Republic of Ghana

Ministry of Communications & Digitalization

Ghana Digital Acceleration Project
IDA CR 7096-GH
(P716126)

Terms of Reference

For

CONSULTANCY FOR THE DRAFTING OF PKI REGULATION

JANUARY,2025

1. BACKGROUND

The Ministry of Communications and Digitalization (MOCD) deployed a National Root Public Key Infrastructure (PKI) for Ghana in 2020. The primary objective of this critical infrastructure is to provide the foundation infrastructure to secure our digital and cyber space for trusted transactions.

Ghana has currently ramped up its efforts in digitalizing its economy. We are systematically migrating the economy from in-person transactions to a digital one. All government services are expected to be fully migrated unto an electronic platform latest 2030. The private sector space is even advanced in migrating most transactions online.

Digital trust is very key if a nation will succeed in the digitalization of its economy. Most international bodies and businesses that have successfully migrated their businesses electronically require most transactions and data to be encrypted or digitally signed if you will transact with them. The PKI technology is now one of the most used and accepted global technology used in securing data and transactions in the cyber space.

Ghana is seeking to migrate not only its transactions but all citizen and business documents to a digital version to promote more efficiency and transparency in doing business. The first major step to achieving this is the passage of the Electronic Transaction Act (ACT 772) which provides the legal mandate for the implementation of PKI and its related technology and services in Ghana. Ghana has proceeded further to deploy the National Root PKI infrastructure.

The National Information Technology Agency is now the agency that operate and manage the National Root PKI infrastructure. Therefore, NITA is the root certifying authority (Root CA) for issuing digital certificates in Ghana. NITA will ultimately determine the validity of every digital certificate in Ghana and will certify "foreign" issued certificates. NITA will license other entities to issue digital certificates as Certificate Service Providers (CSP), who in turn will issue digital certificates to end users in the private sector. NITA is seeking to further strengthen ACT 772 by introducing specific regulations for the PKI industry. This is to support the objectives of licensing and certifying Certificate Authorities to open the market and provide internationally benchmarked practices for the industry.

This consultant for the assignment will also be expected to develop a Request for Proposal (RFP) to solicit proposals from prospective Certificate Service Providers to provide digital certificate services in Ghana after the regulations have been adopted.

2. OBJECTIVES

The objectives of this assignment are as follows:

- Draft a regulation for Ghana's PKI's industry

- Develop RFP to provide digital certificate services in Ghana

The regulations is expected to address the following areas as in the diagrams below.

