REQUEST FOR PROPOSALS

(*PROCUREMENT OF SERVICES)*
For Simple Assignments

SERVICES FOR

Development of biometric identity management system
for the State Migration Service of the Republic of Azerbaijan

Prepared by

IOM International Organization for Migration
OIM Organisation Internationale pour les Migrations
OIM Organización Internacional para las Migraciones

Baku, Azerbaijan
03 April 2017

REQUEST FOR PROPOSALS
RFP No.: *AZ-005-2017*

Mission: *Republic of Azerbaijan*

Project Name: *Consolidation of Migration and Border Management Capacities in Azerbaijan*
WBS: *TC.0663.AZ10.54.11.002*

Title of Services: *Development of biometric identity management system*

IOM International Organization for Migration
OIM Organisation Internationale pour les Migrations
OIM Organización Internacional para las Migraciones

Request for Proposals

The International Organization for Migration (hereinafter called **IOM**) intends to hire Service Provider for *Development of biometric identity management system for the State Migration Service of the Republic of Azerbaijan* for which this Request for Proposals (RFP) is issued.

IOM now invites Service Providers/ Consulting Firms to provide Technical and Financial Proposal for the following Services*: Establishment of an integrated database for the collection of biometric data; ~~Establishment of the system for printing biometric cards; Establishment of biometric identification system;~~ Improvement of the existing modules; Development of new modules; Improvement of software for the development of statistical data.* More details on the services are provided in the attached Terms of Reference (TOR).

The Service Provider /Consulting Firm will be selected under a Quality –Cost Based Selection procedures described in this RFP.

The RFP includes the following documents:

Section I. Instructions to Service Providers/ Consulting Firms
Section II. Technical Proposal – Standard Forms
Section III. Financial Proposal – Standard Forms
Section IV. Terms of Reference
Section V. Standard Form of Contract

The Proposals must be delivered through e-mail to bakutender@iom.int - on or *before 03 May 2017, 18:00, Baku time*. No late proposal shall be accepted.

IOM reserves the right to accept or reject any proposal and to annul the selection process and reject all Proposals at any time prior to contract award, without thereby incurring any liability to affected Service Providers/ Consulting Firms

Ilham Kazimov

Procurement / Logistics Coordinator
International Organization for Migration (IOM)

IOM is encouraging companies to use recycled materials or materials coming from sustainable resources or produced using a technology that has lower ecological footprints.

Table of Contents

Section I - Instructions to Service Providers/ Consulting Firms

1. Introduction

1.1 Only eligible Service Providers/ Consulting Firms may submit a Technical Proposal and Financial Proposal for the services required. The proposal shall be the basis for contract negotiations and ultimately for a signed contract with the selected Consultant Firm.

1.2 Service Providers/ Consulting Firms should familiarize themselves with local conditions and take them into account in preparing the proposal. Service Providers/ Consulting Firms are encouraged to visit IOM before submitting a proposal and to attend a pre-proposal conference if is specified in Item 4.3. of this Instruction.

1.3 The Service Providers/ Consulting Firms costs of preparing the proposal and of negotiating the contract, including visit/s to the IOM, are not reimbursable as a direct cost of the assignment.

1.4 Service Providers/ Consulting Firms shall not be hired for any assignment that would be in conflict with their prior or current obligations to other procuring entities, or that may place them in a position of not being able to carry out the assignment in the best interest of the IOM.

1.5 IOM is not bound to accept any proposal and reserves the right to annul the selection process at any time prior to contract award, without thereby incurring any liability to the Service Providers/ Consulting Firms.

1.6 IOM shall provide at no cost to the Service Provider/ Consulting Firm the necessary inputs and facilities, and assist the Firm in obtaining licenses and permits needed to carry out the services and make available relevant project data and report (see Section IV. terms of reference).

2. Corrupt, Fraudulent, and Coercive Practices

2.1 IOM Policy requires that all IOM Staff, bidders, manufacturers, suppliers or distributors, observe the highest standard of ethics during the procurement and execution of all contracts. IOM shall reject any proposal put forward by bidders, or where applicable, terminate their contract, if it is determined that they have engaged in corrupt, fraudulent, collusive or coercive practices. In pursuance of this policy, IOM defines for purposes of this paragraph the terms set forth below as follows:

- Corrupt practice means the offering, giving, receiving or soliciting, directly or indirectly, of any thing of value to influence the action of the Procuring/Contracting Entity in the procurement process or in contract execution;

- Fraudulent practice is any act or omission, including a misrepresentation, that knowingly or recklessly misleads, or attempts to mislead, the Procuring/Contracting Entity in the procurement process or the execution of a contract, to obtain a financial gain or other benefit to avoid an obligation;

- Collusive practice is an undisclosed arrangement between two or more bidders designed to artificially alter the results of the tender procedure to obtain a financial gain or other benefit;

- Coercive practice is impairing or harming, or threatening to impair or harm, directly or indirectly, any participant in the tender process to influence improperly its activities in a procurement process, or affect the execution of a contract

3. Conflict of Interest

3.1 All bidders found to have conflicting interests shall be disqualified to participate in the procurement at hand. A bidder may be considered to have conflicting interest under any of the circumstances set forth below:

- A Bidder has controlling shareholders in common with another Bidder;

- A Bidder receives or has received any direct or indirect subsidy from another Bidder;

- A Bidder has the same representative as that of another Bidder for purposes of this bid;

- A Bidder has a relationship, directly or through third parties, that puts them in a position to have access to information about or influence on the Bid of another or influence the decisions of the Mission/procuring Entity regarding this bidding process;

- A Bidder submits more than one bid in this bidding process;

- A Bidder who participated as a consultant in the preparation of the design or technical specifications of the Goods and related services that are subject of the bid.

4. Clarifications and Amendments to RFP Documents

4.1 At any time before the submission of the proposals, IOM may, for any reason, whether at its own initiative or in response to a clarification amend the RFP. Any amendment made will be made available to all short-listed Service Providers/ Consulting Firms who have acknowledged the RFP.

4.2. Service Providers/ Consulting Firms may request for clarification(s) on any part of the RFP. Only the request for clarifications must be sent in writing or by standard electronic means and submitted to IOM at the address nmurshudli@iom.int in CC: ikazimov@iom.int at least *7 (seven) calendar days* before the set deadline for the submission and receipt of Proposals. IOM will respond in writing or by standard electronic means to the said request and this will be made available to all those who acknowledged the RFP without identifying the source of the inquiry.

5. Preparation of the Proposal

5.1 A Service Provider/ Consulting Firm Proposal shall have two (2) components:

a) the Technical Proposal, and
b) the Financial Proposal.

5.2 The Proposal, and all related correspondence exchanged by the Service Providers/ Consulting Firms and IOM, shall be in *English*. All reports prepared by the contracted Service Provider/ Consulting Firm shall be in *English*.

5.3 The Service Providers/ Consulting Firms are expected to examine in detail the documents constituting this Request for Proposal (RFP). Material deficiencies in providing the information requested may result in rejection of a proposal.

6. Technical Proposal

6.1 When preparing the Technical Proposal, Service Providers/ Consulting Firms must give particular attention
to the following:

a) If a Service Provider/ Consulting Firm deems that it does not have all the expertise for the assignment, it may obtain a full range of expertise by associating with individual consultant(s) and/or other consultants or entities in a joint venture or sub-consultancy, as appropriate. Service Providers/ Consulting Firms may associate with the other consultants invited for this assignment or to enter into a joint venture with consultants not invited, only with the approval of IOM. In case of a joint venture, all partners shall be jointly and severally liable and shall indicate who will act as the leader of the joint venture.[1]

b) For assignment of the staff, the proposal shall be based on the number of professional staff-months estimated by the firm, no alternative professional staff shall be proposed.

c) It is desirable that the majority of the key professional staff proposed is permanent employees of the firm or have an extended and stable working relationship with it.

d) Proposed professional staff must, at a minimum, have the experience of at least *one year,* preferably working under conditions similar to those prevailing in the country of the assignment.

6.2 The Technical Proposal shall provide the following information using the attached Technical Proposal Standard Forms TPF 1 to TPF 6 (Section III).

a) A brief description of the Service Providers/ Consulting Firms organization and an outline of recent experience on assignments of a similar nature (TPF-2), if it

[1] *This clause shall be included/revised as deemed necessary*

is a joint venture, for each partner. For each assignment, the outline should indicate the profiles of the staff proposed, duration of the assignment, contract amount, and firm's involvement.

b) A description of the approach, methodology and work plan for performing the assignment (TPF-3). This should normally consist of maximum of ten (10) pages including charts, diagrams, and comments and suggestions, if any, on Terms of Reference and counterpart staff and facilities. The work plan should be consistent with the work schedule (TPF-7)

c) The list of proposed Professional Staff team by area of expertise, the position and tasks that would be assigned to each staff team members (TPF-4).

d) Latest CVs signed by the proposed professional staff and the authorized representative submitting the proposal (TPF-5) Key information should include number of years working for the firm and degree of responsibility held in various assignments during the last *one year.*

e) A time schedule estimates of the total staff input (Professional and Support Staff, staff time needed to carry out the assignment, supported by a bar chart diagram showing the time proposed for each Professional and Staff team members (TPF–6). The schedule shall also indicate when experts are working in the project office and when they are working at locations away from the project office.

f) A time schedule (bar chart) showing the time proposed to undertake that the activities indicated in the work plan (TPF-7).

g) A detailed description of the proposed methodology and staffing for training if the RFP specifies training as specific component of the assignment.

6.3 The technical proposal shall not include any financial information.

7. Financial Proposal

7.1 In preparing the Financial Proposal, consultants are expected to take into account the requirements and conditions outlined in the RFP. The Financial Proposal shall follow the Financial Proposal Standard Forms FPF 1 to FPF 4 (Section IV).

7.2 The Financial proposal shall include all costs associated with the assignment, including (i) remuneration for staff (FPF–4) (ii) reimbursable expenses (FPF-5) such as indicated on the page 25. If appropriate, these costs should be broken down by activity. All items and activities described in the Technical proposal must be priced separately; activities and items in the Technical Proposal but not priced shall be assumed to be included in the prices of other activities or items.

7.3 The Service Provider/ Consulting Firm may be subject to local taxes on amounts payable under the Contract. Taxes shall not be included in the sum provided in the Financial Proposal as this will not be evaluated, but they will be discussed at contract negotiations, and applicable amounts will be included in the Contract.

7.4. Service Providers/ Consulting Firms shall express the price of their services in USD without VAT.

7.5 The Financial Proposal shall be valid for *90 days*. During this period, the Service Provider/ Consulting Firm is expected to keep available the professional staff for the assignment[2]. IOM will make its best effort to complete negotiations and determine the award within the validity period. If IOM wishes to extend the validity period of the proposals, the Service Provider/ Consulting Firm has the right not to extend the validity of the proposals.

8. Submission, Receipt, and Opening of Proposals

8.1 Service Providers/ Consulting Firms may only submit one proposal. If a Service Provider/ Consulting Firm submits or participates in more than one proposal such proposal shall be disqualified.

8.2 Official email for submission will be bakutender@iom.int and Format of proposals must be PDF files only.

8.3 Financial proposal should be password protected; password must not be provided to IOM until it's requested by an email; only bidders that pass the technical evaluation will be asked for password.

8.4 Recommended Max. File Size per transmission is 5 Mb; Mandatory subject of email: "RFP No.: AZ-005-2017"; Time Zone to be Recognized: local Baku time

8.5 Any Proposal submitted by the Service Provider/ Consulting Firm after the deadline for receipt of Proposals prescribed by IOM shall be declared "Late".

8.6 The BEAC has the option to review the proposals publicly or not.

9. Evaluation of Proposals

9.1 After the Proposals have been submitted to the BEAC and during the evaluation period, Service Providers/ Consulting Firms that have submitted their Proposals are prohibited from making any kind of communication with any BEAC member, as well as its Secretariat regarding matters connected to their Proposals. Any effort by the Service Providers/ Consulting Firms to influence IOM in the examination, evaluation, ranking of Proposal, and recommendation for the award of contract may result in the rejection of the Service Providers/ Consulting Firms Proposal.

10. Technical Evaluation

[2] *For this purpose, the Mission may have the option to require short-listed Consultants a bid security.*

10.1 The entire evaluation process, including the submission of the results and approval by the approving authority, shall be completed in not more than *30 calendar days* after the deadline for receipt of proposals.

10.2 The BEAC shall evaluate the Proposals on the basis of their responsiveness to the Terms of Reference, compliance to the requirements of the RFP and by applying an evaluation criteria, sub criteria and point system[3]. Each responsive proposal shall be given a technical score (St). The proposal with the highest score or rank shall be identified as the Highest Rated/Ranked Proposal.

