

## NOTICE OF PUBLICATION

**Subject:** Clarifications Batch 2

The Authority hereby publishes its official responses to clarification questions received from prospective bidders during the clarification period, in connection with the RFP for the Supply of System & Card Management.

The attached document contains sixteen (16) clarifications and is made available on both official portals:

- [www.ppa.gov.lb](http://www.ppa.gov.lb)
- [www.tmo.gov.lb](http://www.tmo.gov.lb)

These responses do not modify, amend, or supplement the requirements of the RFP. In the event of any discrepancy between the responses and the RFP, the RFP shall prevail.

All bidders are advised to take note of these responses in the preparation of their submissions. Further batches of clarifications, if any, will be published through the same channels in due course.

رئيس مجلس الإدارة  
المدير العام بالتكليف  
القاضي مروان عبود

٥٩-٢-٢٠١٩

## TMO — Traffic Management Operation

### OFFICIAL CLARIFICATIONS AND RESPONSES

Batch 2 — 16 April 2026

*The Authority hereby publishes its responses to clarification questions received in connection with the RFP for the Supply of System & Card Management. These responses are based on the RFP and do not modify, amend, or supplement its requirements. In case of any discrepancy between these responses and the RFP, the RFP shall prevail.*

#### Section 1: Eligibility and Administrative Clarifications

##### Clarification Q-001

*RFP Reference: Article 4 — Acceptable Bidders / Similar Project Definition*

**Question:** Kindly clarify whether the bidder is required to have prior experience implementing systems specifically related to vehicle registration and driver licensing in other countries, or if it is sufficient to demonstrate experience in implementing similar components and technologies required under this RFP (e.g., smart card issuance, biometric integration, system integrations, etc.).

**Response:**

The RFP requires the delivery of an integrated vehicle registration and driver licensing platform — not a credential-supply solution in isolation. The scope of the Authority's procurement encompasses both (a) the supply of security credentials (driving licenses, vehicle registration cards, and RFID e-stickers) and (b) the end-to-end management of the full credential lifecycle, including issuance, personalization, biometric capture and matching, payment orchestration, identity verification, revocation, renewal, replacement, and integration with the relevant government and private-sector counterparts.

Accordingly, in order to qualify as "similar project" experience under this RFP, a bidder must demonstrate prior experience in the implementation and operation of a system that both supplies AND manages smart security credentials. Experience in credential supply alone, without the associated lifecycle-management and operational functions, does not satisfy this requirement.

Within this eligibility framework, the technical evaluation shall further score more favorably bidders that can demonstrate prior experience on systems of comparable scope to the one sought under this RFP. The relative weighting of similar-project experience is set out in the RFP's technical evaluation criteria and shall be applied by the Evaluation Committee accordingly.

---

##### Clarification Q-002

*RFP Reference: Special Conditions — First-Batch Delivery and Payment Terms*

**Question:** Kindly confirm whether the quantities specified for the first year (DL: 227,424 / VR: 174,016 / RFID: 200,000) will be procured and paid in advance to the awarded supplier.

**Response:**

Bidders are kindly requested to refer to the RFP for the card procurement quantities and payment terms. The relevant sections include the financial evaluation provisions and the Special Conditions of Contract regarding goods pricing and invoicing.

-----

**Clarification Q-003**

*RFP Reference: Special Conditions — Supplier Arrangements and Authority Rights*

**Question:** It is understood that the supplier is required to commit pricing for up to 1,000,000 cards per type over a 5-year period. Kindly clarify whether the Authority reserves the right to change the supplier during this period, or if the awarded supplier retains exclusivity throughout the contract duration.

**Response:**

Bidders are kindly requested to refer to the RFP regarding supplier arrangements and the Authority's rights. The relevant provisions are set out in the Special Conditions of Contract.

-----

**Section 2: Technical Clarifications — Infrastructure and Equipment**

**Clarification Q-004**

*RFP Reference: Activity Schedule — Existing Equipment and Site Inspection*

**Question:** Kindly provide a detailed inventory of the existing hardware assets across all branches and headquarters that are reusable and operational, including branch name, hardware type, quantity, technical specifications, purchase date, warranty expiry date, brand, and current condition.

**Response:**

The specific brand, model, quantities, condition, and site distribution of all existing hardware assets across all branches and headquarters will be disclosed during the mandatory site visit. Bidders are expected to assess the operational requirements during the visit and propose equipment quantities accordingly in their technical offer, included under all-inclusive pricing (PSF, CARC, CGAM). The Authority may establish up to two (2) additional branches (pursuant to Decree 11244/2003, Article 4) in the future, which would fall within the scope of the contract. Bidders may also propose new devices as part of their technical offer.

