TERMS OF REFERENCE

Jamaica: Preparation Grant- Foundation for Digital Government Transformation (FDGT)
GFPP Grant No. TF0C8979-JM – Component 2

Assignment Title: Development of Technical Documentation for the Public Key Infrastructure (PKI)
Reference No: FDGT/PG/CON/1.5

1. Background

In advancing the national **VISION 2030 Jamaica** goals, the Government of Jamaica (GOJ) recognizes that a prosperous Jamaican economy (Pillar 3) with empowered citizens (Pillar 1) requires a resilient, robust, and efficient digital infrastructure, serving as the foundation for modern, digital government services. The build-out of a national digital service framework is essential to reposition government services around citizens' needs - shifting from a model that requires citizens to come to government to one where government is digitally available anywhere, in a simplified, secured, and accessible manner.

In April 2024, the World Bank Group (WBG) conducted a **Digital Economy Assessment (DEA)** of Jamaica's digital landscape. The purpose of the DEA was to identify gaps and make recommendations on policy, strategic and operational issues across Six (6) pillars, digital infrastructure, digital public platforms, digital financial services, digital businesses, digital skills, and the trust environment. The findings revealed, among other things, the need to:

(a) Strengthen institutional capacity and accelerate the implementation of the data privacy/data protection framework.
(b) Improve the affordability of internet services by, *inter alia*, strengthening competition in the telecommunications market.
(c) Address certain barriers that currently impede the inclusive and productive adoption of digital technologies, and
(d) Continue the modernization of the digital financial services ecosystem.

Considering the foregoing and following discussions with the World Bank Group (WBG) and other Government entities, it was proposed in July 2025 to develop a Foundation for Digital Government Transformation (FDGT) programme. To facilitate expediting the scoping and design of the FDGT, the WBG has provided a Grant to the GOJ, through the Office of the Prime Minister (OPM). The Grant is administered by the Information and Communications Technology (ICT) Authority. The wider FDGT programme is expected to comprise activities under the following Three (3) high-level components:

(a) Component 1: Digital Economy Enabling Environment
(b) Component 2: Digital Public Infrastructure and Platforms
(a) Component 3: Digital Skill and Technology Adoption

The need for Government services from anywhere came into sharp focus in October 2025, post Hurricane Melissa, where the need to rapidly reach affected citizens, transparently account for use of international aid, and to deliver targeted support to communities in storm-ravaged areas was made readily apparent.

This consultancy is a technical documentation and adoption-readiness assignment under the Grant and is limited to improving and adding to existing documentation for the GOJ Public Key Infrastructure (PKI), developing practical Ministries, Departments and Agencies (MDAs) integration and eSignature guidance, and recommending actions to strengthen PKI/eSignature adoption and operational readiness.

2. Objective of the Consultancy

The objective of this Consultancy is to produce accurate, maintainable and security-sensitive documentation that enables the ICT Authority and MDAs to understand, operate, integrate with, and adopt the existing GOJ PKI and eSignature services. The assignment shall translate the current PKI environment and technical documentation into practical, easy to use technical documentation, integration guidance and eSignature standards, while identifying gaps, risks, dependencies and adoption-readiness actions for Government consideration.

The main objectives of this consultancy are to:

1. Improve Technical Documentation for the GOJ PKI,
2. Prepare Integration/Interface Guidance for MDAs adopting the PKI and eSignature services,
3. Create eSignature Guidelines and Standards,
4. Develop eSignature Implementation Checklist, and
5. Recommend actions to strengthen adoption and operational readiness.

3. Scope of Work

For the avoidance of doubt, this assignment is a documentation, standards, guidance and adoption-readiness assignment. The Consultant shall not be responsible for procuring, replacing, redesigning or implementing a new PKI platform, providing legal advice, certifying the PKI environment, or integrating individual MDA systems except to the extent needed to prepare practical sample guidance and documentation.