10.3 A proposal shall be rejected at this stage if it does not respond to important aspects of the TOR or if it fails to achieve the minimum technical qualifying score which is *70%.*

10.4 The technical proposals of Service Providers/ Consulting Firms shall be evaluated based on the following criteria and sub-criteria:

	Points
(i) Specific experience of the Service Providers/ Consulting Firms relevant to the assignment:	[*0* - *10*]
At least one software development project similar by Methodology, size and complexity completed successfully during the last year	
No project completed	[*0*]

(ii) Adequacy of the proposed methodology and work plan in response to the Terms of Reference:

a) Technical approach and methodology	15	
b) Work plan	10	
c) Organization and staffing	5	
Total points for criterion (ii):		30

(iii) Key professional staff qualifications and competence for the assignment:

a) Business Analysts	*20*	
b) Implementation Specialist	*10*	
c) Backend Developer	*10*	
d) Frontend Developers	*10*	
e) Database Developer	*10*	
Total points for criterion (iii):		*60*

The number of points to be assigned to each of the above positions or disciplines shall be determined considering the following three sub-criteria and relevant percentage weights:

1) General qualifications	*30%*	
2) Adequacy for the assignment	*50 %*	
3) Experience in region and language	*20%*	
Total weight:		100%

[3] *The criteria, sub criteria and point system may vary depending on the requirement of the Mission*

The minimum technical score St required to pass is: 70 Points (70 %)

10.5 Technical Proposal shall not be considered for evaluation in any of the following cases:

a) late submission, *i.e.*, after the deadline set
b) failure to submit any of the technical requirements and provisions provided under the Instruction to Service Provider/ Consulting Firm (ITC) and Terms of Reference (TOR);

11. Financial Evaluation

11.1 After completion of the Technical Proposal evaluation, IOM shall notify those Service Providers/ Consulting Firms whose proposal did not meet the minimum qualifying score or were considered non responsive based on the requirements in the RFP, indicating that the password for their financial proposal is not required

11.2 IOM shall simultaneously notify the Service Providers/ Consulting Firms that have passed the minimum qualifying score indicating the date and opening of the Financial Proposal. The BEAC has the option to open the Financial proposals publicly or not.

11.3 The BEAC shall determine the completeness of the Financial Proposal whether all the Forms are present and the required to be priced are so priced.

11.4 The BEAC will correct any computational errors. In case of a discrepancy between a partial amount and the total amount, or between words and figures, the former will prevail. In addition, activities and items described in the Technical proposal but not priced, shall be assumed to be included in the prices of other activities or items.

11.5 The Financial Proposal of Service Providers/ Consulting Firms who passed the qualifying score shall be opened, the lowest Financial Proposal (F1) shall be given a financial score (Sf) of 100 points. The financial scores (Sf) of the other Financial Proposals shall be computed based on the formula :

Sf = 100 x Fl / F

Where:

Sf - is the financial score of the Financial Proposal under consideration,
Fl - is the price of the lowest Financial Proposal, and
F - is the price of the Financial Proposal under consideration.

The proposals shall then be ranked according to their combined (Sc) technical (St) and financial (Sf) scores using the weights[4] (T = the weight given to the Technical Proposal = 0.80; F = the weight given to the Financial Proposal = 0.20; T + F = 1)

$Sc = St \times T\% + Sf \times F\%$

The firm achieving the highest combined technical and financial score will be invited for negotiations.

12. Negotiations

12.1 The aim of the negotiation is to reach agreement on all points and sign a contract. The expected date and address for contract negotiation is *June 15, 2017 at IOM Baku, Yashar Husseynov 18, Baku, Azerbaijan*.

12.2 Negotiation will include: a) discussion and clarification of the Terms of Reference (TOR) and Scope of Services; b) Discussion and finalization of the methodology and work program proposed by the Service Provider/ Consulting Firm; c) Consideration of appropriateness of qualifications and pertinent compensation, number of man-months and the personnel to be assigned to the job, and schedule of activities (manning schedule); d) Discussion on the services, facilities and data, if any, to be provided by IOM; e) Discussion on the financial proposal submitted by the Service Provider/ Consulting Firm; and f) Provisions of the contract. IOM shall prepare minutes of negotiation which will be signed both by IOM and the Service Providers/ Consulting Firms.

12.3 The financial negotiations will include clarification on the tax liability and the manner in which it will be reflected in the contract and will reflect the agreed technical modifications (if any) in the cost of the services. Unless there are exceptional reasons, the financial negotiations will involve neither the remuneration rates for staff nor other proposed unit rates.

12.4 Having selected the Service Provider/ Consulting Firm on the basis of, among other things, an evaluation of proposed key professional staff, IOM expects to negotiate a contract on the basis of the experts named in the proposal. Before contract negotiations, IOM shall require assurances that the experts shall be actually available. IOM will not consider substitutions during contract negotiation unless both parties agree that the undue delay in the selection process makes such substitution unavoidable or for reasons such as death or medical incapacity. If this is not the case and if it is established that staff were referred in their proposal without confirming their availability the Service Provider/ Consulting Firm may be disqualified. Any proposed substitution shall have equivalent or better qualifications and experience than the original candidate.

12.5 All agreement in the negotiation will then be incorporated in the description of services and form part of the Contract.

[4] *May vary depending on the requirement of the Mission; normally, weight assigned to Technical is .80 and .20 for the Financial.*

12.6 The negotiations shall conclude with a review of the draft form of the Contract which forms part of this RFP (Section VI). To complete negotiations, IOM and the Service Providers/ Consulting Firms shall initial the agreed Contract. If negotiations fail, IOM shall invite the second ranked Service Provider/ Consulting Firm to negotiate a contract. If negotiations still fail, the IOM shall repeat the process for the next-in-rank Service Providers/ Consulting Firms until the negotiation is successfully completed.

13. Award of Contract

13.1 The contract shall be awarded, through a notice of award, following negotiations and subsequent post-qualification to the Service Provider/ Consulting Firm with the Highest Rated Responsive Proposal. Thereafter, the IOM shall promptly notify other Service Providers/ Consulting Firms on the shortlist that they were unsuccessful and shall return their unopened Financial Proposals. Notification will also be sent to those Service Providers/ Consulting Firms who did not pass the technical evaluation if RFP was not manually submitted - delivered by hand.

13.2 The Service Provider/ Consulting Firm is expected to commence the assignment on June 22, 2017.

14. Confidentiality

14.1.1 Information relating to the evaluation of proposals and recommendations concerning awards shall not be disclosed to the Service Provider/ Consulting Firm who submitted Proposals or to other persons not officially concerned with the process. The undue use by any Service Provider/ Consulting Firm of confidential information related to the process may result in the rejection of its Proposal and may be subject to the provisions of IOM’s anti-fraud and corruption policy.

14.1.2 Since all information contained in the components of the system of the State Migration Service (SMS) of the Republic of Azerbaijan is considered as a state security, SMS requests the winner company to sign an additional commitment document with IOM on security and confidentiality.

Section II – Technical Proposal Standard Forms

TPF-1: Technical Proposal Submission Form

[Baku, Date]

To: Chairperson of the BEAC

Ladies/Gentlemen:

We, the undersigned, offer to provide the Services for *[insert Title of consulting services]* in accordance with your Request for Proposal (RFP) dated *[insert Date]* and our Proposal. We are hereby submitting our Proposal, which includes this Technical Proposal, and a Financial Proposal sealed under a separate envelope.

If negotiations are held after the period of validity of the Proposal, we undertake to negotiate on the basis of the proposed staff. Our Proposal is binding upon us and subject to the modifications resulting from Contract negotiations.

We acknowledge and accept IOM's right to inspect and audit all records relating to our Proposal irrespective of whether we enter into a contract with IOM as a result of this proposal or not.

We understand you are not bound to accept any Proposal you receive.

We remain,

Yours sincerely,

Authorized Signature:
Name and Title of Signatory:
Name of Firm:
Address:

TPF – 2: Service Providers/ Consulting Firms Organization

[Provide here brief (two pages) description of the background and organization of your firm/entity and each associate for the assignment (if applicable).]

TPF – 3: Description of the Approach, Methodology and Work Plan for Performing the Assignment

[The description of the approach, methodology and work plan should normally consist of 10 pages, including charts, diagrams, and comments and suggestions, if any, on Terms of reference and counterpart staff and facilities.]

TPF – 4: Team Composition and Task Assignments

1. Technical/Managerial Staff

Name	Position	Task

2. Support Staff

Name	Position	Task

TPF – 5: Format of Curriculum Vitae (CV) for Proposed Professional Staff

Proposed Position: ____
Name of Firm: ____
Name of Staff: ____
Profession: ____
Date of Birth: ____
Years with Firm/Entity: ____________________Nationality: ______________
Membership in Professional Societies: ____________________________
____
Detailed Tasks Assigned: ____
____

Key Qualifications:
[*Give an outline of staff member's experience and training most pertinent to tasks on assignment. Describe degree of responsibility held by staff member on relevant previous assignments and give dates and locations. Use about half a page.*]

____

Education:
[*Summarize college/university and other specialized education of staff member, giving names of schools, dates attended, and degrees obtained. Use about one quarter of a page.*]

____

Employment Record:
[*Starting with present position, list in reverse order every employment held. List all positions held by staff member since graduation, giving dates, names of employing organizations, titles of positions held, and locations of assignments. For experience in last ten years, also give types of activities performed and client references, where appropriate. Use about two pages.*]

____

Languages:
[*For each language indicate proficiency: excellent, good, fair, or poor in speaking, reading, and writing.*]

____

Certification:

I, the undersigned, certify that to the best of my knowledge and belief, these data correctly describe me, my qualifications, and my experience. I understand that any willful misstatement described herein may lead to my disqualification or dismissal, if engaged.

____Date: __________
[Signature of staff member and authorized representative of the firm] *Day/Month/Year*

Full name of staff member:______________________________
Full name of authorized representative: ___________________

TPF-6: Time Schedule for Professional Personnel

			Months (in the Form of a Bar Chart)												
Name	Position	Reports Due/Activities	1	2	3	4	5	6	7	8	9	10	11	12	Number of Months
															Subtotal (1) ________________
															Subtotal (2) ________________
															Subtotal (3) ________________
															Subtotal (4) ________________

Full-time: ________ Part-time: ____________

Reports Due: ________

Activities Duration: ________

Location ________

Signature of Authorized Representative:

____

Full Name:______________________________

Title : _________________________________

TPF-7: Activity (Work) Schedule

A. Field Investigation and Other Activities														
No.	**Activity/Work Description**	***Duration***												
		1st	2nd	3rd	4th	5th	6th	7th	8th	9th	10th	11th	12th	
1														
2														
3														
4														
5														

B. Completion and Submission of Reports

Reports	Date
1. Inception Report	
2. Interim Progress Report (a) First Status Report (b) Second Status Report	
3. Draft Report	
4. Final Report	

Section III. Financial Proposal - Standard Forms

FPF-1: Financial Proposal Submission Form

[Baku, Date]

To: Chairperson of the BEAC

Ladies/Gentlemen:

We, the undersigned, offer to provide the consulting services for *[insert Title of consulting services]* in accordance with your Request for Proposal (RFP) dated *[insert date]* and our Proposal (Technical and Financial Proposals). Our attached Financial Proposal is for the sum of *[Amount in words and figures]*. This amount is exclusive of the local taxes, which we have estimated at *[Amount(s) in words and figures]*.

Our Financial Proposal shall be binding upon us subject to the modifications resulting from Contract negotiations, up to expiration of the validity period of *[insert validity period]* of the Proposal.

We acknowledge and accept the IOM right to inspect and audit all records relating to our Proposal irrespective of whether we enter into a contract with the IOM as a result of this Proposal or not.

We confirm that we have read, understood and accept the contents of the Instructions to Service Providers/ Consulting Firms (ITC), Terms of Reference (TOR), the Draft Contract, the provisions relating to the eligibility of Service Providers/ Consulting Firms, any and all bulletins issued and other attachments and inclusions included in the RFP sent to us.

We understand you are not bound to accept any Proposal you receive.

We remain,

Yours sincerely,
Authorized Signature:
Name and Title of Signatory:
Name of Firm:
Address:

FPF– 2: Summary of Costs

Costs	Currency	Amount(s)
I – Remuneration Cost (see FPF- 3 for breakdown)		
II - Reimbursable Cost (see FPF – 4 for breakdown)		
Total Amount of Financial Proposal [1]		

[1] Indicate total costs, net of local taxes, to be paid by IOM in each currency. Such total costs must coincide with the sum of the relevant subtotal indicated in all Forms FPF-3 provided with the Proposal.

Authorized Signature:
Name and Title of Signatory:

FPF-3: Breakdown of Costs by Activity

Group of Activities (Phase):[2] ____________________ ____________________	Description: [3] ____________________ ____________________	
Cost Component	Costs	
	Currency	Amount
Remuneration [4]		
Reimbursable Expenses [4]		
Subtotals		

[1] Form FPF3 shall be filed at least for the whole assignment. In case some of the activities require different modes of billing and payment (e.g. the assignment is phased, and each phase has a different payment schedule), the Service Provider/ Consulting Firm shall fill a separate Form FPF-3 for each Group of activities.

