DIGITAL MALAWI PROGRAM PHASE I: DIGITAL FOUNDATIONS PROJECT

Project ID: 160533

TERMS OF REFERENCE FOR PROVISION OF CONSULTANCY SERVICES AS PUBLIC KEY INFRASTRUCTURE (PKI) TECHNICAL PROJECT MANAGER

1. INTRODUCTION

Information and Communication Technology (ICT) is now globally recognized as an essential tool for promoting competitiveness, job creation, sustainable development, and overall poverty reduction. A combination of widespread access to broadband and a robust ICT services ecosystem can offer a powerful platform for reducing poverty, improving human development and increasing government transparency and efficiency. ICTs have the potential to transform business and government - driving entrepreneurship, innovation and economic growth and breaking down barriers of distance and cost in the delivery of services.

It is in recognition of this ambition that the Government of Malawi is implementing a new project in the realm of ICT – the Digital Malawi Project. In recognition of the critical role that ICTs plays in fostering socio-economic development and empowering the poor, the Government of Malawi secured a loan from the World Bank to implement an ICT Project, referred to as "Digital Malawi". The implementation agency for the project is the Public Private Partnership Commission (PPPC). Other stakeholders include Ministry of Information (MoI), e-Government Department and the Malawi Communications Regulatory Authority (MACRA).

2. DIGITAL MALAWI

The overall aim of the Digital Malawi project is to extend and improve access to critical ICT infrastructure for the public and private sectors; improve ICT governance; improve access to government services; and facilitate provision of e-services thereby enhancing public service delivery.

The project consists of three components, namely; digital ecosystems, digital connectivity (infrastructure), and digital platforms and services (e-Government).

3. OBJECTIVE OF THE ASSIGNMENT

The PKI Technical Project Manager (TPM) will support and oversee the creation of national PKI, planned to be put in place to support e-Government, e-Commerce, e-Banking and Digital Signature Solution. The TPM will be responsible for designing, engineering, and supporting the government enterprise PKI solutions that enable the management and monitoring of Digital Certificates, in line with e-Transactions and Cybersecurity act of 2016 and the Malawi PKI Framework. This will include overseeing the creation of CA (root, Intermediate, subordinate), RAs, X.509 PKI Certificates distribution systems.

4. SCOPE OF work

The TPM will be responsible for the following: -

- Overseeing the creation of National PKI infrastructure at the National Data Centre and disaster recovery site, including the setup of one Signing Certification Authority (CSCA) and Multiple Document Signers (DS) and ensure respective collaboration between various stakeholders.
- Oversee the setup of Certification Authority - root, Intermediate, subordinate, Registration Authority (Public and Private), X.509 PKI Certificates distribution systems.
- Liaise with NRB, Department of Immigration and Citizen services, Mobile Network Operators and other MDAs to ensure that their needs are addressed.

- Provide technical expertise to guide teams from various MDAs on applicable PKI uses and vet team requirements.
- Support piloting and rollout of e-signature solutions across various MDAs by providing guidance to key stakeholders on PKI lifecycle, processes, and procedures.
- Provide inputs into functional requirements and technical specifications to be included in tender documents for procurement of various PKI solutions.
- Contribute to the technical direction on all areas of PKI architecture, including policies, standards strategies, automation, and governance.
- Highlight any issues related to monitoring systems and processes, performing system health checks, maintaining system logs, and troubleshooting of system problems including hardware, application, and operating system related issues.
- Oversee the implementation schedules for system deployments and improvements following defined change control processes.
- Brief senior leadership on all PKI related projects and events.

5. **Essential Skills**
    - Good understanding of current PKI technologies and their future direction.
    - Knowledge of PKI concepts, patterns and practices
    - Recent experience of integrating PKI software and hardware components into customer systems.
    - Excellent understanding of cryptographic concepts: symmetric/asymmetric cryptography, secure hash, digital signatures.
    - Experience with certificate-enabled applications, such as SSL/TLS, authentication, IDAM, EFS, 802.1X, Code Signing, etc.
    - Experience with PKI design, implementation and rollout in a medium to large enterprise environment, including certificate policies and profiles
    - Prior experience with e-signatures, signing portals and Mobile IDs
    - Ability to work with multiple teams to identify common PKI requirements and use cases such as device authentication, email, wireless infrastructure, VPN, TLS etc.
    - Prior experience with commercial PKI vendors

Experience and Education:

- Bachelor's Degree in Computer Science, Cyber Security, Network Security or related field with a minimum of 2 years related experience
- IT Certifications including Microsoft Certifications, CISSP, GIAC, Security+, and ITIL v3 Foundation certifications will be added advantage.
- Excellent verbal and written communication skills and experience writing technical documents such as guides, and other training material related to PKI.
- Project/program management experience in enterprise PKI solution deployment, with use of Agile methodology and environments with automated pipelines.

6. Reporting Arrangements

The successful candidate will report to the Chief Executive Officer, PPPC through the Secretary for e-Government Department and Chief Digital Solutions Architect.

7. Duration of the Assignment:

The duration of the assignment will be 12 months and may extend subject to satisfactory performance of the consultant.

8. Facilities to be provided by the Client:

Project will provide appropriate office space and other associated (data, information, furniture, stationeries, etc.) necessary to carry out the assignment.

9. Reporting requirements/deliverable:

The PKI TPM will need the following reporting requirements/deliverables, but not limited to:

- Monthly work plan and progress reports;
- Written inputs into PKI related technical documentations
- Security key performance indicator (KPI) analysis and control reports;
- Any other reports and briefings to management, as required