CENTRAL BANK OF SUDAN

Payment Systems Department

REQUEST FOR PROPOSAL (RFP)

FOR THE

NATIONAL INSTANT PAYMENT SYSTEM (NIPS)

REQUEST FOR PROPOSAL

RFP Reference: CDNIPS202601

HOW TO USE THIS DOCUMENT

This Request for Proposal ("this RFP") is a single, self-contained instrument covering the design, supply, development, implementation and ongoing support of the National Instant Payment System (NIPS) of Sudan as one fully integrated system, comprising the core platform, the Central Bank-owned payment application that will serve as its principal consumer and merchant interface, the merchant, supervisory and integration tools, the USSD access channel and the national dispute management and resolution system.

Document Organisation

Part	Content
Part I	Purpose, background, strategic objectives, programme structure, governance and award arrangements.
Part II	Instructions to Bidders: schedule of events, definitions, submission mechanics, proposal format and content, and commercial and pricing requirements.
Part III	Scope of work for the solution and each of its elements, project delivery, deliverables, knowledge transfer, testing, support and maintenance, licensing and intellectual property.
Part IV	Solution requirements: functional, non-functional, integration, regulatory, analytics, dispute management and technical specifications, each carrying a requirement identifier against which the Bidder must record a response.
Part V	Vendor qualification requirements and the evaluation criteria and selection process.
Part VI	Standard proposal information, standard contract information and indicative contract terms.
Appendices	Pricing worksheet, compliance matrices, reference documents to be provided by the Bank, the bidder comments sheet and the acknowledgement form.

Order of Precedence

In the event of any inconsistency, the following order of precedence applies:

1. This RFP and any addenda subsequently issued against it
2. The Bank's written responses to bidder questions
3. The appendices to this RFP

TABLE OF CONTENTS

PART I: PURPOSE, BACKGROUND AND PROGRAMME STRUCTURE

1. PURPOSE

This Request for Proposal is issued by the Central Bank of Sudan (hereinafter "the Bank" or "the Central Bank"), inviting technical and commercial proposals from qualified Bidders for the design, supply, development, implementation, and ongoing support of the National Instant Payment System (NIPS) of Sudan. NIPS is procured as one fully integrated national system, under a single scope of supply, and comprises:

- **The NIPS core platform** — the national instant payment switch enabling real-time retail payments in the domestic payments in Sudan; and
- **The NIPS payment application and access channels** — the Central Bank-owned and governed mobile payment application, the USSD access channel and the associated merchant, supervisory and integration tools, serving as the primary consumer and merchant interface to that infrastructure, together with the national dispute management and resolution system operating across the whole of NIPS.

1.1 Programme Objectives

The main objectives of the programme are to:

Ref.	Objective
OBJ-01	Implement a National Instant Payment System that enables real-time payments in the domestic payments in Sudan.
OBJ-02	Ensure that the implemented solution supports real-time or near real-time payment transmission on as near to a 24-hour, seven-day (24x7) basis as possible.
OBJ-03	Guarantee interoperability with existing payment and settlement platforms in Sudan, including the Sudan Interbank Settlement System, the Real Time Gross Settlement System (RTGS), and other Sudanese payment methods.
OBJ-04	Facilitate both direct and indirect participation by commercial banks, financial institutions and other payment service institutions operating in the domestic payments.
OBJ-05	Develop user-friendly mobile applications enabling 10 million or more users to conduct instant payments.
OBJ-06	Ensure seamless integration between the consumer channels and the core NIPS platform APIs.
OBJ-07	Deliver an exceptional user experience with sub-five-second payment flows.
OBJ-08	Implement enterprise-grade security and compliance features.

Ref.	Objective
OBJ-09	Support financial inclusion through intuitive, accessible design, including access for citizens without smartphones or reliable internet connectivity.

1.2 Additional Considerations

The Bank seeks a Bidder with a proven track record of delivering the services and solutions outlined herein, a demonstrated awareness of the spectrum of solutions available in the market, and the capacity to manage timelines, deliverables and implementation risks. Other factors that shall contribute to the selection of a Bidder include, but are not limited to, total cost, service and support, ease of use of the proposed solution, and interoperability with existing platforms and third-party applications.

Note: Bidders should note that legislative amendments to the Sudan Payments System Act or related statutes may be required. Proposals should incorporate the flexibility to accommodate potential regulatory changes during implementation.

2. BACKGROUND

2.1 The Central Bank of Sudan

The Central Bank of Sudan, established in 1960, has as its mission *"to foster an environment of monetary stability conducive to economic development, and to ensure a stable and sound financial system through the highest standards of integrity and leadership."*

The Central Bank of Sudan is launching a national instant payment scheme at country level, taking the lead in the digital transformation strategy announced by the Ministry of Digital Transformation since 2025. The project aims to facilitate national immediate transfers between parties of all categories — person to person, person to government, and person to business, and the reverse.

2.2 Payment System Development

The Bank has progressed several projects to drive increased payments efficiency, including:

- The establishment of the Real Time Gross Settlement System (RTGS)
- The introduction of legislation to license and oversee non-bank providers of electronic payment instruments
- The simplification of requirements for account opening
- The increased adoption of digital payment alternatives over the last five years

2.3 Current Retail Payment Landscape

The national payment ecosystem currently exhibits the following characteristics, which the solution is intended to address:

Ref.	Characteristic	Challenge
CL-01	Multiple bank-operated and third-party payment applications	Limited interoperability, fragmented user experience
CL-02	Fragmented customer experience	Users must install multiple applications
CL-03	High cash dependency for retail transactions	Limits financial inclusion and digital economy growth
CL-04	Limited Central Bank visibility into end-user payment behaviour	Hinders evidence-based policymaking and oversight
CL-05	Inconsistent security and consumer protection standards	Exposes users to fraud and disputes

2.4 Strategic Objectives

The goals of the Payment Systems Department are closely linked to the objectives of the solution, which include:

Ref.	Strategic Objective
SO-1	Provide a unified, Central Bank-licensed payment application accessible to all citizens and merchants regardless of their banking relationship.
SO-2	Enable seamless instant payments and transfers across all participating banks, payment service providers and wallet operators through integration with NIPS.
SO-3	Accelerate the transition from cash to digital payments and advance national financial inclusion goals.
SO-4	Establish a comprehensive data ecosystem enabling real-time supervisory oversight, consumer protection and evidence-based policy formulation.
SO-5	Create a scalable platform capable of supporting future payment innovations and government digital service delivery initiatives.
SO-6	Support enhanced commerce by facilitating timely payments.
SO-7	Foster innovation in the domestic payments landscape.
SO-8	Promote a reduction in the size of legitimate but unrecorded economic activity taking place in the informal sector.

