



Community Bank

• Trust • Security • Progress

Tender Document

[Open Tender]

One stage Two Envelop

Supply, Install, Configure, Integrate, Test and Deploy of API Gateway Solution for Community Bank Bangladesh PLC.

Invitation for Tender No: CBBL/HO/ICT/20-2026/834

Dated: 19-07-2026

Tender issued on: 19-07-2026

Invitation for Tender Offer

BID SCHEDULE For

Item Sl.	Item Description
01	Supply, Install, Configure, Integrate, Test and Deploy of API Gateway Solution for Community Bank Bangladesh PLC.

INVITATION TO BID

Community Bank Bangladesh PLC. invites tender from bona fide bidders to submit proposals to offer **Supply, Install, Configure, Integrate, Test and Deploy of API Gateway Solution** for Community Bank Bangladesh PLC. The bidder should be well experienced to complete the task/tasks.

The last date for submission of Tender is **30 July, 2026**. Sealed Quotation Envelope (***Technical & Financial in separate envelopes***) shall be addressed to "Head of GSD, Community Bank Bangladesh PLC., Police Plaza Concord (Level 12, Tower 2), Gulshan 1, Dhaka-1212.", by **03:00 PM**. The bidder may depute their representative at the time of opening of Tender. Also note that technical proposal and live demonstration of the software will be evaluated after completing initial scrutiny of the required documents submitted along with the proposal. Financial proposal of the technically eligible bidders only, will be opened.

EXECUTIVE SUMMARY

Community Bank Bangladesh PLC. (CBBL), a concern of Bangladesh Police Kallyan Trust, is established with a vision to serve communities to progress with tailor-made secured solutions abiding by the highest level of Corporate Governance and Trust.

It aims to contribute to the economic growth of the country by providing financial products & services to communities across geographies. State-of-the-art Core Banking System enables the Bank to manage operations centrally at optimum scale.

Community Bank has expanded its network to 19 branches, 5 sub-branches, 110 service desks, and 191 ATMs/CRMs. With the rapid growth in customer base, digital banking services, and API-driven integrations, the Bank is committed to implementing a robust, secure, and scalable API Gateway Solution to centrally manage, monitor, and protect its application programming interfaces (APIs). The proposed solution will enable seamless integration between internal systems and third-party applications, enhance security and governance, improve API lifecycle management, and ensure compliance with Bangladesh Bank's ICT security guidelines and other applicable regulatory requirements.

Community Bank runs on its three core building blocks: Trust, Security and Progress.

SCOPE OF WORK

Scope of Bid

Bidders are required to propose solutions as specified in the technical and financial proposal for the supply, installation, and implementation of the following items. Bidders are required to propose their solutions under a **two-envelope** system. Bidders are required to quote for the items and are fully responsible for the offered products and implementation of the same as specified in the terms and conditions.

The scope of the bid includes supply, installation, and commissioning of the Software and related services as described below.

Item Sl.	Item Description
01	Supply, Install, Configure, Integrate, Test and Deploy of API Gateway Solution for Community Bank Bangladesh PLC.

The successful Bidder shall be responsible for all the product(s) and service(s) offered by them for project management and co-ordination of the item(s) mentioned above for Community Bank Bangladesh PLC.

Bidder's Qualification

1. The Bidder must have specific experience in implementing API Gateway and API Management Solutions in **at least one (1)** Banks, Non-Bank Financial Institutions, or MFS. Supporting documents (Work Order/Completion Certificate/Client Reference) must be enclosed.
2. The Bidder must submit copies of **at least one (1)** ongoing Service Level Agreements (SLAs) for API Gateway/API Management Solutions provided to Banks, Non-Bank Financial Institutions, or MFS. (Please enclose supporting documents.)
3. The Bidder must have adequate technical resources (minimum **10 qualified technical personnel**) with expertise in API Gateway implementation, API security, system integration, and post-implementation support to ensure successful project delivery and ongoing maintenance.
4. Bidders must submit up-to-date **Income Tax** Clearance Certificate, BIN Registration Certificate, and VAT Registration Certificate.
5. A valid **Trade License** must be submitted.
6. A **Certificate of Incorporation/Registration** must be submitted.
7. Bid Security of **BDT 50,000.00 (Taka Fifty Thousand)** in the form of a Payment Order or Bank Guarantee in favor of Community Bank Bangladesh PLC. The Bid Security shall remain valid for Six (6) months from the date of bid opening and must be enclosed with the **Technical Proposal**.

