UPU UNIVERSAL POSTAL UNION

Call for tenders

Migration of on-premises database to a cloud managed solution

24 March 2025

Table of contents Page

Table of contents (cont.) Page

1 Introduction

1.1 Profile of the UPU

The Universal Postal Union (UPU) was founded in 1874 in Berne, Switzerland, with the main goals of establishing a single postal territory for the reciprocal exchange of letter-post items and adopting common principles for the international postal service in a non-discriminatory manner. Currently comprising 192 member countries, the UPU became a specialized agency of the United Nations in 1948.

The main mission of the UPU is to stimulate the lasting development of efficient and accessible universal postal services of quality, in order to facilitate communication between the inhabitants of the world. It does this by guaranteeing the free circulation of items over a single postal territory composed of interconnected networks, encouraging the adoption of fair common standards and the use of technology, ensuring cooperation and interaction among stakeholders, promoting effective technical cooperation, and ensuring the satisfaction of customers' changing needs. The UPU is thus expected to play a major role in the continued revitalization of postal services.

Furthermore, the UPU facilitates the development of worldwide postal services by providing an information and communication technology framework that allows the designated operators[1] of UPU member countries to concentrate on the delivery of postal services to their customers. In this context, the UPU provides a global network with value-added services, as well as computerized applications for the management of international mail and international postal money orders.

2 Terms and conditions

Unless otherwise indicated in this call for tenders, the term "Bidder" shall refer to any person, company or legal entity submitting a proposal in response to this call for tenders. The term "Vendor" shall refer to any selected bidder.

2.1 Confidentiality

Bidders shall treat in strict confidence all information contained in this call for tenders and its attached documents that is not already publicly known or generally accessible, particularly any documentation marked as confidential and distributed by the UPU to Bidders as additional confidential tender documentation. Bidders shall prevent the disclosure or distribution of all such information to third parties and other entities and persons not expressly authorized herein. In case of doubt, these confidentiality provisions shall nevertheless be observed. All Bidders are obliged to observe these confidentiality provisions before, during and after the tender process. These provisions shall not affect the legal obligations of the UPU and Bidders to disclose information.

Bidders shall not use such information for any purposes other than those associated with this call for tenders. The call for tenders and all attached documents may be distributed or made available only to persons directly involved in the tender process on behalf of Bidders. If external agents or subcontractors are involved in the preparation of the tender documents, this must be indicated and their names provided in the participation notification (see section 2.14).

Bidders shall assume full responsibility for the compliance of their agents, consultants, employees and subcontractors, as well as any third parties involved on their behalf in this tender process, with these rules of confidentiality, and shall be liable for any damages resulting from misconduct or unauthorized disclosure.

If a Bidder violates the confidentiality provisions contained herein, it shall be liable to pay a penalty to the UPU unless it can prove that no fault is attributable to it. This penalty shall not exceed 50,000 CHF per infringement. Payment of any such penalties shall not release Bidders from their obligation to observe these confidentiality requirements.

[1] In accordance with article 2.1.6 of the UPU Constitution, a designated operator is any governmental or non-governmental entity officially designated by the member country to operate postal services and to fulfil the related obligations arising out of the Acts of the Union on its territory.

Bidders wishing to submit a proposal in response to this call for tenders must contact the person(s) specified in section 2.15 below and may, if necessary, request additional information from the UPU in relation to this call for tenders.

Without prejudice to the confidentiality provisions set out above, Bidders agree that the receipt of any such information may be subject to the prior signature of a non-disclosure agreement between the Bidder and the UPU, under conditions to be determined and communicated by the latter.

2.2 Legal status of the Vendor

The Vendor shall be regarded as having, in law, the legal status of independent contractor. The Vendor and its agents, consultants, employees and subcontractors (as authorized by the UPU) shall in no way be regarded as employees of the UPU. Such agents, consultants, employees and subcontractors of the Vendor shall not be entitled to any employment benefits from the UPU. The Vendor alone shall be responsible for due payment of all compensation owed to such agents, consultants, employees and subcontractors, including payment of any employment taxes, benefits, compensation and insurance. The Vendor shall represent and warrant that it will comply with all laws, rules and regulations required by the relevant authorities, including the appropriate withholding, reporting and payment of all necessary taxes.

The Vendor shall be liable for all work performed, including any acts or omissions, by its agents, consultants, employees and subcontractors.

2.3 Scope of the call for tenders

This call for tenders concerns the migration of an on-premises database to the cloud, hosting of the associated data and provision of support services and training for a period of three years. The database in question contains the data for the UPU's Global Monitoring System (GMS), which is used for the tracking of postal items, receptacles and assets.

2.4 Background

The growth of the global e-commerce market has led to a significant increase in international postal volumes. Accordingly, the UPU's GMS programme anticipates substantial growth in data collection requirements as a result of:

– expansion of the RFID unit network;

– growing demand for real-time parcel tracking;

– increasing need for data-driven operational insights;

– significant increases in package volumes.

The management of the expanding data ecosystem is becoming increasingly challenging for the current on-premises data storage infrastructure. To effectively address this challenge, the UPU requires a modern cloud-based data warehousing solution that can:

– automatically scale to accommodate fluctuating traffic patterns;

– dynamically expand storage capacity as data volumes grow;

– maintain consistent performance under varying loads;

– ensure reliable data access for all Union member countries;

– support advanced analytics capabilities.

By transitioning to a cloud managed solution, the UPU seeks to ensure seamless data management, improve operational efficiency and maintain high service standards for Union member countries and their customers, regardless of seasonal variations or long-term growth in postal volumes.

2.5 Objectives

The UPU seeks a qualified contractor to oversee and execute the migration of its existing on-premises database infrastructure to a cloud-based environment. This strategic initiative is aimed at addressing the growing need for enhanced scalability, reliability and performance in managing the UPU's expanding RFID data storage requirements.

The Vendor will be responsible for planning, managing and implementing the migration process to ensure minimal disruption to ongoing operations. This will involve a comprehensive assessment of the current database environment, development of a robust migration strategy and execution of the migration, while adhering to industry best practices and UPU standards.

The key objectives of the project include:

– enhanced scalability: establish a flexible and scalable cloud-based solution capable of accommodating the increasing volume of data generated by the UPU's global operations, particularly during peak periods;

– improved data accessibility and performance: enable faster and more reliable access to data while optimizing the performance of database systems to meet operational demands;

– cost efficiency and maintenance reduction: reduce the cost and complexity of maintaining physical data centres and ensure cost-effective use of cloud resources;

– security and compliance: implement advanced cloud security measures to safeguard data integrity, privacy and compliance with international standards and regulations;

– future-readiness: lay the groundwork for seamless integration with emerging technologies and evolving UPU data requirements.

The Vendor will also be expected to provide post-migration support, including system monitoring, issue resolution and knowledge transfer to UPU personnel to ensure smooth adaptation to the new cloud environment.

2.6 Use of subcontractors

The Vendor shall not assign, sublicense, subcontract, pledge or otherwise transfer or dispose of its tender, or any of the rights and obligations contained therein or in an associated contract with the UPU, without the prior written consent of the UPU.

The approval by the UPU of the engagement of any subcontractor shall not relieve the Vendor of any of its obligations or responsibilities concerning the work performed by such subcontractors.