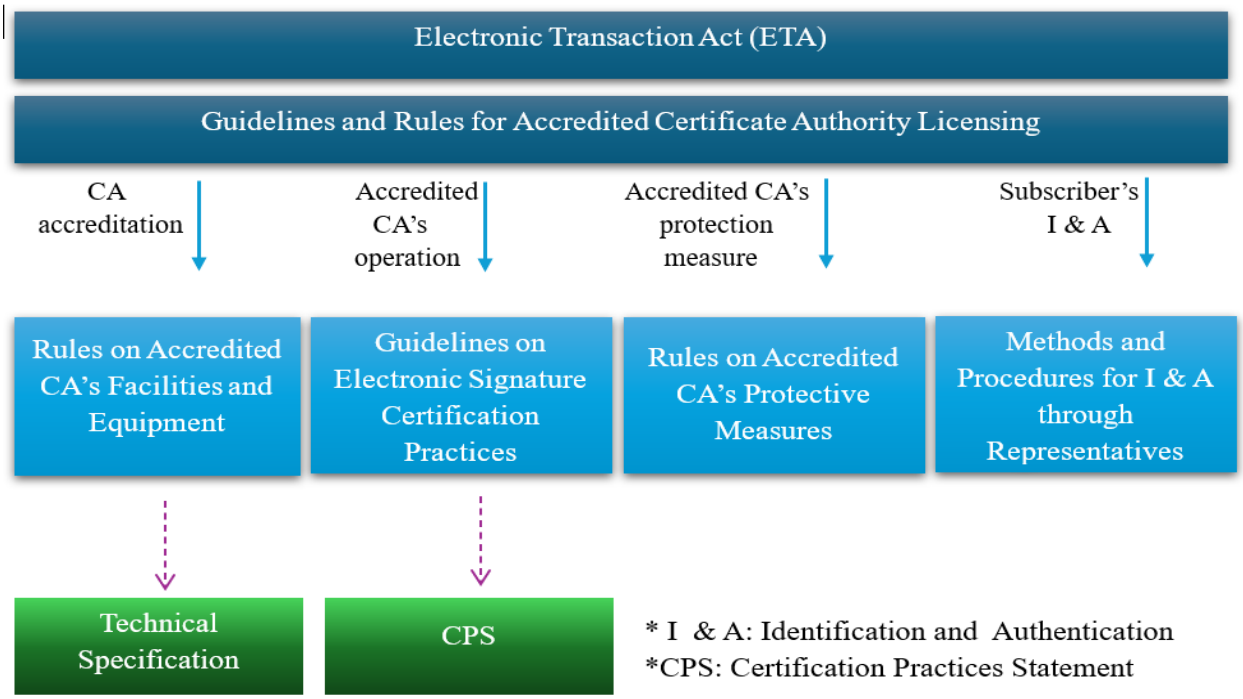

Figure 1

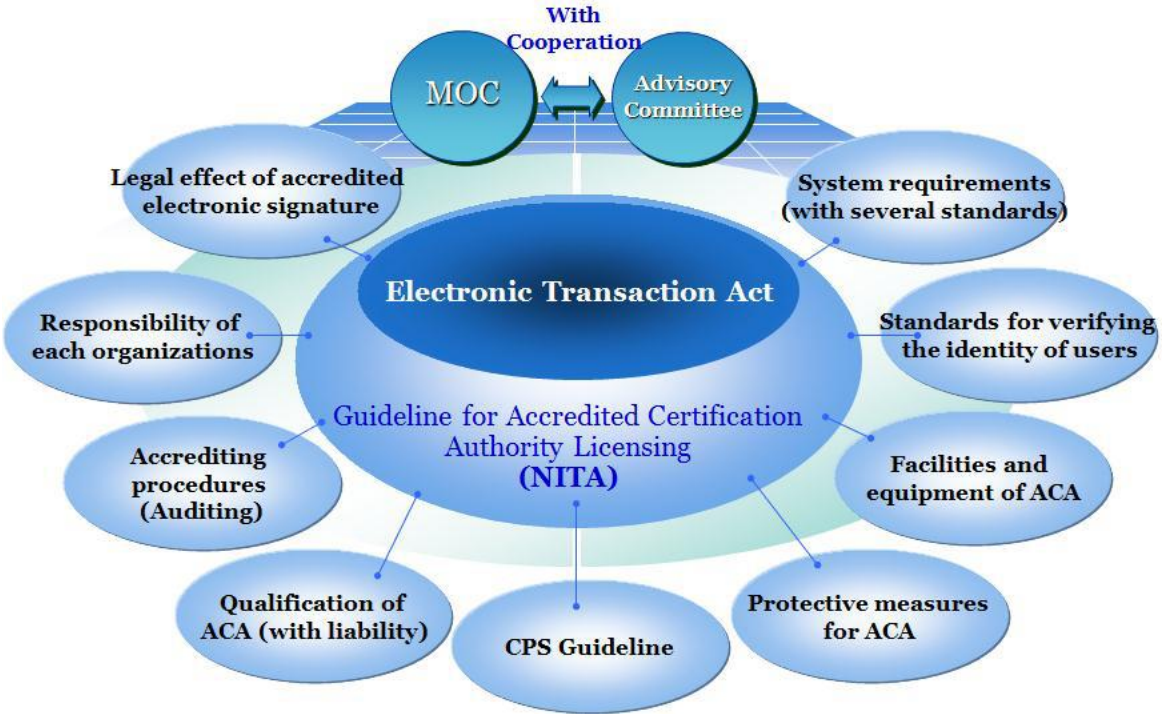

Figure 2

3. SCOPE

The scope of this assignment is in two components. The first component being the development of a regulatory framework and the second component being the development of technical requirement to request for proposals for a certificate authority.