The Consultant will be required to:

(a) Review existing documentation for the GOJ PKI platform and conduct targeted consultations with ICT Authority technical and operational teams and selected MDA representatives to validate documentation needs, integration guidance, adoption barriers and support requirements,

(b) Provide recommendations to strengthen existing PKI platform documentation, to include architecture, components, security controls and backup / Disaster Recovery procedures,

(c) Develop Integration / Interface Guidance to support MDAs integration, to include supported integration patterns, API interface models, authentication and authorisation flows, signing and validation workflows, sample integration scenarios error handling, onboarding steps, testing approaches and support/escalation procedures,

(d) Develop eSignature Guidelines and Standards, to include user responsibilities, signature assurance levels, identity verification requirements, validation procedures, accepted signature formats, cryptographic requirements, timestamping, certificate trust requirements, retention and revocation procedures, FAQs, troubleshooting guides, common integration issues and user support articles,

(e) Develop a PKI/eSignature Implementation Checklist for MDAs, to include governance, legal and policy review, business-process readiness, technical integration, security, privacy, records management, accessibility, training, testing, go-live, support, and operational handover,

(f) Identify and document gaps, risks, assumptions and dependencies that may affect PKI/eSignature adoption,

(g) Recommend actions to strengthen PKI/eSignature adoption and MDA operational readiness, including immediate documentation or operating-procedure fixes, medium-term governance and support improvements, capacity-building needs, integration

support model, change-management considerations, and longer-term scaling opportunities, and

(h) Provide monthly progress reports and a final project report.

4. Consultant Profile

The expert should have at a minimum:

- Master's degree, with specialisation in Computer Science, Cybersecurity, Information Systems, Engineering, Telecommunications, Law and Technology, Digital Government, or other related discipline. **(10 points)**
- Demonstrated experience in PKI, trust services, identity systems, cybersecurity, digital signatures, electronic signatures, certificate lifecycle management, or comparable digital trust assignments, evidenced by Three (3) or more projects / assignments completed successfully in the past Ten (10) years. **(40 points)**
- Demonstrated experience in producing high-quality technical documentation, operating procedures, standards, user guides, knowledge bases, checklists, training/support materials, or similar documentation for technical or public-sector audiences, evidenced by Three (3) or more projects/ assignments completed successfully in the past Ten (10) years. **(30 points)**
- Demonstrated experience conducting government, regulatory, compliance, policy, or operational reviews related to digital trust, cybersecurity, identity, records, digital services, or electronic transactions, evidenced by Three (3) or more projects / assignments completed successfully in the past Ten (10) years. **(20 points)**

5. Schedule of Deliverables and Reporting Requirements

The ICT Authority is the Contracting Authority and is responsible for final approval of any contractual amendments and payments.

The designated representative for the supervision of this consultancy is the Grant Project Manager, who will approve all deliverables, subject to consultation with the relevant project implementation personnel and the ICT Authority CIO.

The intended start date is August 2026, and the period of implementation is 16 weeks from this date or up to 16 December 2026, whichever is earlier. Below is the schedule of deliverables with the timeline for submission and approval, as well as the associated payment for each deliverable:

ID	Deliverable	Minimum Content	Submission Date	Review Period	Payment %
D1	Inception Report	• Updated work plan • Project risk register • Document request list • Proposed stakeholder consultation list • Kick-off meeting minutes	1 week after contract signing	1 week	10%

ID	Deliverable	Minimum Content	Submission Date	Review Period	Payment %
D2	Current State PKI Technical Assessment	● Review and document the existing PKI platform, including where applicable: o Certificate lifecycle management o Registration Authority processes o Key management procedures o Security controls o User administration o Backup and disaster recovery o Monitoring and audit capabilities	5 weeks after contract signing	1 week	10%
D3	PKI Technical Documentation Suite	● Prepare professional technical documentation including: o Architecture documentation: Data flows, trust relationships & security zoning o Operations documentation: SOPs and procedures for certificate issuance and revocation, backup and restoration, and incident management o Administrative documentation: Roles & responsibilities and access control matrix N.B. This will be based on existing technical documentation and not all created from scratch	10 weeks after contract signing	1 week	20%
D4	PKI/eSignature Integration / Interface Guidance	● Practical guidance for MDAs integrating PKI/eSignature services. This shall include: o Supported integration models, API authentication and service workflows, document signing workflows, certificate validation processes, recommended security controls, logging and audit requirements and common implementation patterns	11 weeks after contract signing	1 week	10%
D5	eSignature Guidelines, Standards & Knowledge base	● Develop eSignature Guidelines, to include User responsibilities, signature assurance levels, identity verification requirements, validation procedures and security precautions ● Develop eSignature Standards to include, accepted signature formats, cryptographic requirements, interoperability requirements, timestamping, certificate trust requirements, retention, revocation procedures, audit evidence requirements and governance and compliance expectations	12 weeks after contract signing	1 week	20%

