Terms of Reference

"Republic of Cameroon – Strengthening Cybersecurity Foundations" Technical Assistance

Contract type	Consultant (firm)
Expected start date	September 2024
Duration of the assignment	9 months

I. BACKGROUND

1. The World Bank (WB) has been assisting the Government of Cameroon (GoC) with advancing a trust framework needed to bring more individuals, and public and private sectors to transact online. The Acceleration of the Digital Transformation of Cameroon Project (PATNUC)[1] financed by the WB aims at increasing digital inclusion and the use of digital agricultural solutions by selected agricultural value chain actors. Among other activities, modernization of legal and regulatory framework to promote digitalization and stregnthening of nation cybersecutiy capabilities are in scope. The WB is also helping the Government modernize (and digitalize) identification and civil registration ecosystem to improve access to and the delivery of public and private services.[2]

2. The GoC has been advancing over the years in building a trust framework needed to bring more individuals, and public and private sectors to transact online: the Law of 2010 (2010-012) on Cybersecurity and Cybercrime, the Law on E-commerce (2010-021), and the Decree (2019-150) on the organization, functioning, and mandate of the National Agency for Information and Communication Technologies (*Agence Nationale des Technologies de l'Information et de la Communication*, ANTIC), the main regulatory and implementing agency for handling cybersecurity and domain names, as well as regulating electronic activities across the Government. In 2018, the National Cybersecurity Strategy (*Politique Nationale en matière de Protection, de Sécurité des Réseaux de Communications Electroniques et des Systèmes d'Information, de Certification et d'Audit de Sécurité*) was developed ; however, it is yet to be operational. In 2019, a Cybersecurity Capacity Maturity Model (CMM) assessment was conducted by WB in partnership with the Global Cyber Security Capacity Centre and recommended the maturity level was at the start-up level.

II. ASSIGNMENT OBJECTIVES

3. The objective of this assignment is two-fold:
   (i) Help the GoC revise the National Cybersecurity Strategy and strengthen the capacity of key entities to prevent, mitigate, and respond to cyber incidents.
   (ii) Assess the feasibility of implementing e-signatures at a national level. The assignment should cover key aspects such as the technical, legal, and operational requirements, the benefits and challenges, as well as the potential impact on e-transactions and interactions. The assignment should include the assessment of the existing public key infrastructure (PKI) and if it needs to be scaled up for the implementation of high-trust electronic signatures; various PKI implementation approaches and architectures should be considered.

[1] The project is implemented by the Ministry of Posts and Telecommunications (*Ministère des Postes et Télécommunications*, MINPOSTEL), the Ministry of Livestock, Fisheries and Animal Industries (*Ministère de l'Elevage, des Pêches et des Industries Animales*, MINEPIA), and the Ministry of Agriculture and Rural Development (*Ministère de l'Agriculture et du Développement Rural*, MINADER).

[2] See the findings of the ID4D Diagnostic: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099012324023052410/p1795471b60b614c14d0214b971aed2105a95cebf79b

III. SCOPE OF WORK

4. The Consulting firm (henceforth 'Consultant') will work under the direction of the WB Task team to deliver the following:

Workstream I:

1. Conduct a gap analysis, starting with the cybersecurity of digital infrastructure in Cameroon, based on international standards and best practices (e.g., e.g., OECD, ITU, NIST) adapted to Cameroon's context as needed;
2. Following the gap analysis, provide clear and actionable policy recommendations.
3. Support the update of Cameroon's national cybersecurity strategy based on the gap analysis and policy recommendations;
4. Provide a phased roadmap based on the national strategy with clearly defined short-, medium-, and long-term cybersecurity priorities tailored to Cameroon's cyber risk and level of cybersecurity maturity and an action plan for implementation (including a framework allocating roles, responsibilities, and general principles);
5. Conduct in-person and/or virtual capacity-building workshops for a large audience of relevant government stakeholders presenting the findings and recommendations of the analysis, strategy, and roadmap. Prepare relevant materials, such as presentations; and workshop reports, identify and help secure participation of high-profile international cybersecurity experts; participate in the workshop under a discussant and/or moderator roles, etc.

Workstream II:

1. Conduct a stakeholder mapping to identify key stakeholders of the development of trust services, including public- and private-sector providers and relying parties, as well as individuals and civil society representing a diverse array of users;
2. Assessment of public and private sector needs for secure and trusted electronic transactions in Cameroon (including e-signatures) and development of use cases and legal and technical requirements for a risk-based approach to e-signature assurance promoting international mutual recognition;
3. Evaluate the current trust framework for e-signatures and trust services and conduct a gaps analysis against the assessed use cases and requirements;
4. Provide recommendations for improvements to the trust framework for e-signatures and trust services to address identified gaps while also promoting alignment with international standards, and facilitating the development of markets for e-signature and trust services;
5. Develop requirements for a robust, scalable and sustainable PKI architecture to facilitate improved security and privacy for electronic transactions and promote the adoption of electronic signatures by public and private sectors;
6. Conduct a market assessment for local and regional providers of PKI and trust services, including public and private sector actors;
7. Create an implementation roadmap for putting in place the e-signature and PKI architecture
8. Conduct one or several in-person workshops with stakeholders within and outside of government to build capacity and dissemination of deliverables, to ensure adoption and buy-in across Government stakeholders. Prepare relevant materials, such as presentations, and workshop reports, participate in the workshop under a discussant and/or moderator role, etc.