[2] Names of activities (phase) should be same as, or corresponds to the ones indicated in Form TPF-8.

[3] Short description of the activities whose cost breakdown is provided in this Form.

[4] For each currency, Remuneration and Reimbursable Expenses must coincide with relevant Total Costs indicated in FPF-4 and FPF-5.

Authorized Signature:
Name and Title of Signatory:

FPF-4: Breakdown of Remuneration per Activity

[Information provided in this Form should only be used to establish payments to the Service Provider/ Consulting Firm for possible additional services requested by Client/IOM]

Name of Staff	Position	Staff-month Rate
Professional Staff		
1.		
2.		
3.		
4.		
5.		
Support Staff		
1.		
2.		
3.		
4.		
5.		

[1] Names of activities (phase) should be same as, or corresponds to the ones indicated in Form TPF-8.

[2] Short description of the activities whose cost breakdown is provided in this Form.

Authorized Signature:
Name and Title of Signatory:

FPF-5: Breakdown of Reimbursable Expenses

[Information provided in this Form should only be used to establish payments to the Service Provider/ Consulting Firm for possible additional services requested by Client/IOM]

Description[1]	**Unit**	**Unit Cost**[2]
1. Subsistence Allowance		
2. Transportation Cost		
3. Communication Costs		
~~4. Printing of Documents, Reports, etc~~		
~~5. Equipment, instruments, materials, supplies, etc~~		
6. Office rent, clerical assistance		

[1] Delete items that are not applicable or add other items according to Paragraph 7.2 of Section II-Instruction to Service Providers/ Consulting Firms

[2] Indicate unit cost and currency.

Authorized Signature:
Name and Title of Signatory:

Section IV. Terms of Reference

IOM is an inter-governmental organization with 166 Member States and 8 states holding Observer status. Since 19 September 2016, IOM is part of the UN system as a related organization. IOM presence in Azerbaijan dates back to 1996. IOM has been implementing a variety of projects in line with its mission to assist the Government of Azerbaijan in meeting the operational challenges of migration, advance understanding of migration issues, encourage social and economic development, and uphold the human dignity and well-being of migrants. On 1st September 2014 IOM started the implementation of the project “Consolidation of Migration and Border Management Capacities in Azerbaijan (CMBA)” funded by the European Union and co-funded by BP and Co-venturers. The aim of this project is to enhance the capacities of Azerbaijani authorities in the area of migration and border management in line with relevant EU-Azerbaijan Agreements, in particular the Visa Facilitation and Readmission Agreements.

Summary of the Action

The IOM invites eligible bidders to submit proposals for implementation of biometric identity management system for the State Migration Service that will enable quick and accurate enrolment and verification of Persons (Visitors, Immigrants, Refuges) in SMS operations, furthermore to issue related biometric card. The IOM will carry out the bidding process to identify service provider(s) who is experienced in implementing biometric identity management systems in diverse locations and who will be sensitive to the varied work of the organisation. The requirements catalogue contained in this RFP details the functional, IT and non-functional requirements for the System as well as describing the key business processes, quality requirements, the core functionality requirements, as well as the technological environment and requirements for the new System.

Purpose

The biometric project has the following stated aims:

- Establishment of an integrated database for the collection of biometric data
  - Biometric database collection module
  - Biometric database verification module
  - Integration of the biometric information collected on IAISS and SRP systems to the UMIS.
  - Biometric database archive module
  - Registration of requests for deletion of biometric data
  - Biometric subsystem administrative module
  - Audit register for biometric subsystem module
- ~~Establishment of the system for printing biometric cards~~
  - ~~Electronic personalization module of the permanent residence permit, temporary residence permits and refugee cards with the biometric data~~
- ~~Establishment of biometric identification~~

    - Module for forwarding of biometric information to other state information systems
    - Identification module of individuals based on biometric information
    - Module for fixed and portable inspection stations
    - Integration of biometric information with other UMIS modules

In order to fulfil these aims, the IOM wishes to procure a biometric System based on proven technology to enable persons (immigrants, visitors, refuges) to be enrolled, to have their identity subsequently verified and to issue related biometric card. The detailed requirements are set out in Section B of this document ("the Requirements"). In broad terms, IOM requires a System which best enables the capture, transmission, storage, verification of biometrics and prints biometric cards which must:

- Deliver a fast, intuitive, secure, durable and easy to use enrolment solution that enables to capture biometric information of Persons in related workstations
- Provide a secure, resilient, scalable data storage capability
- Allow secure, accurate, real time verification of Persons including the secure transmission of data
- Allow data to be shared securely across workstations and headquarter, providing the flexibility to verify, taking account of limited connectivity in the more remote areas of operation
- Conform with industry standards and best practice
- Allow for interoperability and alignment with existing SMS Systems, such as UMIS System
- Be operational and future-proof for a minimum of five years
- Conform with SMS policies and international standards on security and data protection, with auditable safeguards and controls covering the integrity of the System and data privacy

Be scalable so that it can be used in both high-volume locations as well as smaller sites and allow for the phased deployment by country operation and future development/larger scale use in future

1.1. Format of Response

The Supplier should ensure that their response contains a compliance matrix that details for each Requirement (see Appendix 2), where in their response they have addressed that Requirement and any Requirements that have not been complied with. SMS bears no responsibility for failing to award marks for compliance to a Requirement where such compliance is not detailed in the compliance matrix. The format for the compliance matrix should state the requirement number, whether or not it has been complied with in full, in part or the supplier is non-compliant and then reference the paragraph number in the response that addresses this requirement.

2. *Description of Requirements*

2.1. *Introduction*

The requirements and processes will provide context around the current role of biometrics in SMS. The Requirements have been catalogued under the following headings:

- **Functional and processes** – the Requirements in this area cover the processes of Enrolment~~, Verification and Card printing~~. The functional Requirements describe what will be expected from the new System in terms of the quality and accuracy of Enrolment~~, Verification and printing biometric cards~~
- **Technical** – The Technical Requirements cover the IT Requirements for the new System and how the system must be compatible with existing SMS architecture
- **Non Functional** – The non-functional Requirements cover the quality and user experience of the System as well as covering areas such as,Training and support, Audit, Management Information and Future Requirements

2.2. *Notes about the Requirements*

Each Requirement has been categorised as “Must”, meaning they must be complied with or “Could” / “Should meaning they are options that SMS would like to explore further.

The System must be compliant with both the Design Principles and the “Must” Requirements. Where the Supplier believes that any of the Requirements or any elements of the proposed System have conflicts with the Design Principles the Supplier shall highlight this, by providing reasoned arguments why and options for resolving the conflict. Furthermore, where the Supplier has made any assumptions when responding to a specific requirement, these should be documented by the Supplier and clearly labelled as an assumption.

Where the Supplier believes that any of the Requirements provided by SMS materially compromise best practice or are contrary to the Supplier’s recommendations for addressing the scenarios described in this RFP, the Supplier shall detail such areas of conflict or compromise and detail their proposal for addressing the same.

2.3. *Design Principles*

Any proposed System must be compliant with the Design Principles outlined below. Proposed solutions that do not conform to any of these principles must be detailed in the Suppliers response by stating the reasons why the solution does not comply with the Design Principles and by proposing alternative solutions. The Design Principles are as follows:

- The System must be capable of Enrolling and Verifying the identity of a Person (visitor/immigrant/refegue) using their fingerprints as a biometric identifier
- The Supplier must ensure that the System is compatible with software to capture facial recognition (biometric photo) data in addition to fingerprints when required

- The Supplier should ensure that the System is based on proven technology that can be supported by evidence of real-world usage in projects that are comparable in scope to the work of SMS
- The System must be capable of capturing the Biometric Data of a broad range of persons with a wide variety of ages, abilities, disabilities and backgrounds
- The System must be able to be used in SMS operations including the Enrolment and Verification of identity in remote locations such as enrolment workstations and portable inspection stations
- The Supplier should ensure that any System proposed is designed to allow the activities of Enrolment and Registration to be conducted in a manner that is fast, accurate, effective and builds on working practices already in operation within SMS and as described in these Requirements
- The System should conform with industry best practice principles and standards for capture, storage, verification and transmission of biometric and electronic data and best practice principles for user access, security and fraud prevention
- The System should be designed to be global but scalable such that it can be implemented in phases and subsequently grow and adapt with the needs of SMS and the changes in the biometric marketplace
- The System should be independend in terms of used technology, database systems, fingerprint devices~~, card printers and etc~~. SMS holds the right to select the devices and proposed system must be complient with the standards that can be integrated with any standard devices.
- The System should has API structure to integrate with used devices and should be capable to work with various SDKs independently.
- The Supplier must ensure that any System proposed has a minimal impact on other users of the existing SMS IT infrastructure
- The System is intended to be in operation for a period in excess of five years. Therefore, the System proposed by the Supplier should have this in mind and should be supported (without material adaptations) for the duration of this five year period and beyond
- Any System should also provide the future to personalise and issue “smart cards”, “passports” containing individual Biometric Data captured (ex: work permission cards, refegue passports etc.)
- The System should not contravene any SMS rules or procedures included within this RFP or as updated from time to time

2.4. Requirements

2.4.1. Functional Requirements and Processes

The Functional Requirements and Processes have been broken down into the following areas:

- Enrolment
- Verification
- ~~Biometric Card Printing~~
- ~~Identification~~

2.4.1.1. Enrolment

When SMS (State Migration Service) registers a newly arrived Person (visitor, refegue, immigrant), the office must systematically establish identity through various processes. Individual registration sets out to achieve this by gathering data from the Person approaching SMS. Once Person is registered, they can receive access to services and assistance from State Migration Service.

Under the new System it is proposed that, prior to Persons registration, Biometric Data to be captured and authenticated using a 1:N verification against the existing Biometric Data records of previously enrolled individuals. This will determine whether or not the Person has already enrolled. If the Person has enrolled, the System should automatically re-direct the Operator to the existing record associated with that Person. If the Person has not enrolled, the Operator should be able to store the Biometric Data and either create a new record or associate that enrolment with an existing UMIS record (as long as the existing UMIS data already confirms identity through non-biometric means). UMIS System does not include associated Biometric Record at this stage. After a while when SMS starts using Biometric system, UMIS will have associated Biometric Record in time. For this reason this verification will become mandatory during the enrolment to check if UMIS already has associated Biometric Record for the Person.

Enrolment is a critical process in identity management since nearly all subsequent identity confirmations will require a reliable, fast and efficient 1:1 biometric verification thereafter. Therefore, the System should be capable of ensuring that a high quality biometric is taken quickly and efficiently at enrolment that later allows real-time Verification against existing records on a 1:1 basis when the Person requires access to additional services. The Supplier should assume that the total initial target population for Enrolment will be circa three million with an estimated ten million total Persons over time. However, as this System is expected to be in use by SMS for in excess of 5 years, it is critical that the System is scalable, by country operation and as increases in Enrolments are required.

