products.

Recommendations: The Ministry of ICT should establish the “Standards requirements for Accredited CA’s trustworthy System and equipment” that create and manage digital certificates. Compliance with these requirements must be mandatory before the accreditation of CA in Malawi.

4.1.5 Issuance and management of digital signature certificate

The Electronic Transaction and Cybersecurity Act of 2016, section 55 – 60 define the requirements of the issuance and management of digital signature certificate. The management of digital signature certificate means the process of issuance, renewal, revocation, suspension, and notification of certificate.

The issuance and management of digital certificate are the most critical services for any CA. The issuance and management of certificate must adhere and comply to strict rules and policies. The trust of Digital certificate or Digital Identity (Digital ID) rely on the process applied to issue the certificates and how certificates are managed after they have been issued.

Recommendation: In addition to the Act, the Authority of CA in Malawi should establish strict rules and policies to issue digital and manage digital signature certificates. These policies should comply with the requirements defined in the Electronic Transaction and Cybersecurity Act 2016, and with the industry's best practices. The following elements should be considered in the development of the policies related to the issuance and management of digital certificates:

(a) Identification and Authentication of subscribers should be clearly defined in the Certification Policy and Certification Policy Statement (CPS) of the Root CA and Accredited CA;

(b) The management of lifecycle operational requirements should be clearly defined in the Certification Policy and Certification Policy Statement (CPS) of the Root CA and Accredited CA;

(c) Registration Practice Statement (RPS) defining the procedure and how the digital certificate is issued and managed should be defined by Registration Authority (RA). Also, Accredited CA should periodically audit RA to ensure compliance with CP and RPS.

4.1.6 Generating a key pair

The Electronic Transaction and Cyber Security Act of 2016, section 62 (1) state the need to generate the key pairs with trustworthy system.

Recommendation: To ensure the protection of private or signing keys, the Authority of CA should establish the "**Standards requirement for the Key pair generation system and electronic signature creation devices.**"

4.1.7 Control of a private key

The Electronic Transaction and Cybersecurity Act of 2016 in section 64 (1), states that the subscriber is responsible for protecting his private key corresponding to his public key and shall prevent its disclosure to an unauthorized person.

Recommendation: The Accredited CA should establish an agreement form to be signed by both the subscriber and the Representative of a CA, generally the Registration Authority (RA). The agreement must clearly state the responsibility of each party.

4.2 PKI Governance structure

4.2.1 Benchmark of PKI Governance in other countries

Country	National PKI Governance Framework
Rwanda	The law nº 18/2010 of 12/05/2010 relating to electronic messages, electronic signatures and electronic transactions mandate the Rwanda Utilities Regulatory Authority (RURA) the Controller of Certification Authority (CCA) in Rwanda, for this purpose the National Root CA is managed by RURA as a regulatory function. RURA operates the National Root CA system and sign public key of accredited CAs in Rwanda. Rwandan Information Society Authority (RISA) was Accredited by RURA as the Government Certification Authority (Gov CA), RISA Operate the Gov CA system and issue digital certificate users (i.e. citizens and organizations).
Kenya	The Kenya Information and Communications Act of 1998 mandate the Communication Authority of Kenya to license and regulate Electronic Certification Service Providers (E-CSPs) for this purpose the National Root Certification Authority (RCA) is managed by the Kenya Information and Communications as a regulatory function. And the Government Certification Authority (GCA) is managed by the ICT Authority (ICTA) issue digital certificate for authentication and digital signature to users.
Tunisia	The National PKI system (i.e. The National Root CA, Public Issuing CA and Private issuing CA) is managed by the National Electronic Certification Agency TUNTRUST, a non-administrative public company under the supervision of the Ministry of Communication Technologies and the Digital Economy. The management of the entire PKI infrastructure and facilities are managed by the same entity.
Mauritius	The Information and Communication Technologies Act 2001 mandate the ICT Authority as the Controller of Certification Authorities in Mauritius. The Controller of CA operate the National Root CA system, it certifies the technologies, infrastructure and practices of all the Certification Authorities (CA) licensed, recognized and approved to issue Digital Signature Certificates to users. It is ICT Authority’s responsibility to monitor that certification-service-providers comply with the obligations imposed on them by law. In this respect, the Controller of CAs will maintain a publicly accessible database containing a CA disclosure record for each licensed, recognized and approved CA.
Benin	The digital code Law 2018, of the Republic of Benin establishes the Supervisory Body for Trusted Service Providers in the Republic of Benin, the body is under the Ministry of ICT. The decree No 2018 - 530 on the institutional governance framework of the national PKI system Mandate:

	ANSSI (Agence Nationale de Sécurité du Système d'Information) operate the National Root CA. And ASSI (Agence des Services et des Systèmes d'Information) manage the Government Certification Authority (GCA)
India	The Information Technology Act, 2000 mandates the Ministry of Electronics and Information Technology as the Controller of Certifying Authorities (CCA) to license and regulate the working of CAs in India. The CCA operates, the Root Certifying Authority of India (RCAI) and certifies the public keys of CAs using its own private key. The CCA also maintains the Repository of Digital Certificates, which contains all the certificates issued to CAs in the country.

4.2.2 The Malawi Electronic Transaction and Cybersecurity Act 2016

The Malawi Electronic Transaction and Cybersecurity Act 2016, Article 51 (1-3) “Authority to appoint a Certification Authority”, provides the regulation to be established by the Minister in consultation with the Authority. MACRA is the Authority in charge of the Accreditation of CA in Malawi, maintains a register for the Certification Authorities, and do such other things as necessary for the implementation of the Act.

Based on the understanding of the Act, MACRA is the accreditation body of Certification Authorities in Malawi, and the Ministry is the Policy Authority (PA).

There are other participants or stakeholders in the establishment of a National PKI system, but the Electronic Transaction and Cyber security Act 2016 does not define the roles and responsibilities of each stakeholder. The consulting team recommends to identify the entities responsible of the following functions; entity responsible of the Root Certification Authority (Root CA), entity responsible to issue certificates to subscribers (i.e. issuing Certification Authorities) and Registration Authority (RA) (i.e. entities that will be responsible of verifying and authenticating the identity of subscribers).

Recommendation 1: To successfully establish a National PKI system, the consulting team recommend to define and establish a comprehensive Governance structure for the National PKI system. The following functions should be considered:

(i) The Policy Authority (PA): responsible for PKI policies, regulations, and standards;

(ii) CA Accreditation Body: responsible for accreditation and auditing the Certification Authorities in Malawi;

(iii) Root Certification Authority (Root CA): responsible for certifying the Accredited Certification Authorities in Malawi;

(iv) Issuing Certification Authority (e.g. Government CA or a Private CA): responsible for issuing digital certificates to subscribers (i.e. natural person, legal person, or computers)

(v) Registration Authority (RA): responsible for identification and registration of certificates of subscribers (i.e. Digital certificates applicants).

Recommendation 2: Based on the Electronic Transaction and Cyber Security Act 2016, Article 51 (2), the Minister in collaboration with the Authority should establish the following regulations and guidelines:

(i) CA accreditation criteria and auditing procedures;

(ii) Regulation for Accredited CA's System and equipment

(iii) Regulation for Accredited CA's protective measures

(iv) Policy and procedures governing the operation and subscription to certification services

4.3 e-Government

4.3.1 Existing e-Government applications

The analysis of e-Government provided information on the existing and future applications in the public sector. The Government already implemented different digital services such as Ascyuda and Msonkho Online for TAX and Customs, IFMIS, Birth and Death electronic registration, Business electronic registration, e-VISA, Personal Property Security Registry, the current HR Management System, etc.… Besides, many more digital services and platforms in eGovernment such as eGovernment Procurement platform and e-Banking are under development.

Based on the information collected through questionnaires and workshops, these applications now apply basic security functions to authenticate users (i.e. Username and Password) and basic electronic signature (i.e. scanned handwriting signature) to sign electronic transactions. To secure these applications, there is a strong need to develop a National PKI system to ensure the integrity, authentication, non-repudiation, and confidentiality in e-Government, eCommerce, and e-Banking services. The table below provides a summary of key developed applications and proposed security services to protect them.

Table 1: e-Government applications

No	Name of the Application	Department	Users	Priority	Proposed Security services
1	Automated System for Customs Data (Ascyuda)	Malawi Revenue Authority	400	High	Authentication and Digital signature
2	Msonkho Online	Malawi Revenue Authority	Unlimited	High	Authentication and Digital signature
3	IFMIS	Department of Account General	1000	High	Authentication and Digital signature
4	Human Resource MIS	Department of Human Resource	400	High	Authentication and Digital signature
5	National Identification Information System	National Registration Bureau	120	High	Authentication

6	Electronic Birth Registration System		80	High	Authentication and Digital signature
7	Electronic Death Registration System		80	High	Authentication and Digital signature
8	Malawi Business Registration System	Department of Registrar General	Open	High	Authentication and Digital signature
9	Personal Property Security Registry		All Banks	High	Authentication and Digital signature
10	eVisa issuance System	Department of Immigration and Citizen Services	unlimited	High	Authentication and Digital signature
11	Passport Issuance System		120	High	Authentication
12	TEVET MIS		unlimited	High	Authentication
13	Malawi Traffic Information system	Directorate of Road Traffic	150	Medium	Authentication and Digital signature
14	Intellectual Property Administration Systems		60	Medium	
15	Forestry Cadaster MIS	Department of Forestry	Unlimited	Medium	Authentication and Digital signature
16	IFMIS	Local Councils in districts	28 districts	Medium	Authentication and Digital signature
17	GeoData MIS	Department of Geological Survey	unlimited	Low	
18	Labor Market Information Systems	Ministry of Labor	unlimited	Low	
19	Hotspot Indicator Information System	Ministry of Local Government	110	Low	
20	Local Authorities MIS		110	Low	
21	Local Authority Performance Information Systems		110	Low	
22	Village Action Plan System		400	Low	
23	Mining Rights Administration System	Department of Mining	100	Low	

4.3.2 Priority PKI applications

Through the discussion with the eGovernment working group and eGovernment Procurement (eGP) project team, the eProcurement services will be available by the end of Q1 2021, this puts a high pressure to fast track the implementation of the National PKI system in order to provide authentication and digital signature services to eGP users. The PKI consulting team recommends to adopt an agile approach to implement the National PKI system and start with a small size PKI system to quickly address the needs of eGP security services.