2.7 Use of the emblem, name and initials of the UPU

Bidders shall not advertise or otherwise make public the fact that they intend to provide, are providing or have provided services to the UPU, or use the emblem, name or initials of the UPU in connection with their business for purposes of commercial advantage or goodwill, without prior and explicit permission from the UPU. Bidders shall take all reasonable measures to ensure compliance with this provision by their agents, consultants, employees and subcontractors.

2.8 Collusive bidding, anti-competitive practices and any other similar conduct

Without prejudice to the provisions in sections 3 and 4 below, Bidders (including their agents, consultants, employees and subcontractors) shall not engage in any collusive bidding, anti-competitive practices or any other similar conduct in relation to:

– the preparation and submission of tenders;

– the clarification of tenders;

– the conduct and content of any negotiations, including final contract negotiations.

For the purposes of this call for tenders, collusive bidding, anti-competitive practices and any other similar conduct may include the disclosure to, or exchange or clarification with, any other Bidder of information (in any form), whether or not such information is confidential to the UPU or to any other Bidder, in order to alter the results of the call for tenders in such a way that would lead to an outcome other than that which would have been obtained through a competitive process. In addition to any other remedies available to it, the UPU may, at its sole discretion, immediately reject any tender submitted by a Bidder that, in the UPU's opinion, has engaged in any collusive bidding, anti-competitive practices or any other similar conduct with any other Bidder in relation to the preparation or submission of tenders, whether with respect to this call for tenders or other procurement processes conducted by the UPU.

2.9 Intellectual property

This call for tenders and all its attached documents, including any content, forms, statements, concepts, projects and procedures explicitly or implicitly forming part of the call for tenders, constitute the exclusive intellectual property of the UPU. This call for tenders is communicated to the various Bidders with the sole purpose of assisting them in the preparation of their respective tenders. Any hard copies of this call for tenders shall be destroyed or returned to the UPU by unsuccessful Bidders at the request of the UPU.

2.10 Privileges and immunities

Nothing in or relating to this call for tenders, the activities described herein or any potential agreements related thereto shall be deemed as a waiver, expressed or implied, of any of the privileges, immunities and facilities that the UPU enjoys as a specialized agency of the United Nations system, pursuant to the Swiss Host State Act and the Agreement on Privileges and Immunities of the United Nations (on Swiss territory), the Convention on the Privileges and Immunities of the Specialized Agencies (outside Switzerland), and any other conventions and laws recognizing and/or granting such privileges, immunities and facilities to the UPU and its officials (such as the International Organizations Immunities Act in the case of the United States of America).

Accordingly, the Vendor shall expressly acknowledge and agree that the property and assets of the UPU, including any archives, data, documents and funds belonging to the UPU or held by it (including, without limitation, the data/hosting environments and servers pertaining to or associated with the provision of the services, as well as any data or documents in any form belonging to or held by the UPU on behalf of UPU member countries and their designated operators), are inviolable and shall be immune from search, requisition, confiscation, expropriation and any other form of interference, whether through executive, administrative, judicial or legislative action. The Vendor shall immediately contact the UPU in the event of any attempt to violate or any violation of the UPU's privileges and immunities, and shall take all reasonable measures to prevent such violations.

In the light of the UPU's status as a specialized agency of the United Nations (and without prejudice to the observance, by the UPU, of any sanctions established by the United Nations Security Council), Bidders shall expressly certify their legal and operational willingness and ability to provide the services on a non-discriminatory basis for the benefit of all eligible entities established and/or situated in the territory of any UPU member country, irrespective of the existence of diplomatic relations between a Bidder's country of incorporation and/or operation and any UPU member country (including its designated operators).

2.11 Tax exemption

Pursuant to article III, section 9, of the Convention on the Privileges and Immunities of the Specialized Agencies, the UPU is exempt from all direct taxes and from customs restrictions, duties and charges of a similar nature in respect of articles imported or exported for its official use.

Furthermore, as an intergovernmental organization and a specialized agency of the United Nations, the UPU is exempt from value-added tax (VAT) in Switzerland (OLTVA, article 22; *Instructions 2001 sur la TVA*, articles 574, 816 and others), as well as in other countries. Therefore, all prices shall be indicated in "net" form, without VAT or similar taxes.

2.12 Language

Bidders must submit all tender documents entirely in English].

2.13 Signature

Tender documents shall be signed by a representative (or representatives) duly designated and authorized to act on the Bidder's behalf and with the authority to legally bind the Bidder and accept the terms and conditions of this call for tenders.

2.14 Participation notification

Upon receipt of this call for tenders, Bidders shall send confirmation of participation to the contact person(s) listed in section 2.15, in line with the deadline indicated in section 2.20.

2.15 Contact persons

Secretary of the Tenders and Procurements Committee
Universal Postal Union
International Bureau
Weltpoststrasse 4
3015 BERNE
SWITZERLAND

Tel: +41 31 350 35 02
E-mail: caa@upu.int

2.16 Further inquiries and questions

Bidders must send any questions regarding the content of this call for tenders or any requests for clarification in writing to the contact person(s) listed in section 2.15 by 4 April 2025.

Answers to questions submitted by Bidders, as well as any additional information and updates relevant to this call for tenders, shall be published on the UPU website at www.upu.int/en/Universal-Postal-Union/Procurement.

2.17 Delivery of tenders and deadline

All tenders must be submitted to the UPU by e-mail only to RFP-2025-008@upu.int with "RFP 2025-008-Migration of on-premises database to cloud managed solution" as the subject line.

The deadline for the submission of tenders is **18 April 2025 at 17.00 CEST**.

The UPU shall not take into consideration any tenders received after this date and time. Furthermore, it shall not accept any tenders sent to any e-mail address other than that specified above or sent by any other means.

There shall be no charge to the UPU for the preparation and submission of tender documents by Bidders.

2.18 Evaluation procedure

The objective of the UPU's evaluation process is to ensure the selection of a qualified, reliable and experienced Vendor capable of providing the specialized services and fulfilling the objectives set out in this call for tenders.

The UPU shall conduct its evaluation procedure with a view to determining as objectively as possible the tender that best meets its specific requirements. All tenders submitted shall be subject to an in-depth assessment, at the UPU's sole discretion, in order to enable the UPU to engage the most appropriate service provider.

The prescribed structure of tenders, as set out in section 3, is mandatory for all Bidders. The UPU shall not take into consideration any tenders that do not fulfil the mandatory criteria.

The deliberations of the UPU Tenders and Procurements Committee (TPC) are strictly confidential. The TPC shall submit a report on its evaluation of the tenders received to the Director General of the UPU International Bureau, together with its final recommendation, for his assessment and authorization.

The UPU is not bound to accept the lowest tender and reserves the right to accept all or part of a tender. In awarding the contract, account will be taken of both the overall costs of the work and of the nature and quality of the services to be provided. The UPU reserves the right to negotiate prices and terms and conditions of contract after receipt of tenders.

Bidders will be informed of the outcome of their tender as soon as possible after the UPU has made its final selection.

Details of the applicable bidder eligibility criteria and tender assessment criteria are provided in sections 4.8 and 4.9.

2.19 Modification, suspension or cancellation of the call for tenders

The UPU reserves the right, at its sole discretion and at any time before the conclusion of the tender process (i.e. at any time prior to the signature of the relevant contract with the Vendor), to modify, suspend or cancel all or part of this call for tenders.

