REPUBLIC OF KENYA

COUNTRY: KENYA
PROJECT: KENYA DIGITAL ECONOMY ACCELERATION PROJECT (KDEAP)
IMPLEMENTING AGENCY: Information and Communications Technology Authority (ICTA)
PROJECT ID: P170941; Credit Numbers 7289-KE and 7290-KE

TERMS OF REFERENCE

FOR:

Request for Expression of Interest for: Consulting Services for Review, Assessment and Provision of Professional Recommendation on the Current Deployment of the National Public Key Infrastructure (NPKI)- Government Certification Authority (GCA) in compliance to on E-CSP Regulatory Compliance (Individual Selection)

Contract No: KE-ICTA-438071-CS-INDV

Issue Date: 12th November 2024

Closing Date: 28th November 2024 at 10:00AM

Client:
The Chief Executive Officer,
ICT Authority
Telposta Towers 12th Floor, Kenyatta Ave
PO Box 27150 - 00100 Nairobi Kenya
Tel: +254 20 2089061/ 2211960 Fax: +254 20 2211960
Email: procurement@ict.go.ke , info@icta.go.ke
Website: www.icta.go.ke

1. BACKGROUND

The Government of the Republic of Kenya (GoK) has received financing in the amount equivalent to US$390 Million equivalent from the World Bank towards the cost of the first phase of the Kenya Digital Economy & Acceleration Project and it intends to apply part of the proceeds to payments for goods, works, non-consulting services and consulting services to be procured under this project.

The project will include the following components as included in the Project Appraisal Document (PAD).

Component 1: Digital Infrastructure and Services: The aim of this component is to increase access to high-speed internet for individuals, industry, and government—the 'foundation of the foundations' of a digital economy and strengthen Kenya's role as regional digital leader—while leveraging investments from the private sector

Component 2. Digital Government and Services: This component will invest in the foundational digital services, platforms, architectures, and policies needed to transform the way the Government communicates and conducts its internal operations.

Component 3. Digital Skills and Markets: This component aims to equip young Kenyans with digital skills and strengthen their abilities to access and compete in domestic and regional markets through supporting skills development, to study mechanisms to improve access to affordable devices and through enhancing the enabling environment for e-commerce to support Kenya's role as a regional digital hub.

Component 4. Project Management: This component will support project implementation, coordination, for the Project Implementation Unit (PIU) within ICTA and capacity building.

Component 5: Contingent Emergency Response Components: This component will be activated in the event of an emergency. The Gok intends to apply a portion of the proceeds of the Credit to cover activities under sub-components 1.5 (Enhancing Regional Digital Integration). The project aims to accelerate digital transformation at the regional level focusing on critical digital enablers that 'future-proof' economic growth and leveraging Kenya's leadership role in the region to facilitate the adoption and implementation of regionally harmonized frameworks for digital integration.

2. NATIONAL PUBLIC KEY INFRASTRUCTURE CURRENT STATE.

The Ministry of Information, Communications and the Digital Economy through the ICT Authority as a licensed Electronic–Service Content Provider (E-SCP) and as the Government Licensed Certification Authority (GovCA) and the Communication Authority (CA) as the regulator and the Root Certification Authority (RCA) have implemented the National Public Key Infrastructure (NPKI).

The NPKI system is a critical component for securing Kenya's e-commerce and Digital Economy as it assures both the safety and integrity of electronic transactions and online services for the Kenyan public such as e-government, e-commerce, e-health, e-tax, e-insurance, e-learning, amongst others and ultimately spurring e-commerce and digital trade. The same forms a very integral part of the Government's Digitalization agenda and supporting the secure adoption of e-government services.

