TMO — Traffic Management Operation

Lebanon — Vehicle Registration & Driver Licensing RFP

OFFICIAL CLARIFICATIONS AND RESPONSES — Batch ١٢

The following clarifications are published in response to questions received from prospective bidders during the RFP clarification period, and are read together with the RFP and its issued Addenda Nos. ١, ٢ and ٣. These responses do not modify the RFP except where they reflect an issued Addendum; in case of discrepancy, the RFP and its issued Addenda prevail. Thirty-seven (٣٧) clarifications follow.

Clarification Q-٠٠١

RFP Reference: Law ٨١/٢٠١٨ - data protection (DPIA / RoPA)

Question: The RFP mandates compliance with Law No. ٨١/٢٠١٨ on Electronic Transactions and Personal Data, including DPIA, RoPA, and data subject rights. However, the implementation decrees for Law ٨١/٢٠١٨ have not yet been fully issued. Which specific provisions does the Authority consider enforceable today? Is the SI expected to implement the full GDPR-equivalent framework proactively, or only the provisions that are currently enforceable under Lebanese law?

Authority's response: The applicable requirements are those specified in the RFP (§١,٧٠,٣ and §١,٧١): a DPIA and RoPA (prior to UAT for biometric processing), auditable in-system data-subject-rights workflows, and no cross-border data transfer without the Authority's prior written approval. Being defined in the RFP, these are binding contractual obligations upon award, enforceable as contract terms irrespective of the issuance status of any implementing decree under Law ٨١/٢٠١٨; the Authority will not narrow or reinterpret them. The system shall additionally conform to further regulatory parameters as they issue, at no additional cost.

Clarification Q-٠٠٢

RFP Reference: Workflow models - BPMN ٢,٠ / DMN ١.x

Question: The RFP mandates 'TO-BE BPMN ٢,٠ process models and DMN ١.x decision models' as authoritative build artifacts. Does the Authority require a runtime BPMN engine that executes these models directly (e.g., Camunda, Elsa, Flowable), or are the BPMN/DMN models acceptable as documentation artifacts with equivalent logic implemented in code? A runtime engine adds significant infrastructure complexity but provides visual process monitoring and non-developer process modification.

Authority's response: The Authority does not require any specific workflow tool or runtime engine — the technical approach is the bidder's choice. Per §١,٥٥, the BPMN ٢,٠/DMN ١.x models shall drive the build and remain traceable in the RTM, and the platform's business rules and parameters shall be adjustable through configuration rather than code. How the bidder achieves this is its own decision, provided both hold.

Clarification Q-٠٠٣

RFP Reference: Environments (DEV / TEST / UAT / SEC / PROD)

Question: The RFP mandates ٥ environments: DEV, TEST, UAT/PRE-PROD, SEC, and PROD. With a microservices architecture (١٧+ services), each environment requires a full infrastructure stack. Does the Authority expect full production-parity for all ٥ environments, or can lower environments (DEV, TEST) be scaled down? The SEC environment alone (production-parity per RFP) represents a full duplicate of the production infrastructure.

Authority's response: All five environments — DEV, TEST, UAT/PRE-PROD, SEC and PROD — are required, on-premises; a bid that does not provide all five does not conform. The RFP specifies production-parity for the SEC environment (dedicated to independent third-party security testing) and does not impose production-parity on the other environments. It does not prescribe the sizing of the non-SEC environments; bidders size each to its function — with UAT/PRE-PROD adequate for representative acceptance, migration-rehearsal and performance testing at the target volumes — and describe and justify this in the technical proposal. All environment provisioning falls within the all-inclusive scope.

Clarification Q-٠٠٤

RFP Reference: Performance targets and measurement

Question: The RFP specifies 'P٩٥ ≤ ٢,٠s for read operations' and 'API ≥ ٢٠٠ TPS sustained, burst ≥ ٦٠٠ TPS'. These targets must be achieved while running TLS ١,٣, mTLS, field-level encryption for PII, RBAC/ABAC, and immutable audit logging. Has the Authority conducted any baseline performance testing of these combined requirements? Are these targets measured at the API gateway level or at the individual service level?

Authority's response: The performance targets — interactive P٩٥ ≤ ٢,٠s for reads, P٩٩ ≤ ٥,٠s, and ≥ ٢٠٠ TPS sustained / ≥ ٦٠٠ TPS burst — are contractual acceptance criteria, to be achieved with the mandated security controls in place and demonstrated by the bidder's own capacity and load tests under production-like conditions at the acceptance gates. These targets are not contingent on any Authority pre-testing and are not subject to relaxation. Interactive latency shall be measured end-to-end as delivered, and throughput at the platform API layer, not on an individual-service basis; the bidder shall state its measurement methodology in the technical proposal. The RFP permits encryption of sensitive data by field-level or full-disk means, at the bidder's choice, so reconciling the required security controls with the stated performance targets is part of the bidder's design responsibility.