5. The Consultant should notify the WB Task team about areas that, in its view, may need complementary analysis or that could be beyond the Scope of Work as set forth above. The Consultant will also be responsible for identifying information necessary to ensure the successful execution of the mandate, and to assure an exhaustive and comprehensive analysis of all technical and regulatory issues affecting the study.

IV. DETAILED CONSIDERATIONS WORKSTREAM II

Electronic Signature Ecosystem

- *Risk-based approach:* The e-signature ecosystem should implement a risk-based approach to cater to various use cases, each associated with different levels of risk and therefore requiring different levels of assurance. This can help balance the need for security with the goal of broad accessibility and adoption. Such a tiered approach could help to ensure that the benefits of e-signatures are accessible to all, not just to those with advanced technical capabilities, while also ensuring sufficient security for high-risk transactions.
- *Interoperability:* The e-signature ecosystem should be compatible with different types of digital documents and systems. In particular, compatibility with the ID systems must be assured. This requires adherence to widely accepted standards and protocols that enable seamless integration and data exchange.
- *Alignment with Standards.* The e-signature ecosystem should promote alignment with existing frameworks and standards at local, regional, and international levels, with the aim of laying the foundation for mutual recognition of e-signatures across sectors and jurisdictions.
- *Technology Neutrality.* The e-signature ecosystem should adopt a technology-neutral approach to ensure flexibility and adaptability in the face of rapidly evolving technological advancements. It encourages innovation by allowing for the incorporation of new technologies as they emerge and become validated. This approach also helps avoid potential issues of obsolescence, vendor lock-in, reduced competition, or excessive reliance on certain implementation models for all types of transactions.
- *Inclusion:* The system should be designed to reach and cater to all demographics, including those without access to the internet or digital devices, rural populations, people with disabilities, the elderly and other vulnerable groups. In particular, there should be planning for registration and issuance of e-signature accounts and devices.

National Public Key Infrastructure

- *Tiered Assurance Levels:* The national PKI implementation should operate on the premise of a national e-signature trust framework with tiered levels of assurance, where not all e-signature applications will need the high security provided by a PKI.
- *Interoperability:* The PKI should be designed to be interoperable with other systems, both within the country and internationally. This can facilitate cross-border transactions and future integrations with other systems.
- *Private Sector Participation:* Consideration should be given to private sector participation in providing some elements of the PKI, for example, by acting as Certificate Authorities (CAs) or Registration Authorities (RAs), or both, if this can promote competition, innovation, security, scalability, and resilience or lower costs.
- *Security and Trustworthiness:* Security is paramount in a PKI system. Strong measures to prevent unauthorized access, data breaches, and cyberattacks should be implemented. The system should also be transparent and accountable to build trust.
- *Scalability and Flexibility:* The system should be scalable to handle increasing usage over time. It should also be flexible to accommodate new technologies and security practices as they evolve.
- *Accessibility and Usability:* The system should be accessible and easy to use for all citizens and individuals. This may involve user-friendly software interfaces, device form factors, and support services.

- *Certification and Accreditation:* Processes for certification and accreditation of CAs and other entities involved in the PKI should be robust, transparent, and independent. Alignment with international standards, such as for trust service providers, should be explored.
- *Risk Management:* Implement a strong risk management framework, considering potential threats to the security and integrity of the PKI and mitigating measures.
- *Revocation and Recovery:* Establish processes for certificate revocation and key recovery in case of loss, compromise, or changes in user information.

V. METHODOLOGY

6. The Consultant is expected to use its professional experience and own judgment with regard to developing the methodology for this assignment and document accordingly in its technical proposal, alongside the following, but not limited to, requirements: (i) a proposed schedule needed to carry out the assignment in high quality within the stated timeframe; (ii) the estimated number of man-days required to accomplish all tasks and the proposed staffing (detailed CVs), (iii) any proposed associations or subcontracting, if required, along with detailed information on the expertise of the contractors on the tasks and topics of this tender including references to previous, relevant project, (iv) identification of possible risks and suggestions for mitigation, (v) identification of proposed modifications to be made to these Terms of Reference, (vi) proposed cost estimate, provided separately in the financial proposal.

