

**Ministry of Information Technology, Communication and Innovation**

**Request for Information (RFI)**

**from Potential Suppliers for the**

**“Development of a SuperApp based on Verifiable Digital Credentials in a Secure ID Wallet”**



**Reference No: MITCI/RFI/02/2025-26**

**Date Issued: 11 September 2025**

**Project Overview**

The Ministry of Information Technology, Communication and Innovation (MITCI), prior to issuing a bidding document, is seeking information from potential suppliers with capabilities to design, develop and implement a SuperApp that integrates a Digital ID wallet. This Super App should be able to interface a digital Assistant which makes the digital ID wallet easier for less tech-savvy users by reducing manual navigation.

**Purpose of this RFI**

The objectives of the RFI are to:

* Gain a comprehensive understanding of available market solutions for integrating Distributed Identifiers (DIDs) into the SuperApp’s identity and authentication system.
* Gather information on potential technologies and platforms (including open source) that support both W3C and ISO mDoc standards-based workflows.
* Explore the capabilities, experience and qualifications of potential Suppliers.
* Identify approaches to ensure scalability, security and compliance with privacy regulations

**Description of Requirements and Scope of Project**

* The MITCI intends to implement a SuperApp and integrate multiple functions, including identity verification and payment platform into a unified digital ecosystem. This initiative has the potential to transform service delivery by creating a seamless, efficient and citizen-centric digital experience.
* Development of a SuperApp and integrate Self-Sovereign Identity through W3C compliant DIDs and support implementation of verifiable credentials for e.g mobile driving license (mDL), birth certificates, marriage certificates, etc. in alignment with emerging standards.
* To leverage on MauPass platform for authentication to the SuperApp.
* The solution shall support selective disclosure of information including the use of Zero-Knowledge Proofs (ZKPs) (e.g., proving age without disclosing a date of birth, etc). It must also include robust credential revocation /recovery mechanisms. An effective consent management for selective disclosure should be available.
* Development of a Verifier App - to enable third parties to verify the credential without the need to contact the issuer. Online/offline verification including verification of printed documents. All actions on digital wallet/ verifications to be audit trailed.

1. **In order to comply with the above requirements, this digital ID wallet should be built to comply with both the W3C Verifiable Credentials (VC) model and the ISO mDoc standard which means**:

* The ISO mDoc workflow enables a digital ID wallet to receive signed mDocs (issuance), generate mPresentations with selective disclosure of requested attributes including zero-knowledge proofs (presentation) and support both online PKI-based verification and offline trust-list-based verification, ensuring secure and interoperable digital identity.
* W3C standards workflow ensures that a digital ID wallet can receive VCs (issuance), generate VPs with selective disclosure of claims including zero-knowledge proofs (presentation) and support both online and offline verification through a stack of interoperable specs — VC Data Model, DID Core, cryptographic proof suites, and APIs.
* The wallet should be able to implement multiple DID methods so the same software can:
* Issue a VC with a did:web (anchored to an official gov domain) for legal trust.
* Issue a VC with a did:peer for privacy-preserving selective disclosure in user-to-user interactions.
* Still support did:ion or did:ethr for global, decentralised use cases.
* Use blockchain-based DIDs for use cases requiring strong decentralisation and anchoring on a public ledger as the trust anchor.

Or

* Use non-blockchain DIDs (like did:web, did:peer) for:
  + - faster, simpler resolution.
    - integrating with existing government PKI or ISO mdoc trust frameworks.
* The wallet should be able to handle protocol selection automatically with the use of a middleware or the wallet’s protocol manager to decide which flow to run based on the verifier’s request type.

1. **Interfacing of a Digital Assistant with the Digital ID Wallet**

* Natural Language Interaction whereby the assistant acts as a voice/chat interface on top of the wallet app.

Users can ask the assistant things like:

* + “Show me my driver’s license.”
  + “Renew my ID.”
* Transaction Support
  + Initiating payments by voice: “Pay $50 to John with my bank card.”
  + Confirming transactions with biometrics (fingerprint/FaceID) after the assistant triggers the request.
* Personalised Guidance
  + Proactive reminders: “Your ID expires in 30 days, do you want to renew?”
  + Expense summaries and insights (“You spent $200 on transport this month”).
* Security and Privacy Layer

The assistant never directly handles raw credentials. Instead, it sends requests to the wallet’s secure API, which executes the action within the secure element or trusted environment. Authentication (PIN, FaceID, fingerprint) is still enforced before sensitive actions.

1. **As an option indicate the possibility of Integrating a sovereign cloud with the digital ID wallet by hosting issuers, trust registries, revocation/status services, and verification endpoints in jurisdiction-controlled infrastructure, ensuring data sovereignty, legal compliance, selective disclosure with ZKPs, and secure online/offline verification.**

Potential suppliers are requested to review all the information provided in this RFI and submit their responses using the designated Response Form/Questionnaire.

**Presentation or Demonstration**

The MITCI reserves the right to invite any respondent(s) to carry out a presentation or demonstration of a prototype of their proposed solution within three (3) weeks following formal notification from the Ministry.