3. SYSTEM STRUCTURE — SOLUTION ELEMENTS

The solution sought under this RFP is a single, fully integrated national instant payment system, delivered under one scope of supply and comprising the following elements, each of which forms part of one indivisible deliverable:

Element	Name	Summary
Core layer	NIPS Core Platform	The national instant payment switch: clearing and settlement, participant management, proxy identifier (alias) directory, ISO 20022 messaging, interoperability with the national switch and RTGS, administration, reporting and billing.
User layer	NIPS Payment Application	The Central Bank-owned consumer and merchant mobile application and its supporting back-end platform, merchant tools, supervisory tools and integration layer.

Element	Name	Summary
Cross-cutting	Dispute Management and Resolution System	A single national dispute management system covering the full lifecycle of consumer, merchant and inter-participant disputes, claims, reversals and adjudication, delivered by the service provider as an integral part of the solution (Section 28).
Channel	USSD Access Channel	A menu-driven channel available on all GSM handsets without internet connectivity, mandatory for financial inclusion, delivered as part of the overall solution.

3.1 Solution Overview

The proposed solution will encompass the following key functional capabilities:

- The secure transmission of payment messages and the availability of final funds (settlement) to the payee, occurring in real time or near real time, on as near to a 24-hour, seven-day basis as possible.
- The use of ISO 20022 messaging standards, where applicable, for richer and more structured data, enhancing customer insights and experience, better payment reconciliation, and faster processing.
- Utilisation of a real-time settlement model between participants, as opposed to a deferred net settlement model.
- The ability for end users to utilise multiple types of proxy identifiers (aliases) to perform payments.
- Application Programming Interfaces (APIs) to allow for integration and interoperability, including an interface with the central bank's digital currency.
- Configurability for high availability to allow for uptime on as near to a 24x7 basis as possible.

3.2 Core Solution Requirements

Overall, the selected core solution must:

Ref.	Requirement
CSR-01	Be a commercial off-the-shelf (COTS), real-time settlement solution that aligns with the functional requirements defined in this RFP.
CSR-02	Have been successfully implemented for at least one central bank in the last 18 months.
CSR-03	Be configurable to meet the current and future operational needs of the Bank.
CSR-04	Include standardised APIs to enable seamless integration with other existing payment systems.
CSR-05	Be stable, secure and accessible, supporting continuous service delivery, transparency and user trust.
CSR-06	Readily integrate with the Sudanese Pound (SDG) for ease of payment and settlement in the domestic market.

Note on the payment application: The requirement for a commercial off-the-shelf product applies to the core platform. The payment application is expected to be a Central Bank-branded application; bidders may propose a configurable product base, but all custom-developed elements are subject to the intellectual property terms in Section 20.

3.3 Future Abilities

The Central Bank of Sudan requires the ability to add further features to the solution, including but not limited to:

Ref.	Future Feature	Description
FF-01	Remittance Services	Regional and international money transfer capabilities
FF-02	Request to Pay	Ability to request payments from other clients
FF-03	Dynamic QR Payments	Dynamic QR codes for merchant payments
FF-04	Card Scheme Integration	Future integration with international card schemes (Visa, Mastercard)
FF-05	Cross-border Services	Cross-border payment and settlement capabilities

Bidders must clearly indicate how their proposed solution can be extended to accommodate these future requirements without significant re-architecting.

4. GOVERNANCE AND OWNERSHIP MODEL

The Bank will retain full ownership, governance and operational oversight of the solution. Bidders must structure proposals to reflect the Bank as the system operator.

Element	Provision
Ownership	The Central Bank of Sudan retains full ownership of the platform, the payment application, its brand, and all user and transaction data. The Bank shall maintain full control and unequivocal rights to all data stored, created and developed as part of this contract.
Licensing	The system and its payment application operate under a Central Bank of Sudan licence with direct regulatory oversight.
Governance	The Central Bank Payment Systems Committee provides strategic direction. Project governance runs from the Governor through the Project Steering Committee to the Bank's Project Manager, who interfaces with the Prime Bidder; subcontractors sit under the Prime Bidder.
Operations	Day-to-day operations may be delegated to a qualified service provider under a strict service level agreement and oversight regime.
Revenue Model	Transaction fees, merchant discount rates and value-added services, as determined by Central Bank policy.
Legislation	Bidders should note that legislative amendments to the Sudan Payments System Act or related statutes may be required. Proposals should incorporate the flexibility to accommodate potential regulatory changes during implementation.

5. TYPES OF PROPOSALS AND CONTRACT AWARD

5.1 Types of Proposals

Bidders are required to submit one proposal in the form of two documents: a technical proposal document and a separate cost proposal document (Section 10). Bidders are limited to one proposal per Prime Bidder. Bidders may collaborate with others who may be included as subcontractors on multiple proposals. The result will be one contract between the Bank and the Prime Bidder for the complete solution.

The Prime Bidder shall be wholly responsible for meeting the requirements of the RFP, for submission of the proposal, and for performance of the entire contract awarded to it. The Bank will consider the Prime Bidder to be the sole point of contact with regard to all contractual matters, including payment of all charges.

5.2 Delivery Approach

Bidders must propose the complete solution as a single, fully integrated system. Bidders must state clearly which of the following delivery approaches is being offered:

Option	Description
Option A	A fully integrated solution in which the core platform, the payment application and all channels are delivered from a single product base by the Prime Bidder
Option B	An integrated solution in which the payment application and channels are delivered from a distinct product base or by a subcontractor, with clearly defined integration touchpoints to the core platform, for which the Prime Bidder remains wholly responsible

Partial proposals will not be accepted. A proposal that does not cover the complete scope of the solution set out in this RFP — the core platform, the payment application, the merchant, supervisory and integration tools, the USSD access channel and the dispute management and resolution system — will be rejected as non-responsive.

5.3 Contract Award

A contract awarded by the Bank will be based upon the criteria, standards and weighting identified in this RFP as applied to the solution proposal. Each Bidder's proposal will be considered as a whole solution, without limitation, including software and services proposed, qualifications of the Bidder and any subcontractors, and cost.

The Bank reserves the right, at its sole discretion and in the best interest of the project, to:

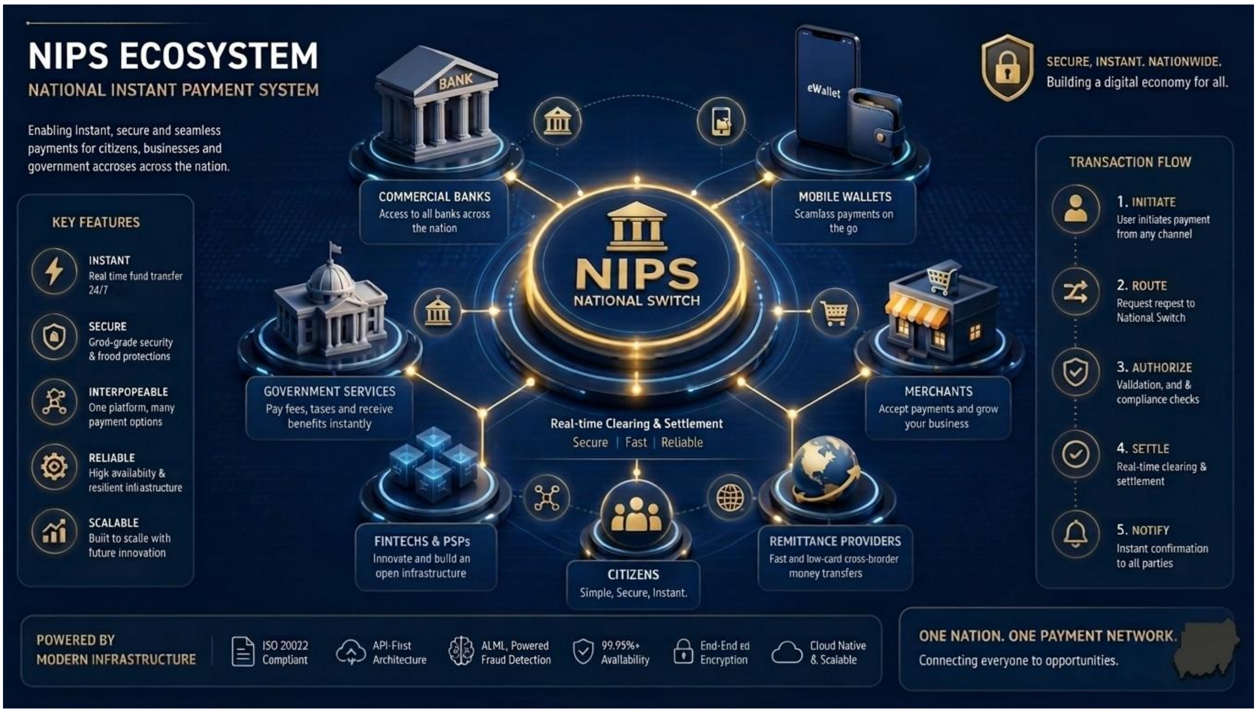
Ref.	Award Option
AW-01	Award a single contract to one Bidder for the entire solution and services
AW-02	Award multiple, separate contracts to more than one successful Bidder, if it deems that this approach delivers the best value and enhances the project's objectives. This could include, but is not limited to, engaging more than one prime vendor to distribute the workload or the project phases for redundancy and risk mitigation, provided that the solution is delivered, integrated and operated as one system.

In the event of a multiple contract award, each successful Bidder will be individually responsible for their respective portion of the scope of work, while the Bank retains ultimate responsibility for overall solution integration and project management. Bidders will be informed of any such decision during the contract negotiation phase.

The Bank further reserves the right to award to other than the lowest bidder, to negotiate with selected bidder(s), to conduct proof-of-concept evaluations, and to cancel or reissue this RFP.

5.4 Contract Terms

The terms of service are anticipated to commence within two to four weeks of the contract agreement. A kickoff meeting to align objectives is required, followed by the other key documents, including project scope and timeline for completion. The indicative contract duration is an initial term of three years from production go-live, renewable for an additional two-year term by mutual agreement.



NATIONAL INSTANT PAYMENT SYSTEM (NIPS) ENTERPRISE ECOSYSTEM ARCHITECTURE

PART II: INSTRUCTIONS TO BIDDERS

6. SCHEDULE OF EVENTS

The following table provides the Schedule of Events for this RFP through contract execution. The contract term and work schedule set out herein represent the Bank's best estimate of the schedule that will be followed. If a component of this schedule (such as the proposal submission deadline) is delayed, then the rest of the schedule will be adjusted as needed.

Event	Date	Time
Request for Proposal issue date		—
Deadline for submitting questions		—
Date for question responses		—
Proposal submission deadline		+02:00GMT
Shortlisted vendor presentations		—
Notice of Intent to Award		—
Contract sign-off		—

Note: All questions regarding this RFP must be submitted in writing by the date indicated above, which will typically be fourteen days before the submission deadline. Responses to all questions will be published as an addendum to all registered bidders.

7. DEFINITION OF TERMS

Term	Definition
Automation	The technique of making a process or a system function operate automatically.
Bidder	Any recipient of this RFP who submits a proposal. All references that would normally use the words Firm, Vendor, Offeror, or Respondent have been changed to Bidder for consistency.
The Central Bank / the Bank	The Central Bank of Sudan, including the related entities seeking the services described in this RFP, the Bank's employees, and independent consultants and vendors retained by the Bank for this project.
Commercially Available	The material or goods must be available from a Bidder that provides ongoing support, maintenance and licensing. Shareware and public domain software are not considered commercially available.
Contract / Agreement	A signed agreement for the services between the successful Bidder and the Bank.
Contractor	The vendor selected as the Prime Bidder as a result of this RFP.
Disaster Recovery	The ability to recover from the loss of a complete system or site, whether due to natural disaster, system failure or malicious intent. Strategies include replication and backup/restoration.
EOL / EOVS	End of Life / End of Vendor Support.

Term	Definition
High Availability	The capability to maintain continuous operation and service delivery, minimising downtime and ensuring user access even in the face of component failures or disruptions.
Must / Shall / Mandatory / Required	A requirement that must be met in substantially unaltered form for the proposal to receive consideration.
NIPS	The National Instant Payment System procured under this RFP as one integrated system, comprising the core platform, the payment application, the merchant, supervisory and integration tools, the USSD access channel and the dispute management and resolution system.
Payment Application	The Central Bank-owned consumer and merchant payment application, and its supporting back-end platform, forming an integral part of NIPS.
On-premises	IT infrastructure hosted on an organisation's premises, allowing full control over server management, security, and maintenance of networking equipment and data storage.
Orchestration	The automation of linked workflows.
Project	The objective of the contract as a whole; the sum total of all elements of the contract.
Proposal	The submission from a Bidder in response to this RFP.
Role-Based Access Control (RBAC)	An access control method that assigns access rights based on user roles in the organisation.
Services	Labour, resources and materials provided by the Contractor as required to execute the Agreement.
Should / Desirable	A requirement having a significant degree of importance to the objectives of this RFP.
Solicitation	The invitation by the Bank to submit formal quotations, bids, tenders, proposals or statements of qualifications.
Subcontractor	The party contracted with the Prime Bidder to deliver part or all of the solution, having no direct contractual relationship with the Bank.
Successful / Winning Bidder	The successful proponent to this RFP who enters into a written contract with the Bank.
Supplier	An individual, Bidder, consultant or group awarded an agreement under a Bank solicitation invitation.
TBD	To Be Determined.

8. PROPOSAL INSTRUCTIONS

8.1 Proposal Inquiries

All inquiries, interpretations or clarifications, either administrative or technical, regarding this RFP must be requested by email no later than the date indicated in the Schedule of Events. All non-proprietary written questions will be answered in writing and conveyed to all Bidders. Oral statements concerning the meaning or intent of the contents of this RFP by any person are not binding.