Requirement ID	**Requirement Description**	**Importance** (Must / Could / Should / Future Req)
2.4.1.1.1.	The Supplier must provide a System that comprises or supports a standard Biometric Capture Device that captures the Biometric Data belonging to a Person, creates a Biometric Record on the Database and associates this Biometric Record with a UMIS Record held in the UMIS system	Must
2.4.1.1.2.	The Supplier must ensure that the Biometric Capture Device is capable of capturing high-quality fingerprint Biometric Data (e.g. NFIQ=1 for fingerprints) from a broad age-range of Persons at Enrolment. The Supplier shall detail the full quality parameters for their proposed method of capturing fingerprint Biometric Data including	Must

Requirement ID	Requirement Description	Importance (Must / Could / Should / Future Req)
	effective age ranges (including any variable quality data according to age) and supporting evidence for all quality parameters including details of any laboratory, field or user studies	
2.4.1.1.3.	The Supplier must ensure that the System is capable of supporting the capture of facial recognition data as well.	
2.4.1.1.4.	The Supplier must complete the information contained at Appendix 1 (Quality Requirements) relating to the performance of their proposed System in Enrolment scenarios	Must
2.4.1.1.5.	The Biometric Capture Device and Processing System must be capable of capturing Biometric Data and creating a Biometric Record at Enrolment quickly and efficiently. The Supplier shall detail the time taken to : • capture Biometric Data • perform Verification for Enrolment purposes (1:N); and • provide a response to the Operator	Must
2.4.1.1.6.	The System must provide the opportunity to associate that enrolment with an existing UMIS record (as long as the existing UMIS data already confirms identity through non-biometric means) or create new record with Biometric Data	Must
2.4.1.1.7.	The Biometric Record created by the System at Enrolment must contain the following information: • Biometric Data • UMIS numeric identifier • Time and date of creation of Biometric Record • Operator who created the Biometric Record	Must
2.4.1.1.8.	The Supplier shall provide suitable illustrations or documentation describing the proposed Enrolment process including the process for collecting Biometric Data from the following age and range of Persons: • Ages 0-4 years • Ages 5-14 years • Ages 14-59 years • Ages 60+ years • Persons with degraded or poor quality fingerprints • Persons with missing fingers • Persons with disfigured faces	Must
2.4.1.1.9.	The Biometric Capture Device must be able to capture Biometric Data from Persons from a variety of locations and occupations. As such, it is expected that a Person	Must

Requirement ID	**Requirement Description**	**Importance** (Must / Could / Should / Future Req)
	encountered may have particularly abraded fingerprints, a higher than typical instance of missing fingers or other such factors that may make collecting fingerprint Biometric Data problematic. Therefore, any Biometric Capture Device proposed by the Supplier should maximise the likelihood of capturing usable Biometric Data from such Persons. The Supplier shall provide details of what features of the Biometric Capture Device address these issues and the impact of these features (if any) on the relevant Quality Requirements	
2.4.1.1.10.	The Supplier shall provide details of whether different models of their proposed Biometric Capture Device are available that could potentially cope with varying scenarios of high volumes, low volumes, portable scenarios and desk-based scenarios or other potential Enrolment and Verification variations, provided it is understood at all times that any different models of Biometric Capture Device must capture sufficient quality of Biometric Data and provide compatible matching capabilities between models	Must
2.4.1.1.11.	The Supplier shall ensure that the System and/or the Biometric Capture Device has quality checking functionality such that the Operator is notified quickly of whether or not the Biometric Data captured at Enrolment is of sufficient quality to comply with the Quality Requirements	
2.4.1.1.12.	The Supplier shall ensure that any communications to the Operator including on the quality of data captured or whether or not a match has been made (to a Biometric Record or to Biometric Data already held in the System) are presented in a clear and unambiguous way and can be readily understood by the Operator	
2.4.1.1.13.	The Supplier shall ensure that where the first attempt to capture Biometric Data that meets the Quality Requirements is unsuccessful, the System is capable of allowing multiple attempts by an Operator to capture Biometric Data that is of sufficient quality and notifying the Operator when such data has been successfully captured. In the event that the System has not captured Biometric Data of sufficient quality to meet the Quality Requirements after a defined number of attempts, the System should be capable of utilising the Biometric Data from the previous attempts that was closest to the required	

Requirement ID	**Requirement Description**	**Importance** (Must / Could / Should / Future Req)
	threshold to create the Biometric Record	
2.4.1.1.14.	The Supplier could provide separate Biometric Capture Devices capable of capturing a single form of biometric (for example separate finger print devices and face capture machines)	
2.4.1.1.15.	The Supplier could provide a multi-modal Biometric Capture Device capable of capturing multiple biometrics simultaneously	Could
2.4.1.1.16.	The Biometric Data captured by the Biometric Capture Device must be stored as a Biometric Record. The System must not allow the same Biometric Data to be stored against two different Biometric Records, associated with a UMIS records. If biometric templates are generated, the System must be capable of capturing and storing images in addition to templates	
2.4.1.1.17.	Where the System utilises multiple different Biometric Capture Devices (for example a fingerprint scanner and face capture machine), the System must store both sets of Biometric Data against the same Biometric Record	
2.4.1.1.18.	The System must ensure that all Biometric Records contain fingerprint Biometric Data. During the enrolment, ten-printing, palms and thumbs should be printed and stored. Ten-printing and palms record will be used for 1:1 verification.	
2.4.1.1.19.	The Supplier shall ensure that the fingerprint Biometric Capture Device shall be capable of capturing not less than four fingerprints simultaneously. If the Supplier believes that the Quality Requirements can be met by capturing less fingers, this should explained with supporting evidence	
2.4.1.1.20.	The Supplier shall ensure that where the Biometric Capture Device proposed performs facial recognition, it shall be capable of exporting the photograph captured for the Biometric Record to the UMIS Record and e-cards	
2.4.1.1.21.	The Supplier shall ensure that where the Biometric Capture Devices captures multiple biometric reference points such as multiple fingers, it is also capable of capturing less biometric reference points in the event that the Person is for example missing a finger(s)	
2.4.1.1.22.	The System must be able to store Biometric Records in a Database that enables 1:1 and 1:N Verification. The Database will typically include Biometric Records for 200,000 Persons	
2.4.1.1.23.	The Supplier shall provide details of the time taken to	

Requirement ID	Requirement Description	**Importance** (Must / Could / Should / Future Req)
	complete a 1:1 and 1:N search and Verification against the Biometric Records held in the Database in Appendix 1 (Quality Requirements)	
2.4.1.1.24.	The System must be capable of performing Enrolment in scenarios where there is limited or no connectivity in remote areas and the Supplier shall detail how it proposes to address this issue, such proposal must include options such as intermittent data reconciliation, use of mobile communications. The Supplier shall detail the advantages and constraints such solution imposes on the System and any impact on the time taken to complete the relevant functions (e.g. 1:1 or 1:N Verification)	
2.4.1.1.25.	The Supplier shall ensure that the Enrolment process performed by the System is efficient, non-threatening and non-invasive for the Person concerned	
2.4.1.1.26.	The Supplier shall ensure that the Enrolment process is capable of being performed by an Operator with limited technical knowledge and a minimum of training and experience. Accordingly, all actions relayed to or required of the Operator in the capture of Biometric Data or the creation of a Biometric Record should be simple, unambiguous and involve as few steps as possible to complete	
2.4.1.1.27.	The Supplier shall ensure that fraudulent use of the System by the Operator, either in collusion with the Person or independently, is minimised through appropriate System design including the inability to create duplicate Biometric Records, store the same Biometric Data against different Biometric Records or associate the same Biometric Record against multiple UMIS Records	
2.4.1.1.28.	The Supplier must ensure that when the Biometric Data belonging to a Person is located in the System and the Operator views the Biometric Record, this must automatically direct the Operator to the UMIS Record	

2.4.1.2. ***Verification***

The Verification of a Person typically takes place after initial registration when a Person requires access to services or SMS has to verify individual identity for other purposes. This may include provision of legal documents, work permissions, refegue passports and many other forms of assistance. Additionally, these services are often provided in very high volumes and as such, the System must be able to verify the identity of the Person and their entitlement to services quickly and accurately.

At present, a Person has identity verified through UMIS itself. At registration, UMIS requires that an Operator collect personal details from the Person and a unique identification number (Person_Code) is accordingly assigned automatically. When subsequently providing assistance (usually repeatedly over a period of many years), the same details are used to search UMIS to determine whether the Person is already registered and therefore entitled to access the relevant services and support from SMS. It is envisioned that the System will give the Operator the option of performing Verification through UMIS, through the System or through an identity document. Therefore, the System must allow an Operator to:

- Locate through a 1:N Verification of the Biometric Record, locate a Person and then subsequently view the associated UMIS Record, or
- locate a Person through their UMIS Record and then subsequently perform a 1:1 Verification against the associated Biometric Record, in case biometric record has been captured before, or
- locate a Person through their UMIS Record and then subsequently associate newly captured biometric record with corresponding UMIS record, if no biometric record is available till this operation for the Person, or
- locate a Person approaching with identity card, trough 1:1 verification to verify if the card belongs to this person and 1:N verification to find related UMİS record of card holder

Finally it is also envisioned that the Verification process may also be used as an opportunity to re-capture or refresh the Biometric Data belonging to a Person as required by the System.

Requirement ID	**Requirement Description**	**Importance** (Must / Could / Should / Future Req)
2.4.1.2.1.	The Supplier must complete the information contained at Appendix 1 (Quality Requirements) relating to the performance of their proposed System in Verification scenarios	
2.4.1.2.2.	The Supplier shall ensure that the System is capable of performing Verification whilst addressing the same challenges (such as variety of Person backgrounds, difficult operating conditions etc.) as detailed in the Requirements for Enrolment	
2.4.1.2.3.	The Supplier must ensure that an Operator can identify a Person through capturing their Biometric Data and performing a 1:N Verification against the Biometric Database (or specified sub-set thereof as detailed in 2.4.1.2.13). Once the System has located the Biometric Record, the System should automatically direct the Operator to the associated UMIS Record	

Requirement ID	Requirement Description	Importance (Must / Could / Should / Future Req)
2.4.1.2.4.	In the event that an Operator has searched and located the UMIS Record belonging to a Person, the Supplier must ensure that UMIS/System notifies the Operator of whether a Biometric Record is associated to that UMIS Record	
2.4.1.2.5.	If a Biometric Record is not associated with a UMIS Record, the System must enable the Operator to create a Biometric Record (at the Operator's discretion) in accordance with the Registration Requirements	
2.4.1.2.6.	If an Operator has been notified that a UMIS Record has a Biometric Record associated with it, the System must enable the Operator to perform a 1:1 Verification (using the Biometric Capture Device)	
2.4.1.2.7.	The System must be able to Verify the Biometric Record of a Person on a 1:1 basis as fast as possible. The Supplier shall provide details of the actual Verification data for the System proposed, including factors that can increase or decrease the time taken to perform Verification including but not limited to size of population held on the Database and speed of data connection to Database	
2.4.1.2.8.	The System must be capable of performing Verification in scenarios where there is limited or no connectivity. The Supplier shall detail how it proposes to address this issue, such proposal to include options such as use of mobile communications or local instances of the Database	
2.4.1.2.9.	The Supplier shall ensure that where the Biometric Data captured matches the Biometric Data held in a Biometric Record, the Operator receives a clear and unambiguous message that the Person has been identified in accordance with the Quality Requirements and the Operator is then automatically directed to the associated UMIS record for the Person	
2.4.1.2.10.	The Supplier shall ensure that if the identity of the Person is not verified using Biometric Data and the Person Biometric Record cannot be located, the Operator receives a clear and unambiguous message that either the Person does not have UMIS record which requires new registration or Biometric Record has not been associated with UMIS record for this Person. In this case Operator must be able to search UMIS for Personal information and associate (if record found) with Biometric Record, or if there is no any information in UMIS, Operator must be able to register this Person in UMIS associated with captured Biometric Record.	

Requirement ID	**Requirement Description**	**Importance** (Must / Could / Should / Future Req)
2.4.1.2.11.	The Supplier shall ensure that where the Supplier or the System recommends that Biometric Data held in the Biometric Record be re-captured after a defined period of time, the Operator is notified when such time period has elapsed and is offered the option of capturing the Biometric Data of the relevant Person the next time the UMIS Record or Biometric Record belonging to that Person is accessed. The Supplier shall detail the impact on the Quality Requirements if such re-capture of Biometric Data is not performed	
2.4.1.2.12.	The Supplier should ensure that the System does not require any manual intervention from Operators or SMS personnel to perform the Verification process once initiated	
2.4.1.2.13.	The Supplier must ensure that the System enables Operators to perform a 1:N Verification having previously selected certain sub-sets of data in the Biometric Database, for example selecting sex, age cohort, location etc.	
2.4.1.2.14.	The System in performing 1:1 or 1:N search against the Database must specify match accuracy rates through False Positive Identification Rate (FPIR) and False Negative Identification Rate (FNIR) ROC (Receiver Operating Characteristic) curves. System match performance should be tuneable based on specified TAR and FAR rates. These rates should only be set by SMS system administrators and not Operators.	

*2.4.1.3. **De-duplication***

Depending on achievable biometric image quality and design features of the system, it may be possible for duplicate biometric Person records to be enrolled into the System which may need to be resolved periodically.

Requirement ID	**Requirement Description**	**Importance** (Must / Could / Should / Future Req)
2.4.1.3.1.	The System must be capable of merging instances of the Database without allowing duplicate Biometric Records to be created. The Supplier should detail in their response the	

Requirement ID	Requirement Description	Importance (Must / Could / Should / Future Req)
	System performance characteristics for merging instances of the Database and the associated N:N verification	
2.4.1.3.2.	The System must include functionality to identify and facilitate resolution of likely duplicate Biometric Records at all Database. Where the System does detect duplicate Biometric Records, the System must be capable of notifying the relevant Operator of the same and detailing which Biometric Records are duplicates	
2.4.1.3.3.	De-duplication operations should be optimised to minimise impact on operational activities (for example a routine background process rather than a major annual exercise)	
2.4.1.3.4.	The Supplier shall ensure that the System offers the functionality such that when instances of the Database are merged and duplicate Biometric Records are detected, the relevant Operator has the option of retaining the Biometric Record that best meets or exceeds the Quality Requirements	
2.4.1.3.5.	The Supplier shall detail in their response what if any features are available (including but not limited to the use of selecting sub-sets of data) that will improve the performance of the Database merging operation and the associated N:N verification process	

2.4.1.4. *Identification*

Requirement ID	Requirement Description	Importance (Must / Could / Should / Future Req)
2.4.1.4.1.	Supplier shall provide module as a part of the system for forwarding of biometric information to other state information systems.	
2.4.1.4.2.	Supplier shall provide Identification module of individuals based on biometric information. This will reduce the multiple UMIS records belonging to the same person, where there might be different personal data for the Person.	
2.4.1.4.3.	Supplier shall provide module for fixed and portable inspection stations.	
2.4.1.4.4.	Supplier shall Integrate the biometric information system with other UMIS modules.	

