

DEPARTMENT OF NATIONAL REGISTRATION
REPUBLIC OF MALDIVES

REQUEST FOR PROPOSAL

**Supply and Implementation of a National Multimodal
Identity Resolution Platform with Trusted Timestamping**

RFP reference	DNR/RFP/2026/04
Issue date	12 / October / 2026
Version / status	1.0 — Issued
Clarification deadline	15 /October / 2026 at 12 :00 Maldives time (UTC+5)
Proposal submission deadline	21/ October / 2026 at 10:00 Maldives time (UTC+5)
Procurement contact	Procurement Section, Department of National Registration. procurement@dnr.gov.mv, 3033264

In this document the words "shall" and "must" denote mandatory requirements, "should" denotes an evaluated preference and "may" denotes a permission.

Contents

Contents	2
Section 1 — Introduction and Scope of Work	4
1.1 Invitation.....	4
1.2 Background and objectives	4
1.3 Scope of supply.....	4
1.4 Out of scope.....	5
1.5 Definitions and interpretation	5
1.6 Governing procurement framework.....	6
Section 2 — Tender Particulars	7
Section 3 — Technical Requirements and Compliance Sheet	11
3.1 Identity Resolution and Workflows	11
3.2 Fingerprint and Facial Processing.....	13
3.3 Deployment, Performance and Accuracy	18
3.4 Integration and Relying-Party Services	22
3.5 Trusted Time-stamping and DNR HSM Integration.....	24
3.6 Security and Data Protection	26
3.7 Implementation and Acceptance.....	30
3.8 Facial Recognition Models and Compute Efficiency	34
3.9 Facial Enrolment and Template Storage.....	36
3.10 Optional Module: Live Video Recognition	38
Section 4 — Pre-qualification	40
4.1 Experience of the Bidder.....	40
4.2 Delivery capability and team	42
4.3 Mandatory documents.....	45
4.4 Delivery programme.....	46
Section 5 — Instructions to Bidders.....	47
5.1 Complete proposal	47
5.2 Language and format.....	47
5.3 Clarifications and amendments.....	47
5.4 Pricing, currency and taxes.....	47
5.5 Proposal validity and bid security	47
5.6 Confidentiality and integrity	47
5.7 Deviations and assumptions	48
5.8 Submission and clarification of proposals	48
5.9 Rights of DNR	48
5.10 Award and contract	48
Section 6 — Evaluation Method	49

6.1 Evaluation stages.....	49
6.2 Scoring summary	49
6.3 Technical requirements (40 marks).....	49
6.4 Experience of the Bidder (15 marks).....	50
6.5 Delivery capability and team (15 marks)	50
6.6 Price (30 marks).....	51
6.7 Rating scale for experience and team.....	51
6.8 Ranking, panel and ties.....	52
Section 7 — Principal Contract Terms.....	53
Section 8 — Architecture and Resource Response.....	55
8.1 Benchmark protocol	55
8.2 Timing boundaries.....	55
8.3 Evaluation evidence	56
Annex A — Bidder Declaration	57
Annex B — Financial Response	58
B.1 Mandatory scope and evaluated price	58
B.2 Optional and separately priced items.....	58
Annex C — Reference Schedule	60
Annex D — Team Schedule and CV Format	61
D.1 Team schedule	61
D.2 CV format	61

Right-click and choose "Update Field" (or press F9) to refresh the table of contents after editing.

Section 1 — Introduction and Scope of Work

1.1 Invitation

The Department of National Registration of the Republic of Maldives (DNR) invites proposals from qualified and experienced bidders for the supply, implementation, integration, testing and commissioning of a National Multimodal Identity Resolution Platform with trusted timestamping (the Platform).

The Platform is a production system of national importance. It should provide fingerprint and facial matching, identity verification, 1:N identification and duplicate detection against the identity records held by DNR and shall provide controlled verification services to other Government agencies and approved relying parties designated by DNR.

1.2 Background and objectives

DNR is the national authority for the registration of citizens and the issuance of national identity records. The Platform supports the Government's paperless public-service commitment and the Maldives 2.0 agenda by strengthening the integrity of identity records within Civil Registration and Vital Statistics (CRVS), preventing duplicate and fraudulent registrations, and providing a trusted basis on which other agencies can verify the identity of citizens and residents.

The Platform shall be designed from the outset for multi-agency use. Initial relying-party use cases include beneficiary verification for Government subsidy programmes and identity verification in support of the Maldives Monetary Authority's planned centralised eKYC service. Further agencies designated by the Government, which may include the Maldives Inland Revenue Authority, shall be onboarded under the governance arrangements described in Section 3.4.

DNR remains the sole authority for identity records and adjudication decisions. Subsidy eligibility and payment, financial-sector customer due diligence and tax administration remain the responsibilities of the respective agencies. This procurement supplies verification and integration capability; delivery of those agencies' business systems is outside its scope.

1.3 Scope of supply

The scope comprises the following, all of which shall be included in the mandatory price unless expressly identified as optional:

- Perpetual, irrevocable licences for all software comprising the Platform, including matching engines, models, integrated database, API services, operator interfaces and administration tools, granted to DNR with no recurring licence fee, together with delivery of the Platform source code to DNR as required by requirements 3.7.10 and 3.7.11.
- An AI-assisted web application firewall and API protection component (requirement 3.6.9), delivered as part of the Platform with a licence of not less than three (3) years including all updates.
- Supply, installation and commissioning of the server, storage, GPU and network hardware on which the Platform runs, as a hyper-converged infrastructure meeting the minimum specification in requirement 3.3.2, installed at the DNR sites in Section 2 and owned by DNR, together with the proposed architecture for it.
- Design, installation and configuration of the Platform on that infrastructure, including production, recovery and test environments as specified in Section 2.

- Migration of the agreed existing identity records, photographs and fingerprint records, including initial template generation and reconciliation.
- Implementation of enrolment, verification, duplicate-review and exception workflows approved by DNR.
- A trusted time-stamping function within the Platform, with its signing keys generated and protected in DNR's existing Hardware Security Module (HSM), and integration with the DNR systems identified in Section 2.
- A relying-party service layer enabling controlled, auditable verification services for approved Government agencies.
- Security hardening, security testing, deployment checks, documentation, knowledge transfer and on-the-job training.
- One (1) year of warranty and local technical support commencing on Final Acceptance, with separately priced renewal options.

1.4 Out of scope

- Supply, replacement or expansion of HSM infrastructure. DNR has procured and operates an HSM under a separate project and will make it available to the Platform; the time-stamping function, its integration with the HSM and the key and certificate set-up within the HSM are in scope.
- Delivery or modification of relying-party agencies' business systems. Live integration with a specific agency is in scope only where Section 2 expressly includes it.
- Supply of fingerprint scanners, portrait cameras and other capture hardware, which DNR procures under a separate procurement; the Platform's compatibility with such devices is in scope under requirement 3.2.9.
- Capabilities expressly identified as optional in Section 3, which shall be priced separately and are excluded from the mandatory evaluation.

1.5 Definitions and interpretation

Term	Meaning
DNR	The Department of National Registration of the Republic of Maldives, the procuring entity and the owner of the Platform and all data within it.
Platform	The complete solution procured under this RFP, including software, database, interfaces, configuration and documentation.
Bidder	An enterprise registered in the Republic of Maldives as a small or medium-sized enterprise that submits a proposal. Joint ventures and consortia are not permitted.
Supplier	The successful Bidder following contract award.
Relying Party	A Government agency or other organisation approved in writing by DNR to consume verification services from the Platform.
1:1 verification	Comparison of a presented biometric sample against the record of a single claimed identity, returning a match or non-match decision.

Term	Meaning
1:N identification	Search of a presented biometric sample against the enrolled population, returning ranked candidates for adjudication.
Template	A processed biometric representation (fingerprint minutiae template or facial feature representation) derived from a sample image.
PAD	Presentation attack detection: the automated detection of artefacts or spoofing attempts at the point of biometric capture.
Time-stamping function	The RFC 3161 time-stamping function delivered as part of the Platform, whose signing keys are generated, stored and used only within the DNR HSM.
DNR HSM	The hardware security module procured and operated by DNR, made available to the Platform through the interface stated in Section 2.
Tender Particulars	The deployment, workload and commercial parameters published by DNR in Section 2, which bind all Bidders to the same basis.
Provisional Acceptance	DNR's written confirmation that deployment under Section 3.7 is complete, that the Platform operates as stated in the proposal, and that it has entered production use.
Final Acceptance	DNR's written confirmation that the Platform has operated in production for the stabilisation period in Section 2 without unresolved critical or high defects.
Mandatory	A requirement that must be met in full. The words "shall" and "must" denote mandatory requirements; "should" denotes a preference that is evaluated; "may" denotes a permission.
Optional	A capability that Bidders may offer and price separately and that is excluded from the mandatory compliance gate.
Perpetual Licence	A licence granted to DNR for an unlimited term that cannot be terminated or suspended by the Supplier or its licensors, is not conditional on the payment of any recurring fee, and permits use for the Platform's purpose by DNR and the Relying Parties it approves.
Source Code	Human-readable source code, build scripts, configuration, database schemas, model files and the documentation needed for a competent engineer to build, deploy, modify and maintain the software without the Supplier.

1.6 Governing procurement framework

This procurement is conducted under the Public Finance Act (Law No. 3/2006) and the Public Finance Regulation (Regulation No. 2017/R-20) of the Republic of Maldives, as amended, and the applicable circulars of the Ministry of Finance. In the event of inconsistency between this RFP and the governing framework, the governing framework prevails. Nothing in this RFP creates a contract or an obligation on DNR to award.

Section 2 — Tender Particulars

The particulars in this section bind all Bidders to the same deployment, workload and commercial basis. Where a requirement in Section 3 refers to a published figure, the figure in this section applies. These particulars form part of the contract.

Ref	Parameter	Particular
2.1	Initial population and migration volume	Persons: 450,000 identity records, comprising all Maldivian citizens registered with DNR, including minors and records of deceased persons retained for lifecycle integrity. Face images: 450,000 ID-card portraits, one current portrait per person, JPEG, plus historical portraits where held. Fingerprint records: 350,000 persons with ten-print (4-4-2 slap) records at 500 ppi, WSQ; remaining persons have no fingerprints on file and shall be flagged for capture at next contact. Source formats: DNR identity-card system database export (CSV/JSON with image references), image files as held; sample extract of 1,000 de-identified records provided to Bidders on request under non-disclosure.
2.2	Planning horizon and licensed capacity	Planning horizon: five (5) years from Final Acceptance. Licensed capacity: 600,000 persons at year 1; 700,000 at year 3; 800,000 at year 5, with up to five facial templates and twenty fingerprint templates per person. Relying Parties: a minimum of ten (10) Relying Parties and fifty (50) consuming applications by year 5, with no per-Relying-Party licence charge.
2.3	Workload and acceptance thresholds	Peak workload (sustained for 60 minutes): 1:1 verification 20 transactions per second; facial 1:N search 2 per second; fingerprint 1:N search 1 per second; combined multimodal search 1 per second; 50 concurrent operator sessions; 200 concurrent API sessions. End-to-end latency at the gallery size in 2.2 (year 1): 1:1 verification $p_{95} \leq 2$ s, $p_{99} \leq 3$ s; facial 1:N $p_{95} \leq 5$ s; ten-print 1:N $p_{95} \leq 10$ s; combined $p_{95} \leq 15$ s. Timestamped transaction duration reported separately. Retrieval recall for any approximate index: ≥ 0.99 at top-50 against exhaustive search. Accuracy limits on DNR-approved test data at the operating thresholds: face 1:1 FNMR $\leq 2\%$ at FMR 1 in 100,000; fingerprint 1:1 (two fingers) FNMR $\leq 1\%$ at FMR 1 in 10,000; face 1:N FNIR $\leq 2\%$ at FPIR 0.1%; ten-print 1:N FNIR $\leq 0.5\%$ at FPIR 0.1%. Reported demographic differentials shall not exceed three times the overall rate for any sex or age group.
2.4	Indicative candidate-retrieval target	10 milliseconds p_{95} for indexed facial candidate retrieval from a prepared template at the year-1 gallery size, top-50, 2 searches per second, recall ≥ 0.99. Not binding; reported for information and considered in the scoring of Sections 3.3 and 3.8.