Questions should be sent electronically to:

Detail	Information
Recipient	Tenders Committee, Central Bank of Sudan
Subject Line	CDNIPS202501 — National Instant Payment System (NIPS) Solution — Request for Proposals

8.2 Delivery of Proposal

Electronic copies of the proposal must be received by the date and time stated in the Schedule of Events. Faxed, hardcopy or oral proposals will not be accepted and could result in disqualification. A Bidder's failure to submit its proposal within the submission timeline will disqualify the proposal; late proposals or amendments will not be accepted for evaluation.

All proposals must consist of a single electronic version of the proposal, including all required attachments (which may be separate electronic documents but must be clearly identified), accompanied by a digitally signed transmittal letter as described in Section 9.2. The Cost Proposal must be submitted as a separate electronic document.

Requirement	Specification
Format	PDF format with searchable text
Subject Line	"NIPS RFP Proposal — [Bidder Name]"

8.3 Required Review

Bidders should carefully review this solicitation for defects and questionable or objectionable material. The Bank must receive comments concerning defects and objectionable material at least five days before the proposal opening. This will allow issuance of any necessary amendments and help prevent the opening of a defective solicitation. Protests based on any omission or error, or on the content of the solicitation, will be disallowed if these faults have not been brought to the attention of the Bank, in writing, at least five days before the time set for bid opening.

8.4 Errors and Omissions

If, prior to the date fixed for submission, a Bidder discovers any ambiguity, conflict, discrepancy, omission or other error in this RFP or any of its exhibits and appendices, the Bidder shall immediately notify the Bank in writing and request modification or clarification. Modifications may be made by addenda prior to the response deadline. Clarifications will be given by written notice to all active Bidders, without divulging the source of the request.

8.5 Addenda

The Bank may modify this RFP, any of its key action dates, or any of its attachments prior to the date fixed for submission, by issuance of a written addendum posted to its website. Addenda will be numbered consecutively as a suffix of the RFP reference number.

8.6 Amendments to Proposals

Amendments to, substitutions of, or withdrawals of proposals will only be allowed if acceptable requests are received prior to the deadline set for receipt of proposals. No amendments, substitutions or withdrawals will be accepted after the deadline, unless in response to the Bank's request.

8.7 Right of Rejection

Bidders must comply with all terms of this RFP and all applicable laws governing the Republic of Sudan. The Bank may reject any proposal that does not comply with all of the material and substantial terms, conditions and performance requirements of this RFP, without incurring any liability or obligation to inform the Bidder of the grounds for the Bank's action.

The Bank may waive minor informalities that:

- Do not affect responsiveness
- Are merely a matter of form or format
- Do not change the relative standing or otherwise prejudice other offers
- Do not change the meaning or scope of the RFP
- Are trivial, negligible or immaterial in nature
- Do not reflect a material change in the work
- Do not constitute a substantial reservation against a requirement or provision

The Bank reserves the right to refrain from making an award if it determines that to be in its best interest.

8.8 Subcontractors

Please look at the bidding announcement

8.9 Conflict of Interest

Each proposal shall include a statement in the transmittal letter indicating whether or not the Bidder or any individual working on the contract has a possible conflict of interest (for example, employment by the Bank) and, if so, the nature of that conflict. The Bank reserves the right to cancel the award if any interest disclosed from any source could either give the appearance of a conflict or cause speculation as to the integrity of the solution by the Bidder. The Bank's determination regarding any question of conflict of interest shall be final.

8.10 Bidder's Certification

By signature on the proposal, Bidders certify that they comply with:

Ref.	Certification
CERT-01	The laws of the Republic of Sudan, including Value Added Tax (VAT) compliance and holding a valid business licence
CERT-02	All terms and conditions set out in this RFP

Ref.	Certification
CERT-03	A condition that the proposal submitted was independently arrived at, without collusion, under penalty of perjury
CERT-04	The requirement that the offer will remain open and valid for the validity period stated in Section 8.13

If a Bidder fails to comply with CERT-01 through CERT-04, the Bank reserves the right to disregard the proposal, terminate the contract, or consider the contractor in default.

8.11 Non-collusion

The Bidder's signature on a proposal submitted in response to this RFP guarantees that the prices, terms and conditions, and services quoted have been established without collusion with other Bidders and without effort to preclude the Bank from obtaining the best possible competitive proposal.

8.12 Confidentiality and Disclosure of Proposal Content

All proposals and other material submitted become the property of the Bank and may be returned only at its option. All proposal information, including detailed price and cost information, will be held in confidence during the evaluation process and prior to the time a Notice of Intent to Award is issued.

Trade secrets and other proprietary data contained in proposals may be held confidential if the Bidder requests this in writing and the Bank agrees in writing to do so; material considered confidential by the Bidder must be clearly identified with a brief statement of the reasons for confidentiality.

Bidders shall treat all RFP information as confidential and shall not disclose it to third parties without written permission, and shall not use RFP information for purposes other than preparing and submitting a proposal.

8.13 Validity Period

Proposals shall remain valid and open for acceptance for a period of not less than **180 days** from the proposal submission deadline. Pricing shall likewise remain valid for a minimum of **180 days**from the submission deadline.

8.14 System Demonstrations

The Bank reserves the right to require a Bidder to make system demonstrations of the proposed solutions onsite at its main office in Khartoum. All costs associated with a demonstration shall be borne entirely by the Bidder.

9. PROPOSAL FORMAT AND CONTENT

Bidders must organise their proposals in the structure below. The proposal comprises a Technical Proposal (Volumes 1, 2, 3 and 5) and a separate Cost Proposal (Volume 4).

9.1 Proposal Structure

Volume	Content	Page Limit
Volume 1	Cover page, transmittal letter, table of contents, and executive summary (concise overview of the proposed solution, excluding pricing information; bidders are encouraged to highlight factors that distinguish their proposal).	Executive summary: 10 pages
Volume 2	Technical proposal: introduction, bidder background, experience and references; solution architecture and general system design; functional and non-functional requirement response matrices; integration approach; security architecture; technology stack justification; innovation and value-added features; responses to Appendices B, C and D.	75 pages
Volume 3	Implementation plan: project methodology and governance; detailed work plan with milestones; resource plan and team structure; risk register and mitigation strategies; the vendor risk management programme; testing strategy; training and knowledge transfer plan.	40 pages
Volume 4	Commercial proposal (submitted as a separate electronic document): detailed cost breakdown; three-year total cost of ownership worksheet; payment schedule proposal; licensing and subscription terms; pricing assumptions and exclusions; post-warranty support options.	20 pages
Volume 5	Compliance and qualifications: compliance matrix for mandatory requirements; draft contract including confidentiality and non-disclosure clauses; company registrations and certifications; valid tax compliance certificate; National Insurance Board certificate (if applicable); current business licence; audited financial statements; insurance certificates; reference project details; key personnel CVs; attachments and supporting documentation.	No limit

9.2 Cover Page and Transmittal Letter

The first page of the Bidder's proposal must be a cover page containing the following text:

CENTRAL BANK OF SUDAN — PAYMENT SYSTEMS DEPARTMENT — RESPONSE TO RFP No. CDNIPS202501, NATIONAL INSTANT PAYMENT SYSTEM (NIPS) SOLUTION REQUEST FOR PROPOSALS

The cover page must also include the Bidder's name, contact person, contact telephone and/or fax number, address, city, state, country, postal code and e-mail address.