2.4.1.5. Biometric Identity Cards

~~SMS will issue smart cards and passports that store the Person Biometric Data and additional information. Biometric Identity Cards will include the following:~~

- ~~Permanent Residence Permit Identity Card (PRPIC)~~
- ~~Temporary Residence Permit Identity Card (TRPIC)~~
- ~~Refugee Travel Document (RTD)~~
- ~~Refugee ID Card (RIDC)~~

~~Requirement ID~~	~~Requirement Description~~	**Importance** (Must / Could / Should / Future Req)
2.4.1.5.1.	~~Supplier shall provide System (software and hardware) that enables SMS to issue smart cards and Refeguee Travell Documents (book/passport style)~~	
2.4.1.5.2.	~~Proposed system should be available to work with various printers from different vendors. Supplier should provide the list of supported vendors for hardware/printers.~~	
2.4.1.5.3.	~~Proposed system should comply to work with cards/books from different manufactures.~~	
2.4.1.5.4.	~~System shall prevent wasted materials and other failures by human error and by machine with low performance~~	
2.4.1.5.5.	~~Verification of MRZ (Machine Readable Zone) to prevent passport / card forgery~~	
2.4.1.5.6.	~~System shall enable Multiple book / card issueing for laborsaving. Supplier shall provide the multiple card issueing limit.~~	
2.4.1.5.7.	~~Smart card descriptions and specifications are described in Appendix3. Supplier shall ensure that proposed system enable to implement relevant requirements.~~	
2.4.1.5.8.	~~Supplier shall provide detailed description for the way of identification, encoding, engraving and verification of both cards and books (passport style RTD).~~	
2.4.1.5.9.	~~Input Unit:~~ ~~The system shall provide an Input Unit/Tray that can hold a large stack of cards up to 200. Cards then will fed in to the system automatically.~~	
2.4.1.5.10.	~~Card / Book identification unit :~~ ~~System should be capable to identify card/book with a number or barcode either from a pre-printed information source or pre-programmed information from the chip. For further personalization process, system should retrieve required data from host computer.~~	
2.4.1.5.11.	~~Chip encoding unit:~~ ~~System should be capable to encode personal data (including biometric data) into the integrated contact/contactless chip. Verification should be done~~	

~~Requirement ID~~	~~Requirement Description~~	**Importance** (Must / Could / Should / Future Req)
	~~whether data is applied correctly and wasted cards should be separated.~~	
2.4.1.5.12.	~~Laser Engraving Unit:~~ ~~System should enable to engrave the biometric photo and personal data into the front and backside of the card/related page of book. Advanced secure laser engraving methods should be supported such as MLI/CLI. Proposed laser engraving quality should allow to incorporate hidden information in the photograph.~~	
2.4.1.5.13.	~~Verification Unit:~~ ~~System should be capable to verify issued card information (including the visual data and data in chip) against relative information in host machine, to determine whether the information is applied correctly.~~	
2.4.1.5.14.	~~Output Unit:~~ ~~System should enable to stack the finished/approved cards/books in the output tray, where the operator can remove these cards/books at anytime or during the operation. System should stopo automatically when the last card/book has been processed.~~	
2.4.1.5.15.	~~System should be capable of logging all activities/actions performed on the system, commands, and errors, also should provide detailed description of the reason for errors.~~	
2.4.1.5.16.	~~System should have a useable user interface / screen that offers safe and easy operation, clear menus in a language of choice.~~	
2.4.1.5.17.	~~The Supplier shall ensure that the Person Biometric Data is capable of being stored on a smartcard/book and that the System offers SMS the ability to issue smartcards/book with no material alterations to the System.~~	
2.4.1.5.18.	~~Smartcard capabilities of the System proposed must be able to comply with the following standards:~~ • ~~ISO/IEC 7816 Identification cards — Integrated circuit cards~~ • ~~ISO/IEC 14443 Identification cards — Contactless integrated circuit cards~~ • ~~ISO/IEC 19795-7 Testing of on-card biometric comparison algorithms~~ • ~~ISO/IEC 24787-1 Identification cards — On-card biometric comparison~~ • ~~ICAO TAG-MRTD/17-WP/11 standard Extended Access Control~~ • ~~ICAO 9303 Campliance~~	

~~Requirement ID~~	~~Requirement Description~~	**Importance** (Must / Could / Should / Future Req)
	• ~~Basic Access Control~~ • ~~Passiv Authentication~~ • ~~Extended Access Control~~ • ~~CC EAL 5+ Level complicance certificate~~	
2.4.1.5.19.	~~Smartcard capabilities of systems proposed must be able to operate with the following platform products:~~ • ~~MS Windows® Smart Card Framework~~ • ~~Microsoft Forefront Identity Manager~~ • ~~Forefront Threat Management Gateway (TMG)~~	

2.4.2. Technical Requirements

The following section outlines the technical requirements for both the Hardware and Software of the proposed system, plus context around existing SMS systems and the Requirements to ensure the data is stored and transmitted in a secure manner. The IT Requirements have been broken down into the following areas:

- ICT Architecture
- Data sharing
- IT Security

A short description of the UMİS system is detailed below:

UMİS is the system for managing individual and family registration for Persons (Refegues, Immigrants, and Visiors) and supporting certain applications and operational processes. UMIS was first developed in 2008 to meet SMS’s migration services data management requirements. Since then, UMIS has been used extensively in the country and has become the main repository for storing personal data of Persons to SMS and other government organizations. The UMIS database contains around XX million records.

A new version of this system is currently being developed using the technical platform listed below:

- Microsoft .NET / MVC /
- As for the client systems, Angulat JS, Bootstrap
- As for the database, Oracle 11g

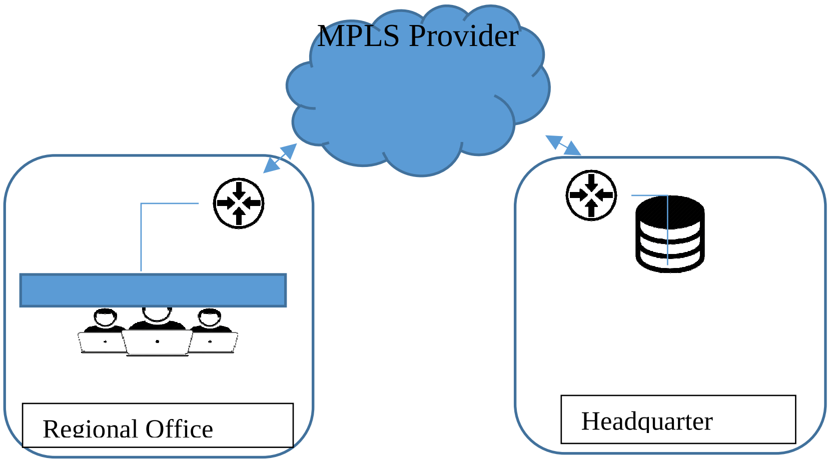
*2.4.2.1. **ICT Architecture***

The ICT Architecture section outlines the Software and Hardware Requirements, the relationships bbetween the different elements and how the System will operate in exceptional circumstances. SMS will provide ICT infrastructure and application support for all the products and technologies described in Section 2.4.2 Technical Requirements. This includes desktop computers, x64 virtual servers, storage and networking which will be configured as defined by the Supplier.

Requirement ID	**Requirement Description**	**Importance** (Must / Could / Should / Future Req)
2.4.2.1.1.	The Supplier must specify System architecture, topology, sizing and overall quantities of all ICT components for the System	
2.4.2.1.2.	The Supplier shall provide the System comprising the System Hardware, the Software and any other parts of the System (but not including those specified to be provided by SMS ("Provided Items"). The Provided Items are as follows: • Microsoft Windows Desktop Computers • Microsoft Windows Laptop and Tablet Computers • Local Area Networking based on Ethernet standard protocols. • Wide Area Networking • Microsoft Windows x64 Servers (Physical and Virtual with Microsoft Hyper-V) • Power, Cooling and other environmental facilities to operate ICT equipment	
2.4.2.1.3.	The Supplier shall ensure that the items proposed, when combined with the Provided Items shall together form the System. Any item required to make the System operational that is not included in the Provided Items shall be the responsibility of the Supplier, whether or not such item is included in the Supplier's response	
2.4.2.1.4.	The Supplier shall provide the Specifications and detailed descriptions of both the Software and Hardware that they propose to use in their response. Where any element of the System requires the Provided Items to be of a particular specification, the Supplier shall detail this	
2.4.2.1.5.	The Supplier shall provide a detailed response outlining the relationships between the elements of Hardware, Software and network components	
2.4.2.1.6.	The Supplier shall provide details regarding the relationship between functional components of the System	
2.4.2.1.7.	The Supplier should detail how the configurations will differ in High-Availability (HA) and Disaster Recovery (DR) situations	

2.4.2.2. *Wide Area Network Environment*

The following section outlines how the Supplier shall provide Hardware and Software compatible or interoperable with the specific conditions experienced on UNHCR's Wide Area Network infrastructure. Note that UNHCR's preference is not to have local servers. Should these be required, the Supplier must provide full and detailed system configuration of any local server or appliance required.

Requirement ID	**Requirement Description**	**Importance** (Must / Could / Should / Future Req)
2.4.2.2.1.	The Supplier must ensure that the System is capable of operating with the following Network Protocols: • Internet Protocols (TCP/IP, UDP, etc.) with support for both IPv4 and IPv6 • HTTPS (TLS/SSL) encryption • Network Address Translation	
2.4.2.2.2.	The Supplier must ensure that the System is capable of operating in approximately X (regional offices) selected SMS locations connected with a MPLS provider:  	

*2.4.2.3. **Data sharing***

The data (including Biometric Data) that the new System will be recording will be highly sensitive and as a result the data when being shared should be secured in accordance with Best Practices.

Requirement ID	**Requirement Description**	**Importance** (Must / Could / Should / Future Req)
2.4.2.3.1.	The Supplier shall ensure that the System processes and design should accord with ISO 27001:2013 for Information Security Management Systems	
2.4.2.3.2.	The Supplier shall ensure that any information collected concerning a Person should be stored only where and when it is needed to fulfil the approved purposes of the System	
2.4.2.3.3.	The Supplier shall ensure that all data that is transmitted by the System must be encrypted to an appropriate industry/commercial standard to avoid accidental or malicious loss of data	
2.4.2.3.4.	The Supplier shall ensure that Biometric Data is stored separately in any Database from personal data such that the impact of any loss of data is minimised	
2.4.2.3.5.	The Supplier shall ensure that any and all attempts to access, modify, duplicate or otherwise interact with data is traceable by a System Administrator with appropriate permissions	
2.4.2.3.6.	The Supplier shall ensure that the Biometric Data when transmitted can be proven to originate from an approved point and accepted by the target System	
2.4.2.3.7.	The Supplier shall ensure that the Biometric Data when transmitted can only be accessed by the intended recipient and cannot be substituted with alternative data	
2.4.2.3.8.	The Supplier shall ensure that the Biometric Data when transmitted does not suffer degradation or become irrevocably lost if there is network or power outages	
2.4.2.3.9.	System APIs/SDKs should use the BioAPI 2.0 standard or equivalent to facilitate the use of biometric devices from a range of vendors	
2.4.2.3.10.	The Supplier shall ensure that all Biometric Data is transmitted in accordance with industry standard for image quality, such as that specified in Appendix 1	

2.4.2.4. IT Security

As previously stated, the System will be capturing, transmitting and storing highly sensitive personal data. SMS will require any new System to conform to industry and commercial best practice in regard to IT Security.

Requirement ID	**Requirement Description**	**Importance** (Must / Could / Should / Future Req)
2.4.2.4.1.	The Supplier shall ensure that System resources (for example System ports) on all Hardware devices should be disabled if not required	
2.4.2.4.2.	The Supplier shall provide firewall technology for all System Hardware devices to prevent external attacks	
2.4.2.4.3.	The Supplier shall ensure that the OS and other patches should be applied in line with SMS IT security policies as provided from time to time	
2.4.2.4.4.	The Supplier shall ensure that the System allows tiered access so privileges levels can be set to reflect seniority, responsibility and allow segregation of duties	
2.4.2.4.5.	The Supplier shall ensure that the following roles are created in the System: System Administrator, Local Administrator and Operator. The System Administrator must be able to add, delete and modify roles and access levels	
2.4.2.4.6.	The Supplier shall ensure that the System allows each Operator to have a unique and individual account access protected by a strong password that conforms to ISO 27001:2013 and allows Operators to change their password when required. The System should forces Operators to re-enter a password after a period of idle time	
2.4.2.4.7.	The Supplier shall ensure that the System allows each Operator to log out at any time	
2.4.2.4.8.	The Supplier shall ensure that the System has the ability to permanently delete stored Biometric Data as required and following appropriate controls to prevent accidental deletion. The System should ensure that permanent deletion can only be performed by a level of seniority to be specified by SMS	

2.4.3. Non Functional Requirements

The Non Functional Requirements represent the Requirements that capture the quality aspects of the System plus additional Requirements not covered by the previous sections.