-----

**Clarification Q-005**

*RFP Reference: Article 30 — Contract Requirements: Infrastructure and Technical Support*

**Question:** Kindly confirm whether the awarded contractor is responsible for infrastructure maintenance and connectivity. If yes, please provide the scope of infrastructure and network components, existing architecture details, and list of technologies, operating systems, and software currently in use.

**Response:**

Confirmed. The awarded contractor is responsible for the full networking and IT infrastructure scope — including supply, configuration, maintenance, and ensuring redundant paths — as part of the all-inclusive



scope. Connectivity between the main data center, disaster recovery center, and branch sites is in place. The Authority coordinates WAN/telecom services. The Authority may establish up to two (2) additional branches (pursuant to Decree 11244/2003, Article 4), for which the contractor will be responsible for configuring the connectivity infrastructure. Any fiber connectivity will be provided by Ogero at the cost of the Authority. Further details on the existing infrastructure, architecture, and technologies in use will be available during the mandatory site visit.

---

#### **Clarification Q-006**

*RFP Reference: Annex 1 — Biometric System Integration*

**Question:** Regarding biometrics, kindly clarify whether the bidder is required to integrate with the existing AFIS system, or replace it entirely. In case of integration, please provide details of the current AFIS system (vendor, architecture, APIs, standards, etc.).

**Response:**

The RFP requires integration with the existing biometric system, not replacement. The Authority operates an existing Automated Fingerprint Identification System (AFIS). The current facial photograph capture is used for printing on the driving license card and is not part of biometric matching. Further details on the AFIS system — including vendor, architecture, APIs, and integration requirements — will be disclosed during the mandatory site visit.

---

#### **Clarification Q-007**

*RFP Reference: Article 32 — Project Implementation Plan / Annex 1 — Data Migration*

**Question:** Kindly provide detailed information regarding data migration from legacy systems, including estimated data volume (records, size), types of data (vehicles, drivers, violations, documents, etc.), and data quality considerations.

**Response:**

The RFP requires a full comprehensive data migration from the existing system to the new platform, with record standardization via the Unified Traffic File (UTF) as a separate workstream. The migration methodology is specified in the RFP and includes ETL/ELT mapping, deduplication rules, data quality logging, reconciliation reports, staging migration trials, and go/no-go decisions for cutover. The volume and types of legacy data to be migrated will be disclosed during the mandatory site visit. Transaction statistics for the period January to September 2025 are provided in the RFP as reference indicators.

---

### **Section 3: Commercial and Financial Clarifications**

#### **Clarification Q-008**

*RFP Reference: Article 29 — Reference Value and Performance Bond*

**Question:** Regarding the calculation of the performance bond ( $7\% \times (5 \times \text{CARC}) + \text{Goods Basket}$ ): Kindly confirm whether the Goods Basket valuation should be based on 1,000,000 units per item (financial evaluation) or actual first-year quantities (DL: 227,424 / VR: 174,016 / RFID: 200,000).

**Response:**

Bidders are kindly requested to refer to the RFP for the performance bond calculation methodology. The relevant provisions are set out in Article 29 (Reference Value) and the financial evaluation section (Goods Basket definition).

---

#### **Clarification Q-009**

*RFP Reference: Annex 1 — Vehicle Inspection Integration Module*

**Question:** The RFP requires real-time API integration with all licensed vehicle inspection centers. Kindly provide: (a) number of currently licensed inspection centers at go-live; (b) whether a standardized API already exists or the SI must define one; (c) communication protocol (REST/SOAP? OAuth? JSON/XML?); (d) will the Authority facilitate API onboarding agreements or is this the SI's responsibility; (e) are any inspection centers currently API-capable.

**Response:**

The RFP requires real-time API integration with all licensed vehicle inspection centers, including both government-run and licensed private centers. The system must support center governance, licensing criteria, digital QA scoring, and automated SLA dashboards per center. The licensing and regulation of vehicle inspection centers is subject to a separate process currently underway by the Authority. Regardless of the number of centers, the system must be designed to support integration with any licensed center — whether government-run or private — through a standardized API defined and implemented by the SI. The SI is expected to define and implement the standardized API schema as part of their proposed system. The Authority will facilitate initial onboarding agreements with inspection centers. The number of currently licensed inspection centers will not be disclosed during the mandatory site visit, but questions regarding integration requirements may be raised during the visit.