The table below provides a summary of priority applications that require PKI security services. These applications should be considered to promote the use of a digital signature at a large scale in the Government and private sector and at the individual level.

Table 2: PKI priority applications

No	Applications	Description of security services required
1	e-Taxation / e-Custom	Strong user authentication and digital signature integrity
2	e-Budget / e-Account	Strong user authentication and digital signature integrity
3	e-Procurement	Strong user authentication, digital signature integrity, and encryption
4	e-Payment / Internet Banking	Strong user authentication and digital signature integrity (Bank account, Credit Card No.), integrity and non-repudiation of the transactions
5	e-Administration	Strong user authentication and digital signature integrity
6	Citizen Portal	Strong user authentication and digital signature integrity

4.3.3 Electronic Passport (e-Passport) and National ID Card

Since 15th January 2020 the Government of Malawi started issuing electronic Passport (e-Passport), in the electronic passport project a Country Signing Certification Authority (CSCA) and a Document Signer was implemented as part of the electronic Passport project. These systems allow the department of Immigration and Citizenship services to digitally sign electronic Passport in order to maintain the authenticity and integrity of personal data in the chip of electronic passport.

The Government of Malawi also issues citizens a Biometric Card with an imbedded chip in the NID project. A Country Signing Certification Authority (CSCA) and a Document Signer (DS) was implemented as part of the project. These systems allow the National Registration Bureau (NRB) to digitally sign electronic Passport in order to maintain and check authenticity and integrity of personal data in the chip of the NID Card.

Recommendation: Currently the Government of Malawi operates two Country Signing Certification Authority (CSCA) one for e-Passport and another one for National ID. Based on requirements a Country should have only one Country Signing Certification Authority (CSCA) and multiple Document Signers (DS). The consulting team recommend to consolidate the PKI for e-Passport and NID to one CSCA and two DS (i.e. one for NRB and the department of Immigration).

4.4 National Data Center

The Government of Malawi have initiated the implementation of the National Data Center (NDC), this data center will provide hosting services for most of Government computer systems. However, it was not confirmed if the hosting of the National PKI system was considered in the planning to implement the National Data Center project. The consulting team together the Infrastructure working group recommend to establish a PKI Data center that comply with the "Regulation of Accredited CA's Protective Measures" to be established by the Ministry of ICT in collaboration with MACRA. The Accredited CA's Protective Measures should take into consideration the following security requirements:

- Accredited PKI machines Room; PKI systems should run in PKI Data center physically protected (Root CA and Accredited CA systems facilities)
- Multiple Access Control; Physical access control to prevent unauthorized persons from access the PKI system room;
- Security system; Physical Lock (i.e. fire proof safe box), Intrusion detection system and Monitoring and controlling the Accredited CA system room;
- Disaster Prevention System; Early detection and extinction of a fire, power supply and flood disaster prevention;
- Network security; Redundant network, firewall, IPS and SMS/NMS.

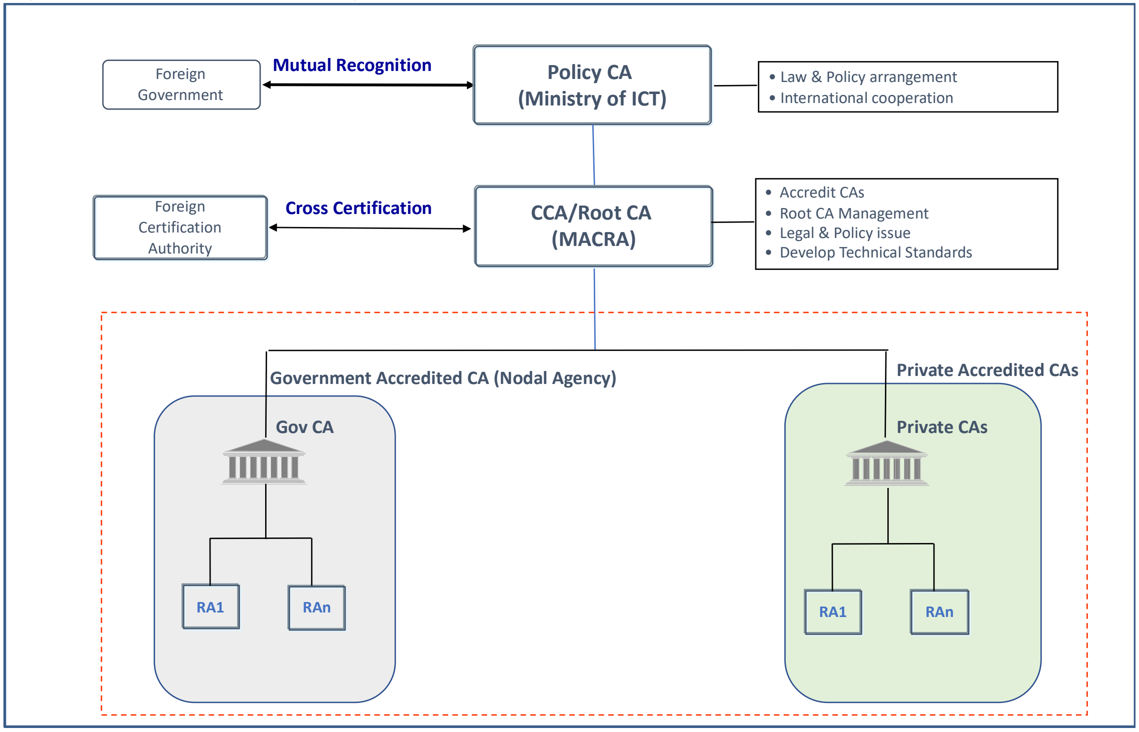
Part II: National PKI Framework

5. National PKI Governance

To ensure the proper functioning of the NPKI system, the consulting team recommends to establish a National PKI Governance structure to develop and manage the National PKI system in order to issue reliable “Digital Certificate or Digital ID” in Malawi.

The Governance of the National PKI system has four major components; the Policy Authority (PA), the Controller of CAs (CCA), the Root CA and the issuing CAs. Based on the benchmark results of the PKI Governance in other countries such as Rwanda, Kenya, Mauritius and India, the regulator or CCA operate the National Root CA system and sign the issuing CAs using its own private key.

Figure 2: PKI Governance organization structure



5.2 The National PKI Policy Authority (PA)

The “Electronic Transaction and Cyber Security Act of 2016” empowers the Ministry of ICT to establish regulations in collaboration with the Authority. Considering the critical role of the Ministry of ICT in establishing ICT strategy, laws, and policies related to digital identities, the consulting team recommends the ministry of ICT to set up a National PKI Steering committee with a member from key stakeholder institutions in Government and private sector (e.g. Office of the President, Ministry of ICT, Ministry of Justice, Ministry of Defense, MACRA, NRB, ICT Authority, Central Bank, Telecom Operator, etc.).

The Roles and responsibilities of the PKI Policy Authority:

- Set the vision and strategy of “Digital ID” in Malawi;
- Make a final decision of CA accreditation based on the report from the CA Accreditation Body;
- Steer the national PKI in the right direction with proper policies, rules and regulations;
- Promote the use of PKI technology to secure e-Government, e-Commerce and e-Banking services.

5.3 Regulator or Controller of Certification Authorities (CAs)

The “Electronic Transaction and Cyber Security Act, 2016” empower MACRA with the role to accredit, manage and maintain a register for the Certification Authorities (CA) and do such other things as necessary in Malawi. The consulting team recommend to establish the procedure for CA Accreditation criteria and auditing. To perform the accreditation and auditing procedure more efficiently the following elements should be considered:

1. CA applicant should apply their accreditation to MACRA;
2. The CA applicant should submit the CA accreditation application to MACRA along with other required documents. The required documents are listed below;
    - CA accreditation application
    - Identification certificate of business representative (National ID, birth, change name etc.)
    - The articles of association
    - Documentary evidence for Technical ability, Financial ability and possession of facilities and equipment required to be CA in accordance with “Electronic Transaction and Cyber Security Act, 2016” and regulations
    - Business plan
    - CP & CPS (Certificate Policy & Certificate Practice Statement)
    - (if any) Other documents requested by MACRA

3. MACRA should review and evaluate the documents based on the evaluation criteria;
4. MACRA should conduct actual auditing and verification of the CA applicant;
5. MACRA should check the policies and systems of the CA applicant based on the evaluation criteria;
6. Based on the results of audit, in consultation with the National PKI Policy Authority in this case the Ministry of ICT, MACRA should take the final decision to grant or reject the accreditation of the CA applicant.

5.4 Root Certification Authority (Root CA)

The Root CA is the highest authority level in the PKI and represents the "trust anchor" for the chain of trust in the context of digital certification services. The Root CA is self-signed and used to certifies or sign the Accredited Certification Authorities, renewal and revocation of CA certificates and Authority revocation lists (ARL) publication. The Root CA does not issue digital certificate to subscribers, only Accredited CA or issuing CA issue digital certificates to subscribers (i.e. natural person, legal person or applications).

Based on the benchmark of PKI Governance and the “Electronic Transaction and Cyber Security Act, 2016”, Article 51 (1-3), the consulting team recommend MACRA as the Controller of CAs (CCA) in Malawi to operate the National Root CA system.

Roles and responsibilities of the National Root CA:

- Issue and sign issuing CAs certificates with Root CA private key;
- Renew or Revoke the CAs certificates in case of non-compliance with applicable Law, policies, regulations and Standards;
- Develop technical standards for digital Identities and related certification technology;
- Issue necessary criteria and guidelines for accreditation of CAs to ensure the security and interoperability of systems and certificates, as well as compliance with the prescribed standards for digital signatures;
- Periodic Audit of accredited CAs to ensure compliance of CP and CPS, Law, Regulations and PKI Standards;
- Support international cooperation on certification services including mutual recognition and cross-certification;
- Promote the use of digital signature in Malawi.