Clarification Q-٠٠٥

RFP Reference: API design - mTLS, partner certificates, versioning

Question: The RFP requires 'mTLS for all API calls' and 'breaking changes require a new major version and ≥١٨٠ days deprecation notice'. With ١٥+ external integration partners (MoF, AFIS, Insurance, Inspection, Notaries, ISF, DGGS, etc.), does each partner currently support mTLS?

Who is responsible for issuing and managing client certificates for external partners? What happens during the ١٨٠-day deprecation window if a partner cannot upgrade?

Authority's response: mTLS is enforced for the platform APIs under §١,٤ and applies to service-to-service and external-partner APIs where applicable. The bidder shall integrate with each partner's available secure interface, provide the required sandbox, mock servers, example payloads and conformance test suite for onboarding, and implement resilient handling including retries, circuit breakers and fallbacks, irrespective of partner maturity. Certificate issuance and rotation shall be handled through the Authority-owned, on-premises PKI implemented and operated by the bidder, including offline Root CA, HSM-protected Issuing CAs and automated certificate rotation. Cross-party trust shall be coordinated through the Authority, all within the all-inclusive scope. Per §١,٤, breaking changes require a new major version and at least ١٨٠ days' deprecation notice, during which the prior version shall remain available in parallel to allow partner migration. Any partner-specific exception or extension shall be coordinated with and approved by the Authority; the bidder may not unilaterally disrupt partner integrations.

Clarification Q-٠٠٦

RFP Reference: Staff/admin authentication - FIDO٢ / WebAuthn

Question: The RFP mandates 'FIDO٢/WebAuthn for staff/admin portals' with 'shared accounts prohibited' and 'device IDs bound to user sessions'. Does the Authority currently have FIDO٢ security keys deployed or budgeted for all ٥٠٠+ staff users across all branches? If not, is the SI expected to supply, configure, and manage physical security keys for every staff member? What is the fallback if a key is lost or damaged at a remote branch?

Authority's response: Staff and admin authentication is part of the new platform and within the all-inclusive scope. Under §١,٧٢, staff workstations and thin clients shall support WebAuthn/FIDO٢ or platform biometrics, such as Windows Hello or Touch ID, for interactive login with MFA; shared accounts are prohibited, and device IDs must be bound to user sessions and recorded in the audit log. The RFP does not mandate physical security keys for every staff member and specifies TOTP as a fallback. The authentication method and mix are therefore part of the bidder's design, provided the required controls are met; if the bidder proposes physical security keys or related hardware, these shall be included in the all-inclusive price. The figure of ٥٠٠ in §١,٩١,٣ is the concurrent-peak internal staff user load metric, not a headcount and not a per-device count. Provisioning shall be sized by the bidder to the actual users and workstations. Enrollment, recovery and re-issuance procedures, including at remote branches, are the bidder's responsibility, with TOTP as the specified fallback. The Authority's current arrangements are not the baseline for the Greenfield platform.

Clarification Q-٠٠٧

RFP Reference: CGAM guarantee - force majeure / change in law

Question: The CGAM is 'the minimum USD amount of total annual revenue from PSF across all eligible transactions in one contractual year'. If actual PSF revenue falls below CGAM, the

Administration pays the difference. However, what happens if transaction volumes drop due to factors outside the SI's control (economic crisis, pandemic, government shutdown, new legislation)? Is CGAM payable regardless of cause, or are there force majeure exclusions?

Authority's response: CGAM is the contractually guaranteed annual minimum: at each year-end, if actual annual PSF revenue is below CGAM, the Authority settles the difference up to CGAM. The interaction of this guarantee with force-majeure events is governed by the RFP's force-majeure and by applicable Lebanese law.

Clarification Q-٠٠٨

RFP Reference: Financing and payment

Question: Financing comes from TMO's budget and potentially State contributions, paid over 'a maximum of five (٥) years'. Given the PSF generates revenue monthly, what is the mechanism if the Administration's budget allocation is delayed or insufficient to cover CGAM? What recourse does the SI have if CGAM payments are not made within the specified ٦٠-day invoice payment period?

Authority's response: Financing and payment are the Authority's obligation, governed by the RFP's payment provisions which the Authority will meet accordingly. The budget-delay and insufficiency scenarios raised are hypothetical and outside the scope of this clarification.