Ref	Parameter	Particular
2.5	Evaluated-cost horizon and energy rate	Evaluation horizon: five (5) years. Energy rate applied identically to every Bidder for the supplied hardware: MVR 4.90 per kWh at the Bidder's declared power draw at 60% utilisation, for all nodes in all environments. Hardware is supplied with the bid and priced in Annex B; no other hosting rate applies.
2.6	Sites and environments	Production: DNR data centre, Malé. Recovery: protected backup copies replicated to the Government data centre operated by Maldives Digital Services (MDS); restoration of the verification service within a recovery time objective of eight (8) hours and a recovery point objective of one (1) hour. No second cluster is required; within the production cluster, loss of either node shall not stop the verification service, although loss of the GPU node reduces performance to the degraded mode declared under requirement 3.3.2. Test/training: logically separated environment on the same two-node cluster with synthetic or de-identified data, sized at not less than 10% of production resources. Network: all environments on the Government Network operated by MDS; Relying-Party access through the DNR API gateway only; no direct database access.
2.7	DNR integration endpoints	Systems: (a) DNR identity-card management system — authoritative person record, portrait and card lifecycle; (b) DNR civil registry / birth and death registration system — lifecycle events. Authoritative identifier: the Maldivian national identity number (format: letter A followed by six digits), immutable for life. Interface specifications: provided to the Supplier at contract signature; DNR will expose read access to the authoritative record and a lifecycle-event feed through documented database views or web services.
2.8	DNR HSM	DNR operates a hardware security module procured under a separate project: [make and model], FIPS 140-2 or 140-3 Level 3 validated, accessible to the Platform over the network through PKCS#11 (and, where supported, KMIP or the vendor REST interface). DNR will provide the Supplier with a dedicated partition or slot, the client software and credentials for it, and access to a test partition within thirty (30) days of contract signature. DNR holds all HSM administrative credentials; the Supplier receives application-level credentials only.

Ref	Parameter	Particular
2.9	Relying-party policy	Relying Parties receive 1:1 verification and DNR-approved attributes only. No Relying Party is authorised for 1:N search; any future authorisation requires a written instrument issued by DNR under the applicable law and a change to the Platform configuration recorded under requirement 3.4.4. Initial Relying Parties: (a) the National Social Protection Agency, for subsidy beneficiary verification — live integration included in the mandatory scope; (b) the Maldives Monetary Authority centralised eKYC service — interface readiness and sandbox included in the mandatory scope, live integration priced per Annex B line O3 when the MMA service is ready. Further agencies: onboarded at the per-agency price in Annex B line O3.
2.10	Remote and unattended capture	In scope. Channels: mobile application (Android and iOS) software development kit and a web-browser capture component, for use by Relying Parties under DNR approval. Assurance: liveness and presentation attack detection meeting requirement 3.2.4 and the injection controls in requirement 3.2.6; capture-assurance indicator returned with every verification.
2.11	Capture devices	Fingerprint scanners and portrait cameras are procured by DNR under a separate procurement and are not supplied under this RFP. DNR will select devices from the compatibility schedule submitted by the successful Bidder under requirement 3.2.9. Devices will be certified to FBI Appendix F (ten-print stations) or FBI PIV-071 / FAP 30 or higher (counter scanners), and cameras will meet ISO/IEC 19794-5 and ICAO 9303 portrait requirements. Indicative quantities for the Bidder's planning only: 8 ten-print stations, 40 counter scanners and 48 cameras.
2.12	Stabilisation period	Ninety (90) calendar days of production operation between Provisional and Final Acceptance, during which the availability target in 2.14 must be met and no critical or high defect may remain open.
2.13	Delivery and completion deadlines	Physical delivery to the DNR site of the complete hardware and software stack (the delivery milestone defined in Section 7, Payment terms; installation is not part of it) within eight (8) weeks of contract signature. Provisional Acceptance within twelve (12) months of contract signature. DNR dependencies: interface specifications and sample data at signature; data-centre space, power and network for the two nodes available by week 2; HSM partition and test access by day 30 (see 2.8); full migration data extract by month 3; NSPA interface specification by month 4; DNR acceptance-test team and adjudicators available from month 8.
2.14	Service availability target	99.5% monthly availability of the production verification API, measured at the DNR API gateway as successful responses within the latency limits in 2.3, excluding planned maintenance of not more than four (4) hours per month notified seven (7) days in advance. Enrolment and adjudication functions: 99.0%. Operation in the declared degraded mode after a node failure counts as available provided the degraded-mode latency stated by the Bidder under requirement 3.3.2 is met.

Ref	Parameter	Particular
2.15	Proposal validity and bid security	Validity: one hundred and twenty (120) days from the submission deadline. Bid security: two per cent (2%) of the total mandatory price, as an unconditional bank guarantee from a bank licensed in the Maldives or confirmed by one, valid for one hundred and forty-eight (148) days from the submission deadline.
2.16	Submission method and address	Electronic submission in PDF to the DNR procurement email address _____ or the Government e-procurement portal, with the Section 3, Section 4 and Section 8 responses also in editable form, and one (1) printed original delivered to the Department of National Registration, _____, Malé, Republic of Maldives, by the deadline on the cover page. The financial proposal shall be in a separate file or sealed envelope.

Section 3 — Technical Requirements and Compliance Sheet

This section is the technical requirements and the compliance sheet in one. Each requirement is numbered and has a response column. Bidders shall respond to every requirement in the response column, stating Comply, Partially or Not Comply, and shall use the remarks column to state the offered capability and version and the exact location (document, section and page) of the supporting evidence in the proposal. No proof of concept, pilot or live demonstration is required or will be requested at the evaluation stage; DNR evaluates the proposal and the evidence it contains. A response of Comply without locatable evidence is treated as unsupported.

Every requirement is either Mandatory or Optional. Requirements marked Mandatory form the mandatory scope and are scored under Section 6.3; a proposal that states a deviation from a mandatory requirement is not evaluated further, and a proposal must reach the minimum technical score in Section 6.3 to be considered for award. Requirements marked Optional are priced separately, are not scored and do not form part of the mandatory scope. Some requirements can only be checked after contract award, because they depend on DNR data, DNR infrastructure, the DNR HSM, the delivered hardware or an acceptance-stage test. These are marked "Post-award verification" in the requirement text. For each of them the Bidder's response at submission shall be a written statement of compliance, in the remark's column or in the technical proposal, confirming that the Bidder will fulfil the requirement in full and describing how. That statement is binding on the Supplier and is sufficient for evaluation. DNR will check these matters during deployment and will raise any concern with the Supplier for resolution before Provisional Acceptance. Nothing in this section requires a Bidder to test on DNR data or DNR infrastructure before award.

Where this section refers to a standard, the edition current at the issue date of this RFP applies unless otherwise stated. Naming a product, algorithm, index type or processor does not by itself satisfy any requirement; compliance is assessed on evidence.

3.1 Identity Resolution and Workflows

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
3.1.1	Platform scope The Supplier shall provide one integrated Platform supporting fingerprint matching, facial matching, biographic record linkage, 1:1 verification and 1:N identification against the DNR identity record set. The Bidder shall identify each matching engine, its developer and version, confirm that it is offered under the perpetual licence required by requirement 3.7.10, and confirm that it is supported by the developer for the full planning horizon in Section 2.	Mandatory		
3.1.2	Authoritative record binding	Mandatory		

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
	Every enrolment, template and search result shall be linked to the DNR authoritative person identifier. Source-system references and lifecycle status shall be preserved. The Platform shall not create or maintain a competing authoritative civil register; the DNR register remains the single source of truth for biographic identity.			
3.1.3	Enrolment and duplicate detection The Platform shall support new enrolment, authorised updates and a search for potential duplicates before any enrolment is approved. Results shall present ranked candidates with match scores, the modality or modalities used, sample quality indicators and the decision threshold in force at the time of the search.	Mandatory		
3.1.4	Adjudication The Platform shall provide an adjudication queue with side-by-side comparison views, operator notes and recorded decisions. A biometric candidate match shall never automatically merge, delete or cancel a civil record. Every resolution shall require an authorised adjudicator, shall record the reason, and shall be subject to a configurable second-level review for defined case types.	Mandatory		
3.1.5	Configurable workflows Enrolment, verification, duplicate-review and exception workflows shall be configurable by DNR administrators, with DNR-approved roles and approval steps. Separate matching thresholds shall be supported for different use cases and Relying Parties. All configuration changes shall be versioned and auditable.	Mandatory		
3.1.6	Inclusive exception handling The Platform shall support persons with missing fingers, unreadable fingerprints, poor-quality facial images or an unavailable modality, and shall route unresolved cases to assisted verification. Inability to provide a biometric shall never be treated as evidence of fraud. Operator interfaces and documentation shall be in English; the Platform	Mandatory		

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
	shall store, search and display Dhivehi names in Thaana script correctly, using Unicode with right-to-left rendering.			