The National Public Key Infrastructure (NPKI) Government Certificate Authority (GCAs) Infrastructure as is currently implemented does not have any inbuilt design resilience and or an Active Disaster Recovery (DR) facility. In the just concluded recent annual E-CSP Audit and Compliance report conducted by the Regulator; Communication Authority (CA), this has been flagged and identified as one of the key risk issues associated with the National Public Key Infrastructure (NPKI) Government/Sector Certificate Authorities platform. In its recommendations, the Regulator (See attached annex report) stated that; **A government's National Public Key Infrastructure (NPKI) needs built-in resilience and high reliability for successful digitization efforts**. This is meant to ensure that;

a) **Security for Critical Infrastructure:** NPKI serves as the foundation for secure digital interactions between citizens, businesses, and government agencies. Any downtime or malfunction disrupts critical services like e-governance, e-payments, and online tax filing.
b) **Online Digital Trust and Confidence:** A reliable NPKI fosters trust and confidence in digital services. Users expect consistent availability and dependable security to ensure their data and transactions are protected.
c) **Security incidents:** A resilient NPKI that can withstand incidents and maintain operations, minimizing disruption and protecting sensitive government data.
d) **Economic Impact:** Downtime in NPKI can have a significant economic impact, hindering business operations and hindering citizen access to essential services.
e) **Global Reputation:** A robust NPKI demonstrates a government's commitment to digital security and positions it as a leader in e-governance.

In essence, a resilient and highly reliable NPKI is essential for secure, efficient, and trustworthy digitization, safeguarding critical infrastructure, promoting economic growth and fostering a positive national image. A resilient and highly reliable NPKI is essential for secure, efficient, and trustworthy digitization, safeguarding critical infrastructure, promoting economic growth, and fostering a positive national image.

3. OBJECTIVE OF THE ASSIGNMENT

The primary objective of this consulting services is to review the implemented National Public Key Infrastructure (NPKI) at the ICT Authority in alignment to the audit findings of the 2023/2024 Annual E-CSP Audit report and develop a plan to implement the recommendations of the audit findings, specifically regarding resilience, high availability and redundancies in line with best practices for NPKI Implementation. (See annexe 1). As part of the exercise, the consultant will review, access and analyse the deployed NPKI technology at the ICT Authority and recommend, advise and propose the best in practice model deployment and how to transition from the As-Is environment to the development of a powerful, and appropriate National Public Key Infrastructure NPKI, with high Availability, secure architecture and services with in-built resilience The scope of services, consultant profile, reporting requirements and other particulars of the assignment are detailed below.

4. SCOPE OF SERVICES AND SPECIFIC TASKS

As per the E-CSP Audit Findings report, the Consultant's scope of work will entail the following tasks:

a) **Carry out the NPKI-GOVCA "As is Analysis":** The consultant will carry out an "As-is analysis" of the current NPKI to clarify exactly how the ICTA NPKI-GOVCA process works today, including any issues or inefficiencies. By analyzing the current state, the consultant will identify the infrastructures' operational efficiency and effectiveness as well as areas and opportunities for improvement.

b) **Evaluate the NPKI-GOVCA Needs and requirements:** The consultant will evaluate and Analyse the current landscape of the ICT Authority's deployed NPKI & digital certificates and trust services. He/she will Identify potential use cases and benefits of the implemented National NPKI and the alignment to the Government's Digitalization & E-Services Roadmap.

c) **Assess the NPKI-GOVCA /Sustainability Requirements:** The consultant will assess the technical architectural deployment of the NPKI implemented, considering existing infrastructure, resources, including best practice and design set-up and the need for Disaster Recovery Centre to provide a resilient, highly available Core Software, Compute, Networking, Storage infrastructure to support the operation of ICTA/GOVCA's.

d) **Conduct the NPKI-GOVCA Costs and Benefits:** The Consultant will conduct the economic and financial feasibility of NPKI implementation, including potential costs and benefits as well as Identify Risks and Challenges.

e) **Undertake a Pre-Upgrade on the GOVCA-NPKI System and Service Audit -** The Consultant will undertake a Gap assessment of the current NPKI system, the network system, server system and NPKI solution system, including related hardware, their configuration, as well as software system and the existing standard operation procedures (SOP). He will then make recommendation on upgrade options available based on the findings.

f) Identify potential risks and challenges associated and or inherent within the current NPKI implementation.

g) **Develop a Roadmap:** Develop a high-level implementation plan with timelines and resource requirements. Recommend the optimal NPKI model for ICTA based on the feasibility assessment.

h) Recommend the optimal NPKI model for ICTA based on the technical assessment.

i) Development of procurement document for the establishment of the recommended solution

5. DURATION AND LOCATION OF THE ASSIGNMENT

The duration of the assignment shall be three (3) calendar months from contract commencement date. The location of the assignment will be in Nairobi, Kenya.