TERMS & CONDITIONS:

1. This invitation for Tenders is open to eligible tenderers from Locally registered companies.
2. The tenderer shall not be under a declaration of ineligibility for corrupt, fraudulent, collusive or coercive practices.
3. The Tenderer with a consistent history of litigation or a number of arbitration awards against it, shall not be eligible to tender.
4. The Tenderer shall have the legal capacity to enter into the contract.
5. The Tenderer shall not be insolvent, bankrupt or being wound up, its business activities shall not be suspended, and it shall not be the subject of proceedings for any of the foregoing.
6. The Tenderer shall have fulfilled its obligations to pay taxes and social security contributions under the relevant national laws and regulations.
7. The Tenderer shall possess the necessary professional and technical qualifications and competence, financial resources, including after-sales service, specific product experience, and reputation.
8. All prices should be in BDT include all VAT and TAX.
9. Financial offer should be valid for minimum six (06) months.
10. The Bank will carry out a detailed evaluation of the quotation according to the information supplied by the bidder through its proposal.
11. Considering the experience, quality, and other factors, CBBL is not liable to select the lowest bidder.
12. The Bank reserves the right to accept or reject any or all quotations at any time prior to award of contract, without thereby incurring any liability to the affected bidder or bidders or any obligation to inform the affected bidder or bidders of the grounds for the Bank's action.
13. Must fulfill CBBL's mentioned functional and implementation requirements.
14. Any bid not accompanied by an acceptable bid security shall be rejected as non-responsive even if that bid is found technically responsive during technical evaluation.
15. The bid security of unsuccessful bidders will be returned after selection of the successful bidder. The bid security of the successful bidder will be returned when the bidder has signed the agreement and furnished the required performance security.
16. The bid security may be forfeited if (a) the bidder withdraws its bid during the period of bid validity specified in the bid form; (b) if a successful bidder fails to sign the contract and (c) if a successful bidder fails to furnish the performance security.
17. Only technically qualified bidder will be eligible for opening financial proposal.
18. Requirement study, Supply, Development, Installation, Configuration, Customization, and commissioning of all components must be done at the pre-determined locations as specified by the Bank at no additional cost within the mentioned timeframes after email or letter confirmation.
19. Ensure support during working hours.
20. Additionally, the vendor will install and configure the DR site (disaster recovery) for Application and Database. In case of any disaster at the primary site, the vendor must ensure the software will run from DR.
21. Onsite Training: Training for users shall be provided at the Bank site, for at least 10 persons.
22. The bidder may offer any additional features in-built with this proposal to enhance the project.

23. Any extra features and/or policies may be included during or after implementation as per requirements of Management.
24. Before Go-Live, the bidder must perform parallel run/test of the solution for 1 (one) month.
25. After implementation, the bidder shall closely monitor the system during the warranty period, which shall be one (1) year from the date of Go-Live. Upon completion of the warranty period, a five (5) year Support Period shall commence.
26. The Bank may raise any other relevant issues for customization with the business need of time, which must be complied with at no additional cost.
27. The bidder must ensure expected performance of the new system as required by Community Bank Bangladesh PLC.
28. The Bank will check and verify the newly developed or configured module supplied in conformity with the approved technical specifications and will notify the bidder if any defects are found. The bidder MUST correct the defects immediately.
29. If the supplied module is found to be defective or otherwise not in accordance with the specifications, the Bank may reject the module by giving notice.
30. The bidder will submit proper documentation and system architecture diagrams as per standard.
31. Downtime of the proposed system: The Bidder must ensure that system downtime remains 0% (Zero) at any stage from commissioning of the system.
32. The bidder has to maintain the standard of delivered products as specified in the Guideline on ICT Security for Banks and Non-Bank Financial Institutions dated June 2023 issued by Bangladesh Bank.
33. The bidder will submit a step-by-step procedure for installation, testing, and commissioning along with a projected time frame within 1 (One) week of issuance of the work order. The bidder will also submit detailed User Acceptance Test (UAT) documentation and User Verification Test (UVT) procedures, which will be signed by the concerned authority of CBBL.
34. Any extra features and/or policies, design may be included during implementation or after implementation as per requirements of Management.
35. For any type of sub-standard quality product from the selected bidder, the Bank reserves the right for outright rejection of the goods, which the bidder will take back at their own cost and replace with acceptable quality within ten (10) days of rejection.
36. The bidder may be invited to give presentations on the product and project methodologies.
37. After the receipt of the work order from the Bank, 10% (ten percent) of project value in the form of Pay Order or Bank Guarantee (BG) for 01 (one) year, or till project completion, whichever comes later, must be submitted.