The Bidder must submit a signed transmittal letter with its response that includes:

Ref.	Transmittal Letter Content
TL-01	The Bidder's legal name and any other name under which the Bidder does business, mailing address, street address for courier services, the name and title of the individual who will sign the contract, the name and title of the Bidder contact person if different, and for each key person a direct telephone number, fax number if applicable, and e-mail address
TL-02	A statement that the individual who signs the transmittal letter is authorised to commit the Bidder
TL-03	A statement that the proposal is effective for the validity period in Section 8.13
TL-04	A guarantee that prices quoted were established without collusion

Ref.	Transmittal Letter Content
TL-05	Acknowledgement that the Bidder has read this RFP and any subsequent addenda
TL-06	A statement indicating whether or not the Bidder or any individual working on the contract has a possible conflict of interest
TL-07	A statement identifying all subcontractors and joint venture partners

9.3 Bidder Background, Experience and References

As the Bank will evaluate the qualifications of key staff proposed by the Bidder, this section must include:

Ref.	Content
BB-01	The proposed team organisation and the designation and identification of key staff
BB-02	The qualifications of the candidate for project manager
BB-03	The qualifications of candidates for key Bidder staff roles (solution design architects, solution engineers, and so on)
BB-04	References covering the last three implementations of the proposed solution

9.4 Proposed Solution

The Bidder must detail the proposed solution up to and including the following:

Ref.	Requirement
PS-01	A brief solution overview of the various solution components, their release history, the current release being proposed, and the number of operational installations of the proposed software
PS-02	A description and illustration of the general system design of the proposed solution
PS-03	A narrative on how the proposed solution addresses the requirements outlined in Part III and Part IV, including the specifications in the appendices, with detailed explanations using Appendix E where required
PS-04	Identification of any additional features, functionality, recommended solution components or services not outlined in this RFP but which the Bidder recommends that the Bank consider, including a description of the features and functions of each additional proposed module
PS-05	A description of the security features of the proposed solution
PS-06	A description of alternative service delivery models (Software-as-a-Service, Application Service Provider, hosted, and so on) available to the Bank, indicating how these might impact the proposed solution
PS-07	Confirmation of the ability to conform to the requirements in Part III and Part IV and the related appendices, or a clear articulation of proposed alternatives
PS-08	Future abilities for the solution: the Central Bank of Sudan requires the ability to add further features to the solution, including but not limited to remittance services, request to pay to other clients, and dynamic QR payments to merchants

The Bidder must provide a point-by-point technical response stating compliance with, or taking exception to, any or all sections of this RFP, and provide sufficient information to allow the Bank to evaluate the proposal. Any deviations or exceptions to the Bank's requirements must be noted. Incomplete proposals, or proposals that do not comply with the Bank's stated requirements, may be eliminated from the selection process at the Bank's discretion.

9.5 Implementation Approach and Work Plan

Bidders are required to describe their proposed implementation approach, clearly identifying each phase, the timeline proposed, and the roles and responsibilities to be performed by the Bidder and by the Bank. The Bidder should clearly indicate the Bank's resource requirements needed to meet the proposed schedule, and shall:

Ref.	Requirement
IA-01	Describe the implementation and project management methodology and approach to ensure a successful implementation
IA-02	Provide a project organisation chart highlighting key staff assigned to the project, with names and resumes for the project manager and other key assigned resources
IA-03	Provide a detailed work plan identifying major activities, tasks, deliverables and resources. The work plan should assume that the project will kick off no more than three weeks after approval of the contract by the Bank
IA-04	Describe the roles and responsibilities of Bank staff during implementation, including the minimal and optimal number of Bank staff members by job category and the expected role and level of effort during each phase
IA-05	Describe the roles and responsibilities of Bank staff required to maintain and update the system during the first five years, including minimal and optimal headcount by job category and ongoing level of effort
IA-06	Describe the change management methodology and activities to be performed during implementation
IA-07	Describe the user acceptance methodology and the responsibilities of Bank staff during testing
IA-08	Describe the training methodology and approach
IA-09	Describe how the use of any alternative service delivery model would impact the proposed implementation approach, work plan and Bank staff level of effort

10. COMMERCIAL AND PRICING REQUIREMENTS

10.1 Cost Proposal

The Cost Proposal must be separated from the remainder of the RFP response documents. The Bank seeks a clear and comprehensive understanding of all costs associated with the acquisition, implementation and ongoing maintenance of the proposed solution. Bidders must itemise all costs inclusive of shipping, taxes (for example Value Added Tax) and duties.

In addition to a detailed cost breakdown, a three-year Total Cost of Ownership worksheet must be completed as part of the cost proposal, using the format in Appendix A.

All cost information must be provided in both USD. Costs must be broken down by solution element — core platform; payment application and channels; dispute management and resolution system; and implementation, training and support services — and consolidated into a single total price for the complete solution.