3.2 Fingerprint and Facial Processing

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
3.2.1	Fingerprint processing The Platform shall extract fingerprint templates, apply quality assessment (NFIQ 2 or an evidenced equivalent) and pre-processing, and flag insufficient samples for recapture or review. It shall support rolled and flat impressions, partial prints and multi-finger matching with up to ten fingers per person. The Bidder shall state the minimum usable image quality, supported resolutions and the handling of amputated, bandaged or worn fingers.	Mandatory		
3.2.2	Fingerprint template characteristics The Bidder shall state the template format, the typical and maximum minutiae counts extracted from good-quality images, the extraction method and the image-quality conditions on which these depend. Minutiae counts are disclosed for information and are not an acceptance criterion; matching accuracy is assessed under requirements 3.3.6 and 3.3.7.	Mandatory		
3.2.3	Facial processing The Platform shall provide face detection, template extraction, and 1:1 and 1:N facial matching. The Bidder shall describe the facial representation used (for example, descriptor dimensionality and landmark set), the supported image resolutions, pose and illumination ranges, and the behaviour at the limits of those ranges.	Mandatory		

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
	Feature or dimension counts are disclosed for information and are not an acceptance criterion.			
3.2.4	Presentation attack detection The Platform shall perform presentation attack detection (PAD) on every facial and fingerprint capture used for enrolment or verification, at attended counters and in any remote channel, and shall reject a sample that fails PAD before any matching takes place. Facial PAD shall detect at least: printed photographs, photographs and videos replayed on a phone, tablet or monitor screen, paper and fabric masks and cut-outs, and silicone or resin 3D masks. Fingerprint PAD shall detect at least: printed fingerprints and fake fingers made of silicone, gelatine, latex, wood glue or similar materials. The Bidder shall describe in the technology statement under requirement 3.2.5 the attack species against which the offered PAD has been tested, the test method used and the error rates obtained (attack presentation classification error rate and bona fide presentation classification error rate), and shall confirm in writing that the Platform rejects the attack types listed above and that the bona fide presentation classification error rate will not exceed 3% for face and 5% for fingerprint in DNR's use. No laboratory certification of the PAD software is required; DNR relies on the written statement and will check these matters during deployment. Facial PAD at attended counters shall operate passively from the captured frames without requiring the subject to perform actions; active challenge-response may be added for remote channels. PAD thresholds shall be configurable by DNR per channel, every PAD decision and score shall be stored with the sample and included in the audit record, and a PAD failure shall never be overridable by an operator alone: any supervisor override shall require a second authorised user, a recorded reason and a timestamped audit entry. Written statement: <i>a written statement of compliance in the proposal or in the remark's column is sufficient; DNR will check this during deployment.</i>	Mandatory		

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
3.2.5	Facial detection and anti-spoofing technology statement The Bidder shall submit with its proposal a technology statement describing the facial capture, detection and presentation-attack-detection technology offered. The statement shall be binding on the Supplier; DNR will check it during deployment. It shall describe, in the Bidder's own terms and with technical specificity: (a) the face detection and landmark technology and how it rejects non-face and partial-face inputs; (b) each liveness and presentation-attack-detection method used, the physical or statistical signal each method relies on, whether it is passive or requires the subject to perform an action, and the attack types each method is intended to defeat; (c) which characteristics of the capture hardware, if any, the software uses or can use to strengthen liveness detection, the camera models with which each such mode has been tested, and how the software behaves when a camera does not provide those characteristics; (d) how the outputs of the individual methods are combined into a single PAD decision and score; (e) the testing performed on the offered PAD, whether by the Bidder, the manufacturer or a third party, stating the exact software version tested, the attack species presented, the test method and the error rates obtained; and (f) known limitations, including performance in low light, with spectacles and head coverings, and across skin tones, with any demographic test results. Generic descriptions that do not identify the signals and methods used will be treated as unsupported. A proposal whose only facial liveness method at attended counters requires the subject to perform actions (for example blinking or turning the head) does not meet this requirement. Written statement: <i>a written statement of compliance in the proposal or in the remark's column is sufficient; DNR will check this during deployment.</i>	Mandatory		
3.2.6	Remote and unattended capture The Platform shall provide a remote capture component for the channels stated in Section 2	Mandatory		

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
	item 2.10, with liveness detection meeting requirement 3.2.4, device and session binding, and a capture-assurance indicator returned with each verification. The component shall detect and reject injection of media that did not originate from the device camera, including virtual-camera drivers, emulators, rooted or jailbroken devices, hooked camera APIs and man-in-the-middle replay of a previous session; it shall bind each capture to a server-issued single-use nonce and a device attestation (for example Android Play Integrity or Apple App Attest) and shall reject any sample whose nonce, attestation or integrity check fails. The Bidder shall state the capture method and shall describe the testing performed on the remote channel and the results obtained, in the same form as requirement 3.2.5; DNR will check effectiveness during deployment. Written statement: a written statement of compliance in the proposal or in the remark's column is sufficient; DNR will check this during deployment.			
3.2.7	Capture integrity and anti-tampering The Platform shall ensure that only images captured live from a registered capture device, at the time of the transaction, can be used for enrolment or verification. Each enrolment and verification workstation and each capture device shall be registered with the Platform and identified by a unique device identifier; the capture client shall sign every captured image and its metadata (device identifier, capture time, PAD result and score, operator identity, session identifier and server nonce) with a device-specific key at the moment of capture, and the Platform shall verify the signature and nonce and reject any image that is unsigned, re-used, altered, older than a configurable validity window, or that originates from a file, clipboard, virtual camera or unregistered device. File upload of images shall be disabled for enrolment and verification workflows; it shall be available only to the migration and adjudication roles for documented purposes, shall be labelled as an uploaded image in the record and audit trail, and shall never	Mandatory		

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
	produce a verification result relied on by a Relying Party. The signed capture metadata and PAD outcome shall be stored with the template and bound into the timestamped evidence record under Section 3.5 so that any later substitution of the image is detectable. The capture client shall be delivered as a signed, integrity-checked application, shall communicate with the Platform only over mutually authenticated encrypted channels, and shall refuse to operate if its integrity check fails. The Bidder shall describe the device registration, key provisioning, key rotation and revocation procedures and shall confirm in writing that a printed photograph, a screen replay, a previously captured image and an injected image are each rejected and logged; DNR will check this during deployment. Written statement: <i>a written statement of compliance in the proposal or in the remark's column is sufficient; DNR will check this during deployment.</i>			
3.2.8	Interchange formats and standards The Platform shall import and export fingerprint images in WSQ, JPEG 2000, BMP, PNG and TIFF; shall support ISO/IEC 19794-2 fingerprint minutiae templates and ISO/IEC 19794-4 finger images; shall support ISO/IEC 19794-5 facial images; and shall exchange records in ANSI/NIST-ITL format. The Bidder shall state the exact editions, profiles and read/write capabilities supported, including conversion from legacy ANSI/NIST-ITL 1-2000 and EFTS records. DNR will check compatibility with its own data during deployment. Written statement: <i>a written statement of compliance in the proposal or in the remark's column is sufficient; DNR will check this during deployment.</i>	Mandatory		
3.2.9	Capture device compatibility Fingerprint scanners and portrait cameras are procured by DNR under a separate procurement and are outside the scope of this RFP. The Bidder shall nevertheless state in its proposal, in the form of a compatibility schedule, every fingerprint scanner model (ten-print live-scan, two-finger and	Mandatory		

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
	single-finger) and portrait camera model with which the offered Platform has been tested and is certified to operate, giving for each the manufacturer, model, certification held (FBI Appendix F, FBI PIV-071 / FAP class, or equivalent), supported operating systems, the driver or SDK version used and whether the integration is native or through a third-party capture SDK. DNR will select devices under the separate procurement from the schedule submitted by the successful Bidder. The Platform shall support, at no additional licence cost, every device on the schedule and any further device certified to FBI Appendix F or PIV-071 that DNR later procures, and the Supplier shall provide the integration, testing and documentation needed to bring such a device into service within thirty (30) days of DNR's request. The Platform shall accept fingerprint images and templates from any compliant device through the interchange formats in requirement 3.2.8, and shall not be tied to a single scanner manufacturer.			
3.2.10	Optional mixed-impression analysis The Bidder may separately describe and price any capability to separate and analyse a mixed set of fingerprint impressions from more than one person. This is a forensic capability; it is not required for civil enrolment or verification and is excluded from the mandatory evaluation.	Optional		

3.3 Deployment, Performance and Accuracy

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
3.3.1	Self-hosted operation All production processing and data shall reside on DNR-controlled infrastructure within the Maldives. Core matching, database, API and administration	Mandatory		

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
	functions shall operate without internet access. The Bidder shall declare every external dependency, including licence activation, update distribution and telemetry, and shall confirm that no data leaves DNR infrastructure without DNR authorisation.			
3.3.2	Hardware supply and hyper-converged architecture The Supplier shall supply, install and commission all server, storage, GPU and network hardware required to run the Platform in every environment in Section 2, delivered as a hyper-converged infrastructure (HCI) cluster in which compute, storage and virtualisation are provided by the same nodes under a single management layer. The cluster shall consist of two (2) nodes. Each node shall meet at least the following minimum specification: thirty-two (32) physical CPU cores; sixty-four (64) GB of RAM; and two (2) TB of usable SSD storage after replication and formatting. One of the two nodes shall additionally be equipped with one NVIDIA RTX PRO 4500 Blackwell GPU (32 GB GDDR7 ECC, PCIe) or equivalent; the cluster therefore contains one (1) GPU. The Bidder shall propose the architecture on this basis, stating the HCI platform, the role of each node, the virtualisation or container layer, storage replication and failure tolerance across the two nodes (including any witness or quorum component required by the HCI platform, which the Bidder shall supply), network design, and how the availability and recovery targets in Section 2 are met. Because only one node carries a GPU, the Bidder shall state which Platform functions depend on the GPU, shall design the Platform so that 1:1 verification, 1:N search and enrolment continue on the remaining node in a declared degraded mode if the GPU node fails, and shall state the latency and throughput achievable in that mode against Section 2. The Bidder shall confirm that the two-node cluster meets the workload and capacity in Section 2 for the full planning horizon and shall state the headroom provided; where it considers the specification insufficient it shall say	Mandatory		

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
	so and price additional nodes under Annex B line O5. All hardware shall be new, shall be supplied with a manufacturer warranty of not less than three (3) years with on-site next-business-day replacement in the Maldives, and shall be registered in DNR's name. The Platform shall deploy on a supported operating system; no particular operating system is mandated. The Bidder shall state supported versions and lifecycle dates for every hardware and software component.			
3.3.3	Integrated database and API server The Supplier shall supply all database and API server components required for the complete Platform, with clustering or redundancy options sufficient to meet the availability target in Section 2, and all required licences. Any dependence on third-party database software, web servers or middleware shall be declared with its licensing basis; components shall not be described as licence-free unless this is evidenced.	Mandatory		
3.3.4	Capacity and scale The Platform shall be sized to the Tender Particulars for the full planning horizon. The Bidder shall state separately the licensed number of persons, facial templates and fingerprint templates, all per-record, per-user, per-core, per-transaction, per-Relying-Party and API limits, and the method and one-time cost of expansion beyond each limit. Expansion shall be granted as a perpetual licence extension and shall not convert any part of the Platform to a subscription.	Mandatory		
3.3.5	Latency and throughput The Platform shall meet the published workload and latency limits separately for 1:1 verification, facial 1:N search, fingerprint 1:N search and combined multimodal search. Measurement shall run from receipt of a complete API request to delivery of the final result and shall include queueing, template extraction, matching and audit. The timestamped transaction duration shall be reported separately. Where Section 2 item 2.4	Mandatory		

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
	publishes an indicative candidate-retrieval target, the Bidder shall report p95 against it; that target is binding only if Section 2 states so.			
3.3.6	Benchmark evidence The Bidder shall provide benchmark results obtained under the protocol in Section 8 at the published gallery size, concurrency and sustained request rate, on the offered hardware configuration or, where that is not available to the Bidder before award, on a comparable configuration with the differences and the expected scaling stated, reporting p50, p95 and p99 latency, throughput, failures and retrieval recall against exhaustive search. Results shall disclose model and engine versions, hardware, template counts, warm and cold conditions and candidate-list size, and shall distinguish retrieval from final matching. DNR will check the committed results on its own data during deployment. Written statement: <i>a written statement of compliance in the proposal or in the remark's column is sufficient; DNR will check this during deployment.</i>	Mandatory		
3.3.7	Independent accuracy evaluation For each offered facial-recognition algorithm, the Bidder shall provide results from the NIST Face Recognition Technology Evaluation (FRTE) 1:1 and 1:N tracks, or an evidenced equivalent independent evaluation, for the exact algorithm version offered or its nearest tested predecessor, including the reported demographic differential performance. For each offered fingerprint algorithm, the Bidder shall provide results from NIST PFT III, MINEX III or an evidenced equivalent independent evaluation. DNR will give greater weight to independent evidence than to Bidder-run tests.	Mandatory		
3.3.8	Availability, resilience and recovery The production verification service shall meet the availability target in Section 2. The Bidder shall describe the high-availability design, failure modes, failover behaviour and the recovery time and recovery point objectives achieved for each	Mandatory		