2.20 Tentative schedule

Publication of call for tenders	24 March 2025
Deadline for submission of participation notification	4 April 2025
Deadline for submission of queries	4 April 2025
Deadline for provision of responses to queries	9 April 2025
Deadline for submission of tenders to the UPU	**18 April 2025 at 17.00 CEST**
Estimated start of engagement	29 May 2025

3 Tender structure – Response format

All information provided by Bidders must be fully compliant with the terms and conditions set out in section 2 above, as well as the provisions of this section and the service requirements listed in section 4 below.

Moreover, the requirements stipulated in this call for tenders must be met in their entirety, according to the structure defined below and following the sequence and numbering provided in this section. The UPU shall evaluate all Bidder responses in accordance with the structure defined herein and shall have the right to reject any tenders that do not fulfil the requirements of this call for tenders.

For each of the requirements listed in this call for tenders, Bidders shall answer with one of the following statements:

– covered;

– covered with limitations (explaining relevant limitations);

– not covered.

Where the answer is “covered” or “covered with limitations”, Bidders shall provide further details and/or examples of existing implementations of their solution in the field (existing use cases).

3.1 Cover letter

Bidders shall submit a cover letter including:

– a statement that the Bidder has read, understands and accepts all provisions of this call for tenders;

– the Bidder’s name, telephone number, postal address and e-mail address, and the name(s) of its representative(s);

– a statement that the Bidder’s tender documents are valid for a minimum period of 120 days.

The cover letter shall be signed by a representative (or representatives) duly designated and authorized to act on the Bidder's behalf and with the authority to legally bind the Bidder and accept the terms and conditions of this call for tenders, and shall also include a confirmation of such authorization by the Bidder.

3.2 Executive summary

Bidders shall provide an executive summary highlighting the most important aspects of their tender.

3.3 Bidder information

Bidders must provide the following information:

– company structure, locations/subsidiaries;
– financial data (turnover, profit, etc.);
– number of employees;
– partners and equity holders of the company;
– company history;
– market position and share in relevant markets;
– customer reference list with descriptions of similar projects;
– quality management certifications and statements;
– company governance and sustainability executive report;
– reference letters.

3.4 Subcontractor information

In the event that Bidders intend to engage a subcontractor for part or all of the services set out in this call for tenders, the following information must be provided with regard to the subcontractor(s):

– company structure, locations/subsidiaries;
– degree of involvement, with a list of services and/or products to be provided;
– customer reference list with descriptions of similar projects;
– company governance and sustainability executive report;
– reference letters.

3.5 Technical proposal

Bidders shall submit a technical proposal addressing all of the requirements set out in section 4 (Service requirements). This proposal should include, as a minimum:

– database type and technical description;
– architecture diagram of the proposed database;
– maintenance model for the cloud managed service;
– expected effort per deliverable and migration schedule;
– description of managerial processes;
– expected response time to e-mails, purchase orders and any other queries that the UPU may have;
– region(s) selected for hosting, with rationale;
– any additional information that Bidders wish to provide regarding the implementation and fulfilment of the requirements set out in this call for tenders.

3.6 Pricing structure

3.6.1 Guidelines for pricing proposal

Bidders shall provide a detailed pricing structure for the services proposed, following these guidelines:

– Bidders shall not include VAT in any of their pricing information (see section 2.11 above). All pricing information shall be set out exclusively in United States dollars (USD);

– All of the technical details required to prepare the tender are provided in section 4 (Service requirements);

– If any "component" does not apply or cannot be provided, "N/A" should be entered in the "cost" column;

– Bidders may include discounts based on volumes or long-term commitments. These should be added as new lines in the relevant table(s);

– If Bidders wish to quote for costs that are not included in the template, new lines should be added in the relevant table(s);

– If Bidders wish to present several costing options, e.g. in view of hosting in different regions or scaling costs beyond the scenarios considered, new lines should be added in the relevant table(s);

– Bidders must specify, in the "comments" column, any service limitations, considerations, observations or additional information that may have an impact on the performance of the components;

– The scenarios should take into consideration a hosting location selected to achieve the most efficient exchange of data between the elements connected to the database. The inclusion of regions offering greater affordability and greater sustainability (if these are not the same) would be advantageous;

– Bidders shall not be allowed to withdraw and resubmit their tender, for any reason whatsoever, after the tenders have been opened by the TPC;

– Bidders shall confirm that the prices quoted in USD are fixed and that there shall be no additional cost to the UPU owing to exchange rate variation (if any) at the time of execution of the contract.

3.6.2 Structure of pricing proposal

The pricing proposal must be structured in three parts, as follows:

– Project implementation: Bidders must provide prices for the implementation phase of the project;

– Operations: Bidders must provide prices for running costs for three different data volume scenarios (see section 4.3), taking into consideration the transactions between the central database and the various services, based on hosting by different cloud providers (see section 4.1);

– Monitoring, diagnosis, maintenance and optimization services: Details must be provided regarding the costs of providing monitoring, diagnostic, maintenance and optimization services.

The templates for the submission of pricing information for each of these elements are provided below.

3.6.2.1 Project implementation

Component	*Description*	*Unit*	*One-off cost*	*Comments*
Assessment and planning	Initial analysis, architecture design, migration strategy	Project		
Data migration	Cost of moving data to cloud, including validation on data integrity	Per GB		
Training	Knowledge transfer to UPU staff regarding use and management of the solution	Per session		

3.6.2.2 Operations

The template for running costs must be completed for each of the three data volume scenarios set out in section 4.3.

Component	*Description*	*Unit*	*Cost*	*Comments*
MQTT broker	Message broker service handling device communication	Per message		
Container service	Host for six microservices with specified RAM/CPU	Per container		
Hot storage	Last two months of data – highest performance tier	Per GB		
Warm storage	Next two months of data – medium performance tier	Per GB		
Cold storage	Next nine months of data – lower performance tier	Per GB		
Frozen storage	Remaining 47 months – lowest cost archive tier	Per GB		
Computing resources	Processing power for database operations	Per vCPU hour		
Memory resources	RAM allocation for database operations	Per GB hour		

3.6.2.3 Monitoring, diagnosis, maintenance and optimization services

Component	*Description*	*Unit*	*Cost*	*Comments*
24/7 support	Critical incident response within one hour	Monthly rate		
Monitoring	System health tracking and alerts	Monthly rate		
Updates and patches	Regular maintenance and security updates	Monthly rate		
Backup service	Weekly backups with six-month retention	Per GB		
Security services	Encryption, access control and compliance tools	Monthly rate		
Optimization	Performance optimization recommendations based on post-migration actual usage data	Per assessment		
Additional training	Add-on training services aimed at three different profiles (administrators, operators and users)	Per training session		

3.7 Delivery and payment schedule

The delivery and payment schedules for project implementation should follow the template provided below.

The services provided by the Vendor for the operation of the system, as well as monitoring, diagnosis, maintenance and optimization, shall be invoiced in arrears on a monthly or ad hoc basis.

The UPU will make payment within 30 business days of receipt of invoice, subject to its acceptance of the services provided according to the criteria defined in section 4.7.