Clarification Q-٠٠٩

RFP Reference: Independent security company - security gates

Question: The RFP mandates an 'independent third-party security company commissioned via a separate tender running in parallel'. Has this separate security tender been published? What is its timeline? If the security company is not yet contracted by the time the SI reaches Gate B (Pre-UAT Build), the SI's entire go-live schedule is blocked by an external dependency it cannot control.

Authority's response: The independent security company is commissioned by the Authority (§١٩,٢); its procurement, engagement and availability for the security and quality gates (§١٩,٣, Gates A–D) are the Authority's responsibility, and the Authority will ensure it is engaged in time for the applicable gate reviews. The status and timeline of that separate procurement are not addressed in this clarification. The bidder remains responsible for its own security readiness, including the CI/CD security testing and gate-ready deliverables required under §١٩. Delays attributable to the Authority do not expose the contractor to delay penalties, in accordance with the Special Conditions; any consequential schedule impact will be addressed by the Authority under the contract.

Clarification Q-٠١٠

RFP Reference: Audit logging — segregation of duties

Question: The RFP states 'the logging/SIEM platform SHALL be operated on a logically and administratively separate system, with a distinct admin team and separate credentials'. Does the Authority have an existing SOC/NOC team to operate the SIEM? If not, is the SI expected to provide a separate operations team exclusively for the audit/SIEM infrastructure, distinct from the application operations team?

Authority's response: The RFP requires the logging/SIEM platform to be operated on a logically and administratively separate system, with a distinct admin team and separate credentials from the application/infrastructure administrators, who must have no rights to delete, alter or stop audit ingestion or retention (§٧٤,٤). The bidder shall provide and maintain this distinct audit/SIEM administration within the all-inclusive scope, kept segregated from its own application/infrastructure administration; its sizing is the bidder's to determine, provided the segregation of duties is fully enforced, including separate administration and credentials and audited break-glass under dual control. Real-time alerts shall be delivered to the Authority SOC/NOC or Authority-designated security operations function with on-call escalation. The bidder shall support handover, integration, secure access and operational runbooks for such function, consistent with the operate-and-maintain model: Authority or Authority-designated Level ١ monitoring/triage, and contractor Levels ٢–٤ technical support and maintenance. The Authority's current arrangements are not the baseline for the Greenfield platform.

Clarification Q-٠١١

RFP Reference: Data Loss Prevention (DLP)

Question: The RFP requires DLP 'across all channels — databases, APIs, documents, portals, and endpoints'. Enterprise DLP requires endpoint agents on every workstation, network appliances, and cloud proxies. Does the Authority expect a commercial enterprise DLP solution, or is a custom-built monitoring/alerting layer acceptable? If commercial, does this apply to all ٥٠٠+ staff workstations across ٧+ branches?

Authority's response: The RFP specifies Data Loss Prevention capabilities to be applied across all listed channels — databases, APIs, documents, portals and endpoints — including data classification, policy-based blocking/flagging, monitoring and alerting, encryption alignment, and compliance reporting (§٧٥). It does not mandate a specific vendor product or a commercial-versus-custom implementation model. These capabilities may be delivered through a commercial DLP product, a custom-built DLP control layer, or a hybrid approach, provided all required capabilities are fully met, tested, and integrated with the platform's audit/SIEM controls. Endpoint coverage is in scope and shall be sized to the actual workstation estate; the figure of ٥٠٠ refers to concurrent-peak internal staff users, not a workstation count. The complete DLP solution shall be proposed and delivered by the bidder as part of the new platform within the all-inclusive scope; no existing solution is the baseline for the Greenfield platform.

Clarification Q-٠١٢

RFP Reference: Notary electronic signatures (phased / PKI-ready)

Question: The RFP references 'qualified electronic signature (PKI-based) using certified tokens/HSM-backed keys' for notaries. Lebanese Law ٨١/٢٠١٨ defines e-signatures but the decrees establishing 'qualified' standards, certification authorities, and trust service providers have not been issued. In the absence of an accredited Lebanese CA: (a) Which PKI standard should the SI implement? (b) Who will act as the Root CA? (c) Will notary digital signatures be legally admissible in court?