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
	environment, and shall confirm in writing that failover and restoration operate as described; DNR will check this during deployment. Written statement: <i>a written statement of compliance in the proposal or in the remark's column is sufficient; DNR will check this during deployment.</i>			

3.4 Integration and Relying-Party Services

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
3.4.1	API and integration pack The Platform shall expose documented REST APIs for enrolment, authorised updates, quality assessment, 1:1 verification, 1:N search, duplicate-case status and evidence retrieval, with an OpenAPI specification, worked examples, error definitions, a versioning and deprecation policy, and a test environment with synthetic data.	Mandatory		
3.4.2	DNR system integration The Supplier shall implement the interfaces to the DNR systems identified in Section 2, including authoritative identity lookup and lifecycle updates. Field, identifier and status mappings shall be approved by DNR. Third-party dependencies and data-reconciliation procedures shall be documented.	Mandatory		
3.4.3	Relying-party onboarding and access control Each Relying Party and each consuming application shall have separate credentials, certificates and permissions, approved by DNR before production access. The Platform shall enforce scoped operations, permitted attributes, rate limits, time-of-day restrictions where configured, and immediate revocation. Transport shall be mutually authenticated and encrypted and	Mandatory		

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
	shall integrate with DNR's approved authentication infrastructure.			
3.4.4	Service tiers and purpose limitation The Platform shall implement service tiers configurable per Relying Party. The default tier shall provide 1:1 verification returning a match decision and DNR-approved attributes only. 1:N search shall not be available to any Relying Party unless DNR enables it for that party under the instrument stated in Section 2 item 2.9. Each Relying Party shall be bound to a recorded purpose, and the Platform shall reject requests outside the approved purpose, scope or attribute set.	Mandatory		
3.4.5	Verification results A verification response shall contain only the decision and the attributes approved for the requesting Relying Party, together with a transaction reference, verification method, capture-assurance indicator, policy and model version, and an evidence reference. Biometric images, templates, similarity scores and candidate lists shall not be returned to Relying Parties by default; any exception shall require DNR configuration and shall be audited.	Mandatory		
3.4.6	Agency integration readiness The Platform shall provide configurable interfaces and data mappings supporting beneficiary verification for subsidy programmes, the Maldives Monetary Authority's centralized eKYC service and other agencies designated by DNR. Live integration with a specific agency is included in the mandatory scope only where Section 2 item 2.9 states so; otherwise, the Bidder shall price it separately on a per-agency basis.	Mandatory		
3.4.7	Relying-party service levels and reporting The Platform shall support per-Relying-Party quotas, service-level measurement (availability, latency, error rate) and monthly usage and performance reports and shall provide DNR with a dashboard of consumption by Relying Party. DNR	Mandatory		

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
	shall be able to suspend or throttle any Relying Party without affecting others.			
3.4.8	Application management and audit The Platform shall record who approved each Relying Party and application, the approved purpose, every permission change and every request outcome. A sandbox environment and onboarding documentation shall be provided for prospective Relying Parties, and the onboarding process shall require DNR sign-off at each stage.	Mandatory		

3.5 Trusted Time-stamping and DNR HSM Integration

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
3.5.1	Time-stamping function and HSM boundary The Platform shall include an RFC 3161 time-stamping function that issues and verifies time-stamp tokens for the events in requirement 3.5.2. The time-stamp signing key, and the DNR-owned trust anchor under which its certificate is issued, shall be generated, stored and used only within the DNR HSM through the interface stated in Section 2 (PKCS#11 or equivalent); no private key material shall exist outside the HSM. The Supplier shall establish the keys and certificates in the HSM under a key ceremony witnessed and approved by DNR, with DNR holding all HSM administrative credentials. The function shall use a trusted time source approved by DNR. It shall be designed so that DNR can, at any time and without changing to the evidence format, direct the Platform to obtain tokens from any other RFC 3161 authority DNR designates. The HSM itself is supplied and operated by DNR and is outside the Supplier's scope.	Mandatory		
3.5.2	Timestamped events	Mandatory		

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
	The Platform shall obtain a trusted timestamp for verification outcomes, enrolment approvals, duplicate-resolution decisions, and changes to identity links, Relying-Party permissions or matching thresholds. Each timestamp shall be bound to a stable transaction identifier, the DNR record reference, the event type, the acting user or application, the decision and the policy and model version in force.			
3.5.3	Evidence integrity The Platform shall create a canonical representation of each event and a cryptographic hash using an algorithm approved by DNR. Only the hash shall be passed to the time-stamping function; raw biometric data shall never be included in a time-stamp request. The timestamp token and the protected event record shall be stored together so that any later alteration is detectable.	Mandatory		
3.5.4	Token validation and evidence export The Platform shall validate the message imprint, nonce where used, timestamp policy, signature and certificate chain of every token received, and shall retain the token with its validation material. It shall export a verifiable evidence package comprising the protected event, its hash, the timestamp token and a documented verification procedure usable by an independent party.	Mandatory		
3.5.5	Outage and retry behaviour If the time-stamping function or the DNR HSM is unavailable the Platform shall queue requests durably and retry under controlled back-off, and shall clearly mark each event as pending or failed until a valid token is obtained. A locally recorded time is not a trusted timestamp; a token obtained later proves existence only from the time of that token. DNR policy, configurable per workflow, shall determine which transactions must wait for a valid token before completing.	Mandatory		
3.5.6	Deployment checks and retention	Mandatory		

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
	The Supplier shall confirm in writing that the Platform provides successful time-stamp issuance and verification, detection of an altered event, rejection of an invalid token, and recovery after an outage of the HSM; DNR will check these during deployment. Retention and access permissions for time-stamp evidence shall be configured to DNR policy. Integration with the DNR HSM, including the key ceremony, is included and shall be performed by the engineers nominated under Section 4.2, drawing on the HSM security experience evidenced under Section 4.1; the availability of the HSM interface to the Supplier shall be identified as a dependency in the delivery programme. Written statement: <i>a written statement of compliance in the proposal or in the remark's column is sufficient; DNR will check this during deployment.</i>			

3.6 Security and Data Protection

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
3.6.1	Access and administration The Platform shall apply role-based access control, least privilege and multi-factor authentication for all privileged and adjudication users, with separation of duties between routine operators, adjudicators, administrators, security administrators and auditors. API secrets and administrative credentials shall be protected and transferred securely to DNR at handover.	Mandatory		
3.6.2	Protection of biometric information All sensitive data shall be encrypted in transit and at rest. Biometric templates, source images, exports and backups shall be protected with DNR-approved key management, with documented key custody, rotation and recovery. The Supplier shall	Mandatory		

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
	not reuse, retain, train models on, or transfer DNR data outside DNR infrastructure for any purpose without DNR's explicit written authorization.			
3.6.3	Audit and monitoring The Platform shall maintain tamper-evident logs of enrolment, search, verification, adjudication, export, deletion, configuration and administrative actions, recording the actor, purpose, time, transaction reference and outcome. Log access shall be restricted and logged. Security-relevant events shall be forwarded to DNR monitoring in a documented format. The timestamping controls in Section 3.5 apply to the events listed there.	Mandatory		
3.6.4	Lifecycle and retention The Platform shall implement DNR-approved retention, archival, correction and deletion rules, including their effect on backups and evidence, and shall preserve the traceability of lifecycle changes. Unauthorized bulk extraction shall be prevented and alerted. Documented export in open, usable formats shall be provided to support transition to another supplier.	Mandatory		
3.6.5	Data protection compliance The Platform and the Supplier's delivery and support activities shall comply with the personal data protection legislation in force in the Republic of Maldives, the information security policies issued by Maldives Digital Services (MDS), and DNR's data-governance policies. The Supplier shall support DNR's data protection impact assessment, shall implement purpose limitation and data minimization by design, and shall provide functions supporting data-subject access and correction requests under DNR control.	Mandatory		
3.6.6	Security verification The Supplier shall harden the delivered operating environment to a recognised baseline and shall perform application and API penetration testing before Provisional Acceptance, using an independent tester approved by DNR who is not an employee of the Supplier, after the Supplier's	Mandatory		

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
	own security testing by the engineers nominated under Section 4.2. Critical and high findings attributable to the Platform shall be remediated and retested before acceptance. Testing shall use synthetic or DNR-approved de-identified data; any controlled testing on production data requires written DNR authorisation. Written statement: <i>a written statement of compliance in the proposal or in the remark's column is sufficient; DNR will check this during deployment.</i>			
3.6.7	Secure development and vulnerability management The Supplier shall provide a software bill of materials for the delivered Platform, shall maintain a vulnerability-management process throughout the warranty and support period, and shall provide security patches for critical vulnerabilities within fourteen (14) days of public disclosure, and for high vulnerabilities within thirty (30) days.	Mandatory		
3.6.8	Backup and business continuity The Platform shall provide scheduled encrypted backups with integrity checking, access-controlled restoration and documented recovery procedures, and the Supplier shall confirm in writing that restoration to an isolated environment and the proposed failover operate as described; DNR will check this during deployment. Built-in backup tools shall integrate with DNR's wider backup policy and do not remove the need for protected off-system recovery copies. Written statement: <i>a written statement of compliance in the proposal or in the remark's column is sufficient; DNR will check this during deployment.</i>	Mandatory		
3.6.9	Application and API attack protection The Platform exposes three externally reachable surfaces: the Relying-Party verification API (Section 3.4), the remote capture endpoints used by the mobile and web capture components (requirement 3.2.6), and the browser interface used by DNR operators and adjudicators. The Supplier shall protect all three with an AI-assisted web application firewall and API gateway,	Mandatory		

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
	delivered as part of the Platform, running on the hardware supplied under requirement 3.3.2 within DNR infrastructure; cloud-hosted or externally operated filtering is not acceptable (requirement 3.3.1). It shall: (a) enforce the Relying-Party credentials, scopes, quotas and rate limits of requirement 3.4.3 at the edge, and block or throttle any client that attempts enumeration of national identity numbers, credential stuffing, bulk verification, or requests outside its approved purpose; (b) fingerprint every TLS client (for example using JA3, JA4 or an equivalent method) and the HTTP behaviour of each session, maintain allow-lists of the fingerprints expected from the genuine capture components and each onboarded Relying-Party integration, and flag or block sessions whose fingerprint does not match the client they claim to be, including scripted tools and modified capture applications, feeding this signal into the injection controls of requirement 3.2.6; (c) maintain session awareness by binding each session and its tokens to the TLS fingerprint, device attestation and server nonce, and by detecting token replay from a different fingerprint, concurrent use of one session from different origins, nonce reuse, abnormal session duration or request sequence, and automation patterns inconsistent with a human operator or a genuine capture flow; (d) apply behavioural and machine-learning anomaly detection trained on the Platform's own traffic, in addition to signature protection against the OWASP Top 10 and OWASP API Security Top 10, with models and rules updated under the lifecycle controls of requirement 3.8.5 and without sending traffic data outside DNR infrastructure; (e) mitigate automatically according to DNR-configurable policy, including blocking, throttling, invalidating sessions, requiring step-up authentication, and raising the capture-assurance risk indicator returned to the Relying Party under requirement 3.4.5; (f) absorb volumetric and application-layer denial-of-service attacks up to the capacity declared by the Bidder, shedding attack traffic before it reaches the matching engines; and (g)			

