REPUBLIC OF CABO VERDE

MINISTRY OF FINANCE

Terms of Reference (ToR)

Provision of Specialized Consultancy Services for the Execution of Phase II of the International WebTrust Compliance Process, Submission to Global Root Programs, and Reinforcement of ARME's PKI Infrastructure

1. Background and Context

The Government of the Republic of Cabo Verde, through the Ministry of Finance and the Special Projects Management Unit (UGPE), is implementing the **Digital Cabo Verde Project (P171099)**, financed by the World Bank's **International Development Association (IDA)**. The Project aims to strengthen Cabo Verde's digital foundations and improve the provision, security, and trustworthiness of digital public services.

In order to scale up and consolidate the results achieved under the parent project, the Government mobilised **Additional Financing for the period 2025–2028**, while maintaining the same institutional and operational arrangements.

The Digital Cabo Verde Project is structured around **three core components**:

- **Component 1 – Legal and Regulatory Environment**, which aims to strengthen the legal, regulatory, and institutional framework governing the digital economy, including digital certification, cybersecurity, trust services, interoperability, and technical compliance;
- **Component 2 – Digital Competitiveness**, which supports the development of enabling digital infrastructure, skills, and market conditions for a secure and competitive digital ecosystem;
- **Component 3 – Digital Public Services and Marketplace**, which focuses on improving the availability, security, and reliability of digital public services for citizens, businesses, and the diaspora.

Within this framework, **Component 1** is of particular relevance to this assignment, as it directly supports the establishment of **trusted digital services**, secure electronic transactions, and international recognition of national digital trust infrastructure.

The **Multisectoral Regulatory Agency (ARME)**, acting as the **State Certification Authority (CA)**, has successfully completed **Phase I of the International WebTrust Compliance Process**. ARME is now positioned to advance to **Phase II**, which encompasses:

- Formal submission to the main global Root Trust Programs operated by browser and operating system vendors (Mozilla, Microsoft, Apple, and Google);
- registration, integration, and continuous maintenance within the **Common CA Database (CCADB)**;
- Reinforcement and upgrading of the **Public Key Infrastructure (PKI)**, including Hardware Security Modules (HSMs), secure servers, and redundancy mechanisms;
- Institutional capacity building to ensure sustainable compliance and operational continuity.

The execution of Phase II is of **high public interest**, as it enables Cabo Verde to secure **international credibility, transactional security, technical interoperability, and digital trust**, which are essential foundations for e-government services, digital identity, electronic transactions, and cross-border digital interactions.

2. Objective of the Assignment

The objective of this assignment is to contract a specialised consulting firm to provide integrated **technical and legal advisory services** for the full execution of Phase II of the International WebTrust Compliance Process, including ARME's submission to global Root Programs, reinforcement of PKI infrastructure, and capacity building to ensure sustainable compliance.

3. Objectives of the Consultancy

3.1 General Objective

To ensure ARME's full international compliance as a Certification Authority through adherence to WebTrust standards, inclusion in global Root Programs, effective management of CCADB obligations, reinforcement of critical PKI infrastructure, and development of internal operational capacity.

3.2 Specific Objectives

The consulting firm shall:

- Prepare, review, and harmonise all technical and normative documentation required for Root Program submissions;
- Submit ARME to the Mozilla Root Program, followed by Microsoft, Apple, and Google Root Programs;
- Ensure registration, maintenance, and continuous updates in the CCADB;
- Reinforce the PKI technical infrastructure, including HSMs and redundancy mechanisms;
- Implement integration with Certificate Transparency (CT) Logs;
- Prepare and support quarterly and annual WebTrust audits;
- Deliver structured technical capacity-building activities;
- Support ARME in establishing sustainable post-project compliance mechanisms.

4. Scope of Services and Expected Outputs

4.1 Documentation and Policy Preparation

Activities

- Review and update Certification Practice Statement (CPS) and Certificate Policy (CP);
- Align documentation with Root Program and CA/Browser Forum requirements;
- Consolidate compliance evidence (CRLs, OCSP, logs, PKI records).