10.2 Cost Breakdown Requirements

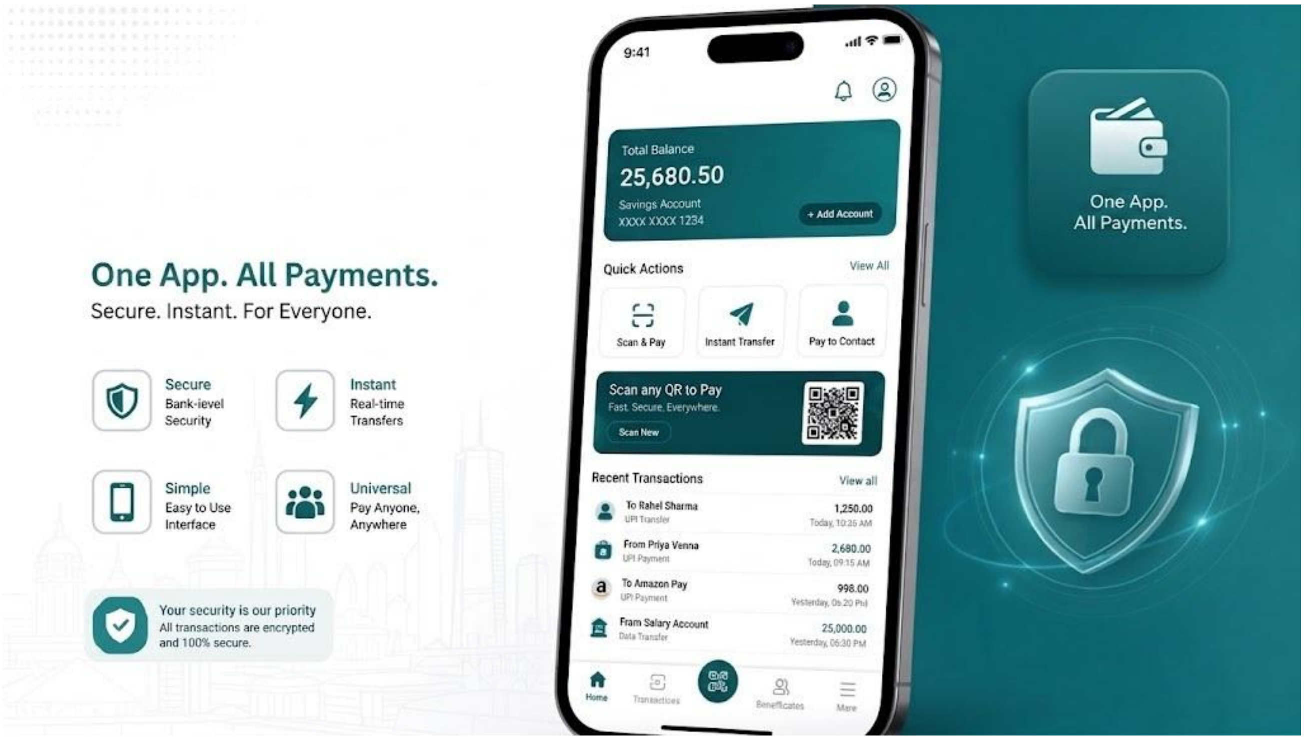
Category	Cost Elements
Implementation Costs	Software licensing (perpetual and subscription); Development effort, by phase and work stream; Infrastructure setup (hardware, cloud services); Testing and quality assurance; Training and knowledge transfer; Project management; Documentation
Ongoing Costs	Annual software maintenance and support; Infrastructure hosting and operations, if applicable; Transaction processing fees, if applicable; Third-party service costs (SMS, hosting, security); Software updates and enhancements
Transaction-Based Pricing	Price per transaction by transaction type; Volume discounts and tier structure; Minimum monthly commitments; Price escalation terms

10.3 Contract Payment Details

This section of the proposal must outline the following terms and conditions, consistent with Appendix A:

Ref.	Payment Term
PD-01	Total contract sum (inclusive of all taxes and charges)
PD-02	Mobilisation deposit
PD-03	Stage payments (milestone-based, tied to delivery and acceptance of specified deliverables)
PD-04	Final payment
PD-05	Retention terms

Payment shall be milestone-based, tied to the delivery and acceptance of specified deliverables, and Bidders shall propose a payment schedule aligned with the implementation phases set out in Section 15.



NIPS PAYMENT APPLICATION — USER EXPERIENCE AND INTERFACE OVERVIEW

PART III: SCOPE OF WORK

11. OVERALL SOLUTION SCOPE

This Part outlines the scope of work for the implementation and deployment of the National Instant Payment System (NIPS) for the Bank as one integrated system, and provides prospective vendors with a clear understanding of the Bank's technical, operational and strategic requirements and expectations.

The selected solution will serve as a foundational component of the Bank's ongoing efforts to modernise the domestic payments infrastructure and support real-time or near real-time payments on a near 24x7 operational basis. The solution must, either directly or indirectly, provide non-discriminatory access to all prospective participants, ensuring equitable participation and fostering financial inclusion. Participants may include licensed commercial banks, financial institutions cand approved non-bank payment service providers.

The Bank intends to utilise an indirect real-time gross settlement model as the primary settlement mechanism (passing the clearing file through the national switch clearing mechanism, or the NIPS providing its own clearing modules). This is to be achieved by using dedicated prefunded RTGS accounts for each.

12. NIPS CORE PLATFORM SCOPE

12.1 Supply of Software and Licences

The Bidder will supply the required licences as they relate to the supply and support of the NIPS solution, as per the Bank's specifications. The Bank will provision all required hardware based on the Bidder's specifications and recommendation; accordingly, Bidders must provide a comprehensive outline of the server sizing and specifications required to support optimal performance, scalability and availability.

12.2 Implementation and Integration Services

The Bidder will be responsible for the installation and commissioning of the entire solution. Installation and commissioning services will include, but not be limited to:

Ref.	Service
IMP-01	Installing the instant payment system solution at the Bank's primary and secondary data centres
IMP-02	Configuring high availability for the solution
IMP-03	Operationalising and optimising the NIPS solution
IMP-04	Configuration of all features included in this RFP
IMP-05	Project documentation
IMP-06	Project hand-over inclusive of user and administrator training
IMP-07	Completion of the project end to end

Ref.	Service
IMP-08	Stepwise documentation for all administrative activity
IMP-09	Post-implementation hypercare support for 60 days following go-live, provided in addition to, and within, the warranty period defined in Section 19

12.3 Vendor Risk Management Programme

The Bidder shall maintain a documented risk management programme consistent with recognised frameworks, together with associated strategies. The programme must cover technology, operations, information security, fraud, privacy, third-party and supply chain risk, and must be applied to the solution through implementation and steady-state operations.

13. PAYMENT APPLICATION, MERCHANT AND SUPERVISORY TOOLS SCOPE

13.1 In-Scope Deliverables

13.1.1 Mobile Applications

Ref.	Deliverable
APP-01	Native mobile applications for Android (version 8.0 and above) and iOS (version 13.0 and above)
APP-02	A Progressive Web Application (PWA) for broader accessibility
APP-03	Tablet-optimised interfaces for merchant point-of-sale scenarios
APP-04	Offline capability for transaction queuing and balance viewing

13.1.2 Back-End Platform

Ref.	Deliverable
APP-05	Application server infrastructure with a microservices architecture
APP-06	An API gateway for secure communication with NIPS, banks, PSPs and third-party services
APP-07	A user identity and access management system
APP-08	A transaction processing and routing engine
APP-09	A real-time notification and messaging service
APP-10	A comprehensive logging, monitoring and analytics platform

13.1.3 Merchant Solutions

Ref.	Deliverable
APP-11	A merchant onboarding portal (web and mobile)
APP-12	Static and dynamic QR code generation and management
APP-13	A merchant transaction dashboard and reporting tools

Ref.	Deliverable
APP-14	A settlement reporting and reconciliation interface

13.1.4 Administrative and Supervisory Tools

Ref.	Deliverable
APP-15	A Central Bank supervisory dashboard with real-time transaction monitoring
APP-16	A risk management and fraud detection system
APP-17	A regulatory reporting and analytics module
APP-18	A user support and dispute management system
APP-19	A configuration and parameter management console

13.1.5 Integration Layer

Ref.	Deliverable
APP-20	Secure APIs and messaging interfaces and USSD to the NIPS core switch
APP-21	Integration adapters for bank core banking systems and wallet platforms
APP-22	A biller aggregation platform for utilities, government services and telecom operators
APP-23	National identity verification system integration (KYC/eKYC)
APP-24	SMS gateway and push notification service integration

13.2 Out of Scope (Initial Phase)

The following features are explicitly excluded from the initial implementation phase but may be considered for future phases:

Ref.	Feature
OOS-01	Cross-border remittance services
OOS-02	Credit origination and lending products
OOS-03	Investment and wealth management features
OOS-04	Cryptocurrency or digital currency wallet functionality
OOS-05	E-commerce marketplace integration beyond payment processing

Note: Bidders should note that Section 9.4 requires the solution architecture to accommodate the later addition of remittance services, request-to-pay and dynamic merchant QR. Exclusion from the initial phase does not relieve the Bidder of the obligation to design for these capabilities.