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
	log every decision with the transaction reference, Relying Party, fingerprint and session identifiers, forward alerts to DNR monitoring under requirement 3.6.3, and bind blocking decisions affecting a verification outcome into the timestamped evidence record under Section 3.5. The Bidder shall name the product or component and state whether it is in-house or third-party. By exception to requirement 3.7.10, the application and API protection may be licensed on a term basis: the mandatory price shall include a licence of not less than three (3) years from delivery, covering all signature, model and software updates and manufacturer support for that period, and the Bidder shall quote the renewal price for years four and five in Annex B. Expiry of the term licence shall not disable any other Platform function. The protection shall be designed, tuned and operated by the security engineers nominated under Section 4.2, and its machine-learning mitigation logic shall be validated by the agentic-AI security engineer nominated under Section 4.2. The Bidder shall confirm in writing that the protection is effective against enumeration, credential-stuffing, replay, fingerprint-mismatch and denial-of-service scenarios; effectiveness is covered by the penetration test under requirement 3.6.6 and DNR will check it during deployment. Written statement: <i>a written statement of compliance in the proposal or in the remark's column is sufficient; DNR will check this during deployment.</i>			

3.7 Implementation and Acceptance

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
3.7.1	Survey and approved design The Supplier shall survey DNR infrastructure and source data and shall deliver for DNR approval,	Mandatory		

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
	before deployment, the solution architecture, resource and licence schedule, interface specifications, security design, data-migration plan, test plan and implementation schedule. Every dependency on DNR or third parties shall be identified with the date by which it is required.			
3.7.2	Migration and reconciliation The Supplier shall import the agreed records with their source identifiers and quality checks, and shall report source and destination counts, rejected records and potential duplicates. Original records and a rollback path shall be preserved. Identity records shall not be merged automatically during migration; every proposed merge shall be submitted for DNR reconciliation approval.	Mandatory		
3.7.3	Installation and configuration The Supplier shall install all supplied software and configure the database, matching engines, APIs, access roles, workflows, backups and the time-stamping function in the production, recovery and test environments specified in Section 2. Licences shall be registered in DNR's name.	Mandatory		
3.7.4	Provisional Acceptance During deployment DNR will check that the Platform operates as stated in the proposal, including fingerprint and facial matching, duplicate review, quality exceptions, interchange formats, Relying-Party access controls, timestamp integrity, backup and restoration, failover, security retest and performance against the Tender Particulars, and will raise any concern with the Supplier in writing. Provisional Acceptance is granted by DNR's written confirmation once the concerns raised have been resolved and no critical or high defect remains open. Written statement: <i>a written statement of compliance in the proposal or in the remark's column is sufficient; DNR will check this during deployment.</i>	Mandatory		
3.7.5	Final Acceptance Final Acceptance shall be granted after the Platform has operated in production for the	Mandatory		

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
	stabilisation period in Section 2 with the availability target met and no unresolved critical or high defects, and after all documentation and handover deliverables have been accepted. Warranty and support commence on Final Acceptance.			
3.7.6	Training and handovers The Supplier shall provide on-the-job training for DNR operators, adjudicators, administrators and security staff, and shall deliver user and administrator manuals, as-built diagrams, API documentation, configuration backups, recovery runbooks and licence records. Credentials, source code and build instructions shall be handed over securely in accordance with requirement 3.7.11.	Mandatory		
3.7.7	Overseas training The Supplier shall provide overseas training for two (2) DNR staff nominated by DNR, covering (a) the administration, tuning and operation of the AI-assisted web application firewall and API protection under requirement 3.6.9, and (b) the administration and use of the proposed Platform, including the matching engines, enrolment and adjudication workflows, Relying-Party management and the time-stamping function. The training shall be included in the mandatory price.	Mandatory		
3.7.8	Warranty and local support The Supplier shall provide one (1) year of warranty and local technical support from Final Acceptance, available for eight hours per day on Government working days (Sunday to Thursday), Maldives time, with an emergency contact outside those hours for critical incidents. Support shall cover defects, security patches, supported software updates and integration troubleshooting. The Bidder shall name the local support team, propose severity-based response and restoration targets and escalation arrangements, and price renewal separately for each subsequent year of the planning horizon.	Mandatory		
3.7.9	Project management and reporting	Mandatory		

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
	The Supplier shall appoint a named project manager, shall maintain a risk and issue register, and shall provide written progress reports at intervals agreed with DNR. The agreed milestone programme shall form part of the contract.			
3.7.10	Perpetual licensing All software comprising the Platform, including matching engines, recognition models, database and API components, operator interfaces, administration tools, capture SDKs and all third-party dependencies, shall be licensed to DNR under a perpetual, irrevocable licence in DNR's name, paid once and included in the mandatory price. The licence shall permit use by DNR and by the Relying Parties DNR approves, in all environments in Section 2, up to the licensed capacity in Section 2 item 2.2, and shall not depend on any recurring fee, licence server, activation service or internet connection. No licence key shall expire. Support and maintenance may be renewed annually at the prices in Annex B, and lapse of support shall not affect the licence or the operation of the Platform. Term licences, subscriptions and usage-metered licences are not acceptable for any mandatory component, with the single exception of the application and API protection under requirement 3.6.9, which may be licensed for a term of not less than three (3) years as stated there.	Mandatory		
3.7.11	Source code delivery and escrow The Supplier shall deliver to DNR, at Provisional Acceptance and after every subsequent release, the complete Source Code of all software developed or adapted for the Platform, including the application layer, workflows, integration adapters, Relying-Party service layer, time-stamping function, operator interfaces, database schemas, build scripts and deployment configuration, with the documentation needed to build and deploy it independently. DNR shall own this Source Code and may use, modify and have it modified by third parties. For any pre-existing third-party component whose Source Code the	Mandatory		

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
	Bidder cannot deliver, such as a commercial matching engine, the Bidder shall identify the component in its proposal, shall deliver the Source Code to an independent escrow agent approved by DNR, kept current with each release and verified annually, with release to DNR on insolvency of the Supplier or licensor, discontinuation of the product or withdrawal of support, and shall confirm that DNR may then use and modify the released code to maintain the Platform. A proposal that neither delivers nor escrows the Source Code of a component is non-compliant with this requirement.			

3.8 Facial Recognition Models and Compute Efficiency

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
3.8.1	Model disclosure and licensing The Bidder shall identify every facial-recognition model offered, its developer, version, exact release and checksum, template characteristics, pre-processing pipeline and inference runtime, and shall provide perpetual licence terms permitting production use by the Government of Maldives, including all dependencies, consistent with requirement 3.7.10. Model training or fine-tuning on DNR data is outside the baseline scope and prohibited without DNR authorisation.	Mandatory		
3.8.2	Initial template generation The Supplier shall generate facial and fingerprint templates from the agreed existing records and bind each to its DNR record, source image and model version. The GPU capacity supplied under requirement 3.3.2 may be used for this initial batch, or temporary additional capacity may be proposed. The Bidder shall state the resources, throughput, elapsed time, quality checks and	Mandatory		

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
	reconciliation procedures, and shall include all commissioning costs. Temporary resources and all data shall remain under DNR control within the Maldives.			
3.8.3	Search architecture and resource efficiency The Bidder shall propose the search architecture for routine facial and fingerprint 1:N operation and shall justify it with measured accuracy, performance and evaluated cost under Section 8. The Bidder shall state how the GPU supplied under requirement 3.3.2 is used for template generation, search and any optional modules, how the Platform behaves if the GPU node fails, and how the design avoids idle accelerator capacity while keeping core functions available on the non-GPU node. The Bidder shall explain index construction, insertion, deletion, persistence, backup and rebuilding, and shall disclose index parameters, resources, build time, retrieval recall and peak-load latency.	Mandatory		
3.8.4	Ongoing Template Generation For each new enrolment or verification image the Platform shall generate a template compatible with the enrolled gallery using the approved model and pre-processing. The Bidder shall state inference latency and throughput separately from search and shall distinguish initial-batch resources from steady-state production and test resources, all within the hardware supplied under requirement 3.3.2.	Mandatory		
3.8.5	Model lifecycle and compatibility Models, pre-processing, templates and indexes shall be versioned, and the Platform shall prevent comparison across incompatible template spaces. For any model update the Supplier shall assess accuracy, resource demand and whether existing images must be re-processed and re-indexed, and shall provide validation, parallel-version cut-over and rollback procedures for DNR approval. These activities shall be performed or directly supervised by the certified AI or machine-learning engineers nominated under Section 4.2. Update costs and	Mandatory		

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
	dependencies shall be disclosed; original images and model provenance shall be preserved under the approved retention policy.			
3.8.6	Architecture and resource schedule The Bidder shall complete the schedule in Section 8 with diagrams showing capture, template generation, indexing, search, decision, audit and timestamping, quantifying temporary and permanent resources, concurrency, throughput, latency, growth and recovery, identifying Supplier-provided and DNR-provided infrastructure, and reconciling licence and operating costs without double counting.	Mandatory		

3.9 Facial Enrolment and Template Storage

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
3.9.1	Detection and alignment For authorised image-recognition workflows the Platform shall detect every face in an image, return a bounding box and result for each, and apply consistent landmark-based or equivalent alignment before template generation. Detector, alignment and recognition model versions shall be documented and recorded with each template.	Mandatory		
3.9.2	Quality gates and unresolved outcomes Before recognition the Platform shall assess face size, sharpness, pose, illumination and detection confidence against configurable thresholds informed by ISO/IEC 29794-5, and shall return a reason and recapture guidance for any rejection. Match thresholds and a best-versus-next-candidate separation margin shall be configurable. Where quality, similarity or separation is insufficient the Platform shall return an unresolved or ambiguous outcome and shall never force a	Mandatory		

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
	named identity. Thresholds shall be calibrated on representative DNR data with reported error rates. Written statement: <i>a written statement of compliance in the proposal or in the remark's column is sufficient; DNR will check this during deployment.</i>			
3.9.3	Multiple-image enrolment The Platform shall support enrolment from several images of the same person, including upload and capture of a short image sequence from an attached camera with a configurable number of frames and duration, reporting acceptance or rejection and the reason for each image, and consolidating accepted images into the enrolled representation. Approved enrolments shall become searchable without model retraining or service restart. Adding images to an existing DNR identity shall require explicit authorisation, and silent duplicate enrolment shall be prevented.	Mandatory		
3.9.4	Template representation and model separation The Bidder shall disclose the template dimensionality, normalisation, similarity metric and score range of each offered model. Where more than one model is offered, compatible templates shall be enrolled for each and their indexes isolated; incompatible templates shall never be compared. Landmark counts, template dimensionality and any feature count disclosed under 3.2.3 are distinct quantities and none is an acceptance criterion.	Mandatory		
3.9.5	Production template storage The Platform shall provide production-grade template indexing and persistent storage with authenticated concurrent access, backup, recovery and a documented scale-out path, supporting DNR identity references, model and version identifiers, image counts and DNR-approved metadata filters. Images and audit history shall be held in appropriately protected stores linked to the same record. The search interface shall be modular and shall support export and index reconstruction.	Mandatory		

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
3.9.6	Operator interface and decision evidence The Platform shall provide a browser-based interface, supported on current versions of mainstream browsers, for authorised enrolment and image recognition, showing face locations, matched DNR identity references or unresolved status, similarity scores and quality or rejection reasons. Score interpretation shall be explained, and similarity shall not be presented as a calibrated probability unless validated. The same functions shall be available through the documented APIs. The Bidder shall disclose the programming languages, frameworks, inference runtimes and dependencies used; no particular product is mandated.	Mandatory		

3.10 Optional Module: Live Video Recognition

This module is not part of the mandatory scope. DNR will activate it, if at all, only for a specific purpose defined in law or Government instrument and only after a data protection impact assessment and written DNR approval. Bidders may offer and price it separately; it is excluded from the mandatory compliance gate and from the rated evaluation.