The abovementioned payment schedules and target dates for delivery of the services are summarized in the following table:

Milestone	*Duration*	*Date*	*Payment schedule*	*Comments*
Start date	–	15 May 2025	–	
Project implementation	4 months	15 May to 15 September 2025	As defined in section 3.7.1	
Operations	32 months	15 September 2025 to 14 May 2028	Monthly	
Monitoring, diagnosis, maintenance and optimization services	32 months on an ad hoc basis	15 September 2025 to 14 May 2028	Monthly for ongoing activities and following delivery for ad hoc requests	
End of services	–	14 May 2028	–	

Bidders are requested to acknowledge the proposed schedule or provide comments.

3.7.1 Project implementation deliverables

Component	*Code*	*Deliverables*	*Parent deliverable (if any)*[2]	*Duration*	*Payment terms*	*Comments*
Assessment and planning	A1	Detailed migration plan, including detailed timelines, milestones and risk assessment				
	A2	Validation scripts for pre-migration data integrity checks				
Data migration	B1	Configured cloud environment with storage, computing and networking resources aligned with the project scope				
	B2	Migration logs and reports documenting the transfer process, including downtime minimization and error handling				

[2] Parent deliverable: Bidders shall identify dependencies between deliverables in order to create a deployment schedule. A parent deliverable is one that prevents the completion of other deliverables. If a deliverable cannot be completed until another has been completed, the code of the deliverable that must precede shall be indicated in the “parent deliverable” column.

For example, if deliverable B cannot be completed until deliverable A has been completed, deliverable A is the “parent deliverable” of deliverable B.

Component	*Code*	*Deliverables*	*Parent deliverable (if any)*[3]	*Duration*	*Payment terms*	*Comments*
Data migration (cont.)	B3	Updated configurations for applications and micro-services to ensure compatibility with the cloud environment				
	B4	Validation and testing reports confirming data integrity and performance benchmarks				
	B5	– Complete documentation set covering technical and operational aspects – Records of document reviews and approvals to ensure accuracy – Version-controlled records to track updates and revisions				
Training	C1	Detailed system documentation, including architecture diagrams, configuration files and troubleshooting guides				
	C2	Training sessions for UPU staff				
	C3	Training materials tailored for each profile (administrators, operators and users)				

3.8 UPU General Terms and Conditions

/ Bidders shall include in their tender a statement of acceptance of the UPU General Terms and Conditions for the Provision of Services, attached hereto for reference.

The final terms of any contract arising from this call for tenders shall be defined by the UPU and accepted by the Vendor. Contract negotiations shall commence only after the final selection of a Vendor by the UPU.

[3] Parent deliverable: Bidders shall identify dependencies between deliverables in order to create a deployment schedule. A parent deliverable is one that prevents the completion of other deliverables. If a deliverable cannot be completed until another has been completed, the code of the deliverable that must precede shall be indicated in the “parent deliverable” column.
For example, if deliverable B cannot be completed until deliverable A has been completed, deliverable A is the “parent deliverable” of deliverable B.

4 Service requirements

4.1 Description of the services

The Vendor will be expected to provide the following services:

– migration of the current database to a cloud managed service;

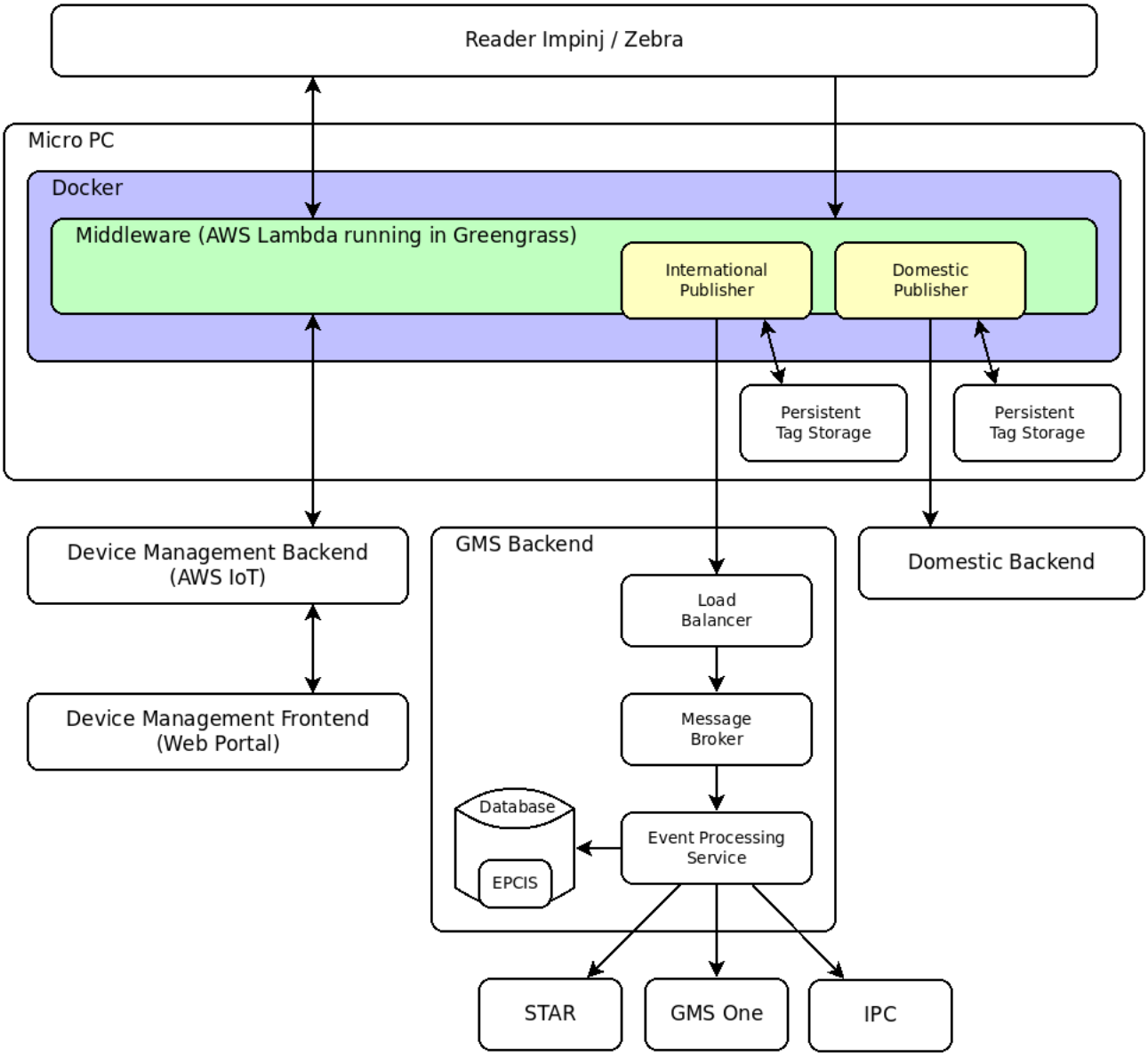
– maintenance and support services;

– training in the use, monitoring and management of the cloud service.

4.1.1 Current infrastructure and environment

To facilitate an understanding of the technical requirements of this call for tenders, this section provides an overview of the current environment that is to be migrated to a cloud managed service.