5.6 Accredited Certification Authority (CA)

The Accredited CA is any public or private entity meeting the Accreditation criteria. Currently, there is no Accredited CA in Malawi to provide digital certification services. At the initial stage, the consulting team recommends the Government to lead the establishment of an Accredited CA to start providing security services in e-Government, e-Commerce, and e-Banking in Malawi. The Accredited CA must be established by law. Depending on the Government's view on “Digital Identity”, the accredited CA can be an existing Government or a private entity.

Considering the “Electronic Transaction and Cyber Security Act, 2016” and the current setup of Government institutions, the consulting team provide two options to operate and manage the Government Accredited CA, and the most suited will be selected during the implementation of this framework:

1. Option 1: The Government Accredited CA is managed by the Agency in charge of ICT, in this case is “Nodal Agency” defined in Malawi Digital Government Strategy.
2. Options 2: The Government establish a dedicated entity “e.g. Digital Certification Agency” responsible to develop and provide digital signature and related trust services in Government and private sector.

   Note: Considering the trend and the high need of “Digital ID” due to COVID 19, the establishment of a dedicated entity is important.

The following are the basic roles and responsibilities of the Government Accredited CA:

- Provide certificate service to subscribers (i.e. Natural person, legal person and devices or servers);
- Issue and manage digital certificates (issue/renew/revoke/reissue etc.);
- Publish certificates and Certificate Revocation List (CRL);
- Handle revocation requests from the owners of the certificates it issued;
- Provide technical support to secure e-government and e-commerce applications;
- Manage and supervise its delegated Registration Authority (RA).

4.5 Registration Authority (RA)

A Registration Authority (RA) is an entity that is responsible for the identification and authentication, and registration of subscribers but does not sign or issue certificates. The consulting team recommend the following three options to manage the subscriber registration function:

- Establish at least one principal RA at the HQ of the Government Accredited CA;
- Delegate the RA function to external entities, these registration authorities are referred as Local Registration Authorities (LRAs);
- Delegates the RA function to relying party (e.g. Banks).

To build a strong ecosystem for the promotion of digital certificate use, the consulting team recommends delegating the function to external Registration Authorities and, in some cases, arrange with its customer or a relying party (e.g. Banks) to perform the RA function. The consulting team also recommends the Government Accredited CA to establish a Registration Practice Statement (RPS) that defines the procedure and the requirements of Registration authorities. The Accredited CA should periodically audit the RA to ensure compliances with RPS.

Key roles of RA are as follows:

- Perform in-person identity vetting of digital certificate applicants;
- Register the user information;
- Issue and manage the subscriber's digital certificates (i.e. issue, renew or revoke certificates);
- Keep related document safely as a requirement to issue a certificate

6. Legal and Regulatory framework

6.1 Legal framework

The Malawi Electronic Transaction and cyber security Act 2016, define important aspect related to electronic signature, digital signature, and digital signature certificate. The law highlights the regulations to be established by the Minister in consultation with the Authority of Accredited Certification Authority. However, some important elements are not clearly defined in the Act, such as; the mandatory use of digital signature in critical services (e.g. e-Government, e-Banking and e-Commerce), requirement for electronic identification, digital stamp or e-Seal, electronic time stamp, internet sites authentication, electronic archiving, etc.…). Also, there is no regulation defining the criteria and requirement for CA accreditation.

6.1.1 Use of Digital signature in eGovernment, e-Commerce and e-Banking

The electronic transaction and cyber security Act of 2016 does not provide a mandatory use of PKI based digital certificates. One of the most effective methods to promote the usage of a digital signature is to establish a law on the mandatory use of a digital signature in e-Government, e-Commerce, and e-Banking services. In addition to the clauses related to digital signature in Electronic Transaction and cyber security Act of 2016, the consulting team recommends the review of the existing the electronic transaction and cyber security Act 2016 or establish a decree that set the mandatory use of digital signature in e-Government, e-Commerce, and e-Banking services in Malawi. The following should be considered:

- **Application of Digital Signatures in E-Government Services in the public sector:** All Government agencies and instrumentalities providing electronic services to their clients must require the use of digital signatures in their respective e-Government services to ensure confidentiality, authenticity, integrity, and non-repudiation of electronic transactions in government.
- **Application of Digital Signatures in E-Commerce and e-Banking Services in the private sector:** In line with its mandate to promote electronic commerce in Malawi, the Government must promote the application of digital signatures in e-Commerce and e-Banking services in the private sector to ensure confidentiality, authenticity, integrity, and non-repudiation of electronic transactions with the private sector.

6.1.2 Digital ID

Article 55 of the Electronic Transaction and cyber security Act of 2016 provides the minimum requirements to issue a “Digital certificate” or “Digital ID” to subscribers. The Minister in charge of ICT in consultation with the Ministry in charge of identification of Natural person and the Ministry in charge of identification of Commerce should establish regulations for Digital identity for Natural person or Legal person to establish a decree or regulation defining the Level of Assurance (LoAs) of different Digital ID.

The LoAs are the degree of confidence (e.g. High, Medium, and Basic). The degree of confidence is determined by the "Identity proofing" during the registration process, how rigorous the process of identifying the person or entity is when applying for Digital ID, the quality of the information provided (e.g. National ID Card, Passport, Driving License, etc.…) and the "authentication mechanism" or the strength of the methods used the during the authentication process to verify his or her identity.

Table 3: LoA and the requirement:

LoAs	LoA Criteria	Authentication mechanism
Basic	• The applicant present ID recognized by the Government (remote or in-person) from an approved external database (e.g. National Population Registry) • The Subscriber keys do not need to be generated and stored in a FIPS 140-2 certified cryptographic module; and	• Single factor authentication method (e.g. UID + Password or PIN)
Medium	• The applicant present ID recognized by the Government (remote or in-person) from an approved external database (e.g. National Population Registry) • The applicant ID verification is performed by registration authority • The cryptographic module must protect the keys against cloning, duplication and tampering as well as against attackers with high attack potential; • The subscriber keys can be generated and stored in a FIPS 140-2 Level 1 or + certified; • Private signature keys must be generated by the subscribers.	• Multi-factor authentication method (e.g. mobile phone + PIN)
High	• In-Person, the applicant presents ID recognized by the Government at an RA. • The applicant ID verification is performed by registration authority • The applicant ID is validated through an approved external database (e.g. National Population Registry) • The cryptographic module must protect the keys against cloning, duplication and tampering as well as against attackers with high attack potential; • The cryptographic module must be reliably protected by the person to whom it belongs against use by others;	• Multi-factor authentication method (certificate +PIN) • Must access private data/keys stored on tamper-resistant hardware token.

	• The signature and authentication keys are generated on the Hardware Security Module (HSM) and never leave in the HSM; • The cryptographic module needs to be FIPS 140-2 Level 2 or + certified. • Private signature keys must be generated by the subscribers.	

6.1.3 Electronic Stamp ("e-Seal")

Electronic stamps are technically equal to digital signatures but have a legally different significance since they can be performed without the direct consent of a physical person and consequently allowing for automated stamping. An electronic seal is defined as "electronic data, attached or logically associated with other electronic data to guarantee the origin and integrity of the data. The current Electronic Transaction and cyber security Act of 2016 does not define the use and the requirements of an authentic e-Seal. The consulting team recommends an amendment of the current Electronic Transaction and cyber security Act of 2016 and set the use and requirements of an e-Seal in e-Government, e-Commerce and e-Banking services in Malawi. An "e-Seal" should meet the following requirements:

(a) be linked to the creator of the stamp in a unique way;

(b) make it possible to identify the creator of the stamp;

(c) have been created using electronic seal creation data that the creator of the seal may, with a high level of confidence, use under his control to create an electronic seal;

(d) be linked to the data with which it is associated so that any subsequent modification of data is detectable.

(e) Is based on a "Digital certificate" that was issued by an Accredited Certification Authority in Malawi or a foreign Certification Authority recognized by the Authority.

In addition to this, the following should be considered while defining the requirements for an electronic seal:

(a) Advanced electronic seal requirements

(b) Qualified electronic seal certificates

(c) Electronic seal in public services

(d) Requirements applicable to devices for the creation and validation of qualified electronic seals

6.1.4 Electronic time-stamp

The time stamp is defined as "a data unit which is created using a system of technical and organizational means which certifies the existence of a document at a given time." The current Electronic Transaction and cyber security Act 2016 does not define the use and the requirements for an electronic time stamp service, the consulting team recommends an amendment of the current law and defines the use of time stamp in an electronic transaction.

The Qualified electronic time stamp should meet the following requirements:

(a) link the date and time to the data so as to exclude the possibility of undetectable modification of these data;

(b) be based on an exact clock linked to coordinated universal time; and

(c) be signed by means of an advanced electronic signature or stamped by means of an advanced electronic seal of the qualified trust service provider, or by an equivalent method.

6.2 Regulationsof CA Accredition

In Section 51, the Electronic Transaction and Cyber security Act of 2016 states that the Minister from time to time issues certification authority accreditation regulations in consultation with the Authority. The first step to implement the legal framework is the drafting and enactment of the regulation under the law on “Electronic Transaction and cyber security Act 2016”. The Ministry in charge of ICT in collaboration with the Authority of Certification Authority has the responsibility to draft and process the enactment of the regulation stating the requirements for Accredited CA PKI system in Malawi.

The following regulations are recommended to be established and approved by the Cabinet of the Minister in charge of ICT:

- Requirements for Accredited CA’s certification facilities
- Requirements for Accredited CA’s Protective Measures

5.2.1 Regulation for Accredited CA's certification facilities

The Accreditation body has to provide a detailed criterion for CA accreditation. The applicant for CA Accreditation should prove that their certification facilities satisfy all the requirements stated in the CA accreditation criteria. After documents evaluation, the accreditation body has to visit CA applicant's facilities and equipment for actual inspection.