The Non Functional Requirements have been broken down into the following areas:

- Operational
- Training
- Reporting and Audit
- Standards
- Business Continuity and Disaster Recovery (BC/DR)

*2.4.3.1. **Operational***

SMS operate in many different environments entire the country. As such, the System must be able to be used in a variety of conditions, require limited maintenance and be operational from the date of deployment.

Requirement ID	**Requirement Description**	**Importance** (Must / Could / Should / Future Req)
2.4.3.1.1.	The System Hardware shall be capable of indicating to the relevant Operator whether its performance or functionality has deteriorated and indicating to the Operator the nature of the deterioration	
2.4.3.1.2.	Where the Supplier has the ability to diagnose or fix any element of the System remotely, these capabilities should be documented in the Supplier's response	
2.4.3.1.3.	The Supplier shall provide details of the operating parameters of the Biometric Capture Device including factors such as display interfaces, power charging method (and if by battery, the operating time between charges) and portability requirements	
2.4.3.1.4.	SMS generally operates with no support or maintenance personnel in regional offices and varying levels of technical experience among System operators. Therefore, the System should be designed to be intuitive to use and so that no specialist maintenance need to be performed by SMS personnel	
2.4.3.1.5.	The Supplier shall upon request provide setup assistance the first deployment of the System on location	
2.4.3.1.6.	The supplier should provide SLA options with detailed descriptions.	

*2.4.3.2. **Training***

The Supplier may be required to perform training for specified SMS staff and shall be required to provide manuals to ensure the System can be used successfully once in operation.

Requirement ID	**Requirement Description**	**Importance** (Must / Could / Should / Future Req)
2.4.3.2.1.	The Supplier shall ensure that members of SMS staff are trained to use the System to a level that enables them to train other SMS staff members. Such training shall be performed at SMS Headquarter and must be conducted by fully qualified members of Supplier personnel (or their relevant subcontractor personnel where applicable) and should be available in the Azerbaijan language or English, as requested by SMS	
2.4.3.2.2.	The Supplier shall provide training that covers the correct use of the Biometric Hardware and System Software, Security, integrity of the data and exceptions	
2.4.3.2.3.	The Supplier shall provide a user manual and support documentation for each unit of System Hardware/Software, to be made available in electronic or hard copy as requested	
2.4.3.2.4.	The Supplier shall ensure that each user manual and support documentation is available in English, Azerbaijan, and as an option in Russian.	

*2.4.3.3. **Management Information and Audit***

SMS will require the functionality to create and run Management Information and Audit reports that allow review and consolidation of the data and prevention of fraudulent practices. SMS will require a solution that will allow users to create, manipulate and change reports based on user rights.

Requirement ID	**Requirement Description**	**Importance** (Must / Could / Should / Future Req)
2.4.3.3.1.	The Supplier should ensure that the System can produce management information reports based on parameters as inputted by the Operators. The Supplier should ensure that the full range of audit function available with the System is specified in their response	
2.4.3.3.2.	The Supplier must allow data extracted from the System to be manipulated using a business intelligence or data warehouse interface	

Requirement ID	**Requirement Description**	**Importance** (Must / Could / Should / Future Req)
2.4.3.3.3.	The Supplier must ensure that Operators will be able to define how they want to view and distribute their reports. For example Excel or PDF or equivalent	
2.4.3.3.4.	The System must allow specified SMS personnel to access audit logs allowing them to see who has created, transmitted, viewed or deleted any data (including Biometric Data)	
2.4.3.3.5.	The Supplier must ensure that access to Management Information or Audit Logs is determined and tiered by Operator access levels, user roles / rights	
2.4.3.3.6.	The Supplier should ensure the System can produce management information reports on biometric factors such as image capture quality or biometric search times for 1:1 and 1:N biometric searches.	

2.4.3.4. ***Standards***

Requirement ID	**Requirement Description**	**Importance** (Must / Could / Should / Future Req)
2.4.3.4.1.	Proposed Systems must comply with the following International Standards. Biometric data: • ISO/IEC 19785-1:2015 - Common Biometric Exchange Formats Framework • ISO/IEC 19794 - Biometric data interchange formats (-4 / -2 templates and etc.) • BioAPI 2.0 - Biometric Application Programming Interface • SDK - Support for all popular software languages including Java, .Net, C/C++ /Andriod, etc. Security: • ISO/IEC 9594-8 - Public-key and attribute certificate frameworks • ISO 27001:2013 - Information security management systems • ISO 22301 - Business Continuity Management Systems	

2.4.3.5. *Business Continuity and Disaster Recovery*

Requirement ID	**Requirement Description**	**Importance** (Must / Could / Should / Future Req)
2.4.3.5.1.	The Supplier must provide details of it how proposes to mitigate the impact to SMS of any business continuity event during the Agreement	
2.4.3.5.2.	The Supplier must provide details of its disaster recovery capability that it will utilise during the course of the Agreement	
2.4.3.5.3.	The Supplier should provide details of any business continuity or disaster recovery strategy that relies on ISO 22301 or similar	

2.5. Use Cases

2.5.1. Enrolment Process

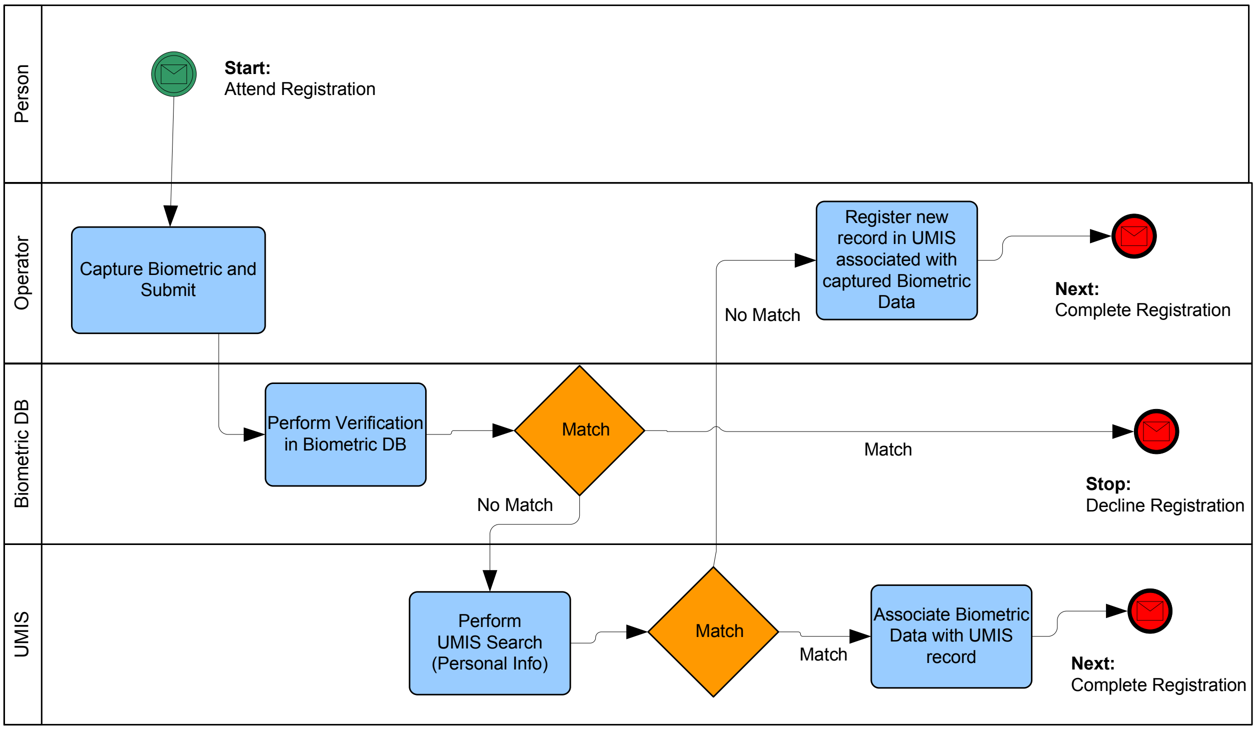
Actors: Person, Operator (Registration Point)

Step 1: Registration - Person attends registration point

Step 2: Enrolment – Operator captures biometric record and submits.

Step 3: Biometric Verification - Search Biometric Record in Biometric DB. Response received could include Match, No Match or Match under different name. If no match is found and UMIS record can not be located, operator perfomrs secondary check.

Step 4: UMIS Verification - Operator performs secondary match to UMIS database by Personal Information. If no match is found at secondary check and Person has two negative matches, Operator proceeds to complete registration. If no match was found at primary check but a match is found at secondary check (indicating Person is registered but biometric data has not been captured), biometric data captured on Biometric Capture Device could be assigned to existing record and stored in Biometric DB accordingly.


Person
Start:
Attend Registration
Operator
Capture Biometric and Submit
Register new record in UMIS associated with captured Biometric Data
No Match
Next:
Complete Registration
Biometric DB
Perform Verification in Biometric DB
Match
Match
No Match
Stop:
Decline Registration
UMIS
Perform UMIS Search (Personal Info)
Match
Match
Associate Biometric Data with UMIS record
Next:
Complete Registration

2.5.2. Verification Process

Actors: Person, Operator (Service Provision Point)

Step 1: Service Provision - Person attends service provision point

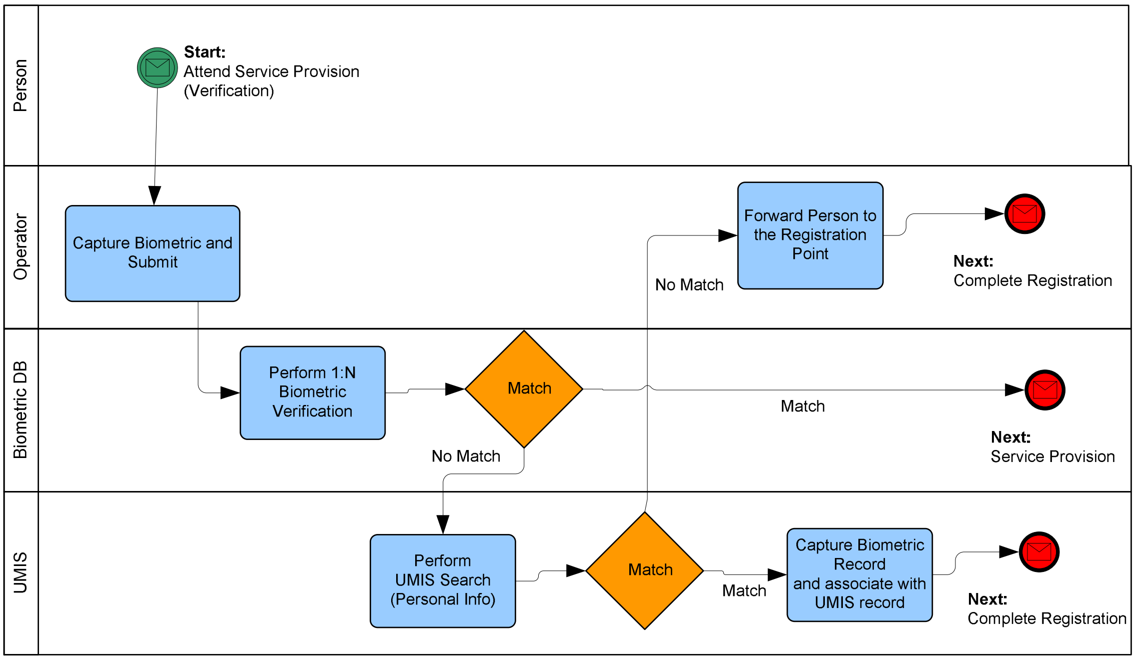
Step 2: Enrolment - Operator captures biometric record and submits.

Step 3: Biometric Verification – System should perform 1:N verification in Biometric Database. If Biometric Record is located, and operator can open the associated UMIS record then service can be provisioned to the Person. If no Biometric Record is located then operator performs a UMIS search.

Step 4: UMIS Verification - Operator performs UMIS verification against the personal information. If no UMIS record has been found, Person should be forwarded to the registration point or operator himself/herself should be available to proceed with registration.

If Person has respective UMIS record available, and indicates that no Biometric Record is held, then operator may capture biometric record and associate with respective UMIS record.