The current UPU GMS RFID infrastructure collects data from RFID devices installed around the world and sends the data to a local repository, as depicted in the following diagram:



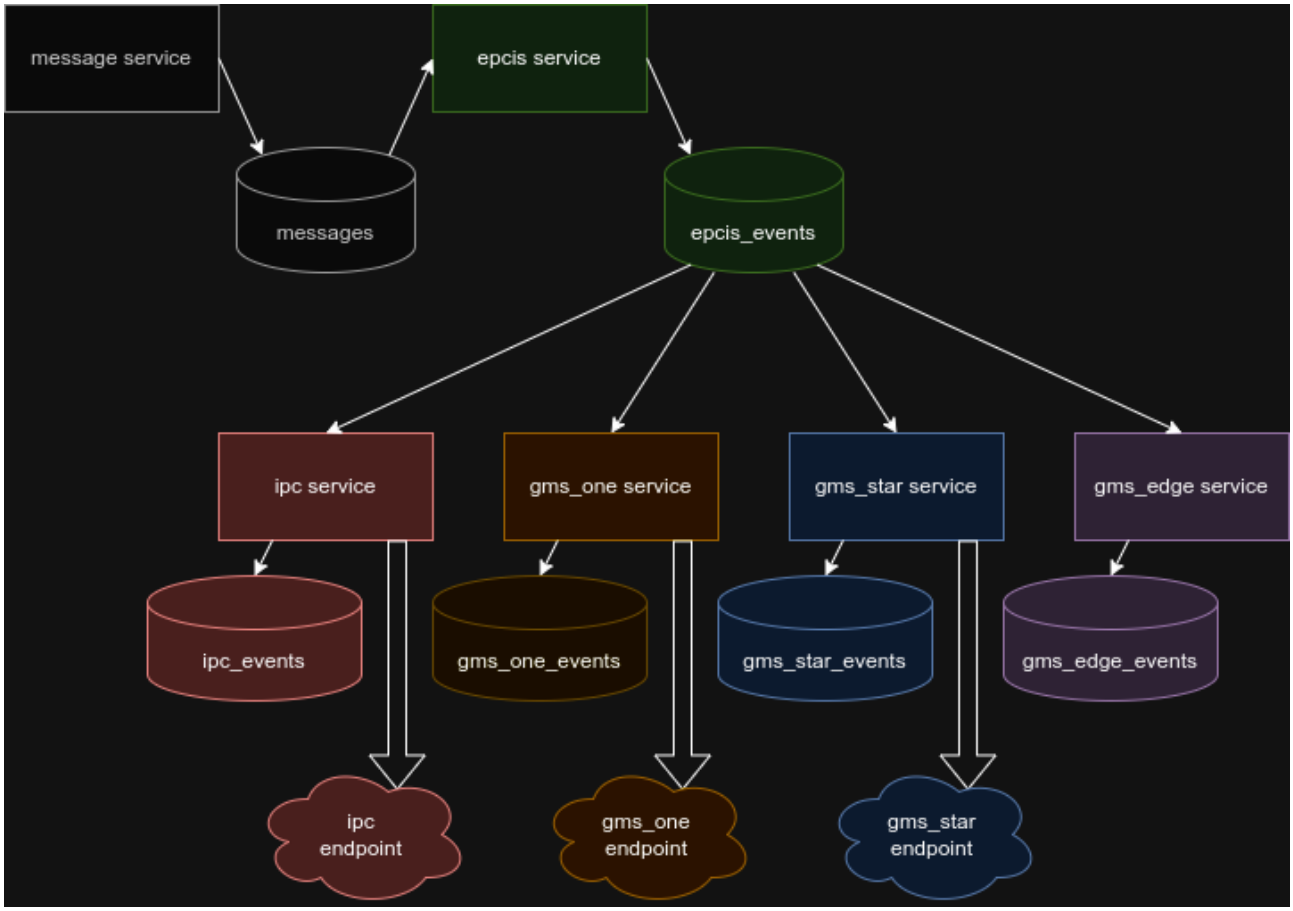
The scope of the migration and cloud managed service is limited to the components within the GMS back-end section.

The GMS back-end infrastructure currently comprises the following components:

– Load balanced MQTT brokers (v5);
– Elasticsearch database server;
– Load balancer servers;
– Internal microservices docker host;
– UAT environment:
  - Database server;
  - UAT servers, docker and MQTT.

The current volume of the database is 20 GB.

Once messages reach the EPCIS database, there are several event processing services depending on different business applications of the data. These events are also stored in the database and pushed to the respective endpoint, when available:



The current reporting tools and endpoints to which the events are pushed from the EPCIS database are hosted locally or in the cloud (AWS and Azure) in the European region.

Therefore, it is requested that Bidders select a host region that supports low-latency communication with these reporting tools and endpoints, and minimizes communication costs.

4.2 Technical requirements of the cloud managed services

4.2.1 Implementation requirements

During implementation, the following key stages should be completed:

– Data migration
  - Snapshot and restore approach

- Dual-write during migration
- Schema compatibility verification

– Validation requirements
  - Pre-migration data integrity checks
  - Document count validation
  - Data structure verification
  - Content sampling tests

4.2.2 Performance requirements

– Query latency: < 200 milliseconds (ms) on average
– Document indexing: < 150 ms
– Uptime SLA: 99% (maximum of 7 hours downtime per month)
– Recovery objectives: 6 hours for recovery time objective (RTO)/recovery point objective (RPO)

4.2.3 Regional considerations for reporting tools and data hosting

Reporting tools and associated data are currently hosted in Switzerland or within the European Union. To ensure optimal performance, compliance and sustainability, Bidders must propose data hosting regions aligned with these requirements.

Bidders may include several options and approaches with regard to the choice of host region and set-up, as follows:

– A choice of several single/primary regions may be proposed
– Single or multiple zones
– Single or multiple regions

For each proposal, Bidders shall provide:

– Configuration details for a single region, multi-zone or multi-region set-up, specifying:
  - Performance improvements, including reduced latencies
  - Data redundancy and disaster recovery benefits
  - Privacy and compliance considerations under applicable laws (e.g. GDPR)
  - Pros and cons of single-region, multi-zone or multi-region deployment, focusing on:
    – Cost: additional expenses for replication and interregional communication
    – Privacy: enhanced compliance or potential risks in data jurisdictions
    – Sustainability: environmental impact of operations in each region
– Estimates for:
  - Initial set-up costs
  - Ongoing operational costs, including bandwidth, computing and storage
  - Potential savings or expenses associated with adopting region-specific optimizations

4.2.4 Security and compliance requirements

– Security requirements
  - TLS/SSL for data transit
  - AES-256 data encryption at rest
  - Access control: role-based access control (RBAC) and IP whitelisting

- Comprehensive audit logging
- Regular vulnerability assessments

– Backup strategy
  - Frequency: daily local backup
  - Retention: six months minimum
  - Encrypted storage and transfer
  - Regular restore testing

4.2.5 Back-end component requirements

The GMS back-end infrastructure must comprise the following components:

– MQTT brokers

– Container platform

– Elasticsearch

– Monitoring and alert integration

This section outlines the technical requirements for each component of the GMS back-end infrastructure.