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
3.10.1	Governance precondition Any live-video capability shall be deployable only for a DNR-approved, purpose-defined workflow with a documented legal basis, defined locations, enrolled population, retention period and oversight arrangements. The capability shall be disabled by default and shall record every activation, its approver and its purpose.	Optional		
3.10.2	Camera ingestion The module shall ingest live video from DNR-approved cameras over secure streaming interfaces. The Bidder shall state supported camera protocols, browsers and interfaces, and	Optional		

Ref	Requirement	Status	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
	shall identify hardware and interface work separately.			
3.10.3	Tracking and temporal confirmation The module shall track multiple faces with distinct track identifiers, detect identity inconsistency when tracks cross or change subject, and aggregate a configurable number of high-quality observations before confirming an identity. Unresolved, tentative and confirmed states shall be distinguished in text as well as colour, and confirmed labels shall change only after a configurable number of consecutive qualifying decisions.	Optional		
3.10.4	Performance and bounded processing The Bidder shall benchmark the number of concurrent streams and frame rates stated by DNR on the proposed server, reporting resolution, codec, faces per frame, gallery size, model, sampling rate, processing time per frame, time to confirmation, dropped frames, stream lag and memory use. The module shall use bounded buffering with an explicit frame-drop policy under overload and shall demonstrate no sustained queue or memory growth at the committed workload. Written statement: <i>a written statement of compliance in the proposal or in the remark's column is sufficient; DNR will check this during deployment.</i>	Optional		
3.10.5	Acceptance and pricing The Bidder shall demonstrate known and unenrolled persons, unresolved outcomes, poor-quality faces, crossings, occlusion, label changes and overload on a DNR-approved test set, providing per-scenario results and limitations, and shall price camera integration, licences, compute, storage, training and support separately. Written statement: <i>a written statement of compliance in the proposal or in the remark's column is sufficient; DNR will check this during deployment.</i>	Optional		

Section 4 — Pre-qualification

This procurement is open to enterprises registered in the Republic of Maldives as small or medium-sized enterprises under the Small and Medium Enterprises Act (Law No. 6/2013). Foreign manufacturers and technology providers may participate only as suppliers of products to such an enterprise and may not bid directly, as a joint-venture member or as a subcontractor; subcontracting of services is not permitted (Section 7).

The Bidder shall complete the response column against every item in Sections 4.1 to 4.3, stating Comply, Partially or Not Comply, and shall use the remarks column to give the exact location of the supporting evidence in its proposal (document name, section and page). Eligibility and the documents in Section 4.3 are assessed Pass / Fail at Stage 1 of the evaluation (Section 6.1); the experience in Section 4.1 and the team in Section 4.2 are rated and scored under Sections 6.4 and 6.5. A response of Comply without locatable evidence is treated as Not Comply. DNR may verify any reference, personnel commitment or document and may reject a proposal whose evidence cannot be verified.

A reference is "verifiable" when it names the client organization, describes the scope, states the completion or commissioning date, and gives the name, designation, telephone number and email address of a client officer authorised to confirm it. DNR may contact the client, request a reference call or make a site visit.

4.1 Experience of the Bidder

The Bidder shall demonstrate the following experience as a firm. Each reference shall be supported by a contract, purchase order, completion certificate or client reference letter, and shall be listed in the reference schedule in the format of Annex C. A single project may be used to satisfy more than one item where it meets the stated criteria for each.

Ref	Category	Requirement	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
4.1.1	Sovereign AI deployments	At least two (2) sovereign AI deployments delivered to a government organisation or to a small or medium-sized enterprise. A sovereign AI deployment is an artificial-intelligence or machine-learning system operating entirely on infrastructure under the client's own control and within the client's national jurisdiction, where model inference and all data processing are performed on that infrastructure and no data, model, derived feature, template or result is transferred to any third-party-hosted or foreign-hosted service. For each: client, nature and scale of the AI or machine-learning workload, deployment architecture and compute platform, commissioning date and whether the system remains in production. Deployments on public cloud or delivered as software-as-a-service are		

Ref	Category	Requirement	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
		not accepted. References in a government identity, civil registration, border control, law enforcement or regulated financial-services context attract a higher rating under Section 6.4.		
4.1.2	Hyper-converged infrastructure	At least one (1) design, supply and deployment of hyper-converged infrastructure hosting a production workload, completed within the past five (5) years, evidenced by a client reference letter. The letter shall state the client, the HCI platform, the number of nodes, the workload hosted and the commissioning date.		
4.1.3	Web application firewall deployments	At least two (2) deployments of a web application firewall or API protection solution protecting a production application or API, completed within the past five (5) years, evidenced by client reference letters. Each letter shall state the client, the product deployed, the applications or APIs protected, whether the Bidder also operates or tunes the solution, and the commissioning date.		
4.1.4	Vulnerability assessment and penetration testing	At least two (2) vulnerability assessment and penetration testing engagements performed by the Bidder's own staff, completed within the past five (5) years, on transactional systems of government agencies of a nature similar to DNR (for example civil registration, identity, revenue, social protection, financial regulation or border agencies). For each: client, system tested, scope and methodology (application, API and infrastructure), and completion date. These references demonstrate capability to deploy and secure the Platform; they do not replace the independent penetration test required by requirement 3.6.6, which shall be performed by a tester not employed by the Supplier.		
4.1.5	HSM security experience	At least one (1) completed project in which the Bidder delivered or integrated a security-related application that uses a hardware security module or public key infrastructure in production, for example digital signing,		

Ref	Category	Requirement	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
		certificate issuance or validation, time-stamping, key management, document or transaction integrity, or authentication based on HSM-protected keys. The reference shall state the client, the application, the HSM or PKI products involved, the Bidder's role, the commissioning date and a client contact authorised to confirm it.		
4.1.6	Product authorisation	For every third-party product proposed (matching engines, models, HCI platform, database, application and API protection and any other component), a written confirmation from the manufacturer or its authorised distributor of the Bidder's right to supply, license and support the product to DNR for the full planning horizon in Section 2.		

4.2 Delivery capability and team

The Bidder shall nominate the team below by name. Subcontracting is not permitted (Section 7): every person nominated shall be an employee of the Bidder, and contractors, freelancers and staff of partner companies shall not be nominated. Personnel of the manufacturer of a third-party product may support the Bidder for that product only and shall be identified as such. One person may fill more than one role only where this is stated as permitted. For each person the Bidder shall submit a CV in the format of Annex D and the certification evidence required. Replacement of any nominated person requires DNR's prior written approval and a replacement of at least equivalent qualifications and experience.

Ref	Role	Requirement	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
4.2.1	Project manager	One (1) project manager with at least five (5) years' experience managing ICT implementation projects, including at least one government project of comparable scale. Responsible for the delivery programme, reporting and risk management under requirement 3.7.9.		
4.2.2	Solution architect	One (1) solution architect with at least five (5) years' experience designing and delivering		

Ref	Role	Requirement	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
		enterprise software stacks (application, database, integration and infrastructure layers), responsible for the overall architecture, the Section 8 response and the integration design.		
4.2.3	Certified AI / machine-learning engineers	At least two (2) engineers each holding a current, valid professional-level certification in artificial-intelligence or machine-learning engineering, namely NVIDIA-Certified Professional (AI) or equivalent. Where an alternative certification is proposed as equivalent, the Bidder shall state the certifying body, the examination requirements and the currency period; DNR's determination of equivalence is final. Introductory or foundational-level certifications are not sufficient where a professional level exists within the same track. Both are jointly responsible for model deployment, threshold calibration, benchmarking, deployment checks and model updates under Section 3.8; at least one shall be available for support escalation at any time during implementation; both shall remain available to DNR for the duration of implementation and the warranty year.		
4.2.4	Security engineers	At least two (2) security engineers, each holding a current, valid offensive-security certification (eCPPT, OSCP, OSCE, CRT0, GWAPT, CREST CRT or equivalent) and each with at least two (2) years' professional experience in deploying and operating web application firewall and API protection solutions in production and in red-team or adversarial testing of web applications and APIs. Responsible for the design, tuning and operation of the protection required by requirement 3.6.9, for the Supplier's own security testing before the independent test under requirement 3.6.6, and for remediation. CVs shall list the certifications with certificate numbers, the WAF products deployed and the red-team engagements performed, with client references where permitted.		

Ref	Role	Requirement	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
4.2.5	Agentic-AI security engineer	At least one (1) engineer holding a current certification in artificial-intelligence or agentic-AI security, covering threats to machine-learning systems, large-language-model applications and autonomous or agentic workflows and aligned with the OWASP Top 10 for LLM Applications and the OWASP agentic-AI threat guidance, or equivalent; DNR's determination of equivalence is final. Responsible for reviewing and validating, before deployment and after every change, every automated or agent-driven workflow in the Platform, including the machine-learning mitigation logic of requirement 3.6.9, any automated adjudication assistance, model-update automation under requirement 3.8.5 and any AI-assisted operator tooling, and for certifying in writing at acceptance that each such workflow has been threat-modelled, tested for prompt-injection, data-leakage, privilege-escalation and unsafe-action risks, and constrained to approved actions with human approval where DNR policy requires it.		
4.2.6	Full-stack engineers	At least two (2) full-stack software engineers, each with at least two (2) years' professional experience developing and maintaining enterprise systems or platforms (front-end, back-end services, APIs and databases), responsible for the development, configuration and maintenance of the Platform application layer, operator interfaces, workflows, Relying-Party service layer and integration adapters, and for the Source Code deliverables under requirement 3.7.11. CVs shall list the systems developed, the technologies used and the Bidder's role.		
4.2.7	Infrastructure, integration and support staff	Named engineers for the deployment of the hyper-converged infrastructure under requirement 3.3.2, for DNR system integration and the Relying-Party service layer (Section 3.4), for the time-stamping function and DNR HSM integration (Section 3.5), for database deployment, and for the local technical support		

Ref	Role	Requirement	Bidder response (Comply / Partially / Not Comply)	Remarks and evidence location
		team under requirement 3.7.8, with the support team based in the Maldives.		
4.2.8	Minimum experience	Every engineer nominated under 4.2.2 to 4.2.7 shall have at least two (2) years of professional experience in the discipline for which he or she is nominated, evidenced in the CV, in addition to any certification required.		
4.2.9	Employment status	Every person nominated under 4.2.1 to 4.2.7 is an employee of the Bidder and is not a subcontractor, contractor or employee of another company, as confirmed in the Bidder declaration (Annex A).		

4.3 Mandatory documents

The Bidder shall submit every document below and shall indicate in the response column where each is located in the proposal. Omission of any document may result in disqualification.