Component 1

- Review of the following documentations
    - Electronic Transaction Act (Act 772)
    - NITA Act (Act 771)
    - Digital Economy Policy Document
    - Ghana Government Enterprise Architecture and Interoperability Framework
    - Cybersecurity Act
    - Data Protection Act
    - Feasibility Study Report for National PKI in Ghana
- Review Ghana's existing PKI architecture and technical specifications.
- Develop an accreditation framework for Certified Authorities (CAs); a detailed accreditation criteria and procedures must be developed to accredit CAs. This should include capital requirement, minimum operators and certification center required to accredit a CA. This framework would include rules on accredited CAs facilities and equipment.
- Help develop forms and template needed for the accreditation process.

- Develop an operational framework for CAs; a detailed operational guideline for CAs to adhere to international operational best practices which will reduce the risk of certificate breaches and its accompanying threats and risk.
- Accredited CAs protection measure; develop rules on accredited CAs protection measures.
- An interoperability framework leveraging architecture principles from the GGEA for accredited CAs; this is to ensure compatibility of signatures and certificate from different accredited CAs and other CAs across the world.
- Compensation Framework that addresses malpractices and non-compliance of CAs resulting in damages to subscribers. The consultant will have to develop this compensation framework per international best practice such as through insurances put in place by CAs.
- Develop a penalty framework for breaches by accredited CAs, Subscribers, Service Providers and other players within the ecosystem; penalties for inappropriate behaviors of CAs, subscriber and service providers must be prescribed. Accredited CA must report the problem to Root CA promptly and prepare a recovery plan.
- Standards and Guidelines.
    - Clear roles and responsibilities of PKI-related authorities must be defined.
    - Detailed criteria of Certificate Practice statements must be issued.
    - Standards of digital signature authentication technology must be developed.
    - Detailed guidelines for the facilities and equipment of the CA must be issued.
    - Detailed guidelines for operations of the CA must be issued. This should include among other things Certification Service, Key Management, Document and Record Management, Test of Operations and Information Providing, Network and Systems, Disaster Recovery and Business Continuity Process.
    - Certification Authority evaluation criteria and detailed criteria of regular audits must be issued.
- Subscriber's identification and authentication procedure; a clear definition of identification requirement for the issuance of a certificate. In this case, all different certificate scenarios must be considered, and identification requirement spelt out clearly for each scenario. Ghana's identification laws must serve as the basis for this. (scenarios like person, entity, device, etc. identification must be considered)
- Identify stakeholders within the PKI domain and carry out both pre-regulation and post-regulation drafting stakeholder engagement. These workshops shall be sponsored as part of the project cost which will be borne by the consultant.
- Carry a study to benchmark regulation practices and models of at least 3 countries including India, South Korea, Singapore and UAE.
- Carry out a study to map out the PKI market in Ghana and identify applications of the PKI services per sector of the economy like government, energy, education, health, finance, security, etc.
- Develop guidelines on Electronic Signature certification practices. The object of this guideline is to lay down details of what certification authorities must observe in

performing certification services by means of asymmetric encryption to ensure safety and reliability of certification practices in accordance with Section 8 of the Electronic Signature.

- Methods and Procedures for Identification and Authentication through representatives.
  - The purpose of this notification is to define the method and procedure of certification authorities' identifying those who want to have a certificate issued by the representative in accordance with the provisions of the latter part of Clause 1 of Section 15 of the Electronic Signature Act and Clause 3 of Section 13-2 of the Enforcement Regulations of the same Act.
  - Draft an outline for a Certificate Practice Statements (CPS) which will be adopted by the root and accredited CAs. The CPS outline should contain information on, for example, management of certificates and key pairs, supplementary services, RA management, and audit management.
  - Identify all the areas of standardization required in the operations of National PKI for both the root and accredited CAs. Draft of the identified CAs should also be submitted for review and possible adoption at the national level in consultation with the Ghana Standards Authority.
  - Develop Technical specifications for interoperability for Certification Authorities.
  - Develop guidelines for the exit and ending of operations by a CA. This will include mergers and takeovers. The guidelines should have a comprehensive laid out plan on activating the intent with the regulator through to when the exit, merger or takeover happens. The guideline should address how already issued certificates will be handled without subscribers security being compromised.
  - Meet with key contacts in government and other institutions, identified as key to this assignment.
  - Organize and participate in all pre-drafting and post-drafting stakeholder engagement workshops to take input and discuss draft proposals for the regulations.
  - Write an interim report for each planned framework and provide a presentation of interim reports at workshops.
  - Collect comments on each draft report or framework and make consequential revisions in the final versions.