Outputs

- Updated and compliant CPS/CP;
- Consolidated compliance evidence package;
- Compliance gap analysis report.

4.2 Submission to Global Root Programs

Activities

- Preparation and submission to Mozilla Root Program;
- Subsequent submissions to Microsoft, Apple, and Google;
- Management of technical interactions via Bugzilla and equivalent platforms.

Outputs

- Mozilla submission dossier accepted for review;
- Complete submission packages for other Root Programs;
- Interaction and resolution log.

4.3 CCADB Registration and Maintenance

Activities

- Registration and configuration in the CCADB;
- Continuous update of artefacts, audit reports, and policies;
- Monitoring of CCADB notifications.

Outputs

- ARME fully registered in CCADB;
- Updated CCADB records;
- CCADB compliance status report.

4.4 PKI Technical Infrastructure Reinforcement

Activities

- Installation and configuration of additional HSMs;
- Upgrade of PKI servers and secure environments;
- Implementation of redundancy, backup, and security hardening.

Outputs

- Operational HSM infrastructure;
- Updated PKI architecture documentation;
- Technical validation report.

4.5 Certificate Transparency Integration

Activities

- Integration with public CT Logs;
- Testing and validation of certificate visibility.

Outputs

- Certificates successfully published in CT Logs;
- CT integration validation report;
- Operational CT procedures.

4.6 Compliance Audits and WebTrust Certification

Activities

- Preparation for quarterly audits;
- Support to the annual WebTrust audit;
- Implementation of corrective actions.

Outputs

- Audit readiness reports;
- WebTrust audit support package;
- Corrective action implementation report.

4.7 Technical Capacity Building

Activities

- Design and delivery of training sessions;
- Knowledge transfer on PKI, WebTrust, and Root Programs.

Outputs

- Training materials and manuals;
- Capacity-building delivery report;
- Sustainability assessment.

4.8 Post-Project Sustainability Support

Activities

- Advisory support during Years 1;
- Periodic documentation and evidence updates.

Outputs

- Annual sustainability support reports;
- Updated compliance documentation;

- Long-term compliance recommendations.

A detailed deliverables schedule covering Year 1 shall be implemented under a Lump Sum contractual approach.

5. Deliverables, Timeline, and Payment Milestones

Nº	Deliverable	Description	Indicative Timeline	Payment After aproval
D1	Inception Report	Methodology, detailed work plan, stakeholder mapping, and risk matrix	Month 1	15%
D2	Updated CPS and CP	Revised and internationally compliant CPS and CP documents	Month 2	
D3	Root Program Submission Package – Mozilla	Formal submission dossier and supporting evidence	Month 4	20%
D4	Root Program Submission Packages – Apple, Microsoft, Google	Complete submission dossiers and responses	Months 5–6	
D5	CCADB Registration and Compliance Report	Validated CCADB records and compliance status	Month 6	15%
D6	PKI Infrastructure Reinforcement Report	Installation of HSMs, system upgrades, and security validation	Months 8–9	15%
D7	Certificate Transparency Integration Report	CT Logs configuration, testing, and validation	Month 7	
D8	WebTrust Audit Support Package	Audit readiness, evidence, and preliminary audit outputs	Month 10	20%
D9	Capacity Building Report	Training materials, sessions delivered, and evaluation	Month 11	
D10	Final Report and Sustainability Plan	Consolidated results, lessons learned, and post-	Month 12	15%

		project compliance roadmap		

Payments shall be linked to the satisfactory completion and validation of each deliverable, under a **Lump Sum contractual approach**, as approved by UGPE.

6. Consulting Firm Requirements

The firm must demonstrate:

- Minimum **10 years of experience** in cybersecurity or critical infrastructure;
- At least **six (6) cybersecurity projects**, including **three (3) implemented in Cabo Verde**;
- Proven experience in **WebTrust, Root Programs, and PKI projects**;
- Demonstrated expertise in **HSMs, CT Logs, CCADB**, and CA operations;
- **ISO/IEC 27001 certification** (mandatory);
- **WebTrust for Certification Authorities certification** (mandatory, CPA Canada).
- Minimum certifications include (as applicable):
  - CISSP, CISA, ISO/IEC 27001 Lead Auditor, CEH, OSCP, CompTIA Security+, CND.
  - All deliverables shall be produced in **Portuguese**.
  - Key Experts must demonstrate fluency in English and Portuguese.
  - Knowledge of Portuguese shall be considered an advantage.