If Person has respective UMIS record available, and indicates that Biometric Record is held but this was not detected during the Biometric Verification, then operator may update biometric record and associate with respective UMIS record, in case operator satisfied of the identity or perform further investigation.


Person
Operator
Biometric DB
UMIS
Start:
Attend Service Provision
(Verification)
Capture Biometric and Submit
Forward Person to the Registration Point
No Match
Next:
Complete Registration
Perform 1:N Biometric Verification
Match
Match
No Match
Next:
Service Provision
Perform UMIS Search (Personal Info)
Match
Match
Capture Biometric Record and associate with UMIS record
Next:
Complete Registration

APPENDIX 1: Quality Requirements

In this section, the following terms are taken to be equivalent and FPIR and FNIR are used for both enrolment and verification:

A) False Accept Rate FAR (% of incorrect verifications); False Positive Identification Rate FPIR
B) False Reject Rate FRR; False Negative Identification Rate FNIR

Operating principles

SMS requires the balance of the system to be towards high accessibility rather than high security, while maximising the quality of biometric data in the system.

Indicative quality requirements* for enrolment

FPIR – c. 1% or lower
FNIR – c. 0.1% or better (FNIR and FPIR are inter-dependent)
Failure To Enroll Rate: Not specified but to be minimized by the solution

*The Supplier should stipulate the exact FPIR, FNIR and FTER of the System they have proposed

False positives will require additional identification steps being required. Following these it will be necessary to enroll the Person's biometrics and associate with the UMIS record to ensure their access to services.

False negatives will result in duplicate enrolments, possibly with different associated identities, requiring subsequent operations to resolve.

Failures To Enroll are highly undesirable and must be minimized by technical and procedural design aspects of the solution.

Indicative quality requirements** for verification

A low False Negative Identification Rate is required at Verification to avoid denying services to legitimate Persons. In order to achieve that, a relatively high False Accept/Match Rate is acceptable. The indicative Quality Requirement 'targets' for the System at Verification are:

FNIR – c. 0.01% or lower (the priority)
FPIR – c. 1% or lower

**The Supplier should stipulate the exact FNIR and FPIR of the System they have proposed

Performance: 1-N matching time

For the System you are proposing please specify and include in your response how long it will take to provide a 1-N match based on differing numbers of Biometric Records in the Database. Please specify the assumptions that underpin the data, for example speed of connection and specification of matching solution.

No of Biometric Records (N)	1-N Match time against Database (mins:secs) for Fingerprints	1-N Match time against Database (mins:secs) for Facial Recognition	1-N Match time against Database (mins:secs) for Multi-Modal
100,000			
250,000			
500,000			
1,000,000			
2,500,000			

Performance: 1:1 matching time

For the System you are proposing please specify and include in your response how long it will take to provide a 1:1 match result based on differing numbers of Biometric Records in the Database. Please specify the assumptions that underpin the data, for example speed of connection and specification of matching solution.

No of Biometric Records (N)	1-1 Match time against Database (mins:secs) for Fingerprints	1-1 Match time against Database (mins:secs) for Facial Recognition	1-1 Match time against Database (mins:secs) for Multi-Modal
100,000			
250,000			
500,000			
1,000,000			
2,500,000			

APPENDIX 2: Supplier Reponse Form

The compliance matrix template below details the format for the Supplier’s compliance matrix. The Supplier must ensure that each Requirement is addressed and their explanation of how this will be met is documented.

Requirement ID	Supplier Response	Requirement Status
[INSERT	[DETAIL RESPONSE TO THE REQUIREMENT]	[INSERT EITHER

Requirement ID	Supplier Response	Requirement Status
REQUIREMENT ID]		“*FULLY COMPLIANT*”, “*PART COMPLIANT*” OR “*NONCOMPLIANT*”]

Abbreviations and Acronyms

Definition	Description
IAISS	Entry-Exit and Registration Interagency Automated Information Search System
SRP	State Registry of the Population
UMIS	Unified Migration Information Service
SMS	State Migration Service
Person	Shall mean the Person which the Biometric Data will be enrolled
System	Shall mean all the components of the Biometric Information System
Enrolment	Shall mean the process of capturing the Biometric Data belonging to a Person, creating a Biometric Record and storing it in the System
Verification	Shall mean the process of determining whether or not the Biometric Data relating to the relevant Person is held in the System or not, either through a 1:1 search, a 1:N search or an N:N search
Supplier	Shall mean the party who has been selected to perform and fulfil the contracted requirements
Biometric Data	Shall mean the biometric data belonging to a Person that is captured by the Biometric Capture Device
Biometric Record	Shall mean the record in the Database containing the Biometric Data belonging to an individual Person that is associated to a UMIS record through the UMIS numeric identifier
NFIQ	NFIQ is a machine learning algorithm
FPIR	False Positive Identification Rate
FNIR	False Negative Identification Rate
FAR	False Accept Rate
TAR	True Accept rate
FRR	False Reject Rate
~~PRPIC~~	~~Permanent Residence Permit Identity Card~~
~~TRPIC~~	~~Temporary Residence Permit Identity Card~~
~~RTD~~	~~Refugee Travel Document~~
~~RIDC~~	~~Refugee ID Card~~
~~MLI~~	~~Multiple Laser Image~~
~~CLI~~	~~Changeable Laser Image~~
BC	Business Continuity
DR	Disaster Recovery

~~**APPENDIX 3: Smart Card Descriptions & Specification**~~

~~*3. Smart Cards*~~

~~This appendix describes description and specification of Smart Cards. Supplier should provide card examples comply with below described requirements.~~

~~*3.1. Description*~~

~~3.1.1. Temporary Residence Permit Identity Card (TRPIC) should comply with ICAO 9303 document~~

- ~~Color – Light Green~~
- ~~Dimensions - 85,6 mm x 54 mm~~

~~3.1.2. Permanent Residence Permit Identity Card (PRPIC) should comply with ICAO 9303 document~~

- ~~Color – Light Blue~~
- ~~Dimensions - 85,6 mm x 54 mm~~

~~3.1.3. On the front side of the card, top left area should include the biometric photo of the card holder with the dimensions of 26 mm x 32 mm. Photo shuold comply with ICAO 9303 document. At the buttom of card holders photo, validity period of card should be indicated and small CLI (Changeable Laser Image) photo of card holder should be engraved.~~

~~3.1.4. Front side of the card:~~

~~3.1.4.1. Top left corner: Colored flag of Azerbaijan Republic should be engraved~~

~~3.1.4.2. After the flag, the following wordings should be written in both Azerbaijan and English languages~~

- ~~For (PRPIC)~~
  - ~~“AZƏRBAYCAN RESPUBLİKASININ ƏRAZİSİNDƏ DAİMİ YAŞAMAQ ÜÇÜN İCAZƏ VƏSİQƏSİ”~~
  - ~~Under above wordings, “PERMIT FOR PERMANENT RESIDENCE IN THE TERRITORY OF THE REPUBLIC OF AZERBAIJAN”~~
- ~~For (TRPIC)~~
  - ~~“AZƏRBAYCAN RESPUBLİKASININ ƏRAZİSİNDƏ MÜVƏQQƏTİ YAŞAMAQ ÜÇÜN İCAZƏ VƏSİQƏSİ”~~
  - ~~Under above wordings, “PERMIT FOR TEMPORARY RESIDENCE IN THE TERRITORY OF THE REPUBLIC OF AZERBAIJAN”~~

~~3.1.4.3. Top right corner: special sign for indicating that card holds an electronic carrier~~

~~3.1.4.4. The following wordings at middle of the card:~~

- ~~“SOYADI/SURNAME”;~~
- ~~“ADI/GIVEN NAME”;~~
- ~~“CİNSİ/SEX”;~~
- ~~“VƏTƏNDAŞLIĞI/ NATIONALITY”;~~
- ~~“DOĞULDUĞU TARİX/DATE OF BİRTH”;~~
- ~~“VƏSİQƏNİN NÖMRƏSİ/CARD NO” (two letters and seven numbers);~~

- ~~“FƏRDİ İDENTİFİKASİYA NÖMRƏSİ/PERSONAL NO”;~~
- ~~“ETİBARLILIQ MÜDDƏTİ/DATE OF EXPİRY”;~~
- ~~“VƏSİQƏ SAHİBİNİN İMZASI/HOLDER’S SIGNATURE”;~~

~~3.1.5. Back side of the card:~~

~~3.1.5.1. On the top the following wordings should be written in both Azerbaijan and English languages~~

- ~~“Bu vəsiqə əcnəbilərə və ya vətəndaşlığı olmayan şəxslərə Azərbaycan Respublikasının ərazisində daimi yaşamaq üçün icazə və etibarlılıq müddətində Azərbaycan Respublikasından getmək və viza almadan Azərbaycan Respublikasına qayıtmaq hüququ verən, habelə həmin şəxslərin ölkə ərazisində şəxsiyyətini və yaşayış yeri üzrə qeydiyyata alındığını təsdiq edən sənəddir./This card is a document authorizing foreigners and stateless persons to reside in the territory of the Republic of Azerbaijan permanently and exit from the Republic of Azerbaijan and return back under visa free regime within its validity period, as well as certifying identity and registration of those persons upon place of residence in the territory of the country.”~~

~~3.1.5.2. The following wordings at middle of the card:~~

- ~~“QAN QRUPU/BLOOD GROUP”;~~
- ~~“VERİLMƏ TARİXİ/DATE OF İSSUE”;~~
- ~~“DOĞULDUĞU YER/PLACE OF BIRTH;~~
- ~~“VƏSİQƏNİ VERƏN ORQAN/AUTHORITY”;~~

~~3.1.5.3. At the bottom of the card 3 lane Machine Readable Optic Zone is required comply with ICAO requirements.~~

~~3.1.5.4. Following personal information shall be indicated within the Card both in Azerbaijan and English languages:~~

- ~~Persons Name~~
- ~~Persons Surname~~
- ~~Place and Date of Birth~~
- ~~Citizenship~~
- ~~Card Issued Organization~~
- ~~Sex (male K/M or female Q/F)~~

~~3.1.5.5. Information within the electronic carrier should be in Azerbaijan language and as an ICAO requirement in English.~~

~~3.1.5.6. State symbols and map of Azerbaijan Republic should be engraved within the card~~

~~*3.2. Specification*~~

~~3.2.1 Smart Card:~~

- ~~With lectronic chip~~
- ~~High quality polycarbonate material~~
- ~~Resistant to the high temperature, light, deformation, impact of chemicals and moisture~~
- ~~does not produce toxic substances when used~~
- ~~ability to prevent forgery~~

~~3.2.2 Electronic carrier of the smart card enables to write, change and read the information~~

~~3.2.3 Security items and methods should be used during the printing:~~

- ~~Country code – AZE~~
- ~~Rainbow printing~~
- ~~Ultraviolet printing~~
- ~~Laser engravement~~
- ~~Microtext and other secure elements~~

~~3.2.4 The state symbols of Azerbaijan Republic should be included within the card, which shall be visible under the ultraviolet light.~~

~~3.2.5 Thickness of the card shall be 0,76 mm, and corners of the card rounded by 3,18 mm radius.~~

~~3.2.6 The storage of the dual interface electronic carrier of the card shall be at least 80 kb. Electronic carrier shall hold the following information of the person:~~

- ~~Biometric photo~~
- ~~One fingerprint from each hand. (for the persons older than 15 years old)~~
- ~~Name of the Azerbaijan republic~~
- ~~State symbol~~
- ~~Country code~~
- ~~Card number~~
- ~~Card holders~~
  - ~~Name, Surname, father name~~
  - ~~Citizenship~~
  - ~~Date and place of birth~~
  - ~~Sex~~
  - ~~Personal identification number~~
  - ~~Height / Eye color / Blood group~~
  - ~~Adress~~
  - ~~Special signs (inabilities, missing fingers etc.)~~
  - ~~Housbands (wifes) surname, name~~
- ~~Card issued organization name~~
- ~~Card issued date~~
- ~~Card validity period~~

~~3.2.7 Electronic carrier shall comply with Basic Access Control, Passiv Authentication, Extended Access Control and complience certificate with CC EAL 5+.~~

~~3.2.8 In order to ensure the security of the information within the electronic carrier, electronic signature technology and cryptographic algoritms shall be imlemented.~~

Monitoring and Evaluation

4.1 Analytics

Before the implementation the contractor should provide the analyst or a group of analysts who need to analyze all the tasks and all the necessary business processes internally.

4.2 Project management

Before starting of development, the project the Project Manager has to provide a detailed activity plan (Gantt chart) and provide the implementation and controlling of the project in further. The project should be accompanied by full instructions on the administration and usage of the software and documentation describing the source code. Also at the completion of the project the contractor delivers all the source code and necessary documents.