14. USSD ACCESS CHANNEL

USSD (Unstructured Supplementary Service Data) is a real-time communication protocol available on all GSM mobile phones without requiring internet connectivity. It operates through short codes (for example *0123#) and provides an interactive, menu-driven interface accessible to any mobile phone user.

14.1 USSD Key Characteristics

Feature	Description
Internet not required	Works on any mobile phone, including basic feature phones
Real-time interaction	Session-based communication with immediate response
Universal compatibility	Supported by 100% of GSM mobile networks
Simple user interface	Menu-driven navigation using the numeric keypad
Arabic and English support	Full bilingual capability, as required by the Central Bank

14.2 Supported Transactions via USSD

Based on prior approvals from the Ministry of Digital Transformation and Telecommunications and all telecom operators in Sudan, USSD serves as an approved and essential access channel for the National Instant Payment System. It ensures that citizens without smartphones or reliable internet access can still participate in instant digital payments, thereby supporting the Bank's financial inclusion objectives.

Ref.	Supported Transaction
USSD-01	Wallet account opening (onboarding)
USSD-02	Balance inquiry
USSD-03	Instant person-to-person (P2P) transfers
USSD-04	Bill payments (utilities, telecom, and so on)
USSD-05	Mobile airtime recharge
USSD-06	PIN change and wallet blocking
USSD-07	Transaction history inquiry

14.3 USSD Technical Specifications

A. Session Flow & Transaction Logic

Ref.	Requirement
USSD-T01	Must support MAP (Mobile Application Part) over SIGTRAN (M3UA) for high-speed, low-latency signalling
USSD-T02	Must support Network-Initiated (NI) USSD Push
USSD-T03	All menus must be optimised for a maximum of 160-182 characters (7-bit) to ensure 100% compatibility with legacy (non-smartphone) handsets
USSD-T04	Must support Data Coding Scheme (DCS) switching between 7-bit (English) and 16-bit UCS2 (Arabic) without session drops

B. Session Timeout Limits

Ref.	Requirement
USSD-T05	Session timeout limits shall be configurable with a default of 20-30 seconds
USSD-T06	The system shall allow for configurable session timeouts based on transaction type and risk profile

C. Security Protocols

Ref.	Requirement
USSD-T07	Anti-SIM Swap Integration: Gateway must interface with MNO's HLR (Home Location Register)
USSD-T08	If a SIM swap is detected within a configurable window (e.g., 24-48 hours), USSD payment functionality must be automatically restricted
USSD-T09	PIN Management: All PIN entries must be transmitted as encrypted blocks and validated against a FIPS 140-2 Level 3 Hardware Security Module (HSM)
USSD-T10	PINs must never be stored in plain text or application logs
USSD-T11	Data Masking: System must automatically mask sensitive information. Accounts, balances, or PANs must only display the last 4 digits (e.g., XXXX-1234) on the handset screen
USSD-T12	Session ID Randomisation: Each USSD session must be assigned a unique, non-sequential Session ID

D. Strategic Access Requirements

Ref.	Requirement
USSD-T13	The service must function identically across 2G, 3G, 4G, and 5G signalling planes
USSD-T14	The vendor must demonstrate the ability to integrate with MNO billing systems for zero-rating capability

15. SOLUTION DELIVERY, IMPLEMENTATION PHASES AND MILESTONES

The Bank seeks to implement the solution in phases. The core platform is to be delivered with an overall completion in 40 to 44 weeks from the firm order date. The payment application and its channels follow a phased delivery aligned to the maturity of the core platform, with national rollout targeted within 18 months of contract effectiveness. Bidders must present a single integrated master schedule for the whole solution, showing the dependencies between its elements.

15.1 Core Platform Milestones

No.	Milestone	Week
1	Solution requirements specification and detailed design	[To be proposed]
2	Software delivery and test environment deployment	[To be proposed]
3	User acceptance testing and security review	[To be proposed]
4	Participant pilot	[To be proposed]
5	Training	[To be proposed]
6	Documentation and project completion sign-off	[To be proposed]

15.2 Payment Application Rollout Phases

Phase	Content	Timeline
Phase 1: Foundation	Requirements finalisation and solution design; infrastructure setup and environment provisioning; core platform development (user management, authentication); NIPS integration development; security implementation and testing	Months 1-6
Phase 2: Core Features	P2P transfer functionality; QR payment implementation; bill payment integration; merchant onboarding portal; administrative and supervisory tools; user acceptance testing	Months 7-12
Phase 3: Pilot Launch	Soft launch with a limited user base (10,000-50,000 users); bank and PSP integration with pilot institutions; performance testing and optimisation; issue resolution and refinement	Months 13-15
Phase 4: National Rollout	Staged national rollout by region; marketing and user education campaigns; merchant acquisition programmes; full bank and PSP ecosystem integration; ongoing optimisation and support	Months 16-18

Dependency: The core platform participant pilot must be completed and signed off before the payment application pilot launch (Phase 3) begins. The Bidder may propose a compressed integrated schedule, provided this dependency is respected and the overall programme completes within 18 months of contract effectiveness.

---

16. PROJECT DELIVERABLES

16.1 Design Phase

Ref.	Deliverable
DEL-01	Business requirements document (updated)
DEL-02	System design document, including a detailed design of the solution architecture inclusive of data and network flows
DEL-03	Security architecture document
DEL-04	Integration specifications
DEL-05	User experience design and wireframes
DEL-06	Data model and database design
DEL-07	Infrastructure architecture diagram

16.2 Development Phase

Ref.	Deliverable
DEL-08	Source code with comprehensive inline documentation
DEL-09	API documentation and integration guides
DEL-10	Database schema and migration scripts
DEL-11	Deployment automation scripts

Ref.	Deliverable
DEL-12	Detailed configurations of the implementation
DEL-13	Test plans and test cases
DEL-14	User manuals, end-user manuals and training materials

16.3 Testing Phase

Ref.	Deliverable
DEL-15	Unit test reports
DEL-16	Integration test reports
DEL-17	Performance test reports
DEL-18	Security test reports (penetration testing and vulnerability assessment)
DEL-19	User acceptance test reports

16.4 Deployment Phase

Ref.	Deliverable
DEL-20	Deployment runbooks and procedures
DEL-21	Operations and day-to-day maintenance manuals
DEL-22	Disaster recovery and business continuity plans, including backup and recovery procedures ensuring recoverability in the event of data loss or corruption
DEL-23	Monitoring and alerting configurations
DEL-24	Capacity planning documentation

17. KNOWLEDGE TRANSFER AND TRAINING

Ref.	Requirement
KT-001	The Bidder shall conduct comprehensive knowledge transfer to the Central Bank technical team, including: architecture and design overview training (5 days); development environment setup and code walkthrough (10 days); operations and monitoring training (5 days); incident response and troubleshooting training (5 days); and security administration training (3 days).
KT-002	The Bidder shall provide train-the-trainer programmes for customer support and merchant support teams.
KT-003	All training shall include hands-on exercises and documentation in English and Arabic.
KT-004	In-person installation and administration training must be included in the solution delivery. The vendor must provide adequate and appropriate training to personnel identified by the Bank, incorporating certified training material delivered by a certified trainer for efficient operation of the system. The trainer must have at least two years of experience and have delivered training in the specific domain concerned. The training programme must be well defined and scoped, and the outcome of the training must be first- and second-level certified users.
KT-005	A detailed training plan with specifications for training courses, schedules, site and requirements must be defined and delivered.