All costs associated with the presentation or demonstration shall be borne by the potential suppliers.

**Important Note:**

**It is important to note that:**

1. **Any financial information provided will be used to assist in budgetary estimation for the project and will be kept confidential.**
2. **Potential suppliers are responsible for all costs associated with the preparation and submission of their response.**
3. **Publication of RFI not constitute an Invitation for Bid and does not oblige Government of Mauritius to procure services referred in the RFI.**
4. **Your response will assist in the conception of technical specifications to be included in the bidding document for the SuperApp project.**

**Review Criteria**

The MITCI will review all responses received according to the key criteria below:

* **Technical Capabilities: Feasibility, security, and interoperability of the proposed solution.**
* **Experience and Expertise**: Proven experience with DIDs, Digital wallet and related technologies.
* **Scalability and Flexibility**: Ability to scale up the SuperApp with increasing users and credentials.
* **Compliance**: Adherence to privacy regulations and data protection standards.
* **Financial Capability**: Check financial soundness and ability to execute the project over long term

Should the MITCI thereafter decide to carry out a bidding exercise, same would be conducted in accordance with the Public Procurement Act 2006.

**Confidentiality**

All responses to this RFI will be treated as confidential and used solely for the purpose of gathering insights for this project. Potential Suppliers should not include any proprietary or sensitive information unless clearly labeled as such.

**Potential suppliers are requested to review all the information provided in this RFI and submit their responses using the designated Response Form/Questionnaire.**

**Instructions to Prospective Suppliers/firms**

**Proposal Submissions**

Proposals in response to this RFI, together with any additional information and / or supportive documents, shall be addressed to the **Permanent Secretary, Ministry of Information Technology, Communication and Innovation, 6th Floor, SICOM Tower, Wall Street, Ebene** and must be placed in a sealed envelope, clearly marked:

**“DEVELOPMENT OF A SUPERAPP BASED ON VERIFIABLE DIGITAL CREDENTIALS IN A SECURE ID WALLET)” Ref: MITCI/RFI/02/2025-26**

The sealed envelope should bedeposited in the Tender Box situated **on 6th Floor, SICOM Tower** at the **Ministry of Information Technology, Communication and Innovation, Wall Street, Ebene** or submitted/sent by registered post or Courier Service located at the **Registry of the Ministry of Information Technology, Communication and Innovation, 6th Floor, SICOM Tower**, **Wall Street, Ebene** on or before **10 October 2025 at 13.30 hours (Mauritian time)**.

Prospective Suppliers/firms requiring any clarification on this RFI shall notify the **Ministry of Information Technology, Communication and Innovation** by addressing a written request to the **Permanent Secretary**, **Ministry of Information Technology, Communication and Innovation,** through email at [**prampadarath@govmu.org**](mailto:prampadarath@govmu.org) **with copy to the Secretary, Departmental Bid Committee, e-mail address: mmaureemootoo@govmu.org** 14 days before the closing date of the RFI.

The **Ministry of Information Technology, Communication and Innovation** will respond to any request for clarification **within 7 days before the deadline for submission** of the RFI. Replies to all requests for clarification received from respondents shall be made available to all prospective firms.

**Information Required**

As stated above, the objective of this RFI exercise is to compile as much useful information as possible from prospective suppliers on the **DEVELOPMENT OF A SUPERAPP BASED ON VERIFIABLE DIGITAL CREDENTIALS IN A SECURE ID WALLET.** In this respect, suppliers are required to fill in the Questionnaire as detailed hereunder:

Response Form/Questionnaire

To be filled by the Potential Supplier (All fields marked with an ‘\*’ are mandatory)

Please feel free to expand the answer box as needed or attach additional pages if more space is required.

|  |  |  |
| --- | --- | --- |
| No | General Company Information | |
|  | Name of Company\* |  |
|  | Company’s Authorised Representative | |
| * Name\*: |  |
| * Address\*: |  |
| * Telephone\*/Fax Numbers\*: |  |
| * Email Address\* |  |
|  | Experience   * Development of SuperApp   *Include examples of projects, scope, technologies used, platform supported (iOS/Android/AppGallery)*   * *Capabilities with integrating public and private blockchain networks in large-scale apps*   *Include specific blockchains worked with (e.g Ethereum, Hyperledger etc), architectural approaches and scalability considerations.*  *Any previous experience with Self-Sovereign Identity (SSI) systems, Verifiable Credentials (VCs) and Digital wallet.*   * *use of Zero-Knowledge Proofs (ZKPs)*   *Provide examples of your experience or knowledge in implementing ZKPs, specifically in the context of Verifiable Credentials (VCs) and Distributed Identifiers (DIDs).*   * Verifier App   *Online/offline & verification of printed documents including consent management on the Digital wallet*   * Ability to design, audit and deploy smart contracts/broker services.   *Highlight any tools used (e.g Truffle, Hardhat, Slither) and past deployment examples.*   * Experience with W3C compliant DIDs *Describe your experience in issuing, storing and verifying W3C-compliant DIDs. Mention any relevant standards implemented (e,.g. DID Core, Verifiable Credentials), identity frameworks used and real-world deployments.* * Experience with ISO mDoc standards which covers issuing, storing, and verifying ISO/IEC mDocs, implementing 18013-5 and 23220 series standards, integrating with PKI trust frameworks, and delivering real-world pilots for national ID, driver’s licenses, and cross-border verification. * Multi-platform development framework used   *e.g. Flutter, React Native etc.* |  |
|  | Staff Details  *Key personnel that could be assigned to the project highlighting their relevant skills, expertise and experience.* |  |
|  | Financial capability  *To support and execute large-scale implementation (over 500k citizens expected)*  *To provide audited financial statement for the past 3 years* |  |

