GOVERNMENT OF SAINT LUCIA

Ministry of the Public Service, Transport, Information and Utilities Regulation

REQUEST FOR EXPRESSIONS OF INTEREST

CONSULTING SERVICES – FIRMS SELECTION

QUALITY AND COST BASED SELECTION (QCBS)

Project Name	Caribbean Digital Transformation Project (CARDTP)
Loan/Credit/Grant No.	IDA Credit #6682-LC
Assignment Title:	Consultancy for the Development of a Government of Saint Lucia (GOSL) Secure Wallet with Digital Payment and Integration Solutions
Reference No:	LC-DPS-513171-CS-QCBS
Country:	Saint Lucia

1. Background

The Government of Saint Lucia has received financing from the International Development Association (IDA) (the "Bank") in the form of a Credit toward the cost of the Caribbean Digital Transformation Project. The Ministry of the Public Service, Transport, Information and Utilities Regulation, as the implementing agency, intends to apply a portion of the proceeds of the Credit to eligible payments under the contract for the Consultancy for the Development of a Government of Saint Lucia Secure Wallet with Digital Payment and Integration Solutions.

2. Objective of the Assignment

The objective of the assignment is to design, develop and implement a secure Government of Saint Lucia Government Secure Wallet with an integrated Digital Payment System, secure document-management capabilities and integration with relevant Government services and platforms.

3. Scope of the assignment

To deliver this objective, the Consultant will be required to undertake a comprehensive set of technical, operational, and regulatory activities, including the following:

- Conduct detailed requirements gathering and analysis to inform system design and functional specifications.
- Develop the overall system architecture and technical design for the Government Wallet and digital payment solution.
- Build secure, scalable mobile and web applications supporting wallet functions and digital payments.
- Integrate the solution with existing government platforms, including digiGov and the National Authentication Framework.
- Implement secure digital payment capabilities and related document-management features.
- Incorporate cybersecurity, privacy, and data-protection controls aligned with international standards.
- Establish business continuity and disaster recovery arrangements for the solution.

- Deliver user training, operational guidance, and structured knowledge-transfer activities.
- Provide warranty support to ensure stability and performance during the initial operational period.
- Prepare all necessary documentation and support the Government of Saint Lucia in securing regulatory approval for the Government Wallet, including assessment of the FinTech legal and regulatory framework to ensure compliance with existing laws and policies
- Deploy the solution within the hosting infrastructure provided by the Client, including servers, storage, networking, virtualization platform, and operating systems, and configure all required components to ensure full operational readiness

4. Duration of the assignment

The estimated duration of the Services is 50 weeks.

5. Shortlisting Criteria

Interested Consulting Firms will be shortlisted based on the following criteria:

i. At least five (5) years of proven experience in the design, development and implementation of digital payment platforms, Government Secure Wallets or comparable FinTech solutions.

ii. Demonstrated experience integrating ICT or payment systems with government platforms, databases or service portals, including the use of application programming interfaces (APIs) and authentication services.

iii. Proven experience in developing and deploying secure, scalable web and mobile applications with strong user-experience and interoperability features.

iv. Demonstrated capacity to implement secure solutions aligned with internationally recognized standards, including PCI DSS, ISO/IEC 27001, ISO 20022 or equivalent standards.

v. Successful completion of at least three (3) assignments of similar scope and complexity, such as national-level payment systems, e-government platforms or enterprise-level systems-integration assignments.

vi. Demonstrated experience delivering assignments for public-sector clients in the Caribbean, the Organization of Eastern Caribbean States (OECS) or comparable jurisdictions.

vii. Prior experience managing assignments financed by international development partners, such as the World Bank, Caribbean Development Bank or United Nations Development Programme, will be considered an advantage**.**

Interested Consulting Firms must provide sufficient information to demonstrate that they possess the required qualifications and relevant experience to perform the Services. The information submitted should include:

a) a profile of the firm and a description of its core business;

b) details of relevant experience in digital payment platforms, Government Secure Wallets, FinTech solutions, secure mobile and web applications, government-system integration and cybersecurity;

c) descriptions of comparable assignments, including the name of the client, country, scope of services, contract period, completion status and contact information for verification; and

d) details of any proposed joint-venture member or sub consultant and the nature of the proposed association.

Key Experts will not be evaluated at the shortlisting stage. Therefore, individual experts' CVs are not required with the Expression of Interest.

A firm may submit an Expression of Interest (EOI) individually if it considers itself fully qualified to undertake the assignment. Consultants may also form a joint venture or sub consultancy with other firms should they wish to enhance their qualifications and capacity.

The Attention of interested Consultants is drawn to paragraphs 3.16 and 3.17 of the World Bank's Procurement Regulations for IPF Borrowers (July 2016, revised), setting forth the World Bank's policy on conflict of interest.

A Consultant will be selected in accordance with the Quality and Cost-Based Selection method set out in the World Bank Procurement Regulations for IPF Borrowers.