Table 4: Accredited CA's certification facilities requirement:

Check Points	Requirements
Facilities to manage user registration and digital certificates	• It has a function to register and manage subscriber information included in the certificate. • It has a function to store subscriber certificate and others in a secure manner.
Facilities to create and manage the signature keys	• It has a function to create and manage the digital signature key of the certification authority • It has a function to store the digital signature key securely
Facilities to create/issue/manage certificates	• It has a function to create/issue/store/notify a certificate • Validity verification and auditing security function are also pertained
Time-stamping facilities	• A time-stamping function is pertained
Security system facilities	• Protects systems that are providing certification services and infrastructure
User facilities	• It has a function to manage user's digital signature key and certificate on user computer, token or smart card • It has a function to verify the digital signature and certificate • A time-stamping function is pertained

5.2.2 Regulation for Accredited CA's Protective Measures

The Accredited CA applicants have to make documents to prove that their protective measures satisfy all the requirements. After accreditation, accredited CAs have the responsibility to report to the Authority for any change of the protective measures.

5.2.2.1 PKI Machine Rooms

To enhance the security of PKI system, access control is the most effective method to restrict of access to PKI room, a PKI system operator should have access only in the PKI room that hosts the system he manages, he cannot have access to all PKI rooms at the same time.

Figure 3: National PKI Center

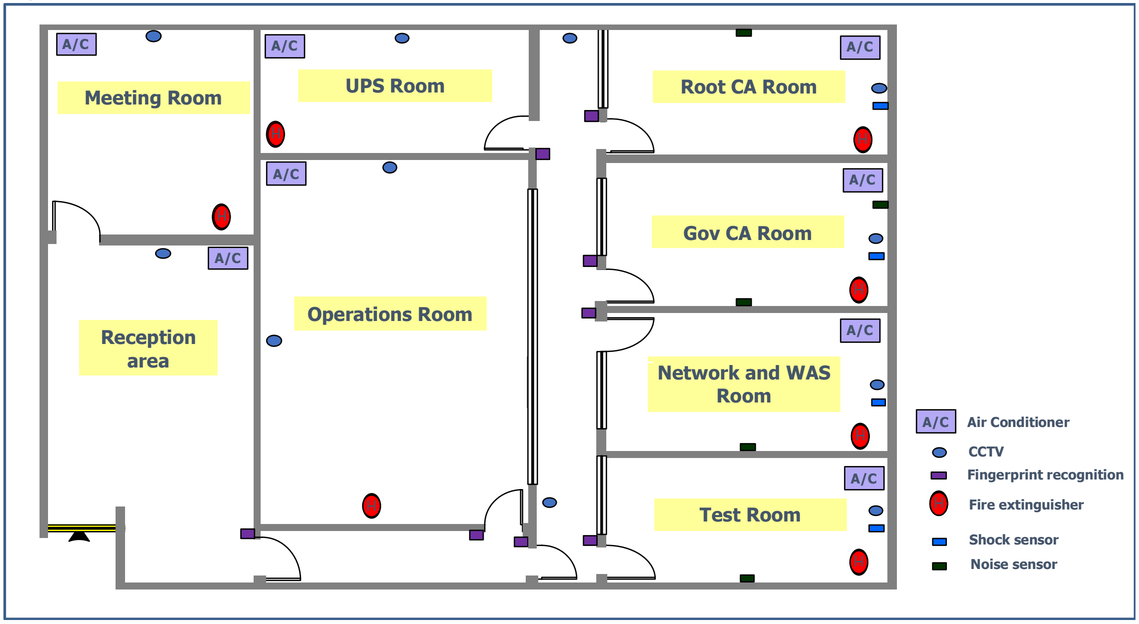


Table 5: PKI rooms requirement

Check Points	PKI rooms requirements
PKI machine rooms	• Different core PKI systems shall be installed separately in different room (e.g. Root CA room, Accredited CA Room, Network room, test-bed room, etc.…) and shall be operated independently of each other. Measures should be taken against any damage from fire or water flooding. • PKI Center's stability is very important and the Center should be constructed as an extendable structure when necessary.

5.2.2.2 Multiple Access Control

The basic requirement for PKI data center is multi-factor authentication, an authentication method that requires the presentation of two or more authentication factors to access PKI data center premises. The biometrics security system enhances the security level efficiently. Moreover, it is necessary to keep the records of all access to PKI data center. The table below provides multiple access control requirements.

Table 6: Multiple access control requirements

Check Points	Requirements
1. Access control and audit records	• Priority should be given in storing data to the devices whose log information cannot be modified or deleted. The data should be retrievable for audit purposes.
2. Bio-feature-based and possession-based identification	• The identification system should be multi-tiered with mixed use of biology-based, knowledge-based and possession-based systems. For example, fingerprint or password or smart card information shall be used together to access PKI data center.

5.2.2.3 Disaster Prevention

The disaster prevention system is one of the cores of the PKI data center. Loss of power, exposure to fire and water can cause significant and instant damage to information processing hardware and consequently affect the service offered by the PKI Data center. As a consequence, the following shall be mandated to prevent damage caused by fire exposure. The table below defines the minimum requirements of the disaster prevention in the PKI data center:

Table 7: Disaster prevention requirement

Check Points	Requirements
1. Fire prevention and protection	Fire alerting, prevention , suppression and protection shall be in place in each room hosting CA PKI system so that even in case of emergency the PKI systems are not affected.
2. Water prevention	CA system and equipment shall be installed at a certain height such that it is not in danger of exposure to water.
3. Power	To survive a blackout, Uninterrupted Power Supply (UPS) or a Generator shall be in place to supply sufficient power for a minimum of six hours operation in the absence of commercial power.
4. Air Conditioning	The CA PKI Data center shall be equipped with heating and air conditioning systems to control temperature and relative humidity to keep the systems and security devices in optimal

	conditions.

5.2.2.4 Physical security

The PKI data center should be secured enough in order to ensure a certain level of security. Otherwise, it will not be possible to win trust. The following minimum physical security requirements should be considered while establishing the PKI data center:

Table 8: Physical Security system requirement

Check Points	Requirements
1. Physical Lock	• A fire proof safe box is required to safely keep important keys and data. For example, keys for Root CA and Accredited CA shall be backed up into HSM token and stored into safe.
2. Intrusion Detection Device	• Sensors of fire and vibration are to be installed and operated 24 hours a day to detect any intrusion attempt.
3. Monitoring and controlling devices	• Surveillance cameras have to be set up at various points in the PKI data center, and high-quality recording devices shall be operated.

5.2.2.5 Network security

The PKI system is a network-based online service system. Thus, the security of the network is one of the main issues for the entire system security. To enhance the stability of the system, it is important to have a High Availability (HA) configuration especially the core network equipment, internet, and web application firewalls. Systems to manage and monitor the security of the network, system failure, and performance of servers must be established. The National PKI system should be segmented into different zones (Reception Network):

- Reception Network or DMZ; hosting PKI systems facing the internet
- Operation internal network; hosting PKI Backend systems and Databases
- Secure internal network; highly secure zone, hosting the Root CA and Accredited CA systems.

Table 9: Network security requirements.

Check Points	Requirements
1. Redundant network Devices	• All network equipment in production environment should be configured in High Availability (HA)

2. Firewall/Intrusion Prevention System (IPS)	• The firewall and IPS are required to control the incoming and outgoing network traffic by analyzing the data packets and determining whether they should be allowed through or not, based on the applied rule set.
3. SMS and NMS	• The SMS and NMS systems are required to monitor and administer the network and system efficiently.

5.2.2.6 System security

All the operational information of each PKI system shall be logged and stored for periodic auditing, where possible, the security audit logs shall be automatically collected. sAll security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

Table 2 : Requirements for PKI System Security

Check Points	Requirements
1. Safe and reliable system	• Policies against intrusion shall be implemented on each system so that manager and operator can have access and conduct maintenance works on a regular basis. Also, necessary to guarantee security by applying tools like secure OS.
2. Generating & storing records	• All security events (i.e. operational activities and intrusion attempts) shall be detected, logged for periodic audit, reported and adequately tracked login accesses (for authorized and unauthorized users).
3. Other equipment	• Security of other systems necessary for certification services such as web server, name server (DNS Server) and mail server, shall be maintained.

5 PKI Policies and Standards

5.2 PKI Standards

PKI standards are important to provide interoperability with other accredited CAs and foreign PKI systems, so the Authority of Accredited CA in Malawi must establish PKI standards tailored to the Malawi environment. Malawi does not have the PKI standards yet, so it is open to adapt all globally recognized PKI standards.

Standards without specific scope and profiling cause obstacle to interoperability among all PKI related entities as well as accredited CAs.

For example, in the standard of digital certificate profile, it can be necessary to include a field for the Unique Personal Identification Number (PIN) for natural person identification and Tax Identification Number (TIN) for legal person and entities. Also, the imposition of the specific standard with which should be complied can be a protection for a local company against global PKI products.

This framework defines PKI Standards for Digital Certificate Profile, Algorithm, Protocol, and Key Security. These standards should comply with RFC (Request for Comments) document that contains technical and organizational notes about the Internet associated with an active IETF (Internet Engineering Task Force) Working Group.

5.2.1 Digital certificate Profile

Profile is a definition that specifies the format of a certificate, CRL, DN, and Unique Personal Identification Number (PIN) for natural person or Tax Identification Number (TIN) for legal person integrated into a digital certificate.

Certificate and CRL profile define things like version, serial number, signature, issuer, or validity that are associated with issuing a certificate. It should comply with RFC5280, and its forms are using profiles of the X.509 v3 certificate and X.509 v2 Certificate Revocation List (CRL) for use on the Internet. All certificates and CRL issued by the Accredited CA should maintain the interoperability features among Accredited CAs.