4.2.5.1 MQTT requirements

The MQTT (message queuing telemetry transport) brokers serve as the backbone for message delivery within the GMS back-end architecture. The following requirements ensure robust, scalable and secure operations:

– Protocol compliance: support MQTT protocol version 5.0, providing enhanced features such as:
  - Improved message control options
  - Support for session expiry and shared subscriptions
  - Enhanced error reporting and diagnostics for message flows

– Authentication and security
  - Implement username/password-based authentication initially to secure connections
  - Ensure readiness for future upgrades to x.509 certificate-based authentication for greater security
  - Enable TLS/SSL encryption for all broker-client communications to protect data in transit

– High availability and load balancing
  - Deploy a cluster of load-balanced MQTT brokers to handle large volumes of messages
  - Configure automatic failover mechanisms to ensure uninterrupted service during node outages
  - Monitor broker health and dynamically redistribute traffic across nodes during peak loads or failures

– Scalability and performance
  - Ensure support for thousands of simultaneous connections (e.g. > 3000 readers)
  - Capability to handle sustained message ingestion rates with minimal latency (e.g. < 100 ms)
  - Built-in mechanisms to handle bursts in traffic without degrading performance

– Monitoring and alerts
  - Integrate monitoring tools to track broker health, message flow rates and connection status in real time
  - Set up alerts for conditions such as excessive message retries, connection failures or broker unavailability

4.2.5.2 Container platform requirements

The container platform hosts the microservices forming the core of the GMS back-end infrastructure. The requirements below ensure flexibility, reliability and scalability:

– Container support
  - Full compatibility with Docker containers for seamless microservice deployment
  - Ensure container orchestration capabilities for efficient resource utilization and management
– Load balancing for microservices
  - Implement a load balancing mechanism to distribute traffic evenly across microservice instances
  - Ensure compatibility with service discovery for dynamic scaling
  - Support health checks and automatic rerouting of traffic from failed instances to operational ones
– Resource allocation: Provide customizable resource limits for each microservice based on operational needs
  - Memory allocation: allow configuration from 2 GB to 6 GB per microservice instance
  - CPU allocation: support allocation from two to four virtual CPUs per microservice
– Scalability and high availability
  - Allow deployment of six or more microservices simultaneously, each with its own resource allocation
  - Support horizontal scaling (adding more instances) and vertical scaling (increasing resources for an instance)
  - Configure automatic scaling policies to respond to workload increases dynamically
– Monitoring and maintenance
  - Enable real-time monitoring of container performance, resource usage and service status
  - Provide tools for managing container updates, including rolling upgrades to minimize downtime
– Integration with existing tools
  - Seamless integration with Elasticsearch and MQTT brokers for data processing and messaging
  - Support APIs for management and interaction with external tools

4.2.5.3 Elasticsearch requirements

Elasticsearch forms the core of the GMS back-end infrastructure, providing indexing and search capabilities for high volumes of events and data. The following requirements ensure that Elasticsearch remains scalable, reliable and optimized for performance:

– Multiple availability zone deployment
  - High-availability configuration
    – Deploy Elasticsearch clusters across multiple availability zones within the chosen cloud provider’s infrastructure
    – Ensure resilience against single-zone failures by enabling cross-zone replication and redundancy
  - Data replication
    – Configure primary and replica shards to distribute data across zones for fault tolerance and improved read performance
    – Use automated mechanisms to rebalance shards in case of node or zone failures

– Node configuration
  - Hot data nodes
    – Deploy a minimum of two nodes dedicated to hot data (frequently accessed data)
    – Optimize nodes for high I/O performance with fast SSD storage and adequate memory (e.g. > 64 GB)
  - Node roles
    – Assign specific roles to nodes (e.g. master, data and ingest) to ensure efficient cluster management and performance
    – Scale the cluster horizontally by adding more nodes as data volume increases
– Performance optimization capability
  - Indexing and query optimization
    – Fine-tune index settings, such as shard and replica count, to balance performance and resource usage
    – Implement caching strategies to reduce query latency, especially for frequently accessed data
  - Scalability
    – Enable dynamic scaling to handle peak workloads and growing data volumes
    – Configure auto-scaling policies to adjust node count based on CPU, memory and storage thresholds
  - Search tuning: Leverage advanced Elasticsearch features, such as query routeing and field data cache optimization, to improve search efficiency

4.2.5.4 Monitoring and alert integration requirements

– Real-time monitoring
  - Integrate with monitoring tools (e.g. Elastic Stack, Prometheus) to provide real-time insights into cluster health, resource utilization and query performance
  - Track key metrics, such as:
    – Query and indexing latency
    – Disk I/O and memory usage
    – Cluster shard status and allocation
– Alert mechanisms
  - Configure alert thresholds for critical events, such as:
    – High query latency (> 200 ms)
    – Node failures or cluster status degradation
    – Insufficient disk space or memory
  - Send alerts via multiple channels (e.g. e-mail or SMS) or integration with incident management tools

4.2.6 Documentation and transfer of knowledge

Detailed and accurate documentation is essential for long-term system operation and troubleshooting. The Vendor will be required to document the technical work and procedures, and to provide this documentation along with user manuals and troubleshooting guides, as follows:

– Technical documentation
  - Comprehensive descriptions of the cloud environment, including configurations for Elasticsearch, MQTT brokers and Docker containers

- Architecture diagrams and system flowcharts

– Operational procedures
  - Step-by-step guides to performing routine tasks, such as system updates, scaling and monitoring
  - Troubleshooting workflows to resolve common issues

– User manuals: Clear instructions for system users on how to query data, generate reports and use system features

– Troubleshooting guides: Detailed problem-solving procedures for technical issues, such as failed queries, service outages and performance bottlenecks

All documentation shall be released following a workflow approval. Bidders shall propose a methodology and tools to track versions, updates and revisions.

Documentation shall be maintained to reflect the most recent system updates, operational procedures and knowledge-base content.

4.3 Data volumes and capacity

As mentioned in section 3.6, the UPU has designed three different data volume growth scenarios. Bidders shall design a scalable solution that takes these different scenarios into consideration, and provide the associated costs in their pricing proposal, as detailed in section 3.6.

The maximum storage retention time will be five years, distributed in four tiers based on data accessibility. The capacity of the cloud managed services must respond to the following needs for each scenario. Data storage requirements are defined in gigabytes (GB):

Scenario description	*Basic*	*Medium*	*Large*
Events per year	92 million	270 million	893 million
Devices	3,000	3,000	3,000
Messages per year	251,000 at 3 KB each	740,000 at 3 KB each	2.4 million at 3 KB each
Processing volumes	*Basic*	*Medium*	*Large*
Device messages	2.4 million per day at 3 KB each		
Service processing			
IPC service	1.2 million per day at 2 KB each		
GMS STAR service	420,000 per day at 1 KB each		
Edge service	2.4 million per day at 2 KB each		
Storage tiers	*Basic (GB)*	*Medium (GB)*	*Large (GB)*
Hot (two months)	105	269	919
Warm (two months)	105	269	919
Cold (nine months)	473	1,210	4,134
Frozen (47 months)	2,468	6,317	21,586

4.4 Maintenance and support service requirements

Bidders are requested to provide information on their proposal for support and maintenance services, which should cover, as a minimum:

– Service desk operations
  - Support services
  - Incident management

– Maintenance and monitoring activities
  - Service level obligations
  - Required activities
  - Monthly stakeholder meetings

The proposal shall take into account the requirements set out below.