Expressions of interest must be delivered in a written form to the address below (in person, or by mail, or by e-mail) by an **extended deadline of Midnight, EST, Monday September 14, 2026**

Further information can be obtained at the address below during office hours

Project Manager
Caribbean Digital Transformation Project (CARDTP)
Division of Public Sector Modernization
Ministry of the Public Service, Transport, Information and Utilities Regulation
William Peter Boulevard, Castries, St. Lucia
Tel: (758) 468-1408 / 468-1407
Email: slu.cardpt@gmail.com. Copied to sheralin.monrose@govt.lc

The detailed Terms of Reference (TOR) for this assignment are annexed to this Request for Expressions of Interest (REOI) for ease of reference.

Ministry of the Public Service, Transport, Information and Utilities Regulation

CARIBBEAN DIGITAL TRANSFORMATION PROJECT

TERMS OF REFERENCE

CONSULTANCY FOR THE DEVELOPMENT OF A GOVERNMENT OF SAINT. LUCIA (GOSL) SECURE WALLET WITH DIGITAL PAYMENT AND INTEGRATION SOLUTIONS

1. INTRODUCTION

In June 2020, the Department of Public Service (DOPS) launched its flagship initiative, the Digital Government Integrated Services Platform (digiGov). This transformative program is designed to enhance government efficiency by leveraging ICTs to make public services more accessible, integrated, and cost-effective. By streamlining and automating public sector processes, digiGov improves service delivery to citizens, businesses, and other government entities—ensuring efficient, secure, and user-friendly interactions across multiple platforms.

digiGov eliminates redundancies, reduces operational costs, and provides seamless access to government services regardless of geographic location or operating hours. It supports Government-to-Government (G2G), Government-to-Citizen (G2C), and Government-to-Business (G2B) interactions, creating an interconnected ecosystem of services. Within Saint Lucia's digital development agenda, digiGov is a catalyst for digital transformation, laying the groundwork for private sector innovation in areas such as open data, analytics, mobile applications, and Artificial Intelligence (AI).

As a significant extension of digiGov, the Government Wallet initiative introduces a Digital Payment System and secure digital storage for government-issued documents, with full integration into core GOSL systems. The Government Wallet will provide a secure, efficient, and intuitive platform for managing digital documents, credentials, and payments. By embedding digital payment functionalities, the Wallet will transform how citizens interact with government services, allowing seamless, cash-lite transactions for:

- Driver's license renewals
- National Identification Card (ID) replacements
- Utility and tax payments
- Fees for permits and certifications
- Other government-related services

Integration with digiGov and other GOSL systems (e.g., Civil Registry, Licenses and Permits, and the GOSL Receipt Information Management System) will enable real-time verification of documents and transactions, strengthening trust and efficiency in government operations.

The Digital Payment System within the Government Wallet will:

- Simplify and accelerate financial interactions between citizens and the government.
- Provide multiple payment options, including credit/debit cards, mobile wallets, and other platforms.
- Reduce reliance on cash, supporting Saint Lucia's transition toward a cash-lite economy.
- Enhance transparency and reduce administrative costs for both government and citizens.
- Promote financial inclusion by expanding access to digital services.

2. OBJECTIVES

The objective of this assignment is to design, develop, and implement a secure Government Secure Wallet Wallet system for the Government of Saint Lucia to support electronic payments, strengthen digital trust, and facilitate integration with government services.

3. EXPECTED RESULTS

The consultancy is expected to deliver a secure, functional, and user-friendly Government Wallet solution through a structured and phased approach. Envisioned components of the solution can be found in **Annex I**. The key outcomes and results are as follows:

a. A clear and comprehensive roadmap for the design, development, implementation, testing, deployment, and operationalization of the Government Wallet with Integrated Digital Payment System, with well-defined timelines, milestones, governance arrangements, and objectives.

b. Comprehensive documentation of business, functional, technical, security, interoperability, and integration requirements, providing a robust foundation for the successful development and implementation of the solutions.

c. A fully developed Government Wallet with integrated Digital Payment System that securely integrates into relevant Government systems, platforms, services, and payment channels.

d. Established technical standards, operational procedures, user guides, and knowledge transfer mechanisms, supported by trained Government personnel capable of administering, maintaining, and supporting the solutions.

e. Successfully tested, validated, and security-assessed solutions that meet all agreed functional and non-functional requirements, including performance, reliability, accessibility, interoperability, and cybersecurity requirements.

f. Fully deployed and operational Government Wallet with integrated Digital Payment System solution that is accessible to authorized users and capable of supporting secure digital transactions, payments and related Government service delivery.

g. Enhanced digital service delivery through the provision of secure, efficient, and user-friendly digital payment capabilities that improve citizen and business access to Government services.

h. Sustainable and Government-owned solutions supported by comprehensive documentation, source code, training, and knowledge transfer to facilitate long-term operation, maintenance, and future enhancement.

i. Stable, reliable, and scalable Government Wallet and Digital Payment System solutions supported by appropriate maintenance, warranty, and operational support arrangements to ensure long-term success and service continuity.