Details of Business and Technical Requirements
RFP (Request for Proposal) for API Gateway Solution

Supply, install, configure, integrate, test, commission, and deploy an Enterprise API Gateway Solution. The proposed API Gateway Solution shall provide a centralized, secure, scalable, and high-performance platform include the following key components:

The bidder must fill each row against each detail requirement to show whether their proposed solution complies with the requirement.

Bidder must fill column 3 for each table with either **A/PA/RM/NA** were -

- **A – Available.**
- **PA – Partially Available.**
- **RM – Roadmap.**
- **NA – Not Available.**

A. General Requirements			
SL	Functional Requirements:	Availability (A/PA/RM/NA)	Comments
1	The platform must act as a single, unified gateway for all API traffic, routing requests to appropriate backend systems with policy enforcement including rate limiting, load balancing, and caching.		
2	Must support REST, SOAP, GraphQL, WebSocket, and gRPC protocols as well as banking-specific message formats (ISO 8583, OFS, etc.).		
3	Built-in policies for converting and validating data formats (JSON, XML). Schema validation and conditional logic must enforce data quality and business rules (Data Mediation).		
4	Authentication and authorization via OAuth 2.0, OpenID Connect, HMAC, Mutual TLS, API keys, IP filtering, encryption, and threat-prevention policies.		
5	Granular IP-based access control (whitelisting / blacklisting) at the API and consumer level.		
6	Must support API versioning so that multiple versions of an API can run simultaneously without disrupting existing consumers.		
7	Support for request / response transformation, header manipulation, and payload rewriting without backend changes.		

SL	Functional Requirements:	Availability (A/PA/RM/NA)	Comments
8	Advanced Traffic Management: Must support advanced microservices resiliency patterns, specifically Circuit Breakers and automated Retry Mechanisms, to prevent cascading failures if backend systems experience temporary latency or outages.		
B. Integration & Orchestration Engine			
1	A No-Code / Low-Code visual designer allowing internal teams to build integration workflows by chaining API calls, mapping fields, and adding conditional logic without requiring custom development.		
2	The engine must invoke multiple backend services concurrently or sequentially and return a single consolidated response to the client (Service Aggregation).		
3	Prebuilt adapters/connectors for core banking, payment processing, loan origination, card switch, CRM, and other ancillary systems.		
4	When backend systems are upgraded or replaced, the platform must absorb changes by adjusting connectors and transformation rules without requiring modifications to consuming channels (Change Abstraction).		
5	Must support direct database / linked server connections Must support direct database connections for legacy system integration where API/Service layers are strictly unavailable, with robust query sanitization to prevent injection attacks and OFS (Open Financial Services) message format for core banking integration.		
6	Pre-Post processing hooks: ability to execute custom logic (validation, enrichment, transformation) before forwarding a request to the backend and after receiving the response.		
7	Support for asynchronous messaging via RabbitMQ and/or Apache Kafka for event-driven integration scenarios.		
8	Finacle CBS Integration: Must support Finacle Integrator (FI) standard message formats, Finacle's specific		