Authority's response: The RFP requires a phased, dual-mode design for notary signatures (§١,٢٣,٢). From go-live, and until digital/PKI signatures are legally recognized and the relevant trust framework is available, the notary continues to carry out the usual notarial procedures and retains the paper instrument; the system captures the notary's handwritten electronic signature on a signature pad, and the notary's scanned document is submitted together with that capture — all bound to the transaction record and archived in the DMS. In parallel, the platform shall be built PKI-ready, including standards-based qualified e-signature capability using certified tokens or HSM-backed keys, certificate-chain validation, and preservation of validation metadata (§١,٢٣,٥), supported by the Authority-operated on-premises PKI. The PKI mode shall be configurable and capable of activation, without code changes, when digital signatures become legally recognized and the applicable national e-signature service or accredited trust framework is available. The bidder is not required to integrate with a certification authority or e-signature service that does not yet exist; however, it is required to deliver the PKI-ready capability now and to complete the integration and activation upon the Authority's request when the legal framework and service are in place, within the all-inclusive scope. Legal recognition and court admissibility of electronic notary signatures remain governed by applicable Lebanese law.

Clarification Q-٠١٣

RFP Reference: Digital driving-licence & vehicle-registration credentials

Question: The RFP requires 'digital versions of both the driving license and the vehicle registration card in the mobile app, with offline-verifiable QR/signatures'. Lebanese Traffic Law ٢٤٣/٢٠١٢ Article ١٤٥ requires physical license plates and Article ١٤١ requires a physical driving license. Has the Authority obtained or is it seeking a legal amendment or ministerial decree recognizing digital driving licenses as legally equivalent to physical cards for roadside presentation?

Authority's response: The bidder shall implement the digital driving-licence and vehicle-registration credentials in the mobile app — with offline-verifiable QR verification and full parity with the physical credentials — exactly as specified in §٣٨,٦. The cited Articles ١٤١ and ١٤٥ of the Lebanese Traffic Law do not mention physical driving licences or physical vehicle-registration cards. Interpretation and legal recognition of the Traffic Law fall to the Authority and the competent Lebanese authorities.

Clarification Q-٠١٤

RFP Reference: Citizen signature-pad captures

Question: The RFP requires 'signature pad capture for citizen/representative signatures, embedded into the transaction artifacts and archived in DMS'. It also requires notaries to apply 'qualified e-signature'. For citizen signatures captured on a signature pad: (a) Are these legally equivalent to wet-ink signatures under Lebanese law? (b) What is the evidentiary weight of a pad-captured signature in Lebanese courts? (c) Is a signature pad capture at a counter sufficient for ownership transfer of a vehicle worth potentially hundreds of thousands of dollars?

Authority's response: The bidder shall implement signature-pad capture of citizen/representative signatures, embedded into the transaction artifacts and archived in the DMS, as specified in the RFP. The pad capture is a captured artifact bound to the record, not a standalone legal instrument; where a transaction legally requires a notary — for example, vehicle ownership transfer — the notary carries out the usual notarial procedures, retains the paper instrument, and scans and submits it alongside the captured signatures, per §١,٢٣,٢.

Clarification Q-٠١٥

RFP Reference: Offline credential verification / revocation

Question: The RFP requires 'offline mode for credential verification (QR/signature check) with secure sync on reconnect'. When the CRL is stale (e.g., phone offline for days), how should the app handle a credential that may have been revoked since last sync? What is the maximum acceptable CRL staleness?

Authority's response: Offline verification is required, but stale-revocation handling is the bidder's design responsibility. Revocation data shall be refreshed at least daily where connectivity is available; the offline acceptance, warning, and reconciliation approach is for the bidder to handle and propose, consistent with the RFP's security requirements.

Clarification Q-٠١٦

RFP Reference: OCR auto-classification accuracy

Question: The RFP requires 'OCR and document classification to extract key fields with ≥ ٩٥٪ auto-classification accuracy on approved samples'. Arabic OCR is less accurate than Latin-script. Is the ٩٥٪ target measured on: (a) machine-printed Arabic only; (b) including handwritten Arabic; (c) mixed Arabic/French/English documents? What constitutes 'approved samples'?

Authority's response: The ≥٩٥٪ target refers to OCR auto-classification accuracy on approved samples prior to go-live, not raw character-by-character OCR accuracy. Field extraction shall use confidence thresholds, with low-confidence fields highlighted for manual verification. The approved samples will be agreed with the awarded contractor at the acceptance baseline, using representative Authority records under confidentiality and with personal data masked; samples are not distributed during bidding, and bidders shall propose their approach on the basis of the RFP.

Clarification Q-٠١٧

RFP Reference: Incident management - SLAs / ٢٤×٧ on-call

Question: The RFP specifies 'P١ (critical service outage) MTTD ≤ ٥ min, MTTR ≤ ٢h' and '٢٤×٧ on-call'. Does the Administration currently have a NOC/SOC providing ٢٤×٧ monitoring, or is this entirely the SI's responsibility? If the SI must provide ٢٤×٧ NOC coverage, this requires a minimum of ٥-٦ FTE engineers in rotating shifts — a significant operational cost over ٥ years.