Overall Results

- **Integrated Digital Platform:** A secure, user-friendly Government Wallet with integrated Digital Payment System accessible through mobile and web platforms, enabling seamless access to government services, credentials, and digital payment capabilities.
- **Secure GOSL Document Management:** Secure storage and verification and validation of key GOSL issued Documents.
- **Enhanced Service Delivery:** Seamless access to government-issued documents, credentials, and digital services, supported by real-time verification, secure transactions, and integration with relevant Government systems and platforms.
- **Digital Payment Enablement:** A fully operational Digital Payment System that facilitates secure, efficient, and interoperable digital payments for Government services, supporting improved convenience for citizens, businesses, and public institutions.
- **Operational Efficiency:** Reduced administrative costs, streamlined processes, improved transaction management, and enhanced service delivery through digital transformation and automation.
- **Capacity Building:** Trained Government personnel equipped with the technical knowledge, operational procedures, and tools necessary to manage, maintain, and sustain both the Government Wallet and Digital Payment System.
- **Security and Reliability:** Robust security, privacy, and resilience mechanisms that ensure data protection, secure payment processing, system integrity, business continuity, and reliable service availability.
- **Sustainability and Government Ownership:** Government-owned and sustainable solutions supported by comprehensive documentation, knowledge transfer, and operational support arrangements to enable long-term management and future enhancement.
- **Regulatory Approval: Prepare the necessary documents and Support the GOSL request for regulatory approval for the wallet. Assess the Fintech legal and regulatory framework to ensure the proposed system is in keeping with the existing framework**

4. SOLUTION OVERVIEW

The Government Wallet is envisioned as a comprehensive and secure digital platform designed to streamline the storage and management of citizens' essential documents and credentials. Accessible via a secure mobile application and web portal, the solution aims to deliver a seamless and user-friendly experience. Key features include:

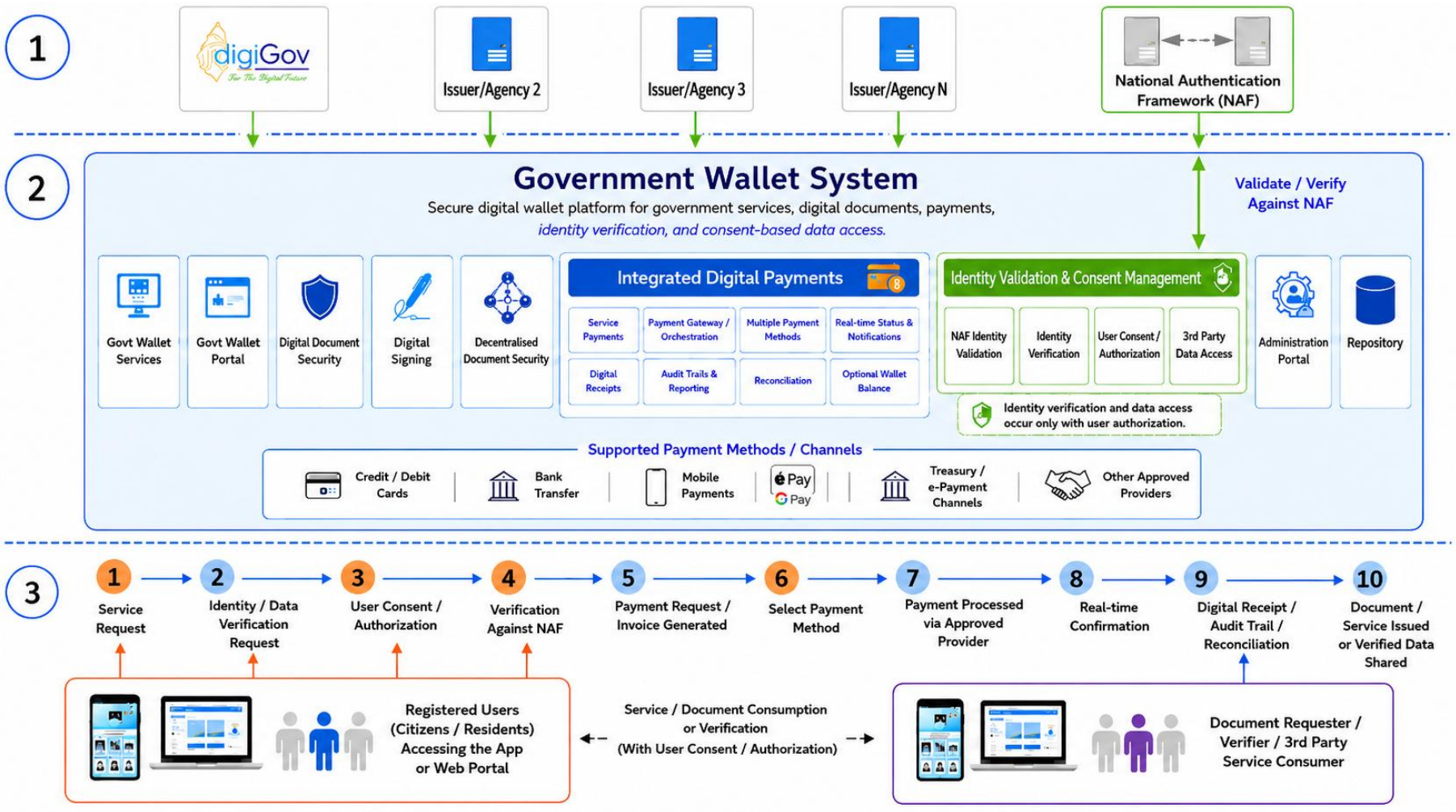
1. **Wallet for Payment of Government Services**