6. REPORTING REQUIREMENTS AND TIMELINE FOR DELIVERABLES

This is a lumpsum contract where the consultant will provide any other expected expertise, and resources required to achieve the deliverable of the assignment. Based on the tasks required for this assignment, the consultant will provide ICTA with the following reports:

Table 1: Reporting Requirements and Timeline for Deliverables

OUTPUTS/ DELIVERABLES	**DESCRIPTION**	**TIMELINE FOR SUBMISSION OF DELIVERABLES AFTER CONTRACT COMMENCEMENT**	**Format of presentation**
Inception Report	This report will provide details of the consultant's understanding of the assignment as well as the methodology and approach to be employed to complete the assignment, with clear and detailed milestones for implementation;	2 Weeks	3 hard copies and 1 digital copies
Detailed assessment report on Current status of the NPKI.	The consultant shall perform the initial NPKI system review, assessing existing NPKI hardware and software systems, and provide the assessment report indicating the identified gaps, issues, and other related queries. This should include an overview of the existing users by category as well as description of future use cases with projections of future demand, in support of recommendations for the PKI upgrades and scale up.	4 Weeks	3 hard copies and 1 digital copies
Detailed Technical E-CSP Audit report Compliance plan:	The Consultant will provide a compliance implementation road-map and design plan that will focus and provide for required implementations for the closure and attainment of the best practise and resilience as well as high availability NPKI Set-up.	8 Weeks	3 hard copies and 1 digital copies

OUTPUTS/ DELIVERABLES	**DESCRIPTION**	**TIMELINE FOR SUBMISSION OF DELIVERABLES AFTER CONTRACT COMMENCEMENT**	**Format of presentation**
Detailed Design "as to be Architecture	The Consultant with Provide a Detailed "as to be Architecture", taking into account the need for Compliance to the E-SCP licensee audit report and all the listed incompliance aspects (See attached annexe1)	10 Weeks	3 hard copies and 1 digital copies
Final report & Slide Presentation to key stakeholders and decision-makers	This will be the consultant's Final Report, which will serve as a comprehensive document Review, Assessment and Provision of Professional Recommendation on the Current Deployed National Public Key Infrastructure (NPKI) Government Certification Authority (GCA). It will showcase the consultant's work and provides a clear picture and insights into the following key aspect; a) Operational Efficiency Report: b) Inherent NPKI set-up Risk. c) Regulatory compliance d) Alignment to NPKI Best Practice on Security engineering. e) Disaster Recovery and High Built-in Resilience and Availability. f) Compliance Report – Findings on Assessment of compliance with relevant standards and regulations, including KICA and ISO/IEC 27001. g) Design Architecture Recommendations h) Follow-up Plan - Recommendations for continuous monitoring and improvement	12 Weeks	3 hard copies and 1 digital copies

All draft and final reports shall be submitted in the prescribed format to:

The Chief Executive Officer,
ICT Authority
Telposta Towers 12th Floor, Kenyatta Ave
PO Box 27150 – 00100
Nairobi Kenya
Tel: +254 20 2089061/ 2211960 Fax: +254 20 2211960
Email: procurement@ict.go.ke , info@icta.go.ke
Website: www.icta.go.ke

Attention:
The Project Coordinator
KDEAP

Upon submission of every report, the consultant is expected to make a presentation of the submitted report to the Client in a scheduled meeting. The acceptance of the report shall be recorded in the minutes of the meeting.