Team members

The consulting firm shall mobilise a multidisciplinary team composed of **up to five (5) Key Experts**. Each expert shall meet the minimum qualifications and experience described below.

K1- Team Leader / Senior PKI & WebTrust Compliance Lead

Qualifications:

- Bachelor’s or postgraduate degree in Computer Science, Information Systems, Cybersecurity, or related fields.

Professional Experience:

- Minimum **7 years of experience** leading large-scale audits or compliance projects related to digital trust infrastructures;
- Proven leadership in **PKI security, WebTrust compliance, and Certification Authority operations**;
- Participation in at least **five (5) PKI or WebTrust-related projects**.

Certifications (minimum):

- CISSP;
- WebTrust Auditor (CPA Canada recognised);
- ISO/IEC 27001 Lead Auditor;
- Additional certifications such as PMBOK, ITIL, or COBIT are an advantage.

Key Responsibilities:

- Overall technical and managerial leadership of the assignment;
- Interface with Root Programs, CCADB administrators, and auditors;
- Oversight of PKI infrastructure reinforcement and compliance activities;
- Leadership of capacity-building activities and quality assurance.

.

K2 – Legal Specialist (International and National Compliance)

Qualifications:

- Postgraduate degree or Advanced degree in Law or equivalent.

Professional Experience:

- Minimum **7 years of legal practice**, including regulatory compliance;
- Proven experience in legal and regulatory frameworks applicable to:
    - digital certification;
    - cybersecurity;
    - data protection;
    - trust services and PKI;
- Demonstrated experience in both **international Root Program requirements** and **national legal frameworks**.

Key Responsibilities:

- Legal review and harmonisation of CPS/CP and related policies;

- Assurance of compliance with national legislation and international Root Program obligations;
- Legal support during audits and Root Program submissions.

.

K3 – Engineering Expert / WebTrust Auditor

Qualifications:

- Degree in Computer Engineering, Computer Science, or related field.

Professional Experience:

- Minimum **7 years of experience** as a senior auditor or engineer in PKI environments;
- Valid **WebTrust Auditor licence**;
- Participation in at least **three (3) WebTrust audits**.

Key Responsibilities:

- Technical evaluation of PKI controls and compliance mechanisms;
- Preparation of audit evidence and internal readiness assessments;
- Technical validation of Root Program and CCADB requirements.

.

K4 – Technical Expert (Cybersecurity & PKI Operations)

Qualifications:

- Degree in Cybersecurity, Information Technology, or related discipline.

Professional Experience:

- Minimum **5 years of hands-on experience** in cybersecurity and critical infrastructure operations;
- Proven experience in PKI operations, HSM management, and secure system hardening.

Key Responsibilities:

- Implementation of PKI infrastructure upgrades;
- Support to CT Logs integration and operational security controls;
- Technical support to ARME operational teams.

K5 – PKI Documentation & Root Program Specialist

Qualifications:

- Degree in Computer Science, Information Systems, or related field.

Professional Experience:

- Proven experience in drafting and maintaining PKI documentation, including CPS, CP, and security policies;
- Direct experience with Root Program documentation requirements;
- Participation in at least **three (3) PKI documentation or Root Program projects**.

Key Responsibilities:

- Preparation and maintenance of PKI documentation;
- Alignment of documentation with Root Program and WebTrust requirements;
- Support to CCADB documentation management.

.

7. Reporting, Ownership, and Confidentiality

All deliverables shall be submitted to ARME under the supervision of the Ministry of Finance and UGPE. All outputs are the exclusive property of the Government of Cabo Verde, and strict confidentiality shall be maintained.