- The platform shall enable individual users (citizens/residents) to securely make payments for Government services through the Government Wallet using approved payment methods and financial service providers.
- The platform shall support integration with multiple payment instruments and channels, including but not limited to credit cards, debit cards, bank transfers, mobile payment solutions, Government Secure Wallets (e.g. Apple Pay and Google Pay), government treasury and other approved electronic payment mechanisms.
- The payment module shall also support integration with the Government Treasury, allowing citizens and residents to deposit funds directly into their Government Wallet through approved Treasury payment points or Treasury-supported channels.
- Where applicable, the platform may support wallet-based functionality, including the ability for users to maintain and utilize account balances, subject to applicable legal, regulatory, and operational requirements.
- The platform shall allow for the payment of Government services delivered via digiGov and other Government platforms and services.
- The platform shall provide real-time transaction status updates, notifications, digital receipts, audit trails, reporting, and end-to-end reconciliation capabilities.

2. **Document Management**
    - Users can securely store and retrieve various types of documents, such as Driver's Licenses, National IDs, birth certificates, and educational certificates.
3. **Secure Authentication**
    - Employing advanced security features, such as Two-Factor Authentication (2FA) and encryption techniques, to protect data both at rest and in transit, ensuring it remains safeguarded against unauthorized access.
4. **Integration with GOSL Digital Identity System**
    - Users will register using their National Identification Number through the National Authentication Framework (NAF) or a Saint Lucia-registered mobile number.
    - The system ensures verification and validation of key documents, requiring NAF ID registration for enhanced reliability.
    - The app shall integrate with digiGov and the National Authentication Framework (NAF) to request, receive, and validate 2FA one-time codes (OTP) during user login.
5. **Direct Integration with DigiGov**
    - The platform integrates seamlessly with the Saint Lucia DigiGov system, allowing government and approved organizations to issue digital documents directly to users' accounts.
    - The Platform will integrate with the DigiGov Payment Module to support payments through Government Secure Wallet module.
    - Non-DigiGov entities can integrate through Secure API integration, enabling wider adoption of the platform.
    - The platform shall securely integrate with digiGov to receive and display transaction notifications and status updates for user-submitted transactions in near real time.
    - The Platform should enable application and payment of digiGov Services.

6. **Integration with other Key GOSL Systems**
    - The Platform will integrate with other key Government systems to retrieve secure documents generated by these systems.
    - Provide integration between the Gov Wallet, GOSL digital Identity system and other GOSL systems to facilitate sharing and validation of data.
7. **QR Code Verification**
    - Support for **QR code scanning** to enable quick and secure verification of document authenticity, enhancing reliability and convenience for users and third parties.

The diagram below provides a high-level overview of the process flow for document issuance by government systems and other approved organizations, and illustrates how registered users, requesters, and verifiers access these documents.



5. SCOPE OF WORK

The Government of Saint Lucia seeks a competent Consultant capable of delivering the **Government Wallet** solution, including its development, deployment, and ongoing maintenance. The scope of work is outlined as follows

Phase 1 – Requirements Analysis and Solution Design

1. **Requirement Analysis**
    - Conduct detailed sessions with government stakeholders to understand the specific needs and expectations for the Government Wallet.
    - Gather requirements for functionality, integration, security, and user experience.
2. **System Design**
    - Develop a comprehensive **System Design Document** that includes:
        - System architecture and components.
        - Data flow diagrams and processes.
        - Security mechanisms to guarantee **C**onfidentiality, **I**ntegrity and **A**vailability (e.g., encryption, access control).
        - Adherence to internationally recognized standards (e.g., ISO, NIST).

Phase 2 – Solution Development

1. Development of Mobile App and Web Portal

a. **Mobile App Development**
    - Deliver fully functional **Government Wallet mobile applications** for both **iOS** and **Android** platforms.
    - Ensure user-friendly and accessible interfaces for seamless user experiences.

b. **Web Portal Development**
    - Develop a **web portal** for desktop and laptop users as an alternative access point for document management, compatible with all browsers (chrome, safari, etc)

c. **Core Features Implementation**
    - User registration and authentication.
    - Document management, including secure storage and retrieval.
    - Integrated Digital Payment Module
    - QR code scanning for document verification.