Authority's response: The P١ targets, including MTTD ≤ ٥ minutes and MTTR ≤ ٢ hours, and the ٢٤×٧ on-call requirement are contractual SLAs. The bidder shall provide the monitoring and observability platform, escalation paths, stakeholder communication templates, status pages, and ٢٤×٧ on-call incident response required to meet them. Observability dashboards shall be shared with the Authority NOC/SOC or Authority-designated operations function. The Authority or its designated function performs oversight and Level ١ monitoring/triage, while the bidder provides Levels ٢–٤ technical support, incident resolution, root-cause analysis and corrective actions. The staffing and shift model required to meet the SLAs is the bidder's responsibility within the all-inclusive scope; the Authority's current arrangements are not the baseline for the Greenfield platform.

Clarification Q-٠١٨

RFP Reference: E-sticker - pricing and activation

Question: The e-sticker module is 'optional' and 'may be phased, deferred, or canceled'. Yet Article ٢٢ rejects any bid that does not price the RFID stickers, and §٢٧,٣ states 'no payments for sticker goods or sticker-specific services are due until Activation Notice'. If the SI must build the entire e-sticker platform but receives no revenue until activation, who bears the development cost? Is this cost expected to be absorbed into the PSF?

Authority's response: The e-sticker digital capability and background readiness are included in the bidder's all-inclusive scope and are not separately payable. Sticker goods and sticker-specific field services must be priced in the offer for comparison and completeness, but no procurement, shipment, commissioning, payment, or financial run-rate shall occur unless and until the Authority issues a written Activation Notice. Accordingly, the platform readiness/build cost is absorbed within the all-inclusive pricing, while sticker goods and activation-dependent field services are payable only upon activation.

Clarification Q-٠١٩

RFP Reference: Document Management System integration

Question: The RFP requires integration with the 'Authority's existing Document Management System'. What is the current DMS product (vendor/version)? Does it expose APIs? Is it on-premises or cloud-hosted? What is its storage capacity and utilization? If the DMS cannot meet the WORM archiving requirements, is the SI expected to replace it?

Authority's response: The new platform shall integrate with the Authority's existing on-premises Laserfiche DMS through its available API/SDK. The bidder is responsible for building and supporting the integration within the all-inclusive scope, but is not required to replace the DMS or assume responsibility for the DMS's own licensing, storage, backup, or core maintenance. Detailed version, configuration, and integration specifications will be provided to the awarded contractor during discovery.

Clarification Q-٠٢٠

RFP Reference: Content Management System & ERP functions

Question: The RFP requires a 'built-in Content Management System' and 'ERP hooks for collections reconciliation, consumables procurement, and HR-driven role provisioning'. Does the Authority currently use an ERP system? If yes, which one? If not, is the SI expected to build ERP-equivalent functionality from scratch within the platform?

Authority's response: The RFP requires a built-in Content Management System and, for three specific functions — collections reconciliation, consumables procurement, and HR-driven role provisioning — ERP hooks or embedded modules. These functions may be delivered as embedded modules within the integrated platform, with no separate external ERP required, or integrated externally at the bidder's choice, within the all-inclusive scope. The Authority's current internal systems are not the baseline for the Greenfield platform.

Clarification Q-٠٢١

RFP Reference: Peak-day capacity and external dependencies

Question: The RFP specifies a peak-day renewal volume of ٥٠,٠٠٠ transactions (~١٠٤/minute). With the mandatory step-by-step wizard (insurance → inspection → fines → payment), each renewal involves ٤-٦ sequential external API calls. Has the Authority verified that external systems (insurance companies, MoF) can handle ١٠٠+ queries/minute from the platform?

Authority's response: The ٥٠,٠٠٠ peak-day renewals figure is a ١٠-year capacity-sizing target under §١,٩١, not the current daily volume. External dependencies shall be handled under §١,٢٥,١٠ through documented SLAs, circuit breakers, bulkheads, retry back-offs, user-facing fallbacks and upstream-SLA monitoring. The number and sequencing of external API calls per renewal is the bidder's design assumption; the bidder shall design the integration approach to meet the RFP's performance and resilience requirements, and the Authority does not warrant third-party throughput at bidder-assumed call rates.

Clarification Q-٠٢٢

RFP Reference: Foreign-national validation - DGGS

Question: The RFP requires 'validate foreign nationals' identity, residency/visa, and entry/exit constraints through DGGS services'. DGGS (General Security) operates classified systems with strict access controls. Has the Authority obtained DGGS approval for API-level integration? What classification level does this data carry? Are there restrictions on where this data can be stored or displayed?