|  |  |  |
| --- | --- | --- |
|  |  | |
| A | Technical Approach | |
|  | Integration Strategy  *Approach for integrating DIDs into a SuperApp ecosystem, including among others APIs, SDKs, blockchain and wallet management. Details about public and private blockchain platforms supported.* *VC broker service for issuing/verifying credentials.*  *Potential Supplier may also provide information on open source platform* |  |
|  | Interoperability  *How will the solution ensure interoperability with existing identity systems, external verifiable credential issuers (Scanning of QR Codes)* |  |
|  | Security and Privacy  *How does the solution ensure security, privacy and compliance. Describe any encryption or data protection strategies used. Use of ISO standards on Privacy (i.e. ISO 27701)*  *How the proposed solution addresses common risks related to method being used or the underlying technology?*  *Use of ISO/IEC 18013-5/7 or the latest in case of mobile driving license (mDL),* ISO/IEC 18004 for QR Code, PDF/UA (ISO 14289) for document format, ISO 22739 for blockchain and distributed ledger. |  |
|  | Architecture - *Provide a sample architecture for the proposed solution* |  |
| B | User Experience (UX) |  |
|  | Onboarding Process  *How the proposed solution will handle user onboarding,* DID creation, and recovery? How does the process remain seamless and user-friendly? |  |
|  | User Control/consent management  *How to ensure that users have full control over their DIDs and the information being shared across other services?*  *How to proceed with selective disclosure of information in a user-friendly manner* |  |
|  | Cross-Service Identity Use  *How will users use their DID across various services within the SuperApp, such as payments and messaging?* |  |
| C | Scalability and Future-Proofing |  |
|  | Scalability –  *in terms of additional users/Issuers/Verifiable credentials for over 500k users expected.* |  |
|  | Future-Proofing  *Describe how additional verifiable credentials from different Issuers would be integrated in the wallet*  *How adaptable is your solution to future standards, evolving regulations (for e.g eIDAS 2.0), or new DID methods?* |  |
| D | Implementation Timeline/ongoing support |  |
|  | *Estimated Timeline for implementing DIDs in the SuperApp, including key milestones, VC broker services and Verifier App* |  |
|  | Maintenance and Support  *Describe the ongoing support and maintenance options available for the solution.* |  |
| E | Reference |  |
|  | Case Studies and References  *Provide details of case studies or references from similar projects where you have implemented DIDs or self-sovereign identity solutions.* |  |
| F | *Regulatory framework*  *Describe in details if any changes in the laws/Regulations is required to establish the Self Sovereign Identity ecosystem and Digital wallet* |  |
| 1. | *Any other additional information* |  |

**Responses are Authorised By:**

|  |  |  |  |
| --- | --- | --- | --- |
| Signature: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Name: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Position: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Date: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Authorised for and on behalf of: | |  | *(DD/MM/YY)* |
| Company: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | |

**NOTE:**

1. The above list of information is not exhaustive and suppliers may submit additional information or support documents including brochures, catalogue and pamphlets to enable the **Ministry of Information Technology, Communication and Innovation** to better assess their experience and capabilities.
2. All information submitted shall be in English.
3. The **Ministry of Information Technology, Communication and Innovation** may request further clarifications from potential project firms during the assessment of the information received in response to the RFI.
4. All costs incurred in the preparation of the proposal for the RFI shall be borne solely by the project firm.

**Way Forward:**

Following the receipt of the information resulting from the RFI exercise, the **Ministry of Information Technology, Communication and Innovation** will carry out a detailed assessment / examination of the information obtained. On the basis of these findings, the **Ministry of Information Technology, Communication and Innovation** will compile a list of potentially qualified suppliers in terms of the project of **the Development of a SuperApp based on Verifiable Digital Credentials in a Secure ID Wallet** detailed in this RFI.

The **Ministry of Information Technology, Communication and Innovation** may, thereafter, proceed with a competitive bidding exercise by launching a procurement exercise to invite potential firms to submit binding offers.

**Procurement Process:**

In the event the Client intends to carry out a competitive bidding exercise, the **Ministry of Information Technology, Communication and Innovation** shall provide along with the procurement document, all the terms and conditions governing the contract.

**NOTE**:

This RFI is not a tender exercise and the **Ministry of Information Technology, Communication and Innovation** reserves the right:

1. to annul this RFI exercise without incurring any liability to any party; and / or
2. not to proceed with a formal procurement exercise subsequent to this RFI.