- Integration with government systems and approved non-government services.

d. **API Development and Integration**
   - Develop secure APIs to facilitate data exchange between the Government Wallet and government systems, ensuring real-time accuracy of information.
   - Integrate the solution with existing government databases, services, and non-government organizations.

e. **Reporting and Analytics**
   - Implement a reporting component to provide metrics but not limited to:
     - System usage.
     - Document uploads and retrievals.
     - User activity.

Phase 3 – Security, Business Continuity and Quality Assurance

1. **Security Measures**

The solution shall implement industry-standard security controls, including but not limited to:

- Data encryption for data at rest and in transit.
- Multi-factor authentication (MFA) for privileged and administrative access.
- Role-based access control (RBAC).
- Security monitoring and logging.
- Regular vulnerability assessments and penetration testing.
- Compliance with applicable cybersecurity standards and Government security policies.

2. **Business Continuity and Disaster Recovery**

The proposed solution shall incorporate a resilient architecture designed to ensure high availability, business continuity, and disaster recovery. At a minimum, Consultants should describe:

- The proposed redundancy and high-availability architecture.
- Backup and recovery mechanisms.
- Disaster recovery arrangements.
- Recovery Time Objective (RTO).

- Recovery Point Objective (RPO).
- Service Availability/Service Level Agreement (SLA).

The solution should, at a minimum, achieve the following service levels (or propose equivalent or better values):

- **Recovery Time Objective (RTO):** One (1) hour or less.
- **Recovery Point Objective (RPO):** Zero (0) data loss (or the closest technically achievable objective, clearly stated).
- **Service Availability (SLA):** 99.98% availability or higher.

Consultants shall clearly explain how the proposed architecture satisfies these requirements and identify any assumptions, dependencies, or cost implications associated with the proposed business continuity and disaster recovery solution.

3. Testing

- Conduct comprehensive testing, including:
  - Unit testing.
  - Integration testing.
  - System testing.

Phase 4 – Deployment and Transition

1. Deployment and Go-Live

The Client will provide the hosting infrastructure including servers, storage, networking, virtualization platform and operating systems unless otherwise specified.

1. Deploy, install, configure, and commission the solution within the Government's designated hosting environment.
2. Configure the application software and all associated components to operate on the infrastructure provided by the Client.
3. Configure all required databases, middleware, application servers, and interfaces necessary for successful implementation.
4. Support system integration, testing, migration, and production cutover activities to ensure a successful go-live.

2. Go-Live Support

The Consultant shall provide post-deployment support to ensure the successful transition of the solution into full operational use. At a minimum, the Consultant shall:

- Monitor the performance and stability of the system following deployment.
- Provide on-site and/or remote technical support to resolve defects, configuration issues, and operational problems identified during the stabilization period.
- Respond to and rectify critical issues within agreed service levels to minimize disruption to operations.
- Support users and system administrators during the transition to live operations.
- Confirm system stability and operational readiness prior to the completion of the go-live support period.

Duration of Go-Live Support

The Consultant shall provide **a minimum of six weeks** of intensive post-implementation (go-live) support following final production deployment and acceptance of the solution. During this period, the Consultant shall ensure the availability of suitably qualified technical personnel to provide timely issue resolution and system stabilization.

3. Knowledge Transfer, User Training, and Documentation

- Develop comprehensive materials for government staff, including step-by-step guides for system features and functionalities.
- Conduct user training sessions to ensure government staff are familiar with the system and can support end-users effectively.
- Provide detailed documentation for system design, APIs, and maintenance processes to support ongoing management.

Phase 5 – Warranty and Maintenance

1. Maintenance and Support .

Minimum warranty period: 10 weeks

- Ensure the stability and reliability of the Government Wallet through regular updates and enhancements.
- Address user-reported issues promptly and effectively to maintain system quality.
- Perform regular security audits and vulnerability assessments to safeguard the system against threats.
- Implement mechanisms to gather user feedback for continuous system improvement.

6. EXPECTED DELIVERABLES AND TIMELINES

The Consultant shall prepare and submit all reports as per the schedule below, electronically in Word and PDF formats to the client. The final report should also be submitted electronically, as well as duplicate hard copies. The language of all deliverables must be in English.

#	Deliverable	Description	Weeks After Contract Signing	Payment %
1	Inception Report	Confirmation of assignment understanding, detailed methodology, work plan, project schedule, governance arrangements, and risk management approach.	3	10%
2	Validated Requirements Document	Functional and non-functional requirements finalized and approved following stakeholder consultations.	9	15%
3	System Design & Architecture Documentation	High-level and detailed system design, security architecture, integration specifications, hosting recommendations, deployment architecture, and implementation plan.	13	15%
4	System Development & System Testing	Development and configuration of the Government Secure Wallet Wallet, including configuration of the Testing/Training and Production environments, completion of functional, integration, performance, and security testing, and submission of a System Test Report.	24	20%
5	User Acceptance Testing (UAT) & Production Deployment	Support UAT, resolve defects, obtain formal client acceptance, complete production deployment, and execute cutover activities.	30	10%
6	Training & Knowledge Transfer	Deliver administrator and end-user training, knowledge transfer sessions, user manuals, technical manuals, and training completion report.	34	10%

7	Go-Live Support & System Stabilization	Provide intensive post-implementation support for a minimum of six (6) weeks, including system monitoring, issue resolution, performance tuning, and operational stabilization.	40	10%
8	Warranty & Maintenance Support	Provide ten (10) weeks of warranty and maintenance support, including bug fixes, security patches, minor configuration changes, and technical support in accordance with the agreed SLA.	50	5%
9	Final Handover & Project Closure Report	Submit the final project report, source code, configuration files, system documentation, sustainability recommendations, and confirm successful completion of the warranty period.	50	5%

7. DURATION

The consultancy is expected to be completed over **50 weeks'** period from contract signature.