DN profile defines the attribute types of DN including object class, object name, serial number, personal info etc. It should comply with RFC2256 and support Universal Character Set Transformation Format – 8 (UTF-8) for international character standard. User software also needs to support all attributes defined in this profile.

Certificate should use the PIN or TIN for its identification and verification, so there should be a profile for PIN or TIN standardized to have interoperability among PKI systems.

5.2.2 Encryption Algorithm

PKI technology uses encryption algorithms of Asymmetric, Symmetric and Digest (hash algorithm) to provide its security function with encryption. The following standards algorithm should be considered in the National PKI standards:

- Asymmetric encryption algorithm: RSA (Rivest Shamir Adleman), DSA (DSS: Digital Signature Standard), ECDSA (Elliptic curve Digital Signature Algorithm) etc. can be used in PKI technology
- Symmetric encryption algorithm: AES (Advanced Encryption Standard), IDEA (international data encryption algorithm).
- Digest algorithm: SHA (Secure Hash Algorithm)-256 and SHA-512 can be used.

It is necessary to specify all features of the algorithm such as key size and parameter in the profile to provide interoperability with other PKI system.

5.2.3 PKI Protocol

PKI technology uses different protocols for issuing a certificate and securing transmission data among PKI systems. The following standards PKI protocols should be considered in the National PKI standards:

- The Certificate Management Protocol (CMP) is an Internet protocol used for obtaining X.509 digital certificates in PKI. It is described in RFC 4210 and is one of two protocols so far to use the Certificate Request Message Format (CRMF), described in RFC 4211, with the other protocol being Certificate Management over CMS (CMC), described in RFC 5273. CMP messages are encoded in ASN.1 (Abstract Syntax Notation.1), using the DER (Distinguished Encoding Rules) method and usually encapsulated in HTTP.
- Certificate signing request (CSR) is a message sent from an applicant to a certificate authority to apply for a digital certificate. The most common format for CSR is the PKCS#10 specification.
- Online Certificate Status Protocol (OCSP) enables applications to determine the revocation state of certificates. It is described in RFC6960. OCSP may be used to satisfy some of the operational requirements of providing more timely revocation information than is possible with CRLs and should be used to obtain additional status information. OCSP client issues a status request to an OCSP responder and suspends acceptance of the certificates in question until the responder responds.
- Lightweight Directory Access Protocol (LDAP) is described in RFC3494. It is an Internet Protocol used to access X.500-based directory services. A publisher should recognize that significant interoperability issues exist between current LDAPv2 implementations. LDAPv3 is technically superior to LDAPv2 and hence should be used instead.

- Time-Stamping Protocol (TSP), as described in RFC3161, should be used to time-stamp data to establish evidence indicating that the data existed before a particular time. For example, it should be used to verify that a digital signature was applied to a message before the corresponding certificate was revoked. TSP allows a revoked certificate to be used for verifying signature which is created prior to the time of revocation. This is an important public key infrastructure operation. The TSP can also be used to indicate the time of submission when a deadline is critical.

5.2.4 Private Key protection

The relevant standard for cryptographic modules is FIPS PUB 140-2. This framework defines the minimum-security Requirements for Cryptographic Modules. The following private key protection measures should be considered in the National PKI policy and standards:

Table 14: Security requirements for HSM for Root CA and Accredited CA:

CA	Subscriber cryptographic modules
Root CA	Hardware HSM, FIPS 140-2 level 3 or plus certified
ACA	Hardware HSM, FIPS 140-2 level 3 or plus certified

Table 15: Security requirements for HSM for Subscriber:

Digital certificate LoA	Subscriber cryptographic modules
Basic	No FIPS 140-2 requirement
Medium	Hardware or software HSM, FIPS 140-2 level 2 or plus
High	Hardware HSM, FIPS 140-2 level 3 or plus certified

5.3 CP and CPS framework

The PKI policy consists of certificate policy (CP) and certificate practice statement (CPS).

A Certificate Policy (CP), as defined in X.509, is a set of rules that indicate the applicability of a certificate to a particular community and/or class application with common security requirements. A CP provides guidance to relying parties, to help them know whether a certificate is appropriate for use in conjunction with a specific application. A CP provides liability protection for a CA, by declaring the intended range of uses for the certificates it issues.

The certificate practice statement (CPS) is a more detailed description of the practices that a CA employs when issuing and managing digital certificates, and it is tailored to the organization's PKI operating procedures, organizational structure, facilities, and computing environment of the Certification Authority. Generally, the CP state what is to be adhered with, while the CPS state how it is adhered with.

Article 54 (1) requires CA to publish certification practice statement, the Authority of the CA should establish a comprehensive CP and CPS that are based on the recommendations of the Internet Engineering Task Force (IETF) for Public Key Infrastructure (RFC 3647) to guarantee the interoperability and high level of security of certification service of CAs in Malawi. The

Authority for CA should be responsible to review and evaluate CP and CPS of CAs and conduct annual audit to ensure compliance. The following items should be considered while defining the Certification Policy:

Table 10: CP and CPS framework

Index	Contents
Identification and authentication	• The procedures used to authenticate the identity of an end user certificate applicant • The criteria for accepting applicants of entities seeking to become CAs or RAs • The authentication procedures for requesting re-key or revocation
Certificate Life-Cycle Operational Requirements	• The requirements imposed upon CAs, RAs, subscribers, or other participants with respect to the life-cycle of a certificate. (Ref: Electronic Transaction and Cyber security Act 2016, Section 55 -59)
Facilities, Management & Operational control	• The Non-technical security controls (physical, procedural and personnel controls) used by CA • Functions of key generation, subject authentication, certificate issuance, certificate revocation, auditing and archiving • The physical controls on the facility housing the entity systems • The requirements for recognizing trusted roles together with the responsibilities for each role
Technical Security controls	• The security measures taken by the CA to protect its cryptographic keys and activation data • Other security controls used by the CA to perform securely the functions of key generation, user authentication, certificate registration, certificate revocation, auditing and archiving
Certificate, CRL and OCSP Profiles	• Define certificate profile to comply with the RFC 3280 • Define CRL profile to comply with the RFC 3280 • Define OCSP profile to comply with the RFC 2560
Compliance Audit & Other assessment	• The list of topics covered by the assessment and the methodology used to perform the assessment • Frequency of compliance audit or other assessment for each entity that must be assessed • pursuant to a CP or CPS

Index	Contents
	• The identity and qualification of the personnel performing the audit or other assessment
Other business and legal matters	• The business issues of fees to be charged for various services • The financial responsibility of participants to maintain resources for ongoing operations and for paying judgments or settlements in response to claims asserted against them

5.3.1 OID Policy

An object identifier (OID) is an extensively used identification mechanism jointly developed by ITU-T and ISO/IEC for naming any type of “object” or "thing" with a globally unambiguous name that requires a persistent name (long life-time). It is important for the interoperability among CAs to identify PKI related object uniquely, once allocated, should not be used for a different object/thing.

Table 11: OID Policy

LoA	Policy Name	OID	Description
High	USB Crypto Token	TBD	Multi Purpose Certificate
	Mobile ID	TBD	Multi Purpose Certificate
Medium	Smart ID	TBD	Multi Purpose Certificate
	Local ID	TBD	Multi Purpose Certificate
Basic	UID + Password + PIN	TBD	Case by case

5.3.2 CA Certificate issuance policy

The certificate issuance policy is necessary to configure Root CA and Accredited CA system for naming, algorithm, key length, validity period, etc. PKI consulting team proposed PKI policy in the table below based on the discussion with Legal and MACRA Staff.

Table 12: CA Certificate profile policy

Type	Root CA	Government CA
Version	V3 (2)	V3 (2)
Certificate DN	cn=Malawi Root CA	cn=Government CA<1 or n>
	ou=Root CA	ou=Gov CA
	ou=MACRA	ou=NODAL
	c=MW	c=MW
Validity Period	20 years	10 years
Key Length / Algorithm	RSA 4096 bit / SHA256	RSA 4096 bit / SHA256
CA Homepage	http://www.rootca.gov.mw	http://www.aca.gov.mw
KeyUsage	CA, TSA Certificate Signing, Off-line CRL Signing, CRL Signing	Subscribers Certificate Signing (individual, corporation, server), Off-line CRL Signing, CRL Signing

5.3.3 Subscriber certificate issuance policy

The certificate issuance policy is necessary to configure Root CA and Accredited CA system for naming, algorithm, key length, validity period etc. PKI consulting team proposed the certificate policy in the table below based on the discussion with Legal and MACRA Staff.

Table 13: Certificate Profile Policy

Type	Natural Person	Legal Person
Version	V3 (2)	V3 (2)
Certificate DN	cn= <Subscriber Name>+<PIN>	cn= <Subscriber and Organization name >+<TIN>
	Ou=Gov CA	Ou=Gov CA
	Ou=NODAL	Ou=NODAL
	C=MW	C=MW
Validity Period	1|2|3 years	1|2|3 years
Key Length / Algorithm	RSA 2048 bit / SHA256	RSA 2048 bit / SHA256
Key Usage	digitalSignature|Non-repudiation| keyEncipherment | emailProtection| clientAuthentication	digitalSignature| Non-repudiation| keyEncipherment | emailProtection| clientAuthentication
Type	**Organisation**	**Server or Service**
Version	V3 (2)	V3 (2)
Certificate DN	cn= < Organization name >+ TIN	cn= Domaine name or IP Address
	Ou=Gov CA	Ou=Gov CA
	Ou=NODAL	Ou=NODAL
	C=MW	C=MW
Validity Period	1|2|3 years	1|2|3 years
Key Length / Algorithm	RSA 2048 bit / SHA256	RSA 2048 bit / SHA256
Key Usage	digitalSignature| Non-repudiation|	digitalSignature|keyEncipherment |dataEncipherment or ClientAuthentication|ServerAuthentication

6 Root CA System Architecture

6.1 Root CA Architecture Production environment (Primary Site)

The Root CA system will be the top in Malawi PKI hierarchy structure that all users will trust, it will be used to issue and sign certificates for:

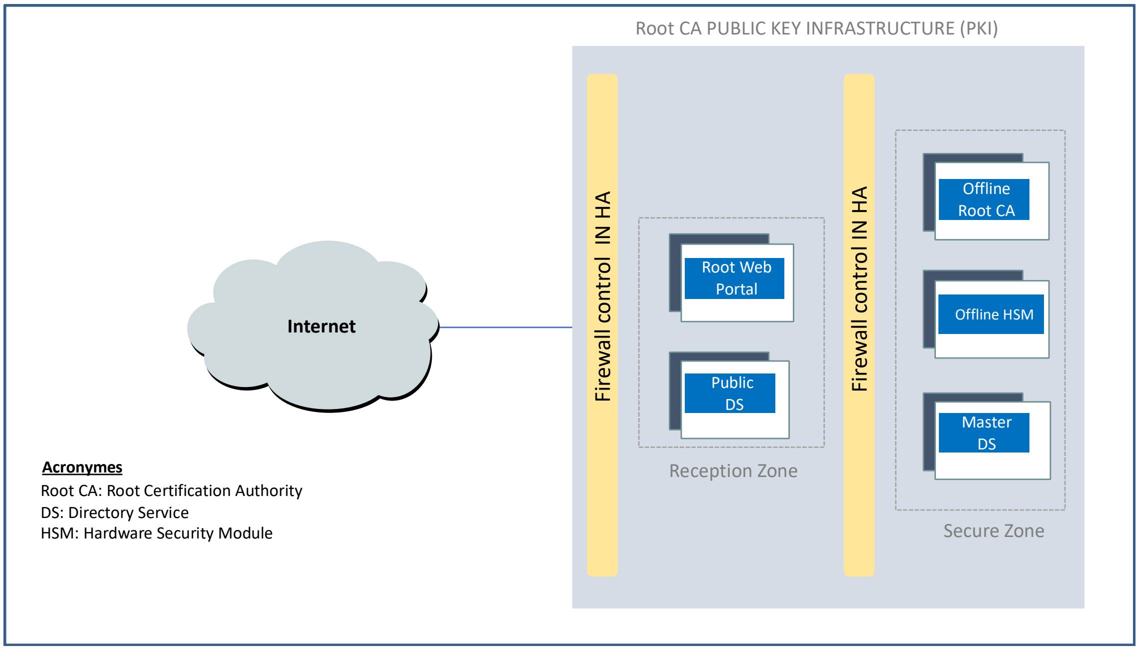
- Self-Signed Root CA Certificate;
- Accredited certification authority (CAs);
- Authority Revocation List (ARL);
- and Time Stamp Authority (TSA).

To ensure high protection, the Root CA should always operate in off-line mode and be hosted in a highly protected environment. In the Root CA system, the consulting team recommends three PKI environments. These are:

1) All Root CA component in production environment will be configured in High Availability (HA) to ensure a stable operation and availability of the PKI services.
2) The Root CA Disaster Recovery (DR) environment will be configured with no HA configuration.
3) The Root CA Test environment will be configured with no HA configuration.

All components in the Root CA production environment must be configured for high availability (HA) to provide redundancy. A redundant firewall should be implemented to control access between different network zones (i.e. External or Internet network, DMZ network, and internal network).

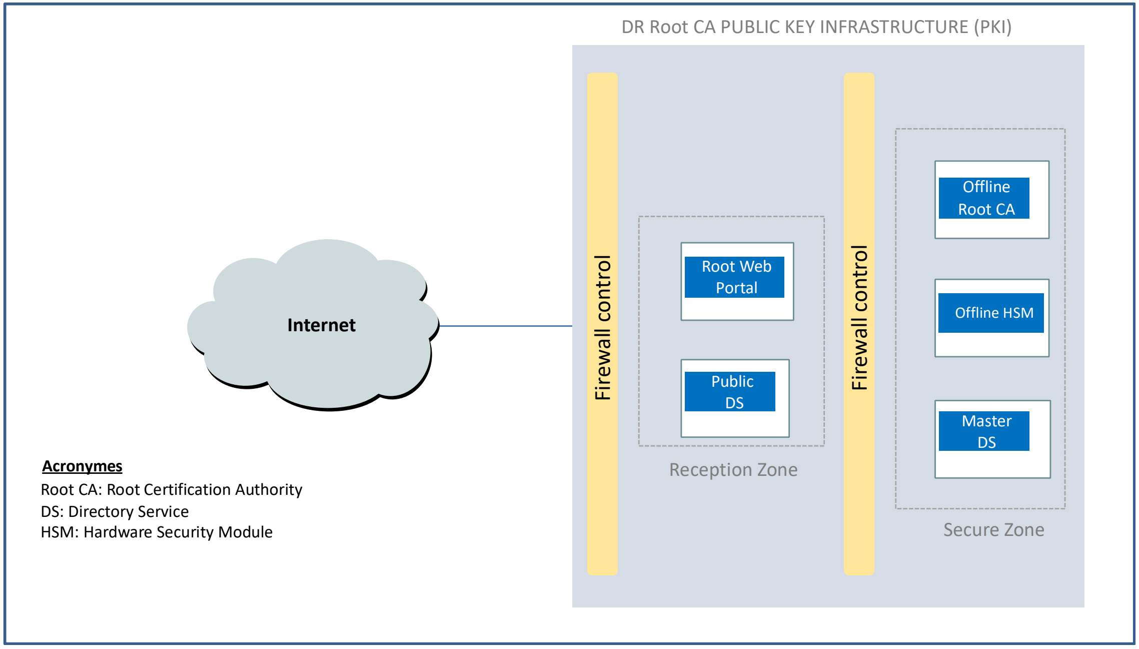
Figure 4: Conceptual Root CA System Architecture



6.2 Root CA PKI System (Disaster Recovery and Test Environment)

The architecture of the Disaster Recovery and Test Environment for the Root CA are identical, there is no High Availability in the Disaster recovery and test environment. A firewall should be implemented to control access between different network zones (i.e. External or Public network, DMZ network, and internal network).

Figure5: DR Root CA conceptual Architecture



6.3 Root CA system components and requirements

The Root CA consists of Root CA System, HSM, A master and public LDAP system, and Root CA Website. The table below summarizes the key components for the root CA PKI system in the Production, DR, and Test environment.

Table 16: Root CA component and specifications

system	Technical requirements for Root CA systems
Root CA System configured in HA	• Shall support HA configuration in production environment, no-HA in DR and no-HA in Test environment • The Root CA shall run offline to maintain tight physical security; • CA Certification, Renewal and Revocation; • Publishes CRLs and ARLs periodically; • The Root CA certificate shall be self-signed and X.509 version 3 certificate standard • The Root CA private keys shall be created and protected in a hardware HSM FIPS 140-2 Level 3 certified • Applies international standards in issuance (RFC 5280)
HSM	• Shall support HA configuration in production environment, no-HA in DR and no-HA in Test environment • Generates and controls digital signature keys for Root CA • Multifactor control configuration (i.e. k-of-n factor will be set to 3-of-5)
Master and Public Directory Service (DS) configured in HA	• Shall support HA configuration in production environment, no-HA in DR and no-HA in Test environment • The Root CA certificate, cross-certificates, subordinate CA certificates, CA policies, CRLs and ARLs will be published in the Root CA LDAP Directory server • Applies international standards in issuance (RFC 3494)
Root CA Web Server	• Shall support HA configuration in production environment, no-HA in DR and no-HA in Test environment • Posts certificate policies, relevant laws and standards • Posts certificate issuance/revocation list • Posts CP and CPS

7 Accredited CA Architecture

The Accredited CA shall be able to issue digital certificates to subscribers (i.e. natural person, legal person and equipment or servers). The Accredited CA shall issue the following types of digital certificates:

- Authentication Certificate, to authenticate users accessing online services in e-Government, e-Banking and e-Commerce.
- Digital signature certificate, to sign electronic transactions or electronic document;
- Digital stamp certificate, to stamp electronic transactions or electronic document;
- Encryption Certificate, to encrypt confidential data or document;
- Email Signing and Encryption Certificate, to sign and encrypt important emails
- Code Signing Certificates, to sign software executable files;
- Server and clients Certificates, to secure communication between the servers and client's machines;
- VPN Certificates, to authenticate VPN users for secure login.

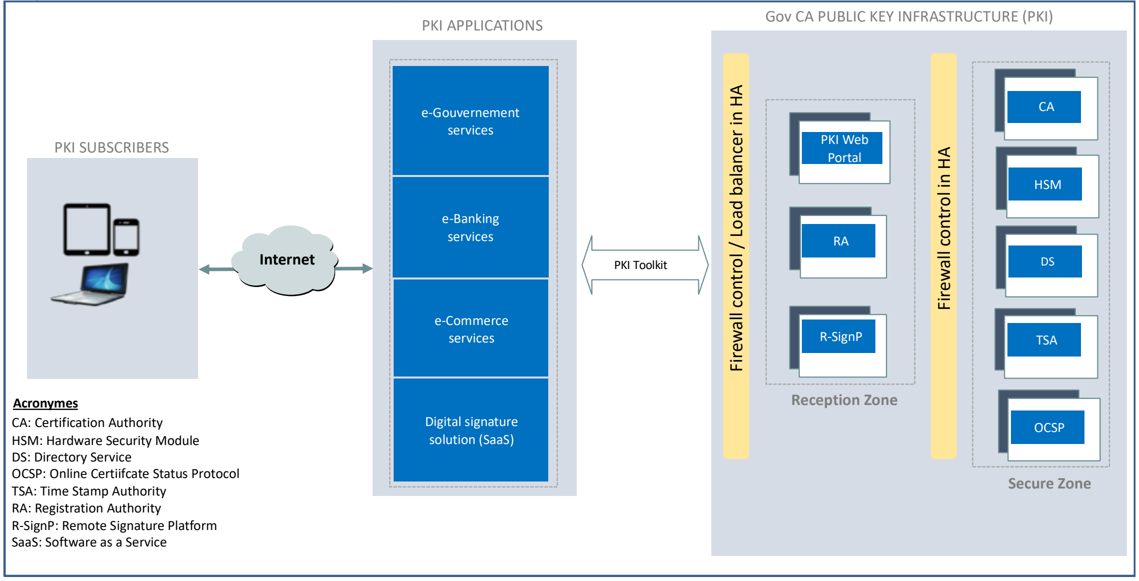
The Accredited CA will be the issuing CA, it will play an essential role in issuing digital certificates to subscribers (i.e. natural person, legal person, and Servers or equipment) in the National PKI system. In the Accredited CA system, the consulting team recommends three PKI environments. These are:

1) Production environment (primary site); All Accredited CA components in production environment will be configured in High Availability (HA) to ensure a stable operation and availability of the PKI services.
2) Disaster Recovery (DR) environment (secondary site); The Accredited CA DR environment will be configured with no HA configuration.
3) Test environment: The Accredited CA Test environment will be configured with no HA configuration.