SL	Functional Requirements:	Availability (A/PA/RM/NA)	Comments
	XML/JSON structures, and ISO 8583 customization out-of-the-box.		
9	Finacle Security & Session: Require support for Finacle's standard security tokens and session management protocols.		
C. Payment & Channel Services			
1	Biller Aggregation: A unified interface to integrate with multiple billers (utility, telecom, government), allowing customers to pay bills through all bank channels.		
2	Payment Rails: Support for domestic and international payment networks including real-time payments, ACH, BEFTN, RTGS, and card networks with built-in ISO 8583 message parsing.		
3	QR & Mobile Payments: APIs to generate, present, and process QR codes for person-to-business (P2B) payments and mobile push payment management.		
4	SMS & Notification Management: Centralized management of SMS notifications, OTP delivery, and alerts with configurable template libraries and delivery reporting.		
5	Terminal Management: Host services for POS terminals and ATMs including message translation and transaction routing capabilities.		
6	Support integration with NPSB (National Payment Switch Bangladesh) and Bangladesh Bank Real-Time Gross Settlement (RTGS) system.		
D. API Catalogue & Asset Management			
1	Central Registry: All APIs must be catalogued in a centralized repository with metadata, versioning, status, and documentation as the single source of truth for the organization.		
2	Role-Based Distribution: Access to API documentation and resources must be restricted based on user profiles (internal developers, partners, regulators).		

SL	Functional Requirements:	Availability (A/PA/RM/NA)	Comments
3	Reusable API Resources: APIs designed around common business entities and functions to enable reuse across multiple applications, reducing duplication and maintenance effort.		
4	Lifecycle Management: Tools for API versioning, deprecation, and retirement with automated consumer notifications and migration guidance.		
5	Knowledge Preservation: Central storage of API definitions, workflows, and policies to ensure integration knowledge persists beyond individual employees and minimizes rework on staff turnover.		
E. Developer Enablement			
1	Auto-Generated Documentation & SDKs: Interactive documentation and software development kits must be automatically generated from API definitions (OpenAPI 3.x / Swagger specification).		
2	Built-in Test Console: Developers must be able to test API endpoints with real or mock data; response times, headers, and payloads must be visible for debugging.		
3	Self-Service Developer Portal: Users can discover APIs, request access, obtain API keys, and monitor usage independently to reduce support overhead.		
4	Automated Health Checks & Test Cases: Automated API health checks and regression test suites to maintain quality as APIs evolve.		
5	Sandbox Environment: A sandbox/mock environment where third-party developers and partners can test integrations without accessing production systems.		
F. Security, Compliance & Observability			
1	Authentication & Authorization: Support for OAuth 2.0, OpenID Connect, HMAC, Mutual TLS, API keys, and fine-grained RBAC policies to protect sensitive banking data.		
2	Data Protection: To ensure message layer security, sensitive parameters in both request and response will be Encrypted. Encryption at rest (AES-256 or equivalent)		