8. EXPERTISE REQUIRED

8.1 The consulting firm must demonstrate the following minimum qualifications and experience:

1. At least five (5) years of proven experience in the design, development, and implementation of digital payment platforms, Government Secure Wallets, or comparable FinTech solutions.
2. Demonstrated experience integrating ICT or payment systems with government platforms, databases, or service portals, including the use of APIs and authentication services.
3. Proven experience in developing and deploying secure, scalable web and mobile applications, with strong user experience and interoperability features.
4. Demonstrated capacity to implement secure solutions aligned with international standards such as PCI DSS, ISO 27001, ISO 20022, or equivalent.
5. Successful completion of at least three (3) assignments of similar scope and complexity (e.g., national-level payment systems, e-government platforms, or enterprise-level integrations).

6. Demonstrated experience delivering assignments for public sector clients in the Caribbean, OECS, or comparable jurisdictions.
7. Prior experience managing projects financed by international development partners (e.g., World Bank, Caribbean Development Bank, UNDP) will be considered an asset.

8.2 **Key Experts and Qualifications**

While Key Experts will not be evaluated at the shortlisting stage, firms must demonstrate at the proposal stage that they can provide a team with the following expertise:

a) Lead Systems Architect / Project Manager

- Advanced degree in ICT, Computer Science, Information Systems, or a related field.
- Minimum of ten (10) years of professional experience in ICT systems design, project management, and implementation of large-scale government or enterprise systems.
- Proven track record in leading digital payment, e-government, or FinTech integration projects.
- Strong knowledge of systems architecture, API integration, and cloud-based solutions.

b) Digital Payment Specialist

- Degree in Finance, ICT, or related discipline.
- Minimum of seven (7) years of professional experience in the design and deployment of digital payment solutions, Government Secure Wallets, or transaction processing systems.
- Familiarity with payment compliance standards such as PCI DSS, ISO 20022, or equivalent.
- Experience with financial regulations and payment integration within the Caribbean context will be considered an asset.

c) Technical Development Specialist (Mobile/Web and Integration)

- Degree in Computer Science, Software Engineering, or related discipline.
- Minimum of seven (7) years of professional experience in mobile and web application development **and** database/system integration.
- Proven expertise in designing and managing secure, scalable applications with robust APIs and interoperability features.

- Experience with database management, system performance optimization, and integration with government service platforms.

d) Cybersecurity and Compliance Specialist

- Degree in Information Security, ICT, or related discipline.
- Minimum of seven (7) years of professional experience in cybersecurity, encryption, cloud security, and compliance frameworks.
- Hands-on experience with secure digital payment environments and fraud prevention.
- Knowledge of international and regional data protection and privacy legislation.

Firms may propose additional experts as required to deliver the assignment effectively.

9. STAKEHOLDER LISTING

The Consultant will engage the following stakeholders during the project:

- Division of Public Sector Modernization
- Department of Transport
- Civil Status Registry
- Division of Labour
- Citizenship Department
- Registry of Companies
- Accountant General's Office
- Treasury
- Electoral Department

10. LIST OF DOCUMENTS

The Consultant will be provided with the following documents: To be confirmed during contract negotiations.

11. REPORTING

The Consultant will:

- Report directly to the Project Manager of the Project Implementation Unit (PIU) within the Ministry of the Public Service.
- Work closely with and other key stakeholders as directed by the PIU to ensure the successful execution of the consultancy.

12. RESPONSIBILITIES

12.1The Consultant will be responsible for the following:

- Cover all necessary expenses, including:
  - Direct staff costs
  - Office space and facilities
  - Computer systems and software
  - Telecommunication systems
  - Travel expenses
  - Hard copy report deliveries
  - Any additional incidentals required to complete the consultancy.
- The Consultant shall remain fully responsible for the performance of the Services, including any activities undertaken by joint-venture members or approved sub consultants
- Respect and comply with the agreed project timeframes, ensuring timely execution of tasks and milestones.
- Conduct all stakeholder meetings in a professional and responsible manner, fostering a collaborative and respectful environment.
- Guarantee the validity and reliability of all tools and instruments developed or utilized by the Consultant for training sessions, workshops, or other engagements.
- Ensure confidentiality of all aspects related to the consultancy process, safeguarding sensitive information.
- Prepare all submissions in English and deliver them in the format and through the media specified by the Project Implementation Unit (PIU).
- Submit all deliverables on or before specified deadlines, maintaining timeliness and alignment with project timelines.