8.1 Accredited CA Architecture production environment

There Accredited CA production environment all components should be configured in High Availability (HA) mode to ensure availability of services. Firewall should be implemented to control access between different network zones (i.e. External or Public network, DMZ network and internal network).

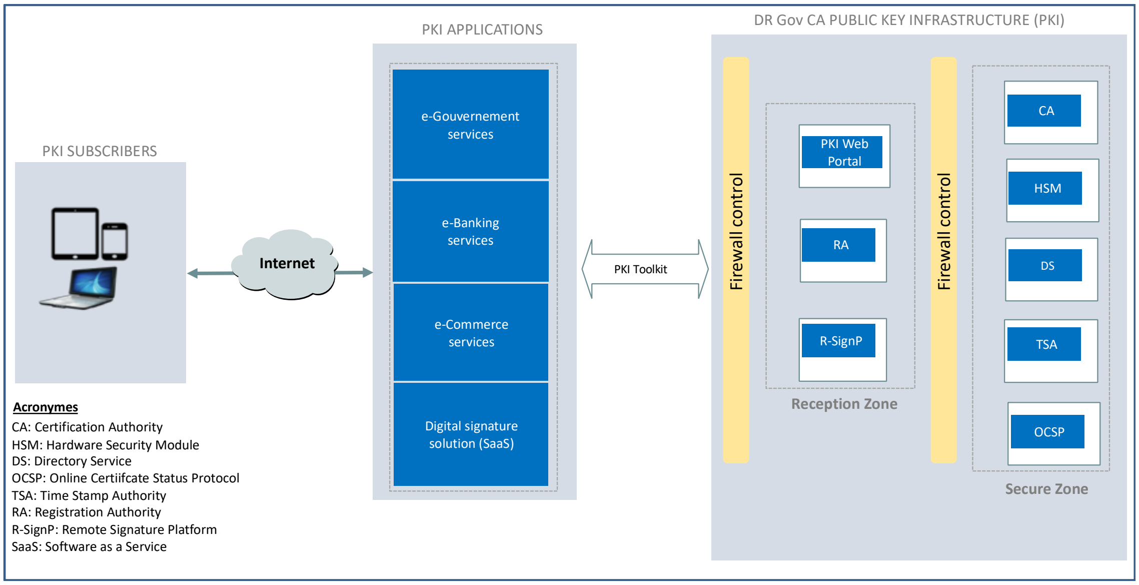
Figure 6: Accredited CA conceptual Architecture


PKI APPLICATIONS
Gov CA PUBLIC KEY INFRASTRUCTURE (PKI)
PKI SUBSCRIBERS
Internet
e-Gouvernement services
e-Banking services
e-Commerce services
Digital signature solution (SaaS)
PKI Toolkit
Firewall control / Load balancer in HA
PKI Web Portal
RA
R-SignP
Reception Zone
Firewall control in HA
CA
HSM
DS
TSA
OCSP
Secure Zone
Acronymes
CA: Certification Authority
HSM: Hardware Security Module
DS: Directory Service
OCSP: Online Certiifcate Status Protocol
TSA: Time Stamp Authority
RA: Registration Authority
R-SignP: Remote Signature Platform
SaaS: Software as a Service

8.2 Accredited CA Architecture DR and test environment

There is no High Availability in the Disaster recovery environment. A firewall should be implemented to control access between different network zones (i.e. External or Public network, DMZ network, and internal network).

Figure 7: DR Accredited CA conceptual Architecture


PKI APPLICATIONS
DR Gov CA PUBLIC KEY INFRASTRUCTURE (PKI)
PKI SUBSCRIBERS
Internet
e-Gouvernement services
e-Banking services
e-Commerce services
Digital signature solution (SaaS)
PKI Toolkit
Firewall control
PKI Web Portal
RA
R-SignP
Reception Zone
Firewall control
CA
HSM
DS
TSA
OCSP
Secure Zone
Acronymes
CA: Certification Authority
HSM: Hardware Security Module
DS: Directory Service
OCSP: Online Certiifcate Status Protocol
TSA: Time Stamp Authority
RA: Registration Authority
R-SignP: Remote Signature Platform
SaaS: Software as a Service

8.3 Accredited CA PKI Systems components and requirements

The architecture of the Disaster Recovery and Test Environment for Accredited CA are identical. The table below summarizes the key components for the Accredited CA PKI system in Production, DR, and Test environment.

Table 17: Accredited CA components and specifications

Components	Technical requirements for Accredited CA systems
Accredited CA System	• Supports HA configuration in production environment, no HA in DR and no HA in Test environment • Creates and manages certificate life cycle management (i.e. issues/renew/revoke/suspend certificates) • Publishes CRLs periodically; • The Accredited CA certificate shall be signed by the Root CA and X.509 version 3 standard • Applies international standards in issuance (RFC 5280) • The Root CA private keys shall be created and protected in a hardware HSM FIPS 140-2 Level 3 certified • The Accredited CA shall support Subscriber key storage containers (i.e. USB Crypto token, smart cards, Crypto SIM Card, Apple Secure Enclave (SE), Android Trusted Execution Environment (TEE) and centralized HSM).
HSM	• Support HA configuration in production environment, no HA in DR and no HA in Test environment • Supports HA configuration • Generates and controls digital signature keys for Accredited CA • Multifactor control configuration (i.e. k-of-n factor will be set to 3-of-5)
Directory Service (DS)	• Supports HA configuration in production environment, no HA in DR and no HA in Test environment • Inquires/manages/stores certificates • Publishes CRLs/ARLs • Supports common LDAP services • Applies international standards in issuance (RFC 3494) • Supports LDAP v3, HTTPS, HTTP, FTP, and TLS 1.0 protocols • Supports Master and Public LDAP
RA System	• Supports HA configuration in production environment, no HA in DR and no HA in Test environment • Registers and manages subscriber's personal information to be included in certificates

	• The RA has to be designed and implemented to support online registration process • The RA software supports multi authorization • The RA supports integration with External Database (e.g. Population Registry) to validate NID number of applicants; • The RA securely communicates with the ACA through an API; • The RA supports certificate issuance on different containers (i.e. USB Crypto token, smart cards, Crypto SIM Card, Apple Secure Enclave (SE), Android Trusted Execution Environment (TEE) and centralized HSM).
OCSP System	• Supports HA configuration in production environment, no-HA in DR and no-HA in Test environment • The trusted OCSP responder shall be used to process the verification and status information requests; • The responder shall respond to requests through OCSP Protocol according to RFC 6960; • Supports digital signing of the OCSP requests and/or responses. • Applies international standards in issuance (RFC 6960) • Supports Certificate Transparency as per [RFC 6292]. • Supports multiple CAs
TSA System	• Support HA configuration in production environment, no-HA in DR and no-HA in Test environment • The TSA supports stamping the local date and time as well as stamping the universal time; • Supports HA configuration • The TSA shall sign each time stamp token using a key generated exclusively for this purpose. • The TSA certificate shall be in accordance to RFC 3820. • The TSA shall be compliance RFC 3161 • The time stamping requests, token responses and error messages shall be compliance RFC 3161 • The TSA responses shall be signed by the TSA • The TSA shall use a trustworthy source of time • The TSA shall include a trustworthy time value for each time-stamp token.
ACA Web portal	• Supports HA configuration in production environment, no-HA in DR and no-HA in Test environment • Posts certificate policies, relevant laws and standards • Issues/manages subscriber certificates

	• Posts rules for certificate affairs • Online application forms for digital certification issuance, renew, revocation and key recovery operation • Integration with RA backend system • The ACA portal should support certificate issuance on different containers (i.e. USB Crypto token, smart cards, Crypto SIM Card, Apple Secure Enclave (SE), Android Trusted Execution Environment (TEE) and centralized HSM.

8.4 Additional digital signature solutions

Table 17: Additional Accredited CA components and specifications

System	Technical requirements for additional Accredited CA systems
Digital Authentication and Signature platform	• Supports HA configuration in production environment, no-HA in DR and no-HA in Test environment • Supports e-signature generation, verification and supports Standard advanced digital signatures (i.e. PDF, XML, CMS, PKCS#7, PAdES, CAdES and XAdES and RSA PKCS#1, etc.) • Integration: RESP API and support OAuth 2.0 / OpenID Connect 1.0; • Integrates with the Registration Authority (RA) application that issue and manage subscriber certificates (i.e. issue, renew and revoke certificates). • Integrates with external data base (e.g. Population Registry) for ID number validation. • Provides and support Mobile ID App with its SDK that is a multifactor authentication method, allowing signing and confirming transactions with digital signature
Digital signature solution (Document signing workflow)	• The digital signature solution should allow users to seamlessly create, review, edit, share document for signature and tracking the approval process; • Provides Mobile apps to digitally sign documents with mobile device (i.e. iOS and Android); • The solution should support users to sign multiple documents in one go, thus saving substantial time in opening the document and signing them one by one; • The solution should support users to sign electronic transaction and document with their signing key stored on either a Mobile device, Remote HSM, USB token or Smart Card.