Authority's response: DGGS integration is a data-minimized validation performed where permitted by law: the platform checks entry/residency status and applies configurable hard-stops where a violation or ban is returned; it does not ingest or replicate DGGS records. Inter-agency access, data classification and handling constraints are arranged by the Authority; the bidder integrates through the interface provided at discovery, within the RFP's security, audit and data-minimization requirements.

Clarification Q-٠٢٣

RFP Reference: Analytics dashboards - freshness / SLAs

Question: The RFP requires 'canned dashboards must load in ≤ ٥s P٩٥' with 'materialized UTN-centric views refreshed per SLA with data-freshness indicators'. For a dataset of ٤M vehicles, ٣,٥M drivers, ١٠M+ payments, and ١٠٠M+ audit log entries, achieving ٥-second dashboard load requires pre-computed materialized views or a dedicated OLAP warehouse. Is the Authority expecting real-time (sub-second) or near-real-time (minutes) data freshness for dashboards?

Authority's response: Canned dashboards shall load in ≤٥s P٩٥ for defined filters, supported by materialized UTN-centric views refreshed per SLA with data-freshness indicators (§١,٢٦,٢). This means the analytics freshness model is SLA-based near-real-time, not a sub-second real-time guarantee; the bidder shall propose the refresh cadence and architecture required to meet the RFP's dashboard, lookup, and reporting requirements.

Clarification Q-٠٢٤

RFP Reference: Digital staff ID cards - PKI-signed QR

Question: The RFP requires 'digital staff ID cards bound to the user's UTN and device' with 'PKI-signed QR for offline/online verification'. This implies every Authority staff member, examiner, driving school instructor, and operator will have a digital credential. Is the Authority expecting the SI to issue PKI certificates to every individual staff member/affiliate? What is the estimated number of individuals requiring digital ID cards?

Authority's response: §١,٢٩ requires a module to issue and manage virtual ID cards for Authority staff and affiliated personnel, including examiners, driving-school owners/instructors, and operators. These cards appear in the app/portal, are bound to the user's UTN and device, and carry a PKI-signed QR with no PII in the QR payload. This is a platform-signed credential: the QR is signed by the Authority PKI and verified using the published Authority public key; it does not require issuing an individual PKI certificate to each person. The population is the Authority's staff and affiliates; the RFP fixes no number, the module shall scale to the required population, and the final count will be provided to the awarded contractor during discovery, all within the all-inclusive scope.

Clarification Q-٠٢٥

RFP Reference: Sites and decentralized centers

Question: The RFP mentions '~٧ branches currently' but also references 'future authorized private centers'. For infrastructure sizing and cost estimation, can the Authority provide the planned number of additional centers in the next ٥ years? Each additional center requires hardware, networking, printers, training, and support.

Authority's response: The current sites are Dekweneh HQ plus seven regional branches, with up to two additional authorized under Decree ١١٢٤٤/٢٠٠٣; per-site equipment and volume data are set out in the statistical/equipment publication issued with Addendum No. ٢.

Clarification Q-٠٢٦

RFP Reference: OCR auto-classification - measurement basis

Question: The RFP requires 'OCR auto-classification accuracy ≥ ٩٥٪ on approved samples prior to go-live'. The system must process Arabic/French/English documents including customs clearances, insurance policies, medical certificates, notary deeds, court documents, and identity cards — each with different layouts. Is the ٩٥٪ target measured per document type or as a global average across all types? Can the Administration provide sample documents for each type during the bid preparation phase?

Authority's response: The ≥٩٥٪ target refers to OCR auto-classification accuracy on approved samples prior to go-live, not raw character-by-character accuracy. Field extraction uses confidence thresholds, with low-confidence fields highlighted for manual verification. The measurement basis — whether per document type or as a defined aggregate across types — will be set in the approved sample set and test protocol agreed at the acceptance baseline, using representative Authority records under confidentiality with personal data masked; samples are not distributed during bidding, and bidders shall propose their approach on the basis of the RFP.

Clarification Q-٠٢٧

RFP Reference: Throughput - platform vs per-service

Question: The RFP requires 'sustain ≥ ٢٠٠ TPS with burst ≥ ٦٠٠ TPS over ٦٠s'. Is this measured for the entire platform (all ١٧+ services combined) or for each individual service? The API gateway receives all traffic, but behind it each service handles only its domain's share. What is the expected traffic distribution across services?

Authority's response: The ≥٢٠٠ TPS sustained / ≥٦٠٠ TPS burst target is measured at the platform API layer as delivered, not on an individual-service basis. The RFP does not prescribe a service count or a per-service traffic distribution; any reference to "١٧+ services" is the bidder's own assumption. The internal distribution across services follows the bidder's architecture, which must meet the aggregate target and be proven through the bidder's capacity tests at the acceptance gates.