Ref	Document	Submitted (Yes / No)	Location in proposal
4.3.1	Company registration certificate issued in the Republic of Maldives.		
4.3.2	SME registration certificate issued under the Small and Medium Enterprises Act (Law No. 6/2013) by the Ministry responsible for economic development, valid at the submission deadline. A proposal from an enterprise that is not so registered is non-responsive.		
4.3.3	GST registration certificate.		
4.3.4	MIRA tax clearance report not older than three (3) months from the submission deadline.		
4.3.5	Reference schedule (Annex C) covering every reference required by Section 4.1, with the client reference letters, contracts or completion certificates.		
4.3.6	Manufacturer or authorised-distributor confirmations required by 4.1.6.		
4.3.7	Team schedule naming every person required by Section 4.2, with CVs (Annex D) and certification evidence.		

Ref	Document	Submitted (Yes / No)	Location in proposal
4.3.8	Technical proposal, including the solution and hardware architecture, the facial detection and anti-spoofing technology statement (requirement 3.2.5), the capture-device compatibility schedule (requirement 3.2.9) and the implementation plan.		
4.3.9	Completed response columns in Section 3 and Section 4, and the Architecture and Resource Response (Section 8).		
4.3.10	Product specifications, independent evaluation results (requirement 3.3.7), PAD test results as described in requirement 3.2.5, benchmark reports and licence terms.		
4.3.11	Itemised financial proposal in the form of Annex B, separately sealed or separately identified.		
4.3.12	Bid security in the form and amount stated in Section 2.		
4.3.13	Deviations and assumptions schedule required by Section 5.7, or a statement that there are none.		
4.3.14	Signed Bidder declaration (Annex A).		

4.4 Delivery programme

The Bidder shall propose a milestone-based programme from contract signature, aligned with the eight-week delivery deadline and the completion deadline in Section 2, showing hardware and software delivery within eight weeks, installation and commissioning, design approval, deployment, migration, integration, testing, training, Provisional Acceptance and Final Acceptance, and identifying DNR infrastructure, the DNR HSM, data access and third-party interfaces as explicit dependencies. The agreed programme shall form part of the contract.

Section 5 — Instructions to Bidders

5.1 Complete proposal

Bidders shall submit one proposal covering the complete mandatory scope, comprising a technical proposal, the completed Section 3 and Section 4 response columns, the Section 8 response, and a separately sealed or separately identified financial proposal. The proposal shall identify the Bidder's legal entity, authorised signatory and contact details, and shall disclose every manufacturer or technology provider whose products are proposed. Joint ventures and subcontracting are not permitted; the Bidder, a registered SME, remains solely accountable for delivery and shall perform the project roles with its own employees as required by Section 4.2.

5.2 Language and format

Proposals and all supporting documents shall be in English. Documents in another language shall be accompanied by a certified English translation. Electronic submissions shall be in PDF, with the Section 3, Section 4 and Section 8 responses also provided in editable form.

5.3 Clarifications and amendments

Requests for clarification shall be sent in writing to the procurement contact by the clarification deadline. DNR shall communicate material clarifications and amendments in writing to all registered Bidders, without identifying the source. Bidders shall acknowledge all addenda in their submission. Only written amendments issued by DNR change the requirements of this RFP.

5.4 Pricing, currency and taxes

Prices shall be quoted in Maldivian Rufiyaa (MVR). Applicable taxes and duties shall be shown separately. Prices shall include all hardware under requirement 3.3.2 with its warranty, and every licence, component, integration, migration, test, training activity and support obligation needed for the mandatory scope, and shall state licence metrics, quantities, capacity limits and environment coverage. All software licences shall be perpetual and included in the year-1 price; the only recurring charges permitted are support and maintenance renewals for years two to five, which shall be quoted separately in Annex B. A proposal that prices any Platform component other than the application and API protection (requirement 3.6.9) on a subscription or term-licence basis is non-compliant. Optional capabilities and future expansion shall be priced separately. No cost shall be counted twice.

5.5 Proposal validity and bid security

Proposals shall remain valid for the period stated in Section 2. Where Section 2 requires bid security, it shall be submitted in the stated form and amount and shall remain valid for twenty-eight (28) days beyond the proposal validity period. Bid security shall be returned to unsuccessful Bidders following award.

5.6 Confidentiality and integrity

Bidders shall treat DNR records and information as confidential and shall use them only for preparing a proposal or delivering the contract. Bidders shall declare any conflict of interest. All evidence shall be accurate and verifiable; DNR may reject a submission containing false or misleading information and may refer it under the governing framework. Bidders shall identify the personnel and arrangements for protecting DNR information during delivery and support.

5.7 Deviations and assumptions

Bidders shall state every assumption, limitation and deviation from this RFP explicitly in a single schedule. A deviation not stated in that schedule shall not be recognised. A deviation from a mandatory requirement results in failure of the technical gate.

5.8 Submission and clarification of proposals

Proposals shall be submitted by the deadline and method stated in Section 2. Late submissions shall be handled under the governing framework. DNR may request written clarification of submitted evidence; a clarification shall not add omitted mandatory scope, change the price or materially change the offer.

5.9 Rights of DNR

DNR reserves the right to accept or reject any proposal, to cancel the procurement at any stage, and to reject all proposals, without incurring liability to Bidders. DNR is not bound to accept the lowest-priced proposal. Costs of preparing a proposal are borne by the Bidder.

5.10 Award and contract

The contract shall record the accepted scope, delivery programme, payment milestones, licence rights, service levels and acceptance criteria, on the terms summarised in Section 7. Acceptance follows the deployment checks and handovers stated in Section 3.7. No award or contract is created by the submission of a proposal or by any notification other than a signed contract.

Section 6 — Evaluation Method

6.1 Evaluation stages

Stage	Assessment
1. Eligibility and completeness	Pass / Fail. DNR confirms that the Bidder is a registered SME (Section 4), that every mandatory document in Section 4.3 is submitted, that the proposal covers the complete mandatory scope with no deviation from a mandatory requirement, that the product authorisations in 4.1.6 are provided, that every nominated person meets the minimum-experience and employment rules in 4.2.8 and 4.2.9, and that bid security and proposal validity comply with Section 2. A proposal failing any of these is not evaluated further.
2. Scored evaluation	Proposals passing Stage 1 are scored out of 100 under Sections 6.2 to 6.6: technical requirements 40, experience of the Bidder 15, delivery capability and team 15, and price 30. The technical, experience and team scores are assessed by the DNR evaluation panel from the written proposal only; the price score is calculated from Annex B.
3. Ranking and award	Proposals are ranked by total score. The highest-scoring proposal that meets the minimum technical score in Section 6.3 is recommended for award.

6.2 Scoring summary

Component	Marks	Basis
Technical requirements (Section 3)	40	Weighted score of the Section 3 response columns, as set out in 6.3
Experience of the Bidder (Section 4.1)	15	Rated assessment of the references, as set out in 6.4
Delivery capability and team (Section 4.2)	15	Rated assessment of the nominated team, as set out in 6.5
Price (Annex B)	30	Lowest evaluated price basis, as set out in 6.6
Total	100	

6.3 Technical requirements (40 marks)

Each requirement in Section 3 marked Mandatory is scored from the Bidder's response and the evidence it references. Optional requirements (3.2.10 and Section 3.10) are not scored. A requirement scores: 1.0 where the response is Comply and the referenced evidence supports it; 0.5 where the response is Partially, or is Comply but the evidence only partly supports it; and 0 where the response is Not Comply, is absent, or is Comply with no locatable or relevant evidence. For requirements marked "Written statement", a clear and specific statement of compliance describing how the requirement will be met with scores 1.0; a generic or qualified statement scores 0.5.

The requirement scores within each group of Section 3 are averaged, the group average is multiplied by the group weight below, and the weighted group results are summed to give a technical score out of 100, which is then scaled to 40 marks.

Minimum technical score: a proposal scoring fewer than twenty-eight (28) of the 40 technical marks (70%) is not considered for award, whatever its other scores.

Group	Section 3 requirement group	Weight (%)
3.1	Identity resolution and workflows	10
3.2	Fingerprint and facial processing, anti-spoofing and capture integrity	15
3.3	Deployment, performance, accuracy and hardware	12
3.4	Integration and Relying-Party services	10
3.5	Trusted time-stamping and DNR HSM integration	8
3.6	Security, data protection and application and API attack protection	15
3.7	Implementation, licensing and source code	10
3.8	Facial recognition models and compute efficiency	8
3.9	Facial enrolment and template storage	12
	Total	100

6.4 Experience of the Bidder (15 marks)

Each item in Section 4.1 below is rated from 0 to 4 on the scale in 6.7, using only the references in Annex C and their supporting documents. The rating is divided by 4, multiplied by the item weight, and the weighted results are summed to give an experience score out of 100, scaled to 15 marks. Item 4.1.6 (product authorisation) is a Stage 1 pass/fail item and is not rated.

Item	Section 4.1 item	Weight (%)
4.1.1	Sovereign AI deployments	30
4.1.2	Hyper-converged infrastructure	15
4.1.3	Web application firewall deployments	20
4.1.4	Vulnerability assessment and penetration testing	25
4.1.5	HSM security experience	10
	Total	100

6.5 Delivery capability and team (15 marks)

Each role in Section 4.2 below is rated from 0 to 4 on the scale in 6.7, using the team schedule and CVs in Annex D and the certification evidence. Where a role requires more than one person, the rating reflects the weakest person nominated for it. The rating is divided by 4, multiplied by the role weight, and the

weighted results are summed to give a team score out of 100, scaled to 15 marks. Items 4.2.8 and 4.2.9 (minimum experience and employment status) are Stage 1 pass/fail items and are not rated.

Item	Section 4.2 role	Weight (%)
4.2.1	Project manager	15
4.2.2	Solution architect	15
4.2.3	Certified AI / machine-learning engineers	25
4.2.4	Security engineers	20
4.2.5	Agentic-AI security engineer	10
4.2.6	Full-stack engineers	10
4.2.7	Infrastructure, integration and support staff	5
	Total	100

6.6 Price (30 marks)

The evaluated price is the Total Evaluated Price in Annex B (line 11): the tax-inclusive mandatory price, including the hardware, all perpetual licences and the three-year application and API protection licence, plus the annual maintenance contract for years two to five, plus the energy cost of the supplied hardware over five years at the Bidder's declared power draw and the rate in Section 2 item 2.5. Separately priced options in Annex B part B.2 are excluded.

Price score = $30 \times (\text{lowest evaluated price among the proposals passing Stage 1} \div \text{the Bidder's evaluated price})$. The lowest-priced proposal therefore scores 30 and every other proposal scores proportionately less.

Arithmetic errors in Annex B are corrected by DNR, unit prices prevailing over totals; the corrected price is the evaluated price. A Bidder that does not accept the correction is disqualified.

6.7 Rating scale for experience and team

Rating	Meaning
0	Not met: the reference, person or evidence is missing, unverifiable or does not satisfy the requirement.
1	Weak: the requirement is met only marginally, or evidence is incomplete.
2	Adequate: the requirement is met as stated, with complete evidence.
3	Good: the requirement is exceeded in number, scale or relevance, with complete evidence.
4	Strong: the requirement is substantially exceeded and the experience or person is directly relevant to a national identity verification platform.

6.8 Ranking, panel and ties

Total score = technical (40) + experience (15) + team (15) + price (30). Scores are calculated to two decimal places. Ties are resolved in favour of the higher technical score, then the higher combined experience and team score, then the lower evaluated price.

Each panel member scores the technical, experience and team components independently; the component score is the average of the panel members' scores. Reasons and evidence references are recorded for every rating. The weights, scales and minimum score in this section are published with the RFP and shall not change after the submission deadline.