SL	Functional Requirements:	Availability (A/PA/RM/NA)	Comments										
	and in transit (TLS 1.2+), plus tokenization and data masking to safeguard confidential customer and financial information. Each Partner/API User will have separate encryption keys for request and response processing. In Transit Encryption Mechanism [Should be further configurable] <table><tr><th>Parameter</th><th>Value</th></tr><tr><td>Encryption Algorithm</td><td>AES</td></tr><tr><td>Key Length</td><td>256 Bit</td></tr><tr><td>Mode</td><td>Cipher Block Chaining (CBC)</td></tr><tr><td>Encryption Type</td><td>Symmetric</td></tr></table> Special Arrangement for Initialization Vector (IV) and Key Generation must be implemented and should be further configurable HSM Integration: Explicitly mandate native integration capabilities with Hardware Security Modules (HSMs) via standard protocols (PKCS#11).	Parameter	Value	Encryption Algorithm	AES	Key Length	256 Bit	Mode	Cipher Block Chaining (CBC)	Encryption Type	Symmetric		
Parameter	Value												
Encryption Algorithm	AES												
Key Length	256 Bit												
Mode	Cipher Block Chaining (CBC)												
Encryption Type	Symmetric												
3	To ensure request authenticity and data integrity, asymmetric cryptography-based digital signatures will be implemented. Signature Method [Configurable] Digital Signatures: To ensure request authenticity and data integrity, asymmetric cryptography-based digital signatures will be implemented. Must support highly configurable payload parsing and parameter concatenation policies for digital signature generation and validation. SHA-256 hashing and PKI standard must be supported. Must integrate natively with enterprise HSMs. <table><tr><th>Parameter</th><th>Value</th></tr><tr><td>Algorithm</td><td>SHA-256</td></tr><tr><td>Cryptography</td><td>Asymmetric</td></tr><tr><td>Standard</td><td>PKI</td></tr></table> Signature Generation - Specific API parameters will be concatenated using delimiter. Example "+" or "~". Must support highly configurable payload parsing and parameter concatenation policies for digital signature generation and validation.fv - SHA-256 hashing will be applied. - Signature will be generated using the partner's private key. Each partner will have a unique signature key pair.	Parameter	Value	Algorithm	SHA-256	Cryptography	Asymmetric	Standard	PKI				
Parameter	Value												
Algorithm	SHA-256												
Cryptography	Asymmetric												
Standard	PKI												

SL	Functional Requirements:	Availability (A/PA/RM/NA)	Comments
4	Threat Prevention: Policies for throttling, rate limiting, and anomaly detection to mitigate DDoS attacks, SQL/code injection attacks, and other API-specific threats. Must comply with OWASP API Security Top 10.		
5	Compliance Readiness: Platform must assist compliance with Bangladesh Bank ICT Security Guidelines, PCI DSS, ISO/IEC 27001, and applicable data-privacy regulations through security audit logging and consent management.		
6	Immutable Audit Logs: All API transactions, access events, and administrative actions must be logged in immutable audit logs retained for a minimum of 5 years as per Bangladesh Bank requirements.		
7	Real-Time Monitoring & Analytics: Operational dashboards providing real-time visibility into API usage, performance metrics, error rates, and system health for proactive monitoring and optimization. Real-Time Monitoring & Analytics: Operational dashboards providing real-time visibility into API usage, performance metrics, error rates, and system health for proactive monitoring and optimization. Integration: Must include ability to export metrics and alerts to standard infrastructure monitoring and SIEM solutions (e.g., Zabbix, Wazuh)		
8	Distributed Tracing: End-to-end distributed tracing and log aggregation (ELK Stack or equivalent) for root-cause analysis and audit requirements.		
9	The solution must undergo a third-party security audit / penetration testing prior to go-live and results must be shared with the Bank.		

G. Open Banking & AI / Future Readiness

SL	Functional Requirements:	Availability (A/PA/RM/NA)	Comments
1	Open Banking & Open Data: Platform must enable secure data sharing with third parties through controlled API exposure with authentication and consent management for participation in current and future open banking initiatives.		

SL	Functional Requirements:	Availability (A/PA/RM/NA)	Comments
2	AI / MCP Integration Readiness: The platform should be capable of exposing managed APIs as Model Context Protocol (MCP) servers to support large language model (LLM) and AI agent integration for future AI-driven banking workflows.		
3	API Monetization: Controlled exposure of APIs enabling subscription-based access for fintech partners or corporate clients to generate new revenue streams.		
4	Analytics-Driven Insights: Usage and performance data to help IT and business teams identify popular services, plan capacity, and optimize products based on customer behavior.		
H. Vendor Independence & Cost Efficiency			
1	Neutral Integration Layer: The platform must provide a vendor-agnostic integration layer reducing reliance on proprietary APIs and bespoke connectors supplied by core banking vendors.		
2	Unlimited API Creation at No Additional Cost: The platform must not charge per-API licensing fees. Unlimited internal and external APIs must be creatable without additional licensing cost. Licensing & Scalability: The vendor must provide a highly scalable, predictable licensing model that does not incur prohibitive costs as the volume of internally managed APIs grows.		
3	Future-Proofing: When internal systems are replaced or upgraded, the platform must shield external applications from changes by abstracting differences through adapters and transformation policies.		
4	Cost Optimization: Centralizing API calls through the gateway should reduce per-user or per-client fees charged by core systems. Reusable APIs and low-code workflows must also cut development and maintenance costs.		
I. Operational Excellence & Business Impact			
1	Rapid Product Delivery: The platform's low-code		