12.2 As the Executing Agency for the Project, the PIU will support the implementation of this consultancy through the following actions:

i. Arrange interviews and provide the Consultant with access to Project documents, existing regulations, legislations, and policies, as well as other

relevant organizational process assets required to carry out the consultancy effectively.

ii. Designate a focal point within the PIU to guide the Consultant, assisting in coordinating activities and providing direction as needed to ensure alignment with project objectives.

iii. Supply the Consultant with all relevant and appropriate information necessary for the consultancy's successful execution, ensuring that the Consultant has access to up-to-date data and resources.

ANNEX I

Envisioned Components of the Government Wallet

The following sections shall provide a brief overview of the key functionalities and components.

- **Mobile Application and Web Portal**

a. The Government Wallet shall be accessible through both a mobile application and a web portal. The mobile application shall be available for both **iOS and Android** devices, ensuring broad accessibility for users.

b. The web portal shall provide an alternative access point for users who prefer to manage their digital documents using a desktop or laptop computer.

c. Both the mobile application and web portal shall provide a consistent, responsive, and intuitive user interface and user experience (UI/UX), ensuring seamless navigation and functionality across platforms.

d. The web portal shall be compatible with the latest stable versions of all major web browsers, including, at a minimum, **Google Chrome, Microsoft Edge, Mozilla Firefox, Apple Safari**, and any other commonly used standards-compliant browsers. The solution shall maintain consistent functionality, performance, and presentation across supported browsers.

e. The mobile application and web portal shall comply with recognized accessibility standards (e.g., **WCAG 2.1 Level AA**) to ensure usability for persons with disabilities.

- **User Registration and Verification**

a. Users shall be able to register using their unique identification number (e.g., National Identification Card (ID)).
b. The registration process should include verification of user identity and contact information as well.
c. Additionally, 2 factor authentication, biometric authentication methods such as fingerprint and facial recognition and the ability to utilize common authenticators

such as Google Authenticator, Microsoft, Authenticator, etc. shall be supported to provide an extra layer of security and convenience for users.

- **User Authentication and Authorization**

a. To ensure that only authorized users can access the Government Wallet, the solution must implement robust user authentication and authorization mechanisms. This is to ensure that documents are only accessible to authorized users and are protected from unauthorized access and breaches.
b. Support third party identity validation and verification for NAF as a service through the wallet. User have full control of their data and can approve, deny or provide selected access to personal data request by third party agencies.
c. The system shall provide users with multiple secure login options. At a minimum, users shall be able to authenticate using their registered mobile number. Consultants may propose additional authentication methods, such as email address, username, or integration with a national digital identity platform, to enhance usability and security.

- **Document Storage and Management**

a. The Government Wallet shall allow users to also upload, store, and manage their own digital documents for safekeeping.
b. The system shall provide 1GB of storage space for registered users, allowing them to upload an unlimited number of documents if the total storage used does not exceed the allocated space.
c. The system shall support various document formats, including PDF, JPEG, and PNG, with each file not exceeding 10MB in size.
d. Users shall be able to manage their own uploaded documents, including viewing, renaming, downloading, moving, and deleting files.
e. The System should allow for automatic documents updates from key GOSL systems on renewal or approval by the relevant authority,
f. Users shall be able to categorize their documents for easy retrieval and search.

g. User shall be able to create folders based on document types (e.g., ID proofs, educational certificates, Govt Issued Certs) or specific purposes to keep your documents organized.
h. The solution should also provide features for document sharing, allowing users to share their documents with government agencies and other authorized entities securely.
i. Features such as easy document categorization, search functionality shall be provided to make it easier for users to manage their documents.
j. Additionally, the system shall facilitate self-attestation of users' own uploaded documents.

- **Integration with Government Services and Partner Organisations**

a. The Government Wallet shall seamlessly integrate with existing government services to enable the publication and retrieval of documents and credentials. This integration is crucial for ensuring that users can access their documents directly from the relevant government systems. For instance, if a user wants to retrieve their Driver's license or ID card, the Government Wallet shall fetch this document from the appropriate government organization's system.
b. Government organizations and other issuers shall be able to push digital copies of documents directly to the user's Government Wallet account.
c. The approved partner organisations such as educational institutions, Fintech industry & private sector organisation shall be able to integrate with the Government Wallet to support payments and third party identify request and verification.
d. APIs to be developed to facilitate secure data exchange between the Government Wallet and organisation's systems.

- **Data Encryption and Security Measures**

a. Security is a paramount concern for the Government Wallet. The solution shall implement comprehensive data encryption measures to protect user information. This includes encrypting data both at rest and in transit, ensuring that it is secure from unauthorized access and breaches.

b. Regular security audits and vulnerability assessments shall be conducted to identify and address potential security risks. The solution must also comply with relevant data protection regulations, such as local data privacy laws, to ensure the privacy and security of user data.