7. The WB may be able to facilitate introductions to key stakeholders based on existing relationships; however, this should not be the default assumption for the Consultant. The WB may also contribute additional relevant data and information related to this assignment and may participate in select stakeholder discussions. Any dissemination and capacity-building workshops shall ensure a broad understanding of the GoC's strategy and roadmap and help clarify various actors' expectations, actions, roles, and responsibilities, and should be held virtually and/or in-person at a suitable local time. The results of the outputs will be consulted upon and validated by relevant stakeholders.

VI. DURATION, DELIVERABLES, AND PAYMENT SCHEDULE

8. The assignment should be completed within a maximum period of nine (9) months from the date of the contract signature.

9. The deliverables expected of the consultants are as follows:

N°	Deliverables	Payment (%)
D1	Inception Report including work plan and timelines	10%
Workstream I		
D2	Gap analysis report (incl. policy recommendations)	20%
D3	Draft National Cybersecurity Strategy (incl. implementation roadmap)	
D4	Action plan for strategy implementation report	20%
	Validation & dissemination workshop presenting the findings and achievements of the assignment (Workstream I)	
Workstream II		
D1 & D2	Stakeholder mapping, assessments of needs, and use cases (incl. legal and technical requirements) report	20%
D3 & D4	Evaluation & gap analysis of the current trust framework for e-signature and trust services, and recommendations for improvement	

D5 & D6	Requirements for scalable and sustainable PKI architecture & market assessment of local and regional providers of PKI	20%
D7	Implementation roadmap for e-signature and PKI architecture	
	Validation & dissemination workshop presenting the findings and achievements of the assignment (Workstream II)	
D8	Final Report (Workstreams I & II)	10%

10. **For the fulfillment of this consultancy, in-country travel (at least three missions—kick-off, consultations, validation, and dissemination workshops) and local presence are highly encouraged.**

11. All final written deliverables should be electronically submitted to the WB Task Team Leader (TTL) in French and English, proofread, and well-formatted in MS Office formats.

12. These deliverables should be structured and authored in an easily understandable fashion and be consistent with the WB's editorial style guide available at https://openknowledge.worldbank.org/handle/10986/33367. These deliveries will be used to support strategic communication and decision-making between the GoC and the WB Task Team. Other than the submission of the deliverables, the Consultant shall regularly communicate with the TTL.

VII. FIRM QUALIFICATIONS

13. The Consultant shall be a firm or consortium of firms (subcontracting other individuals and firms as needed).
14. Proven and successful track record in carrying out similar assignments, particularly in the area of cybersecurity policy consulting, cybersecurity capacity, and skills gap assessments, development of trust framework, e-transactions, e-signatures, and PKI.
15. Key project team members shall consist of experts with recognized cybersecurity certifications and technical experts with a proven track record in carrying out similar assignments and demonstrated knowledge of international standards and best practices in cybersecurity and trust framework for e-signatures, trust services, and PKI.
16. At least one team member shall possess demonstrated expertise in relevant legal and regulatory aspects and be familiar with international instruments and models (e.g., UNCITRAL Model Law and/or e-IDAS Regulation).
17. The Consultant shall have at least 10 years of demonstrable experience in providing relevant advice developing countries. Relevant project implementation and experience in low- and middle-income countries, specifically in francophone Africa, as well as familiarity with the social, cultural, political, and economic context of Cameroon, will be an advantage.
18. Demonstrated ability to work collaboratively with government counterparts and engage with various stakeholders in a consultative process.
19. The successful consultant firm's key personnel are required to be available throughout the duration of the assignment, and a local presence will be an advantage.
20. Fluency in both English and French will be an advantage.

VIII. CLIENT'S AND CONSULTANT'S RESPONSIBILITIES

21. The Consultant will report to the TTL. The Deliverables by the Consultant will be reviewed by the WB Task Team. The Consultant must ensure that the tasks identified above are performed in a result-

oriented manner to achieve the outputs and outcomes expected from the assignment. The Consultant is encouraged to utilize local expertise where appropriate.

22. Based on guidance received by the TTL, the Consultant might have the ability to coordinate and collaborate with other partners/international organizations that would also be financing the strengthening of the trust environment in Cameroon.
23. All information, data and information obtained shall be properly reviewed and analyzed by the Consultant. All such information, data and reports shall be treated as confidential. The Consultant shall make their own arrangements for venue, document reproduction, printing, and reproduction of all reports during the assignment.
24. Travel cost of the Consultant should be included in the whole contract value in the proposal, since this is a fixed fee / lump-sum contract.
25. Status Meetings: The Consultant shall have frequent (preferably) bi-weekly feedback meetings with the Task Team to inform progress made and more importantly, to use such meetings to identify and address any challenges that the Consultant may encounter in the course of the assignment.