Optional capabilities (3.2.10 and Section 3.10) are not scored and are not included in the evaluated price. The Bidder shall state whether each is offered and reference its separate price in Annex B part B.2.

Section 7 — Principal Contract Terms

The contract will be based on the contract form issued by DNR with the notification of award, prepared in accordance with the Public Finance Regulation, and will incorporate the terms summarized below. Bidders shall confirm acceptance of these terms or state any deviation in the deviations schedule.

Term	Summary
Payment terms	100% of the contract price (the Total Mandatory Price in Annex B line 9) is payable on delivery, which is due within eight (8) weeks of contract signature. Delivery means that the Supplier has physically delivered to the DNR site the complete hardware and software stack, comprising the two HCI nodes with the GPU and associated storage and networking, and the software media, licence keys and licence certificates in DNR's name for the facial and fingerprint verification software, the application and API protection (AI WAF) with its three-year licence, and the database, API and operator software, and DNR has signed a delivery certificate confirming receipt. Installation, configuration, integration, migration and the other implementation services follow delivery and are not conditions of payment. Payment is made within thirty (30) days of the delivery certificate against a tax invoice. No advance payment is made. The one-year warranty and support period starts on Final Acceptance and is included in the contract price; the annual maintenance contract for years two to five is invoiced annually in advance.
Performance security	A performance security of ten per cent (10%) of the contract price, in the form of an unconditional bank guarantee from a bank licensed in the Maldives, submitted before the delivery payment is released and valid until thirty (30) days after Final Acceptance. DNR may call the security in whole or in part if the Supplier fails to complete installation, migration, integration, acceptance or handover, or fails to meet warranty obligations.
Liquidated damages	For delay attributable to the Supplier in meeting the eight-week delivery deadline or the Provisional Acceptance deadline in Section 2 item 2.13: 0.1% of the contract price per week of delay, capped at 10% of the contract price. For failure to meet the availability target during support: service credits as agreed in the contract.
Licences and intellectual property	All Platform software is licensed to DNR under a perpetual, irrevocable licence with no recurring fee (requirement 3.7.10), except the application and API protection, which is licensed for a term of not less than three (3) years from delivery with renewal at the prices quoted in Annex B. All software, configuration, data mappings, documentation and other deliverables created for DNR under the contract, and all data and templates within the Platform, vest in DNR on payment. Pre-existing Supplier or third-party software remains the property of its owner, subject to the perpetual licence and to the source-code delivery and escrow obligations in requirement 3.7.11, which survive termination or expiry of the contract and the insolvency of the Supplier.
Data protection and sovereignty	All DNR data remains within the Maldives under DNR control. The Supplier acts on DNR's instructions only, shall comply with the applicable data protection legislation, and shall return or securely destroy DNR data on termination or expiry, with certification.

Term	Summary
Confidentiality	Perpetual confidentiality obligations in respect of DNR data, the Platform's security design and Relying-Party arrangements.
No subcontracting	Subcontracting of any part of the contract is not permitted. All services under the contract, including design, installation, integration, migration, testing, training, warranty and support, shall be performed by the Supplier's own employees named in the proposal. Purchasing third-party hardware and software products from their manufacturers or authorised distributors, and receiving the manufacturer's standard product support for them, does not constitute subcontracting. Replacement of any named person requires DNR's prior written approval.
Warranty and support	As in requirement 3.7.8, followed by the annual maintenance contract for years two to five at the price quoted in Annex B line 10.
Termination and exit	Termination for material breach, insolvency or prolonged force majeure. On expiry or termination the Supplier shall provide exit assistance, data export in the formats required by 3.6.4 and knowledge transfer for a period of six (6) months at the rates quoted.
Governing law and disputes	The contract is governed by the laws of the Republic of Maldives. Disputes shall first be referred to negotiation between senior representatives for thirty (30) days and, failing settlement, to arbitration seated in Malé under the Arbitration Act of the Maldives (Law No. 10/2013), conducted in English.

Section 8 — Architecture and Resource Response

Bidders shall complete one schedule for the offered architecture, attaching diagrams and benchmark reports that use the same stage references. State actual quantities, versions and costs, and identify every resource as Supplier-provided or DNR-provided. This section consolidates all benchmark and timing rules referred to in Section 3.

Stage	Required bidder information
R1 Initial template generation	Models and versions; CPU and accelerator make and quantity; cores, memory and accelerator memory; images per second; batch size; total elapsed time; temporary-resource location and cost.
R2 Index build	Index method and parameters; gallery templates and dimensionality; CPU, memory and storage; initial build and full rebuild time; update and deletion behaviour.
R3 Routine template generation	New enrolment and query template generation; CPU and accelerator allocation; p50, p95 and p99 latency; throughput and concurrency; justification for any permanent accelerator dependency.
R4 Routine search	CPU and accelerator allocation; memory and index size; top-k; p50, p95 and p99 latency and throughput at fixed retrieval recall and biometric thresholds; failures and queueing.
R5 Growth and recovery	Resources by environment; capacity and justified headroom at years one, three and five; failover and restoration; index rebuild, model replacement, re-processing and rollback.
R6 Resource costs	Temporary processing, hardware, infrastructure consumption, licences, energy and support for each year of the evaluation horizon; references to included prices; DNR-provided resources; reconciliation to the evaluated cost.

8.1 Benchmark protocol

Benchmarks shall use the DNR-published number of templates, image mix, top-k, concurrency, query rate and test duration, and shall report warm and cold conditions separately. Query templates shall use the same model, weights and pre-processing as the gallery. Compression, quantisation, filtering, caching and index parameters shall be disclosed; cached query results shall not be substituted for actual search. Approximate retrieval shall be compared with exhaustive search on the same gallery and query set, and biometric error rates shall be reported separately from retrieval recall.

8.2 Timing boundaries

Bidders shall report separately: image-to-template generation; template-to-ranked-candidates retrieval; final biometric decision; complete API response; and timestamped transaction duration. End-to-end measurements shall include production authentication, audit logging and queueing. Any indicative candidate-retrieval target published in Section 2 relates only to indexed facial candidate retrieval from a prepared template.

8.3 Evaluation evidence

Bidders shall provide measured results obtained on the offered resource configuration or, where it is not available to the Bidder before award, on a comparable configuration with the differences and the expected scaling stated, with enough detail (data set description, configuration, commands or scripts, raw outputs) for DNR to reproduce them during deployment. DNR evaluates the written evidence and resource efficiency when scoring Sections 3.3 and 3.8 under Section 6.3; naming hardware attracts no marks in itself, and the architecture is assessed on how well the supplied hardware is used to meet the published workload with justified headroom. Results that cannot be reproduced during deployment constitute a defect.

Annex A — Bidder Declaration

We, the undersigned, declare that:

- Our proposal covers the complete mandatory scope of this RFP, and every assumption, limitation and deviation is stated in the deviations schedule;
- The information and evidence supplied is accurate, complete and verifiable, and we authorize DNR to verify them with the sources named;
- all optional, recurring and third-party charges have been disclosed, and no mandatory cost has been omitted from the evaluated price;
- we have no conflict of interest in relation to this procurement, or have disclosed any such conflict in writing;
- every person named in our proposal for a project role is our employee and not a subcontractor, contractor or employee of another company, and no part of the contract will be subcontracted;
- we accept the principal contract terms in Section 7, subject only to deviations stated in the deviations schedule; and
- Our proposal remains valid for the period stated in Section 2.

Bidder legal name	
Registered address	
Authorised signatory and designation	
Addenda acknowledged (numbers and dates)	
Signature and date	

Annex B — Financial Response

Bidder: _____ **RFP reference:** DNR/RFP/2026/_____

State an amount, or "Included in line [number]", for every line. Prices in MVR unless Section 5.4 permits otherwise. Lines 9 and 10 form the evaluated price under Section 6; line 11 shall reconcile with Section 8 stage R6 and with the licence schedule in the technical proposal.

B.1 Mandatory scope and evaluated price

Line	Component	Amount
1	Hardware: two hyper-converged infrastructure nodes with GPU, storage and networking under requirement 3.3.2, with three-year manufacturer warranty, installation and commissioning	
2	Perpetual Platform software licences (matching engines, models, database and API components) — one-time	
3	Application and API protection (AI WAF) — three-year licence from delivery, including updates and manufacturer support	
4	Implementation services: DNR system integration, workflows and Relying-Party service layer; time-stamping function and DNR HSM integration; migration, initial template generation and indexing; security hardening and penetration testing; training (including overseas training), documentation and handover	
5	Warranty and local technical support — year 1	
6	Other mandatory costs, itemised in an attached schedule	
7	Subtotal, mandatory scope, excluding tax	
8	Applicable taxes and duties	
9	TOTAL MANDATORY PRICE (tax inclusive)	
10	Annual maintenance contract (AMC) for years 2 to 5: software support and maintenance, hardware support extension, and AI WAF licence renewal for years 4 and 5 — total for the four years, with the annual amount shown in an attached schedule	
11	TOTAL EVALUATED PRICE (line 9 plus line 10)	

B.2 Optional and separately priced items

These items are excluded from the evaluated price. State scope, licence basis and recurring charges for each.

Line	Item	Amount
O1	Optional mixed-impression analysis (3.2.10)	
O2	Optional live video recognition module (3.10)	

Line	Item	Amount
O3	Per-agency live integration not included under Section 2 item 2.9 (unit price)	
O4	Perpetual capacity expansion beyond licensed limits (one-time unit prices per metric)	
O5	Additional HCI nodes beyond the two-node cluster (unit price per node to the specification in 3.3.2, with and without GPU)	

Authorised signatory: _____ **Date:** _____

Annex C — Reference Schedule

Complete one row for every reference submitted under Section 4.1. Attach the supporting contract, completion certificate or client letter behind each row, numbered to match. The client contact named must be authorised to confirm the reference and may be contacted by DNR without further notice to the Bidder.

No	Section 4.1 item(s) satisfied	Client organisation and country	Scope delivered: functions, scale, platform and the Bidder's role	Start and completion dates; in production (Y/N)	Client contact: name, designation, telephone, email	Evidence attached (document no.)
1						
2						
3						
4						
5						
6						

Add rows as required.

Annex D — Team Schedule and CV Format

Complete the team schedule for every role in Section 4.2, then attach a CV for each person in the format below. Each CV shall be signed by the person named and countersigned by the Bidder's authorised signatory.

D.1 Team schedule

Section 4.2 role	Full name	Designation in the Bidder's organisation	Years of experience in the role discipline	Certifications held (name, body, number, expiry)
4.2.1 Project manager				
4.2.2 Solution architect				
4.2.3 Certified AI / machine-learning engineers				
4.2.4 Security engineers				
4.2.5 Agentic-AI security engineer				
4.2.6 Full-stack engineers				
4.2.7 Infrastructure, integration and support staff				

Add a row for each additional person nominated under 4.2.3, 4.2.4, 4.2.6 and 4.2.7.

D.2 CV format

1. Full name, nationality and date of birth.
2. Proposed role under Section 4.2.
3. Current designation in the Bidder's organization.
4. Education and professional certifications, with certificate numbers and expiry dates; copies attached.
5. Employment history, most recent first, with employer, dates and position.
6. Relevant project experience, most recent first: client, project, role, dates, and the specific products, platforms or methods used that are relevant to the nominated role.
7. Declaration signed by the person: that the information is accurate, that he or she is an employee of the Bidder and not a subcontractor, and that he or she is available for the role for the duration stated in Section 4.2.