- **Document Sharing**

a. The users shall be able to securely share their documents with government agencies and other third parties. This feature aims to streamline processes such as applying for government services or verifying identity.
b. Users shall be able to remove the sharing at any time, ensuring they have full control over who can access their information.
c. Additionally, users shall be able to set time limits for each consent/sharing, specifying how long a third party can access their documents. This feature is to ensures that users can securely share their documents with authorized entities for a specified period, enhancing privacy and control over their personal information.

- **QR Code for Document Verification**

a. The system shall support the generation of secure QR code for issued documents. This feature shall allow users and authorized entities to quickly access and verify the authenticity and validity of a document by scanning a QR code associated with it.
b. The solution shall include an option to scan Secure QR codes for accessing and verifying the authenticity of documents.

- **Digitally Signed Documents**

a. The system shall include an option for Government agency issued documents as digitally signed documents, ensuring their authenticity and integrity.
b. Additionally, the system shall facilitate self-attestation of users' own uploaded documents.
c. Recipients of these documents shall be able to easily verify their authenticity and integrity by checking the digital signature, ensuring that the documents have not been altered or tampered with.

- **W3C Verifiable Credentials Support**

    a. The system shall provide support for documents and credentials that are issued by organisations in a format that confirm to W3C Verifiable Credentials Data Model (VC DM) 2.0 standards. The W3C VC DM 2.0 standards enhance the security, privacy, and interoperability of digital credentials, ensuring they are trustworthy and verifiable across different systems.

    b. User shall be able to store, view, share and manage the documents and credentials that confirm to W3C VC DM 2.0.

- **Nominee Management Feature**

a. The system shall include a Nominee feature, allowing users to designate a trusted individual who can access their digital documents in the event of the user's incapacity.

b. Users shall have the ability to manage their nominee list, including adding or removing nominees at any time. This management capability is to ensures that users can keep their nominee information up-to-date and make changes as their circumstances evolve.

c. The nominee shall be granted access through a secure authentication process, ensuring the confidentiality of the documents.

- **GOSL Payment Wallet Services**

The platform shall enable citizens and residents to securely make payments for Government services through the Government Government Secure Wallet. The solution shall:

a. Support multiple electronic payment instruments, including, where applicable, credit cards, debit cards, bank transfers, mobile money, Apple Pay, Google Pay, PayPal, and other payment methods approved by the Client.

b. Integrate with approved Government payment gateways and financial institutions to facilitate secure electronic payments.

c. Provide real-time payment status updates, notifications, and digital receipts.

d. Support end-to-end transaction reconciliation, reporting, and audit trails.

e. Be designed to accommodate future integration with additional payment service providers and digital payment mechanisms.

- **Notifications and Alerts**

The system shall provide real-time notifications and alerts to keep users informed about the status of their documents and any actions required. For example, users may receive alerts when a document is about to expire (e.g. Drivers' License) or revoked or when a new document has been added to their Government Wallet. Notifcation and alerts also when third party request and for access and/or verification for Personal Identifiable Information through the wallet.

- **Audit Trails**

To ensure transparency and accountability, the system must maintain detailed audit trails of all user actions. This will allow users to see a history of their interactions with the Government Wallet and provide a record of document access and modifications.

- **Performance**

a. The system shall be designed to efficiently support a high volume of concurrent users and transactions. It shall be scalable to accommodate future growth in the user base, transaction volumes, and digital document storage requirements.
b. The system shall provide fast response times for user actions to ensure a smooth, reliable, and responsive user experience. Consultants shall describe the expected performance characteristics of the proposed solution under normal and peak operating conditions.
c. Availability: The solution shall be designed for continuous operation (24 hours per day, 7 days per week, 365 days per year) and achieve a minimum 99.98% system availability (uptime**)**, excluding scheduled maintenance periods agreed with the Client.
d. The proposed solution should include appropriate high-availability features, redundancy, monitoring, and failover mechanisms to achieve the required availability and minimize service interruptions.
e. Consultants shall clearly describe how the proposed architecture, infrastructure, and support arrangements will achieve the required performance and availability targets, including any assumptions, dependencies, and planned maintenance windows.

- **Administrative Portal**

a. An administrative portal/module shall be provided for government officials and administrators to manage the Government Wallet system.

b. This portal shall include features for user management, document management, partner management, system monitoring, and configuration settings.

- **Reports and Statistics**

The solution shall include a reporting component that provides detailed reports and statistics on system usage, document uploads, user activity, and other key metrics. This information will help administrators monitor the system's usage and make data-driven decisions.

- **User-Friendly Interface**

The user interface of the Government Wallet shall be designed with usability in mind. The goal is to provide an intuitive and accessible interface that users of all ages and technical abilities can easily navigate.

- **Help and Support**

The system shall provide users with access to help and support resources, including FAQs, user guides, and customer support contact options. Users shall be able to find answers to common questions and get assistance with any issues they encounter.

- **Feedback Mechanism**

The system shall allow users to provide feedback on the app's functionality and usability, facilitating continuous improvement. Users shall be able submit suggestions, report issues, and provide general feedback to help enhance the app.