8 PKI implementation phases

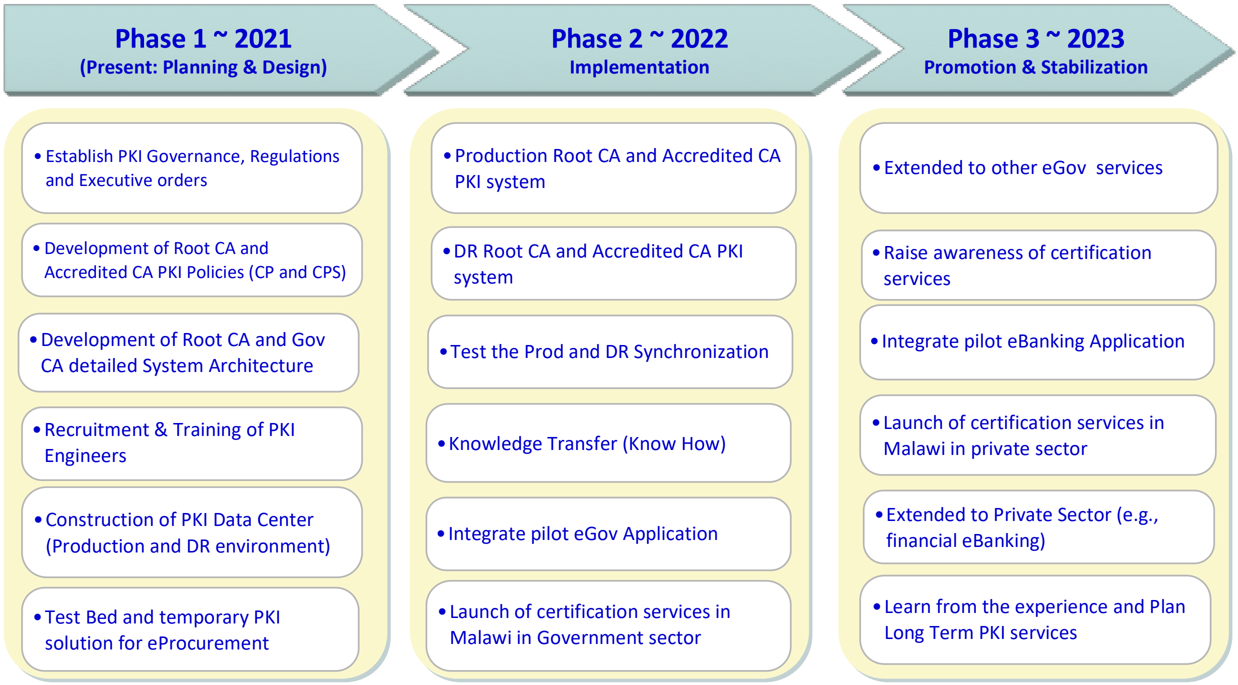
The National PKI system is a critical infrastructure. It requires compliance with standards security requirements and industry best practices to ensure the safety of the infrastructure. The PKI consulting team to implement the National PKI project in three phases:

- Phase I of PKI project will focus on:
    - PKI documentations; i.e. drafting of different PKI regulations, policies and Low Level Designs (LLDs) of Root CA, Accredited CA, Registration Authority, and Remote signing platform.
    - PKI documentations; i.e. drafting of different PKI regulations, policies and Low Level Designs (LLDs) of Root CA, Accredited CA, Registration Authority and Remote signing platform.
    - PKI Pilot for eProcurement, a test bed environment and Construction of PKI Data center.

Note: Considering the urgent need to provide PKI services to the Government eProcurement platform, the consulting team recommends to implement the national PKI system with Agile project implementation methodology. This will allow the Government of Malawi to implement a temporary solution for eProcurement and other key online services in 2021.

- Phase II of the PKI project will focus on:
    - Deployment of PKI system in production environment (Primary site)
    - Deployment of PKI system in Disaster Recovery environment (DR site)
    - Testing of the National PKI system and integrating with pilot eGovernment and e-Banking services
- Phase III of the PKI project will focus on stabilization of the established PKI system and awareness to use digital signature in eGovernment, e-Commerce and e-Banking.

Figure8: Summary of the PKI project phases:



Phase 1 ~ 2021
(Present: Planning & Design)

- Establish PKI Governance, Regulations and Executive orders
- Development of Root CA and Accredited CA PKI Policies (CP and CPS)
- Development of Root CA and Gov CA detailed System Architecture
- Recruitment & Training of PKI Engineers
- Construction of PKI Data Center (Production and DR environment)
- Test Bed and temporary PKI solution for eProcurement

Phase 2 ~ 2022
Implementation

- Production Root CA and Accredited CA PKI system
- DR Root CA and Accredited CA PKI system
- Test the Prod and DR Synchronization
- Knowledge Transfer (Know How)
- Integrate pilot eGov Application
- Launch of certification services in Malawi in Government sector

Phase 3 ~ 2023
Promotion & Stabilization

- Extended to other eGov services
- Raise awareness of certification services
- Integrate pilot eBanking Application
- Launch of certification services in Malawi in private sector
- Extended to Private Sector (e.g., financial eBanking)
- Learn from the experience and Plan Long Term PKI services

9 Action plan and Estimate Budget

Table 18: Action plan and Budget

ID	Action	Description	Responsible	Cost (USD)
		PKI Governance		
1	Validate the PKI Framework and secure the budget	– The framework should be validated by the cabinet.	- Ministry of ICT - MACRA	

2	Implement the national Governance structure	Draft a decree and assign the following roles to identified entities:
		– National PKI Policy Authority (PA);
		– Root Certification Authority (Root CA);
		– Government Certification Authority (Gov CA);
			- Ministry of ICT
			- MACRA	

		PKI Consulting services (PKI Documentation, Training and recruitment of an expert)		
3	Recruit a PKI Expert to support the implementation of project	– Recruit a PKI expert to support the implementation of the national PKI project (i.e. from planning, execution and exploitation)/2 years	- MACRA	$ 300,000
	Recruit PKI System engineers	– Recruit a PKI engineers that will manage and run the National PKI system after implementation for 3 years	- MACRA - Nodal Agency	$ 400,000
4	Enhance PKI legal and regulatory framework	– Draft the regulation for certification Authority covering the accreditation criteria, procedure for CA accreditation and auditing of CA accreditation applicant. – Draft the legal requirements for Electronic identification, Electronic stamp (eSeal), Authentication of internet site, Electronic time stamping and Electronic Archiving. – Draft the decree for the Mandatory use of digital signature in e-Government, e-Banking and e-Commerce	- Ministry of ICT - Ministry of Justice - Ministry of Commerce - MACRA	$ 100,000
5	Define PKI policies and procedures	– Draft and the approval of the Root CA Certification Policy (CP) – Draft and the approval of the Root CA Practice Statement (CPS) – Draft and the approval of the Gov CA Certification Policy (CP)	- MACRA - Nodal Agency	$ 150,000

ID	Action	Description	Responsible	Cost (USD)
		– Draft and the approval of the Gov CA Practice Statement (CPS) – Draft and the approval of the National Disaster Recovery Plan (DRP)		
6	Develop LLD PKI system Architectures	– Root CA Low Level Design (LLD) system architecture design – Gov CA Low Level Design (LLD) system architecture design	- MACRA - Nodal Agency	$ 150,000
PKI Data center construction				
7	Design the National PKI data center, Disaster recovery and test	– PKI Data center interior architecture design – PKI data center facilities (i.e. Electricity, physical security, cooling system, etc.…) architecture design; – Network and Security system architecture design.	- MACRA - Nodal Agency	$ 50,000
8	Construction of the National PKI Data center and the disaster recovery	– Supply of the materials and construction of the primary National PKI data center	- MACRA - Nodal Agency	$ 500,000
		– Supply of the materials and construction of the National PKI Disaster Recovery Site	- MACRA - Nodal Agency	$ 250,000
PKI system deployment				
9	Deployment of Root systems (i.e. production, disaster recovery and test)	– Supply and installation of the Root CA systems (i.e. hardware servers and PKI software licenses for production environment) – Supply and installation of the Root CA systems (i.e. hardware servers and PKI software licenses for Disaster Recovery environment) – Supply and installation of the Root CA systems (i.e. hardware servers and PKI software licenses for Test environment)	- MACRA	$ 500,000
10	Deployment of the Gov systems (i.e. production, disaster recovery and test)	– Supply and installation of Gov CA system (i.e. hardware servers and PKI software licenses for Disaster Recovery environment) – Supply and installation of Gov CA system (i.e. hardware servers and PKI software licenses for Disaster Recovery environment) – Supply and installation of Gov CA system (i.e. hardware servers and PKI software licenses for Disaster Recovery environment)	Nodal Agency	$ 2,700,000
Education and Training				

ID	Action	Description	Responsible	Cost (USD)
11	Training of PKI system engineers	– Training of decision makers on PKI policies – Training of PKI operators on PKI technologies (basic and Advanced) – Training of RA and LRAs on certificate Registration applications – Training of application developer on PKI integration	– Ministry of ICT – MACRA – Nodal Agency	$ 100,000
12	Awareness	– Organize workshops and seminars about PKI and the use of digital signature for the General public, in Government and private institutions	– Ministry of ICT – MACRA – Nodal Agency	$ 50,000
Pilot PKI Integration				
16	PKI enabled applications	– Define the integration plan and integrate at least 5 pilot applications with the National PKI system	Nodal Agency	$ 100,000
RA and LRAs				
13	Procedure to issue certificates to subscribers	– Define certificate application registration form and agreement for subscribers	– MACRA – Nodal Agency	
14	RA office	– Establish the RA office	Nodal Agency	$ 20,000
15	Local Registration Authority (LRA)	– Define the Registration Procedure Statement (RPS) template for RA and LRAs	Nodal Agency	
TOTAL COST OF THE NATIONAL PKI PROJECT				**5,366,000**