ID	Deliverable	Minimum Content	Submission Date	Review Period	Payment %
D6	PKI/eSignature Implementation Checklist	• Implementation Checklist for MDAs adopting PKI/eSignature, to include legal review and readiness in the areas of governance, technical, integration, security, training and Go-Live	13 weeks after contract signing	1 week	10%
D7	PKI/eSignature Adoption Recommendations	• Report recommending actions to strengthen PKI adoption and MDA operational readiness, including immediate actions, medium-term governance, support and capacity-building improvements, integration support model, change-management considerations, risks and dependencies, and long-term scaling opportunities	14 weeks after contract signing	1 week	10%
D8	Monthly project progress reports	• Highlighting all activities, decisions taken, risks, challenges, lessons learned and mitigation strategies	Every 4th Monday after contract signing until completion	1 week	n/a
D9	Final Project report	• Full report on all activities, decisions taken, challenges overcome and lessons learned during execution of the contract. Include identified risks, assumptions and dependencies, final document inventory, document ownership and maintenance recommendations, unresolved issues, and final recommendations for PKI/eSignature adoption	15 weeks after contract signing	1 week	10%

Deliverables must be submitted in soft/electronic copy using Microsoft Word and Adobe PDF (editable format). Where deliverables are subject to revisions following review, the Consultant shall provide the updated version in tracked change and clean formats, along with a review matrix as may be appropriate.

5.1 Acceptance and Revision

Each deliverable shall be deemed "approved" only upon written sign-off by the Grant Project Manager. Acceptance shall be based on: (a) completeness against the Minimum Content specified in the Schedule of Deliverables; (b) factual accuracy and quality of analysis; (c) clarity and professional presentation; and (d) responsiveness to comments raised in earlier review cycles. Each revised submission shall be accompanied by a tracked-changes version and a clean version. The Grant Project Manager shall return consolidated comments within the Review Period stated in the Schedule, and the Consultant shall submit revisions within Three (3) working days of receiving comments unless otherwise agreed in writing.

5.2. Variations

Revisions to the TOR will be accommodated through mutual discussion and agreement with the Grant Project Manager. The Grant Project Manager, as advised by the Procurement Specialist, will issue formal notification concerning any request for variation.

6. Ownership

All deliverables, intermediate outputs, working papers, raw stakeholder inputs and data collection instruments produced under this contract shall be the exclusive property of the GOJ. The Consultant and their personnel shall treat all information accessed during the assignment, including stakeholder responses and any data shared by MDAs, as strictly confidential, and shall not disclose, publish, reuse, or retain such information without prior written consent of the ICT Authority.

7. Client's Input and Counterpart Personnel

All day-to-day operations and communication regarding the implementation of activities under the contract will be handled by the contract supervisor or his/her designate.

The Consultant will work remotely and will only be accommodated at the ICT Authority, for specified activities, as needed and agreed.

8. Conditions

Personal data accessed during the assignment shall be handled in accordance with the Jamaica Data Protection Act 2020.

The Consultant shall declare any actual, potential, or perceived conflict of interest at proposal stage and continuously throughout the assignment, including any current or prospective engagements with vendors of digital government solutions, MDAs being assessed, or other parties with a direct interest in the outcome of the assessment.

Travel as required under this assignment is authorized and should therefore be included as an expense in the Consultant's financial proposal.

The Consultant shall provide the tools & resources required to undertake this assignment, where necessary the client will provide a venue for meetings. The Consultant shall assume responsibility for office space during the conduct of the assignment.