4.4.1 Service desk operations

The service desk serves as the single point of contact for all support and maintenance requests. It shall respond to the following requirements:

– Support services
  - 24/7/365 availability to ensure round-the-clock support
  - The required support channels are: phone, e-mail and a web-based ticketing system for incident tracking and management

– Incident management
  - Incidents shall be categorized by severity, with response times prioritized accordingly:
    – Critical (P1): response < 1 hour, resolution < 4 hours
    – High (P2): response < 2 hours, resolution < 8 hours
    – Medium (P3): response < 4 hours, resolution < 24 hours
    – Low (P4): response < 8 hours, resolution < 48 hours
  - Root cause analysis: for P1 and P2 incidents, the Vendor shall conduct in-depth investigations and provide reports, including the conclusions of the analysis
  - Post-incident reports: for P1 and P2 incidents, the Vendor shall deliver detailed incident reports within five business days following resolution
  - Provision of monthly reports covering key performance indicators, SLA compliance metrics and a summary of resolved and open tickets

4.4.2 Maintenance and monitoring activities

The Vendor is expected to monitor the system and ensure the health thereof, and to proactively anticipate potential issues before they affect operations. Maintenance and monitoring activities shall be balanced to achieve the following service level obligations:

Area	*Metric*	*Comments*
System availability	Ensure the availability of the platform for 99% of the month	Exclude planned maintenance from availability calculations
	Limit unplanned downtime to a maximum of 7 hours per month	
System performance	Response time for queries: < 200 ms (95th percentile)	
	Indexing latency time: < 150 ms (95th percentile)	
	Availability of APIs: > 99%	
Disaster recovery	RTO: 6 hours	The Vendor shall conduct quarterly disaster recovery simulations and report on the results thereof.
	RPO: 6 hours	

Bidders shall state in their tender whether they have sufficient resources to provide any/all of the maintenance and monitoring activities set out in the table below, and must specify whether or not each activity will be covered:

Element	*Description*	*Tools and methodologies*	*Frequency*	*Covered*
Cluster interface	Continuously monitor the health of critical system components, including Elasticsearch clusters, MQTT brokers and containerized services	Provide a centralized dashboard for managing Elasticsearch clusters and MQTT brokers, including functionalities such as: – node scaling and shard reallocation – real-time cluster status and health checks – index creation, deletion and optimization – visual indicators for node status, shard distribution and system uptime		
Tracking of performance metrics	Track and report on system performance trends to anticipate potential bottlenecks	– Monitor query response times, document indexing rates and API availability – Provide detailed monthly reports on performance and capacity trends, including capacity status and planning updates	Monthly	
		– Use historical data to predict future resource needs – Track data growth rates and system usage patterns	Quarterly	
Resource utilization	Continuously track CPU, memory and storage usage for all services	– Identify and provide alerts on resource contention or underutilization – Evaluate CPU, memory and storage usage – Monitor data growth and costs – Include tools to adjust resources dynamically for Elasticsearch nodes, container services and MQTT brokers	Monthly	
		– Propose scaling strategies to handle growth and peaks in demand – Provide evaluation reports and recommendations	Quarterly	

Element	*Description*	*Tools and methodologies*	*Frequency*	*Covered*
Cost tracking	Monitor cloud resource costs in real time, including computing, storage and bandwidth usage	– Offer detailed cost breakdowns by service and region to optimize expenditure – Offer cost impact analysis for scaling decisions to align with budget considerations – Identify opportunities for savings in cloud resources and operations		
Alert system	Corrective and preventive alerts for issues or failures	– Set thresholds for proactive alerts on system health and performance – Configure alerts for critical events, such as: • cluster or node failures • latency spikes or query timeouts • resource usage exceeding predefined thresholds – Support multiple notification channels (e.g. e-mail, SMS) or integration with incident management platforms	One-off	
		Conduct tests to validate alert system integrity and functionality	Quarterly	
Backup monitoring	Maintain robust data backup and recovery capabilities to protect against data loss Ensure all backups are executed as scheduled and offer tools to monitor backup schedules and success rates	– Track backup completion rates and resolve failures immediately – Provide automated alerts for failed or delayed backups – Include restoration management interfaces for testing and disaster recovery scenarios – Deliver compliance reports summarizing backup activities and outcomes	Monthly	
		Conduct tests to validate backup integrity and recovery procedures	Quarterly	

Element	*Description*	*Tools and methodologies*	*Frequency*	*Covered*
Security monitoring	Ensure that the system remains secure against evolving threats	– Set up a security console to centralize security controls, including: • RBAC management • audit logging configuration and review • encryption settings for data in transit and at rest – Enable automated vulnerability scans and remediation tracking – Regularly apply security patches to software and infrastructure	Monthly	
		– Vulnerability assessments: conduct periodic tests to identify and mitigate vulnerabilities – Provide updates on security status and improvements	Quarterly	
Change management	Structured change management to ensure smooth transitions while maintaining system stability	– Standard change catalogue: maintain a list of pre-approved routine changes to minimize delays – Emergency changes: define expedited procedures for high-priority changes – Change Advisory Board: collaborate with UPU stakeholders to review and approve major changes – Validation: test and document all changes before deployment – Reporting: provide monthly reports on change activities and outcomes		
Continuous improvement	Assess trends reported under each item listed in the “tools and methodologies” column for this activity to evaluate the long-term alignment of the system with business goals	– Identify new technology adoption possibilities – Optimize existing processes – Implement best practices	Twice per year	

4.5 Training requirements for UPU staff

A comprehensive training programme must be provided to ensure that UPU staff can effectively manage and operate the new cloud-based GMS back-end system. This training shall be aimed at three profiles – administrators, operators and users – and shall be documented.

4.5.1 Administrators

Training for the administrator profile shall focus on the management of cloud resources, including:

– Elasticsearch clusters;

– MQTT brokers;

– Docker containers;

– Backup and restore processes;

– Performance optimization;

– System scaling.

4.5.2 Operators

Training for the operator profile shall focus on how to perform daily operational tasks, such as:

– Monitoring system health and alerts;

– Performing routine maintenance tasks;

– Addressing common system issues.

4.5.3 Users

Training for the user profile shall provide guidance for end users on interacting with the system, including step-by-step instructions for accessing and querying data.

4.5.4 Training documentation

Training materials shall be tailored for each profile (administrators, operators and users). All training sessions must be supported by clear and concise materials, such as:

– Slide decks and training manuals, including screenshots, diagrams and step-by-step instructions;

– Hands-on exercises and practical examples;

Training materials must be refreshed as necessary to incorporate new features or updates.

The Vendor shall provide a methodology and directory to track:

– Attendance records for all sessions to ensure participation;

– Competency assessments to validate knowledge acquisition.

4.6 Duration of services and implementation schedule

The services are scheduled to commence in May 2025 for a total contract term of three years.

As defined in section 4.1, the services will involve the implementation of a cloud managed solution, the maintenance thereof and associated training activities. Details of the expected duration and schedule for each service are provided in the table below. Bidders should confirm their ability to meet these requirements, or provide comments and propose amendments (i.e. changes or new milestones) to the proposed timelines. It should be noted that:

– Maintenance and support services shall be provided as ongoing activities, including monthly and quarterly reports as specified in section 4.4.2;

– Training sessions shall be provided as required.