Clarification Q-٠٢٨

RFP Reference: Penalties - deficiency-notice definition

Question: The penalty schedule shows escalating fines: ١-١٠ notices = $١,٥٠٠/notice; ١١-٢٥ = $٣,٠٠٠; ٢٦+ = $٤,٥٠٠; with 'severe notice = ٥x regular notice'. The annual penalty cap is ٢٠٪ of CARC. Can the Administration define what constitutes a 'deficiency notice'? Is a single API timeout a deficiency notice? A printer jam? A ٥-minute scheduled maintenance? Without clear criteria, the penalty mechanism could generate hundreds of notices for minor events.

Authority's response: The penalty schedule and annual cap are governed by Special Conditions Art. ٢٣. A deficiency notice is issued only for a documented default against the contractor's contractual obligations or applicable service levels, and must be reasoned and supported by evidence. It is not an automatic notice for every isolated technical event. Events that do not breach an applicable SLA or contractual obligation, including approved scheduled maintenance within the permitted window, do not constitute deficiency notices. The procedure remains governed by Art. ٢٣ and the SLA framework.

Clarification Q-٠٢٩

RFP Reference: On-premises hosting - external delivery channels

Question: The RFP prohibits all cloud services: 'All processing, storage, backups, logs, telemetry, and build artifacts shall be hosted on-premises in Lebanon.' Does this prohibition extend to: (a) mobile app distribution (App Store/Google Play require cloud publishing); (b) push notifications (FCM/APNs are cloud); (c) SMS gateway services (typically cloud); (d) payment gateway services (PCI-DSS gateways are cloud-hosted)?

Authority's response: The on-premises rule (§١٨,١) governs hosting of the system and Authority data: processing, storage, backups, logs, telemetry and build artifacts remain on-premises in Lebanon, with no public cloud for production, DR or telemetry. It does not prohibit necessary external delivery/connectivity channels expressly contemplated by the RFP, such as payment gateways and SMS, provided personal data is not exported beyond what is legally required; client app distribution through app stores, data-minimized push/SMS notifications, and PCI-DSS-compliant payment gateways are therefore permitted, while the platform and Authority data remain on-premises.

Clarification Q-٠٣٠

RFP Reference: E-sticker - cost allocation

Question: The e-sticker module is 'optional' with activation at the Authority's discretion, yet Article ٢٢ mandates pricing for ١,٠٠٠,٠٠٠ RFID stickers. If the Authority decides NOT to activate: (a) Must the SI still develop the complete e-sticker software module at its own cost? (b) If yes, should this development cost be embedded in the PSF or treated as a contingent deliverable? (c) If built but never activated, is the SI entitled to compensation for the stranded development investment? Please clarify the exact cost allocation mechanism.

Authority's response: The e-sticker digital capability and background readiness are included in the all-inclusive scope and are not separately payable, whether or not the programme is later activated (§١,٢٧,٢). Sticker goods and sticker-specific field services are priced in the offer for comparison, but no procurement, shipment, commissioning, payment or run-rate occurs unless and until the Authority issues a written Activation Notice (§١,٢٧,٣) — so no goods investment is stranded, since goods are not procured until activation. Accordingly, the software module carries no separate compensation if the programme is not activated; it forms part of the all-inclusive platform, while goods and activation-dependent services are payable only upon activation.

Clarification Q-٠٣١

RFP Reference: Process discovery - newly identified processes

Question: The RFP requires the SI to 'validate AS-IS and deliver TO-BE BPMN ٢,٠ process models for all in-scope services'. During Process Discovery, if the SI identifies business processes NOT listed in the current scope, how are these handled contractually? (a) Are newly discovered processes within the PSF scope at no additional cost? (b) Is there a formal Change Request mechanism with separate pricing? (c) Is there a cap on additional processes within the PSF? (d) What is the threshold beyond which additional development constitutes a contract amendment?

Authority's response: The TO-BE process modelling under §١,٥٥ covers all in-scope services; processes that form part of those services — including steps currently performed manually — are within the all-inclusive scope and carry no additional cost. For any development or scope beyond that defined in the RFP, the relevant provisions of the RFP apply.

Clarification Q-٠٣٢

RFP Reference: Future development over the term

Question: Over a ٥-year contract, new legislation, regulatory changes, or Authority policy decisions will require new software modules, processes, or integrations not envisioned at bid time (e.g., vehicle emissions testing, EV charging registration, ride-sharing licensing, autonomous vehicle regulations, national digital ID integration). (a) Is all future development included in the PSF at no additional cost? (b) If not, what is the formal mechanism for pricing and approving new development? (c) Is there a guaranteed annual 'innovation budget' within the PSF? (d) Can the Administration unilaterally require new development under the existing PSF, or does material new scope trigger a contract renegotiation?