SL	Functional Requirements:	Availability (A/PA/RM/NA)	Comments
	integration and reusable APIs must shorten development cycles, enabling the Bank to bring new products and features to market quickly.		
2	Standardization: By using industry standards for API design, security, and documentation, the platform must ensure that APIs are consistent and easy for partners to consume. Must also facilitate regulatory approvals and audits.		
3	High Availability: The solution must achieve a minimum of 99.9% system uptime SLA (excluding scheduled maintenance windows) through redundant architecture, load balancing, and automated failover.		
4	Disaster Recovery: Separate DR environment synchronized with the primary data center; Recovery Time Objective (RTO) $\leq$ 4 hours; Recovery Point Objective (RPO) $\leq$ 1 hour.		
5	Scalability: The platform must support horizontal and vertical scaling. Containerized deployment (Docker / Kubernetes) is preferred. Must support multi-node clustering.		
6	Performance: Minimum API response latency < 200 ms (P95) under normal load; minimum throughput of 10,000 API calls per second (TPS) with horizontal scalability; support for minimum 5,000 concurrent API consumers.		
*	The proposed API Gateway Solution must seamlessly integrate with the Bank's Core Banking System (CBS), Islamic Banking CBS (if applicable), Card Management System, Internet Banking, Mobile Banking, Agent Banking, Payment Gateway, Enterprise Service Bus (ESB)/Middleware, Customer Relationship Management (CRM), and other internal and external applications, enabling secure, reliable, and centralized API management across Community Bank Bangladesh PLC.		
*	The proposed solution shall comply with the ICT Security Guidelines, Core Banking Solution (CBS) Guidelines, Cyber Security Guidelines, and all other applicable circulars, directives, and regulatory requirements issued by Bangladesh Bank. The solution shall also support the implementation of future regulatory changes and security requirements through configurable policies without requiring significant application modifications.		

Others Requirement:

- Specify the hardware requirement separately for DC, DR & UAT
- Specify the software requirements separately for DC, DR & UAT

STANDARD FORMAT OF FINANCIAL PROPOSAL

Financial Proposal - Standard Forms

Summary of Costs

Option- 1 (Perpetual License):

Financial Proposal (Details)		
Item Description	Qty	Price (In BDT)
Supply, Install, Configure, Integrate, Test and Deploy (at DC & DR) cost of API Gateway Solution.	1	
Total		
VAT and AIT		
Grand Total (Including VAT & AIT)		

Recurring Costs (AMC)

Module No	Item description		Yearly AMC (Including VAT & AIT) after 1 Year Warranty			
			2	3	4	5
	Particulars		BDT	BDT	BDT	BDT
01	API Gateway Solution.	In amount				
	In percentage (%)					

Additional Customization and Training Cost Per Man-day

Additional customization cost per man-day (Including VAT & TAX) in BDT	Training cost per man-day (Including VAT & TAX) in BDT

Option- 2 (Subscription based License):

Financial Proposal (One Time Cost)		
Item Description	Qty	Price (In BDT)
Supply, Install, Configure, Integrate, Test and Deploy (at DC & DR) one time cost of API Gateway Solution.	1	
Total		
VAT and AIT		
Grand Total (Including VAT & AIT)		

Financial Proposal (Monthly Subscription)		
Item Description	Qty	Price (In BDT)
Monthly Subscription fee of API Gateway Solution.	1	
Total		
VAT and AIT		
Grand Total (Including VAT & AIT)		

Additional Customization and Training Cost Per Man-day	
Additional customization cost per man-day (Including VAT & TAX) in BDT	Training cost per man-day (Including VAT & TAX) in BDT