Section V – Pro-forma Contract

FPU.SF.19.20

IOM office-specific Ref. No.:	
IOM Project Code:	
LEG Approval Code / Checklist Code	

SERVICE AGREEMENT
Between
the International Organization for Migration
And
[Name of the Service Provider]
On
[Type of Services]

This Service Agreement is entered into by the **International Organization for Migration,** Mission in *[XXX]*, *[Address of the Mission],* represented by *[Name, Title of Chief of Mission etc.]*, hereinafter referred to as "**IOM**," and ***[Name of the Service Provider]***, *[Address]*, represented by *[Name, Title of the representative of the Service Provider]*, hereinafter referred to as the "**Service Provider**." IOM and the Service Provider are also referred to individually as a "**Party**" and collectively as the "**Parties**."

1. Introduction and Integral Documents

The Service Provider agrees to provide IOM with *[insert brief description of services]* in accordance with the terms and conditions of this Agreement and its Annexes, if any.

The following documents form an integral part of this Agreement: *[add or delete as required]*

*(a) **Annex A** - Bid/Quotation Form*
*(b) **Annex B** - Price Schedule*
*(c) **Annex C** - Delivery Schedule and Terms of Reference*
*(d) **Annex D** - Accepted Notice of Award (NOA)*

2. Services Supplied

2.1 The Service Provider agrees to provide to the IOM the following services (the "**Services**"):

[Outline services to be provided. Where relevant, include location and how frequently etc. services are to be provided. List all the deliverables and their date of submission, if applicable. Description needs to be as detailed as possible to provide for a reliable yardstick to measure compliance. It may be necessary to attach a description of the Services as an Annex.]

2.2 The Service Provider shall commence the provision of Services from *[date]* and fully and satisfactorily complete them by *[date]*.

2.3 The Service Provider agrees to provide the Services required under this Agreement in strict accordance with the specifications of this Article and any attached Annexes.

3. Charges and Payments

3.1 The all-inclusive Service fee for the Services under this Agreement shall be *[currency code] [amount in numbers] ([amount in words])*, which is the total charge to IOM.

3.2 The Service Provider shall invoice IOM upon completion of all the Services. The invoice shall include: *[services provided, hourly rate, number of hours billed, any travel and out of pocket expenses, (add/delete as necessary)]*

3.3 Payments shall become due *[insert number of days in numbers] ([write figure in words])* days after IOM's receipt and approval of the invoice. Payment shall be made in *[Currency code]* by *[bank transfer]* to the following bank account: *[insert the Service Provider's bank account details]*.

3.4 The Service Provider shall be responsible for the payment of all taxes, duties, levies and charges assessed on the Service Provider in connection with this Agreement.

3.5 IOM shall be entitled, without derogating from any other right it may have, to defer payment of part or all of the Service fee until the Service Provider has completed to the satisfaction of IOM the services to which those payments relate.

4. **Warranties**

4.1 The Service Provider warrants that:

(a) It is a company financially sound and duly licensed, with adequate human resources, equipment, competence, expertise and skills necessary to provide fully and satisfactorily, within the stipulated completion period, all the Services in accordance with this Agreement;
(b) It shall comply with all applicable laws, ordinances, rules and regulations when performing its obligations under this Agreement;
(c) In all circumstances it shall act in the best interests of IOM;
(d) No official of IOM or any third party has received from, will be offered by, or will receive from the Service Provider any direct or indirect benefit arising from the Agreement or award thereof;
(e) It has not misrepresented or concealed any material facts in the procurement of this Agreement;
(f) The Service Provider, its staff or shareholders have not previously been declared by IOM ineligible to be awarded agreements by IOM;
(g) It has or shall take out relevant insurance coverage for the period the Services are provided under this Agreement;
(h) It shall abide by the highest ethical standards in the performance of this Agreement, which includes not engaging in any discriminatory or exploitative practice or practice inconsistent with the rights set forth in the Convention on the Rights of the Child;
(i) The Price specified in Article 3.1 of this Agreement shall constitute the sole remuneration in connection with this Agreement. The Service Provider shall not accept for its own benefit any trade commission, discount or similar payment in connection with activities pursuant to this Agreement or the discharge of its obligations thereunder. The Service Provider shall ensure that any subcontractors, as well as the personnel and agents of either of them, similarly, shall not receive any such additional remuneration.

4.2 The Service Provider further warrants that it shall:

a) Take all appropriate measures to prohibit and prevent actual, attempted and threatened sexual exploitation and abuse (SEA) by its employees or any other persons engaged and controlled by it to perform activities under this Agreement (“other personnel”). For the purpose of this Agreement, SEA shall include:
   1. Exchanging any money, goods, services, preferential treatment, job opportunities or other advantages for sexual favours or activities, including humiliating or degrading treatment of a sexual nature; abusing a position of vulnerability, differential power or trust for sexual purposes, and physical intrusion of a sexual nature whether by force or under unequal or coercive conditions.
   2. Engaging in sexual activity with a person under the age of 18 (“child”), except if the child is legally married to the concerned employee or other

personnel and is over the age of majority or consent both in the child’s country of citizenship and in the country of citizenship of the concerned employee or other personnel.

b) Strongly discourage its employees or other personnel having sexual relationships with IOM beneficiaries.

c) Report timely to IOM any allegations or suspicions of SEA, and investigate and take appropriate corrective measures, including imposing disciplinary measures on the person who has committed SEA.

d) Ensure that the SEA provisions are included in all subcontracts.

e) Adhere to above commitments at all times. Failure to comply with (a)-(d) shall constitute grounds for immediate termination of this Agreement.

4.3 The above warranties shall survive the expiration or termination of this Agreement.

5. Assignment and Subcontracting

5.1 The Service Provider shall not assign or subcontract the activities under this Agreement in part or all, unless agreed upon in writing in advance by IOM. Any subcontract entered into by the Service Provider without approval in writing by IOM may be cause for termination of the Agreement.

5.2 In certain exceptional circumstances by prior written approval of IOM, specific jobs and portions of the Services may be assigned to a subcontractor. Notwithstanding the said written approval, the Service Provider shall not be relieved of any liability or obligation under this Agreement nor shall it create any contractual relation between the subcontractor and IOM. The Service Provider remains bound and liable thereunder and it shall be directly responsible to IOM for any faulty performance under the subcontract. The subcontractor shall have no cause of action against IOM for any breach of the subcontract.

6. Delays/Non-Performance

6.1 If, for any reason, the Service Provider does not carry out or is not able to carry out its obligations under this Agreement and/or according to the project document, it must give notice and full particulars in writing to IOM as soon as possible. In the case of delay or non-performance, IOM reserves the right to take such action as in its sole discretion is considered to be appropriate or necessary in the circumstances, including imposing penalties for delay or terminating this Agreement.

6.2 Neither Party will be liable for any delay in performing or failure to perform any of its obligations under this Agreement if such delay or failure is caused by *force majeure*, such as civil disorder, military action, natural disaster and other circumstances which are beyond the control of the Party in question. In such event, the Party will give immediate notice in writing to the other Party of the existence of such cause or event and of the likelihood of delay.

7. **Independent Contractor**

The Service Provider shall perform all Services under this Agreement as an independent contractor and not as an employee, partner, or agent of IOM.

8. **Audit**

The Service Provider agrees to maintain financial records, supporting documents, statistical records and all other records relevant to the Services in accordance with generally accepted accounting principles to sufficiently substantiate all direct and indirect costs of whatever nature involving transactions related to the provision of Services under this Agreement. The Service Provider shall make all such records available to IOM or IOM's designated representative at all reasonable times until the expiration of 7 (seven) years from the date of final payment, for inspection, audit, or reproduction. On request, employees of the Service Provider shall be available for interview.

9. **Confidentiality**

All information which comes into the Service Provider’s possession or knowledge in connection with this Agreement is to be treated as strictly confidential. The Service Provider shall not communicate such information to any third party without the prior written approval of IOM. The Service Provider shall comply with IOM Data Protection Principles in the event that it collects, receives, uses, transfers or stores any personal data in the performance of this Agreement. These obligations shall survive the expiration or termination of this Agreement.

10. **Intellectual Property**

All intellectual property and other proprietary rights including, but not limited to, patents, copyrights, trademarks, and ownership of data resulting from the performance of the Services shall be vested in IOM, including, without any limitation, the rights to use, reproduce, adapt, publish and distribute any item or part thereof.

11. **Notices**

Any notice given pursuant to this Agreement will be sufficiently given if it is in writing and received by the other Party at the following address:

International Organization for Migration (IOM)

Attn: *[Name of IOM contact person]*

[IOM's address]

Email: *[IOM's email address]*

[Full name of the Service Provider]

Attn: *[Name of the Service Provider's contact person]*

[Service Provider's address]

Email: *[Service Provider's email address]*

12. Dispute resolution

12.1. Any dispute, controversy or claim arising out of or in relation to this Agreement, or the breach, termination or invalidity thereof, shall be settled amicably by negotiation between the Parties.

12.2. In the event that the dispute, controversy or claim has not been resolved by negotiation within 3 (three) months of receipt of the notice from one party of the existence of such dispute, controversy or claim, either Party may request that the dispute, controversy or claim is resolved by conciliation by one conciliator in accordance with the UNCITRAL Conciliation Rules of 1980. Article 16 of the UNCITRAL Conciliation Rules does not apply.

12.3. In the event that such conciliation is unsuccessful, either Party may submit the dispute, controversy or claim to arbitration no later than 3 (three) months following the date of termination of conciliation proceedings as per Article 15 of the UNCITRAL Conciliation Rules. The arbitration will be carried out in accordance with the 2010 UNCITRAL arbitration rules as adopted in 2013. The number of arbitrators shall be one and the language of arbitral proceedings shall be English, unless otherwise agreed by the Parties in writing. The arbitral tribunal shall have no authority to award punitive damages. The arbitral award will be final and binding.

12.4. The present Agreement as well as the arbitration agreement above shall be governed by internationally accepted general principles of law and by the terms of the present Agreement, to the exclusion of any single national system of law that would defer the Agreement to the laws of any given jurisdiction. Internationally accepted general principles of law shall be deemed to include the UNIDROIT Principles of International Commercial Contracts. Dispute resolution shall be pursued confidentially by both Parties. This Article survives the expiration or termination of the present Agreement.

13. Use of IOM Name

The official logo and name of IOM may only be used by the Service Provider in connection with the Services and with the prior written approval of IOM.

14. Status of IOM

Nothing in this Agreement affects the privileges and immunities enjoyed by IOM as an intergovernmental organization.

15. Guarantee and Indemnities

15.1 The Service Provider shall guarantee any work performed under this Agreement for a period of 12 (twelve) months after final payment by IOM under this Agreement.

15.2 The Service Provider shall at all times defend, indemnify, and hold harmless IOM, its officers, employees, and agents from and against all losses, costs, damages and expenses (including legal fees and costs), claims, suits, proceedings, demands and liabilities of any kind or nature to the extent arising out of or resulting from acts or omissions of the Service Provider or its employees, officers, agents or subcontractors, in the performance of this Agreement. IOM shall promptly notify the Service Provider of any written claim, loss, or demand for which the Service Provider is responsible under this clause. This indemnity shall survive the expiration or termination of this Agreement.

16. Waiver

Failure by either Party to insist in any one or more instances on a strict performance of any of the provisions of this Agreement shall not constitute a waiver or relinquishment of the right to enforce the provisions of this Agreement in future instances, but this right shall continue and remain in full force and effect.

17. Termination

17.1 IOM may terminate this Agreement at any time, in whole or in part.

17.2 In the event of termination of this Agreement, IOM will only pay for the Services completed in accordance with this Agreement unless otherwise agreed. Other amounts paid in advance will be returned to IOM within 7 (seven) days from the date of termination.

17.3 Upon any such termination, the Service Provider shall waive any claims for damages including loss of anticipated profits on account thereof.

18. **Severability**

If any part of this Agreement is found to be invalid or unenforceable, that part will be severed from this Agreement and the remainder of the Agreement shall remain in full force.

19. **Entirety**

This Agreement embodies the entire agreement between the Parties and supersedes all prior agreements and understandings, if any, relating to the subject matter of this Agreement.

20. Special Provisions (Optional)

Due to the requirements of the Donor financing the Project, the Implementing Partner shall agree and accept the following provisions:

[Insert all donor requirements which must be flown down to IOM's implementing partners and subcontractors. In case of any doubt, please contact LEGContracts@iom.int]

21. **Final clauses**

21.1 This Agreement will enter into force upon signature by both Parties. It will remain in force until completion of all obligations of the Parties under this Agreement unless terminated earlier in accordance with Article 17.

21.2 Amendments may be made by mutual agreement in writing between the Parties.

Signed in duplicate in English, on the dates and at the places indicated below.

For and on behalf of
The International Organization
for Migration

Signature

____

Name
Position
Date
Place

For and on behalf of
[Full name of the Service Provider]

Signature

____

Name
Position
Date
Place