Authority's response: Configuration-driven changes within the RFP's scope, including fee/rule/regulatory parameter updates contemplated by the RFP, are covered by the all-inclusive PSF. For any development or scope beyond that defined in the RFP, the relevant provisions of the RFP apply.

Clarification Q-٠٣٣

RFP Reference: Vehicle-registration scope / process inventory

Question: The vehicle registration module must support the complete lifecycle for ١٥+ vehicle categories across ٤ departmental sections, each with distinct fee schedules, document requirements, and approval workflows. How many distinct business processes (primary + secondary) has the bidder identified for the Vehicle Registration module alone? Please provide a complete enumerated list with process names in both Arabic and English, mapped to the specific departmental section(s) and the stored procedures or API endpoints that implement each process.

Authority's response: The vehicle-registration scope is set out in the RFP, including the Annex ١ functional requirements and the applicable fee/tariff regulations. Bidders shall base their proposals on those requirements. Enumerating the distinct business processes and producing the TO-BE BPMN models are bidder deliverables under §١,٥٥ and are performed during discovery; the Authority will not prepare a bidder-specific process inventory during the bidding phase. The new platform's internal design is the bidder's responsibility within the defined scope.

Clarification Q-٠٣٤

RFP Reference: PSF - fixed vs escalation

Question: The PSF is a single unified per-transaction fee covering ALL operational costs. Over ٥ years, cost escalation applies (staff salary increases; hardware warranty expiration/replacement; software license renewals; consumables inflation; cybersecurity investment). Is the PSF fixed for the entire ٥-year term with no escalation clause, or is there a mechanism for annual PSF adjustment? If fixed, how does the bidder ensure service quality does not degrade in Years ٤-٥ when costs have risen but revenue per transaction remains flat?

Authority's response: The PSF is a single, all-inclusive per-transaction fee, fixed as bid. The bidder shall price all cost changes related to its own contractual obligations over the contract term, including contractor staffing/support, hardware, licence renewals, consumables and security, into its PSF/CGAM/CARC as its commercial risk; there is no automatic PSF escalation clause. Applicable service levels must be sustained throughout the contract.

Clarification Q-٠٣٥

RFP Reference: Citizen liveness detection

Question: Section §١,٣٩,٢ requires liveness detection for the Physician Portal during remote medical certification. Is a similar liveness verification mechanism required for citizens when submitting applications remotely via the Mobile Application or Citizen Portal? If yes, which service flows require it (e.g., new driving licence application, renewal, ownership transfer)?

Authority's response: Liveness detection is required for the Physician Portal under §١,٣٩,٢ for remote medical certification. The RFP does not require citizen-side liveness detection for remote submissions through the Mobile Application or Citizen Portal. Citizen verification is handled through OTP and, where available/applicable, national e-ID, while biometric enrolment is performed in person. Therefore, no additional citizen liveness requirement applies to new licence, renewal, or ownership-transfer flows.

Clarification Q-٠٣٦

RFP Reference: Automated document-forgery detection

Question: Section §١,٣٨ requires legibility checks, completeness validation, OCR extraction, and AV/malware scanning of citizen-uploaded documents. Is the system additionally required to perform automated detection of document forgery, tampering, or fraudulent manipulation of uploaded files?

Authority's response: §١,٣٨ requires AV/malware scanning, content-type and restricted-content checks, EXIF/GPS stripping, SHA-٢٥٦ hashing, legibility and completeness validation, OCR extraction, and manual review of low-confidence fields. It does not additionally mandate automated document-forgery or tamper-detection capability. Document validation is handled through the stated controls, manual review, and verification of originals where required; bidders may propose additional fraud-detection features, but they are not a mandatory §١,٣٨ requirement.

Clarification Q-٠٣٧

RFP Reference: Mobile NFC chip reading

Question: Is the Citizen Mobile Application required to use the device's built-in NFC capability to read the embedded chip in physical documents held by the citizen — including the driving licence, vehicle registration card, and passport?

Authority's response: No. The RFP does not require the Citizen Mobile Application to use device NFC to read chips in physical driving licences, vehicle registration cards, or passports. The verification model is based on QR/offline-signature mechanisms, and NFC references in the RFP relate to optional contactless card interoperability, not mandatory phone-based chip reading. Foreign-national validation is handled through DGGS integration, not mobile passport-chip reading.

رئيس مجلس الإدارة
المدير العام بالتكليف
القاضي مروان عبود