---

#### **Clarification Q-010**

*RFP Reference: Annex 1 — Payment Engine Architecture (PCI-DSS v4.0)*

**Question:** The RFP requires a PCI-DSS v4.0 compliant multi-channel payment engine. Kindly clarify: (a) which Lebanese-licensed PSPs are approved or preferred; (b) existing POS network or must the SI establish this; (c) who is the Merchant of Record (Authority or SI); (d) MoF Sanadiq al-Maliyyeh cashier API — does it exist.

**Response:**

The RFP requires the bidder to design, implement, and operate a unified multi-channel payment engine supporting all five payment channels specified in the RFP: online card payments via payment gateway, bank branch over-the-counter (EBPP), Ministry of Finance cashier counters (Sanadiq al-Maliyyeh), licensed money transfer companies, and POS at Authority branches and private centers. The payment engine must be designed as an open architecture, enabling integration with any licensed payment service provider, money transfer company, or financial institution that meets the technical and security requirements. The Authority



does not mandate or restrict specific payment service providers — bidders are expected to propose a payment architecture that maximizes channel availability and citizen convenience.

The Authority is the receiving entity for all fees collected. Payment service provider agreements will be held by the Authority. The bidder (SI) is responsible for the complete design, development, integration, testing, certification, and ongoing operation of the payment engine and all associated integrations, included under all-inclusive pricing (PSF/CGAM/CARC). The system must implement automatic fee splitting between the government treasury, the Authority, and third-party beneficiaries as specified in the RFP, with configurable rules per transaction type and periodic settlement with reconciliation reporting.

PCI-DSS v4.0 compliance is required. Authority systems shall not store, process, or transmit cardholder data — all card payment flows must use hosted payment pages, redirect, iFrame, or tokenization so that card data bypasses Authority infrastructure.

Details regarding the current payment infrastructure and integration interfaces will be presented during the mandatory site visit.

-----

## **Section 4: Technical Clarifications — Connectivity and Security**

### **Clarification Q-011**

*RFP Reference: Annex 1 — Network Architecture and Secure WAN*

**Question:** The RFP requires secure WAN/VPN connectivity between all 7 branches and the Primary DC and DR site. Kindly clarify: (a) existing WAN/MPLS/VPN network details, ISP providers, bandwidth, contract expiry; (b) SI responsible for ISP circuit procurement and ongoing costs; (c) backup/redundant links currently in place; (d) physical location of each branch.

**Response:**

Connectivity between the main data center, disaster recovery center, and branch sites is in place. The bidder is responsible for the networking infrastructure — including configuration, maintenance, and ensuring redundant paths — as part of the all-inclusive scope. The Authority coordinates WAN/telecom services. The Authority may establish up to two (2) additional branches (pursuant to Decree 11244/2003, Article 4), for which the bidder will be responsible for configuring the connectivity infrastructure. Any fiber connectivity will be provided by Ogero at the cost of the Authority.

The current active locations are:

- Dekwaneh (Headquarters)
- Regional Branches: Nabatiyeh, Sidon, Ouzai, Aley, Zahle, Jounieh, Tripoli

Further details on the existing WAN infrastructure, ISP arrangements, and bandwidth will be available during the mandatory site visit.

-----

### **Clarification Q-012**

*RFP Reference: Annex 1 — CCTV and Evidence Management*

**Question:** The RFP requires CCTV coverage with 90-day evidence retention at all branches. Kindly clarify: (a) are cameras already installed; (b) IP-based or analog; (c) new infrastructure from scratch or extend existing; (d) existing evidence management system.

**Response:**

The RFP requires a transaction-linked CCTV and evidence management system, including continuous recording at all service counters and lane exits, with tamper-evident storage linked to transactions, ninety (90) day retention with case-lock capability for indefinite retention of flagged footage, and restricted access with audit controls. This is a Greenfield requirement — the bidder is expected to propose a complete CCTV and evidence management solution as part of their technical offer, including IP cameras, network video recording infrastructure, tamper-evident storage, and the software integration layer that links video footage to individual transactions. Basic monitoring exists at some branches and may be leveraged by the contractor if applicable. Details regarding existing branch infrastructure will be available during the mandatory site visit. All CCTV infrastructure is included under all-inclusive pricing (PSF/CARC/CGAM).