Component 2

- Develop technical requirement for operating a Certificate Authority. This should include the requirement for facilities, equipment, operational processes, and all other requirements needed to certify and license a Certificate Authority.
- Staff requirement for the operation of Certificate Authority
- An evaluation criterion that will be used in the selection process of a certificate criteria.
- Develop a Request for Proposal (RFP) for soliciting for Proposals from prospective Certificate Service Providers (CSP)

4. REPORTING AND TIME SCHEDULE

This assignment is expected to take up to five (5) months duration. The consultant will report to the Chief Director of the Ministry of Communications and Digitalization through the Director General of NITA.

The reporting requirements and deliverables are as follows.

Deliverable	Subject	No. of Weeks from start of assignment	Percentage of contract amount payable
Report	Inception Report	2	15
Workshop 1	Initial stakeholder engagement to present the inception report and take their feedback and input.	4	0
Draft Regulation	First Draft regulation for PKI	12	20
Draft RFP	First Draft RFP document to the Client	12	0
Workshop 2	Stakeholder engagement to discuss the draft regulation and take their input on the draft document	15	0
Final Draft for the PKI Regulations	This will be the final draft of the Regulations for PKI after comments from all stakeholders have been incorporated into the initial draft.	18	30
Final Draft Request for Proposal (RFP) Certificate Service Providers	This will be the final draft of the RFP after comments from client has been incorporated into the initial draft.	18	25
Report	Project Closeout Report	20	10

4.1. Conformance to Performance Based Conditions (PBC)

The activity is a Performance Based Condition activity and will require that verification of results and payment for deliverables will conform with the steps agreed upon in the Project Appraisal Document (PAD), the Project implementation Manual (PIM) and the Financial Agreement and the ToR for the Independent Verifier.

As part of the disbursement procedures, an advance to be determined, will be made available for the implementation of the PBCs activities. An Independent Verification Agency, who will be selected competitively will verify results, using the verification protocols outlined in the ToR for the Independent Verifier before subsequent disbursements are made.

The PCU will work with the responsible beneficiary institution to ensure achievement of planned results. Eligible expenditures under PBCs will cover cost of goods, works, non-consulting services, consulting services, incentive schemes, incremental operating costs, and training.

5. PROFILE, EXPERIENCE AND QUALIFICATION OF CONSULTING FIRM AND KEY STAFF

The consultant is expected to be a reputable consultancy firm. The Consultant will be selected Based on experience and capacity in carrying out this type of work. The consulting firm(s) must meet the qualification requirements of at least 10 years of professional experience in developing regulations in the telecommunication and tech industry with some specific experience and knowledge in PKI infrastructure, services, and operations. Experience in Africa or other developing countries will be an added advantage:

The firm will provide a team comprising of the following.

Lead Consultant, Legal and Regulatory Expert

- The Lead Consultant should be holding a first degree or master's degree in law specialising in regulatory, commercial law or company law or relevant area from a recognized University and have a proven, extensive experience of at least 10 years on telecommunication/ICT regulation related issue, with a particular emphasis on PKI technology and cyber security related area.
- The Lead Consultant should have rich experience in PKI technology, digital certificate services and operations of Certificate Authority.
- He/she should have experience drafting regulations in the area of telecommunication, Fintech, eCommerce or other related areas.
- He/she should have a demonstrable track record in project management and in coordinating large diverse teams/stakeholders, in a complex working environment.
- Excellent command of English and report writing skills are required.

PKI Technology Expert

- The PKI Technology Expert should have appreciable demonstratable knowledge with the PKI technology.
- He/she should have experience with PKI related services like electronic signature, device certificates, SSL
- He/she should have experience with the operations of Certificate and Registration Authorities.
- He should have good knowledge of the regulations of at least 3 countries where certificate services is well established.

Project Management Support Officer

- He/She should hold a degree in ICT field from a recognized University and have proven experience of at least 5 years of providing project management support on telecommunication/ICT projects.
- Years of experience to be proved by academic certificates and signed detailed curriculum Vitae.
- Must have proven skills and experience in project management tools and be able to provide project management support to the project.
- Excellent command of English and report writing skills are required.
- Any other relevant qualification and experience will be an added advantage.