# Request for Information (RFI)

## Project: Decentralized Credentialing & Verification Layer (DCVL)

**Entity:** Digital Transformation Office (DTO)
**Ministry:** Ministry of Education and Higher Education (MEHE), Lebanon
**Context:** Higher Education Directorate (HED)

### 1. Purpose & Strategic Context

The Ministry of Education and Higher Education (MEHE) is seeking information for the design and implementation of a **Decentralized Credentialing & Verification Layer (DCVL)**.
The primary strategic driver is the establishment of **"Equal Trust"** (Zero-Trust architecture) between the Directorate of Higher Education and licensed Higher Education Institutions (HEIs). The solution must ensure that the integrity of academic credentials is programmatically guaranteed, preventing any single party from unilaterally issuing or altering a verified record.

This Request for Information (RFI) is issued solely for information and planning purposes and it is separate and independent document from the solicitation and shall not be considered as part of the solicitation.

### 2. The "Equal Trust" Mandate

Vendors must propose an architecture that adheres to these non-negotiable principles:

- **Co-Sovereign Issuance:** A credential is only "Valid/Attested" if it carries the cryptographic signatures of both the issuing HEI and MEHE.
- **Structural Risk Elimination:** The design must eliminate the risk of a "Rogue Admin" at the Ministry or the Vendor level. Critical operations (key handling, signing) should occur at the "Edge" (HEI environment) rather than on centralized Ministry-hosted infrastructure.
- **Interoperability:** Credentials must align with global standards (**W3C Verifiable Credentials** and **Decentralized Identifiers**) to allow instant, independent verification by third parties (employers, foreign universities) without MEHE's direct intervention.

### 3. Expected Functional & Technical Flow

The proposed solution should support the following end-to-end lifecycle:

1. **Data Preparation (HEI):** The University prepares the graduation dataset within their local environment.

2. **Primary Signing (HEI Edge):** The HEI cryptographically signs the dataset using a private key shard/wallet. *Crucial: This signature must be generated locally and never pass through a Ministry-controlled proxy.*
3. **Transmission & Validation (MEHE):** The signed record is transmitted to the Ministry's HEDS/DTO environment for administrative audit and accreditation check.
4. **Co-Signing (MEHE Edge):** Upon approval, the Ministry applies its cryptographic signature.
5. **On-Chain Anchoring:** The "Double-Signed" hash is anchored to a public or hybrid blockchain (e.g., L2) to create an immutable proof of truth.
6. **Student Possession:** The student receives a digital certificate (W3C VC) that they "own" and can share.
7. **Independent Verification:** A third party scans a QR code to verify the proof against the blockchain directly, bypassing MEHE's servers.

## 4. Vendor Technical Questionnaire

The Ministry of Education and Higher Education requests that suppliers/vendors provide as much information as they can to the questions below.

Subsequent to this RFI and the submissions received, the DTO may seek clarifications to the information provided by your organization. In your response, kindly advise an appropriate contact (i.e. name, email address and telephone number) to whom the DTO may request such clarifications.

Please provide explicit answers to the following:

- **Q1: Trust Boundary:** How do you ensure that an HEI's digital signature cannot be intercepted or forged by a Ministry IT administrator?
- **Q2: Key Management:** Describe your approach to **Multi-Party Computation (MPC)**. Where do the key shards live?
- **Q3: Data Privacy:** Confirm that no PII (Personally Identifiable Information) is stored on-chain. How is the "Privacy vs. Integrity" balance managed using Zero-Knowledge Proofs (ZKP)?
- **Q4: Integration:** How does your "Verification Engine" integrate with our existing SQL-based HEDS system without creating a new data silo?
- **Q5: Blockchain Justification:** Why is your chosen ledger approach superior to a standard immutable database (e.g., SQL Ledger) for achieving "Equal Trust"?

## 5. Scope of Submission

Respondents should include:

- **Trust Boundary Diagram:** A map showing exactly where data is signed and where keys are stored.
- **Onboarding Strategy:** How you will onboard 40+ Universities with minimal technical burden on their IT teams.
- **Sustainability Model:** Clarity on transaction (Gas) fees and long-term ownership of the smart contracts.

## 6. Submission Guidelines

This is an RFI only. Responses will be used to define the formal RFP.

Submitted information will be used by the Ministry for internal planning purposes and shall be kept strictly confidential.

Please respond electronically by emailing your response to:

**Emails:** lJabboury@mehe.gov.lb

LRabih@mehe.gov.lb

**Deadline to provide a response: 02/07/2026**