---

**Clarification Q-013**

*RFP Reference: Annex 1 — Mobile Application Security (Certificate Pinning)*

**Question:** The RFP mandates certificate pinning for mobile applications but does not specify the pin target. Kindly clarify: (a) pin to TLS server certificate, Issuing CA, or Root CA; (b) how to handle 90-day certificate rotation given that re-pinning requires forced App Store/Google Play updates.

**Response:**

Certificate pinning is a mandatory security control for both the citizen mobile application and the enforcement application, as specified in the RFP. The RFP requires the contractor to implement an Authority-operated PKI with an offline Root CA and HSM-protected Issuing CAs. Application certificates must auto-renew and rotate at least every 90 days. The pinning strategy must ensure uninterrupted application operation during certificate rotation cycles without requiring application updates to be published on the App Store or Google Play. Bidders are expected to propose their certificate pinning and rotation strategy in their technical offer, demonstrating how the mandatory 90-day certificate rotation is achieved while maintaining continuous application availability.

---

**Clarification Q-014**

*RFP Reference: Annex 1 — Authority PKI and Device-Level Credentials*

**Question:** The RFP references device-level credential requirements for examiner tablets and enforcement handhelds. Kindly clarify: (a) are device credentials issued by Authority PKI (SI enrolls/issues); (b) total number of devices at go-live; (c) certificate validity period; (d) is MDM-based auto-enrollment acceptable.

**Response:**

The RFP requires the contractor to implement an Authority-operated PKI with an offline Root CA and HSM-protected Issuing CAs. All device credentials — including examiner tablets and enforcement handhelds — shall be issued through this PKI infrastructure. The contractor is responsible for the complete design, implementation, enrollment, and ongoing management of all device-level credentials as part of the all-inclusive scope. The total number of devices requiring certificates will be assessed during the mandatory site



visit. Certificate validity periods and the enrollment methodology — including automated enrollment via MDM or equivalent — are implementation details that bidders are expected to address in their technical proposal, ensuring compliance with the security and key management requirements specified in the RFP.

-----

#### **Clarification Q-015**

*RFP Reference: Annex 1 — Notary Electronic Signatures (Dual-Mode)*

**Question:** The RFP requires notaries to apply qualified electronic signatures using certified tokens/HSM-backed keys. Kindly clarify: (a) who procures signing tokens (Authority, Syndicate of Notaries, or SI); (b) who issues notary signing certificates (Authority PKI or national e-signature service); (c) is a Lebanese national e-signature service currently operational.

**Response:**

The RFP establishes a dual-mode approach for notary signatures. In the current phase, the system shall capture the notary's handwritten electronic signature on a signature pad and bind it to the transaction record. Signature pad devices will be purchased by the respective entity that utilizes them and are not required to be priced by the bidder in this RFP.

When digital (PKI-based) signatures are legally recognized under Lebanese law, the system must be capable of supporting qualified electronic signatures using certified tokens or HSM-backed keys, with certificate chain validation and signature metadata preservation. The bidder is responsible for building the system capability to accept and validate qualified electronic signatures. The procurement and distribution of signing tokens to notaries is outside the scope of this RFP and will be determined in accordance with the applicable legal and institutional framework when digital signatures are legally recognized. There is no Lebanese national e-signature service currently operational.

-----

#### **Clarification Q-016**

*RFP Reference: Annex 1 — Authority PKI Infrastructure*

**Question:** The RFP requires an Authority-operated PKI with offline Root CA and HSM-protected Issuing CAs. Kindly clarify: (a) does the Authority currently have HSM hardware deployed; (b) does the Authority currently operate any Certificate Authority; (c) has the Authority previously issued PKI-based credentials to staff, notaries, physicians, or citizens.

**Response:**

The RFP requires the contractor to design, procure, implement, and operate an Authority-operated PKI with an offline Root CA and HSM-protected Issuing CAs, as specified in the RFP. "Authority-operated" means the PKI infrastructure is owned by the Authority and operates under the Authority's name — the contractor is responsible for the complete design, procurement of all hardware including HSMs, installation, configuration, certification, and ongoing operation and maintenance of the PKI throughout the contract period, included under all-inclusive pricing (PSF/CGAM/CARC). The Authority does not perform any technical development, configuration, or operational tasks related to the PKI. Details regarding existing cryptographic infrastructure will be presented during the mandatory site visit in a controlled environment, as this information is security-sensitive and will be disclosed under the confidentiality undertakings signed by all site visit participants.