Milestone	*Description*	*Key activities*	*Deliverables*	*Duration*	*Comments*
Phase 1: Pre-migration assessment	Select the cloud provider, define the migration strategy and set up test environments	Infrastructure analysis – Assess the current architecture, including MQTT brokers, Elasticsearch server, Docker containers and UAT set-up – Review current performance metrics, including query latency, indexing throughput and resource utilization Data inventory – Analyze data volume (20 GB) and growth trends (projected 25 TB) – Identify data structures, schemas and compatibility requirements Definition of requirements – Define scalability, security and compliance needs – Document performance and availability requirements (e.g. 99% uptime, < 200 ms query latency) Risk assessment – Identify risks, such as data loss, downtime and compliance breaches – Develop mitigation strategies, including backup and rollback plans	Assessment report detailing the current environment and gaps Migration strategy document outlining the approach and tools Risk mitigation plan with potential fallback measures Technical architecture design for the target cloud set-up	2 weeks	
Phase 2: Migration planning and testing	Develop and test migration scripts, validate data integrity and prepare rollback plans	Project schedule development – Create a timeline for each migration phase, including milestones – Identify dependencies and critical path activities	Detailed project plan with timelines, tasks and responsibilities	2 weeks	

Milestone	*Description*	*Key activities*	*Deliverables*	*Duration*	*Comments*
Phase 2: Migration planning and testing (cont.)	This phase focuses on detailed project preparation, resource planning and schedule development.	Resource planning – Allocate required cloud resources (computing, storage, networking) – Identify key personnel for execution and oversight Environment set-up planning – Plan for the creation of production and UAT environments in the cloud – Define network configurations, including DNS and firewall rules Test strategy development: Design test scenarios for performance, integration and disaster recovery Rollback planning: Develop rollback procedures for data and application migration failures Communication and stakeholder planning: Develop a communication plan to update stakeholders regularly	Resource allocation plan for personnel and cloud infrastructure Test plan outlining scenarios, success criteria and reporting methods Rollback procedures and escalation workflows Communication matrix for stakeholder engagement		
Phase 3: Set-up and migration	The implementation phase involves setting up the cloud environment, executing migration activities and validating the system.	Environment set-up – Configure cloud infrastructure • Multi-zone availability for resilience • Elasticsearch cluster set-up with hot/warm data nodes • Docker container platform for microservices – Deploy monitoring tools for real-time health tracking and alerts	Fully configured cloud environment Migration execution report with logs and validation results Test results and issue resolution documentation Updated system documentation and training materials	2 months	

Milestone	*Description*	*Key activities*	*Deliverables*	*Duration*	*Comments*
Phase 3: Set-up and migration (cont.)		– Implement TLS/SSL encryption, RBAC and IP whitelisting for security Data migration – Perform initial data synchronization using snapshot and restore – Enable dual-write functionality for real-time updates – Conduct final synchronization during a maintenance window Application configuration – Update API endpoints for Elasticsearch and MQTT brokers – Deploy microservices with updated configurations – Integrate with existing tools and workflows Testing and validation – Conduct unit, integration, performance and security testing – Simulate disaster recovery scenarios to validate RTO/RPO – Execute UAT with stakeholder involvement Documentation and knowledge transfer – Document all configurations, processes and testing outcomes – Conduct training sessions for UPU staff			

Milestone	*Description*	*Key activities*	*Deliverables*	*Duration*	*Comments*
Phase 4: Stabilization	Perform final synchronization, switch traffic to the cloud and decommission on-premises infrastructure This phase ensures that the new system operates smoothly and addresses any post-migration issues.	Performance monitoring – Monitor query latencies, indexing throughput and cluster health – Fine-tune resource allocations based on real-world usage Issue resolution – Address post-migration issues, including performance bottlenecks and security gaps – Apply updates and patches as necessary Training and knowledge transfer – Provide hands-on training for UPU technical staff – Update and finalize system documentation	Performance assessment report detailing system metrics and adjustments Post-migration issue resolution log Finalized training materials and competency assessments Decommissioning plan for the on-premises environment	1 month	
Phase 5: Post-migration optimization	Monitor and fine-tune the system and provide staff training	Deploy maintenance, support and monitoring services	As defined in section 4.4	Ongoing	

4.7 Acceptance criteria for the services provided

Acceptance of the services provided will be defined based on achievement of the criteria set out in this section.

4.7.1 Technical criteria

The system must meet all technical specifications and performance benchmarks:

– Achievement of performance metrics
  - Query response time of < 200 ms (95th percentile)
  - Indexing latency of < 150 ms
– Compliance with security requirements
  - Encryption of data at rest and in transit
  - Implementation of role-based access control and audit logging
– Demonstration of high availability: 99% uptime with appropriate failover mechanisms
– Disaster recovery capability: RTO and RPO of 6 hours
– Monitoring functionality: Real-time monitoring tools with actionable alerts

4.7.2 Operational criteria

The system must be fully functional and ready for operational use, as follows:

– Completion of migration: all data is successfully migrated without loss or corruption
– Delivery of documentation: complete set of user manuals, operational guides and troubleshooting documents
– Completion of training: all relevant personnel are trained and competencies validated
– Establishment of support procedures: support channels and processes are operational
– Verification of monitoring and alerts: a real-time monitoring and alerting system is in place and tested

4.7.3 Business criteria

The system must align with business objectives and user needs, as follows:

– Verification of business continuity: no interruptions to key operations during migration
– Validation of UAT: confirmation from stakeholders that the system meets functional requirements
– Demonstration of SLA compliance: uptime, performance and recovery SLAs are fulfilled

4.8 Bidder requirements/eligibility criteria

In order for their tenders to be considered, Bidders must meet the following mandatory eligibility criteria:

– Experience in data volume management: Bidders must demonstrate experience in implementing and managing solutions that handle data volumes and transaction rates equivalent to or exceeding those specified in the “Large” scenario in section 4.3;
– Experience in the implementation and management of similar cloud infrastructure: Bidders must demonstrate experience of previous projects requiring a cloud infrastructure similar to that set out in section 4.2, including:
  - Implementation of multi-zone and/or multi-region solutions;
  - Configuration of high-availability MQTT v5 services;
  - Management of container platforms for microservices;
  - Implementation of optimized Elasticsearch clusters;
  - Implementation of the specified security and compliance measures.

Tenders that do not meet these eligibility criteria will not be considered for further evaluation. Bidders must provide clear and verifiable documentation demonstrating compliance with these requirements as part of their tender.

4.9 Assessment criteria

Upon verification of Bidders' compliance with the eligibility criteria set out above, tenders will be evaluated based on a scoring system of up to 60 points for the pricing structure and up to 40 points for the technical proposal (including improvements beyond the specifications).

Criteria	*Points obtainable*
Pricing structure	**60**
Competitiveness of quoted prices for migration, ongoing services and optional features	50
Flexibility in pricing models (e.g. fixed-rate vs consumption based)	10
Technical solution	**40**
Technical solution aligned with the specified requirements	30
Technical improvements beyond the specified requirements: – Scalability and performance enhancements beyond the minimum specified requirements – Additional advanced security and compliance features – Improvements to SLAs and response times – Optimizations to the proposed architecture that generate operational or economic benefits – Additional monitoring, management and optimization tools – Improvements to the migration plan that minimize risk or downtime	10

Bidders shall provide evidence of their ability to meet these requirements. The UPU reserves the right to request additional information or clarification regarding Bidders' experience and technical proposals during the evaluation process.

4.10 Additional information

Bidders may include any additional information that they deem necessary or relevant in order for the UPU to gain a clear and detailed understanding of the services being offered.