7. PAYMENT SCHEDULE

The proposed payment schedule based on satisfactory performance of the contract which will be negotiated with the successful consultant will be as presented in Table 2 below.

Table 2: Payment Schedule

S/No.	Deliverables	Timelines after contract commencement	Percentage of the Lump-Sum contract amount
1.	Submission and Acceptance of Inception Report	2 Weeks	20%
2.	Submission and Acceptance of the Detailed assessment report on Current status of the NPKI.:	4 Weeks	20%
3.	Submission and Acceptance of the Detailed Technical E-CSP Audit report Compliance plan:	8 Weeks	20%
4.	Submission and Acceptance of the Detailed Design “as to be Architecture.	10 Weeks	20%
5.	Submission and Acceptance of the Final report & Slide Presentation to key stakeholders and decision-makers.	12 Weeks	20%

Upon submission of every report, the consultant is expected to make a presentation of the submitted report to the Client and the ICT Authority in a scheduled meeting. The acceptance of the report shall be recorded in the minutes of the meeting.

8.0 MINIMUM QUALIFICATIONS AND EXPERIENCE REQUIREMENTS OF THE CONSULTANT

The consultant shall have the following minimum qualifications and experience requirements:

a) **Qualification:** A minimum of a Master's degree in computer science, Cybersecurity, Science/Technology and/or other relevant fields.
b) **General Experience:** A Minimum of 7 years of experience in Cybersecurity program Experienced with FIPS-certified smart cards, HSMs, FIDO-based U2F and UAF tokens, and OATH-based algorithms for TOTP and HOTP protocols.
c) **Specific Experience:** At least five (5) years of experience in risk management and CIIP, preferably at the national level. **PKI Infrastructure Compliance Audit:** Specific experience in leading an audit and compliance efforts for digital trust services, ensuring adherence to frameworks such as Web Trust, SOC 2, and CCA or similar.
d) **Registration/certification:** Relevant certifications, such as **CISA** (Certified Information Systems Auditor) professional certification offered by ISACA (Information Systems Audit and Control Association), or **Certified Lead auditor in ISO 27001**, or Security Manager **(CISM),** or Certified Critical Infrastructure Protection Professional (CCIPP).

9.0 Management and Accountability of the Assignment

The Consultant will be contracted by The ICT Authority, who will manage payment and sign-off of deliverables. All deliverables should be submitted to the Project Coordinator. Written deliverable should be submitted electronically in PDF and editable Word format, allowing for comments/edits to be made.

The ICT Authority shall provide the following to the best of their ability:

- All background data and literature considered relevant for accomplishing or informing the assignment and completing identified tasks at their immediate disposal.
- Access to key officials within the relevant Ministries/Agencies/department and other relevant official entities, as applicable.

10.0 CLIENT'S RESPONSIBILITIES

The consulting services must ensure that the tasks identified above are performed in a result-oriented manner with the sole objective of achieving outputs and outcomes expected from the assignment as has been described in the details above. The consulting services is encouraged to utilize local expertise where appropriate.

The Consultant shall be responsible for the provision of all the necessary resources to carry out the services such as international travel, project transportation for visits in counties, subsistence allowances, accommodation, information technology, and means for communications, reporting materials, insurance and any other required resources. The consultant is expected to undertake activities that will ensure that outputs are consistent with the professional and legal requirements. All outputs will be presented using modern techniques/technology. It is also required that the data is generated through a consultative process that guarantees authenticity and ownership.

11. 0 KNOWLEDGE TRANSFER

Knowledge transfer is considered an integral part of this assignment and should be reflected in the consultant methodology. Ideally, Government should be able to learn how to replicate / update key element of the assignment, if needed, in future.

12. 0 STAKEHOLDER CONSULTATION

The Consultant is expected to engage in stakeholder consultation to deliver the assignment, which should be documented, and shared with Gov agency and WB.

References: http://rootca.go.ke/policy.html
https://www.ca.go.ke/index.php/license-application-forms-fees
E-CSP Technical Rollout Requirements in Kenya
Web trust Accreditation Baseline

END OF TOR