Ref.	Requirement
KT-006	Training competency levels shall be defined as: Level 1 (Basic User), Level 2 (Advanced Operator), Level 3 (Expert Administrator). Certification shall be required for Level 2 and Level 3.
KT-007	All training materials must be provided in both Arabic and English. Materials include: participant guides, instructor manuals, e-learning modules, and quick reference cards.
KT-008	Train-the-Trainer program: 5-day program certifying up to 10 trainers. Includes train-the-trainer manual, assessment tools, and coaching sessions.

17.1 Training Plan

Training Type	Target Audience	Duration	Required Competency Level
Administrator Training	Central Bank Team	5 days	Level 3 (Expert)
Operator Training	Operations Team	5 days	Level 2 (Advanced)
Technical Support Training	Support Team	5 days	Level 2 (Advanced)
User Training	Application Users	2 days	Level 1 (Basic)
Train-the-Trainer	Central Bank Trainers	3 days	Level 3 (Expert)

18. TESTING REQUIREMENTS

Ref.	Requirement
TEST-001	The Bidder shall conduct the following testing activities: unit testing with a minimum of 80% code coverage; integration testing covering all API endpoints and external integrations; performance testing simulating target user loads; security testing including penetration testing and code security review; user acceptance testing with representative user groups; accessibility testing against WCAG 2.1 Level AA; and localisation testing for Arabic and English interfaces.
TEST-002	Test environments shall mirror the production configuration and be maintained throughout the solution lifecycle.
TEST-003	The Bidder shall provide and operate a test environment for bank and PSP integration testing and certification.
TEST-004	Performance testing shall simulate 5,000 TPS with 100,000 concurrent users. System must maintain < 2 second response time for 99% of transactions.
TEST-005	Annual penetration testing and quarterly vulnerability assessments required. All critical vulnerabilities must be remediated within 48 hours.
TEST-006	DR testing shall be conducted quarterly with RTO < 15 minutes and RPO = 0. Full report required within 5 days of each test.
TEST-007	Integration testing with all external systems (NCS, RTGS, banks, PSPs) with documented test cases and success criteria.
TEST-008	UAT with 1,000+ representative users across all user types. Success criteria: 95% task completion rate, 90% satisfaction rate.

18.1 Detailed Testing Requirements

Test Type	Details	Acceptance Criteria
Unit Testing	Minimum 80% code coverage	All test cases pass
Integration Testing	All API endpoints and external systems	100% of integration points function correctly
Performance Testing	5,000 TPS, 100,000 concurrent users	< 2 second response time for 99% of transactions
Security Testing	Penetration testing, code security review	No critical or high vulnerabilities
User Acceptance Testing	1,000+ representative users	95% task completion, 90% satisfaction
Accessibility Testing	WCAG 2.1 Level AA	Pass all accessibility criteria
Localisation Testing	Arabic and English interfaces	Correct RTL display for Arabic

19. SUPPORT AND MAINTENANCE

19.1 Warranty Period

Ref.	Requirement
SUP-001	The Bidder shall provide a comprehensive warranty covering defects, bugs and performance issues for a minimum of 12 months from production acceptance, for the complete solution.
SUP-002	During the warranty period, the Bidder shall provide bug fixes and patches at no additional cost, within the response and resolution times in Section 19.2.

19.2 Severity Levels, Response and Resolution Times

Severity Level	Description	Response Time	Resolution Time
Critical	System unavailable or security breach	1 hour	4 hours
High	Core functionality unavailable for a significant number of users	4 hours	24 hours
Medium	Feature malfunction with a workaround available	24 hours	5 business days
Low	Minor issue or cosmetic defect	48 hours	10 business days

19.3 Post-Warranty Support

Ref.	Requirement
SUP-003	The Bidder shall propose ongoing support models, including: application maintenance and support (L1, L2, L3); infrastructure management (if applicable); 24x7x365 monitoring and incident response; proactive system health checks; regular security patching and updates; and performance optimisation services.

Ref.	Requirement
SUP-004	The support proposal shall include: support team structure and location; escalation procedures; SLA commitments; and the pricing model (annual fixed fee, or time and materials).
SUP-005	The Bidder shall describe the process for handling post-launch enhancements, including change request procedures, impact assessment and estimation methodology, development and deployment processes, and pricing models for enhancements.

20. LICENSING AND INTELLECTUAL PROPERTY

Ref.	Requirement
LIC-001	The Bidder shall provide perpetual, irrevocable licences for all custom-developed software components, with full source code ownership transferred to the Central Bank.
LIC-002	For third-party commercial software components, the Bidder shall: disclose all third-party components and licensing terms; secure perpetual licences with unlimited user and transaction rights where possible; provide alternatives to subscription-based components carrying vendor lock-in risk; and ensure licence transferability in the event of a vendor change.
LIC-003	For open-source components, the Bidder shall: disclose all open-source components and their licences; ensure compliance with licence obligations; avoid copyleft licences (GPL, AGPL) that could restrict Central Bank rights; and provide vulnerability monitoring for open-source dependencies.
IPR-001	All custom code, designs, documentation and artefacts developed under this project shall be owned exclusively by the Central Bank with full intellectual property rights.
IPR-002	The Bidder shall not reuse project-specific code or designs in other projects without explicit written permission from the Central Bank.
IPR-003	The Bidder may retain ownership of pre-existing frameworks and tools brought to the project, provided such tools are licensed to the Central Bank for perpetual use.

Interaction with the commercial off-the-shelf requirement: LIC-001 and IPR-001 apply to custom-developed elements. Where the core platform is a licensed COTS product, the Bidder must state clearly which elements are licensed product and which are custom development, and must satisfy LIC-002 in respect of the product.

PART IV: SOLUTION REQUIREMENTS

21. RESPONSE KEY

This Part sets out the requirements against which proposals will be assessed. Bidders must respond to every requirement using the response key below. Any requirement answered with a code other than "Y" or "A" must be explained in Appendix E: Bidder Comments to Technical Specifications. Any requirement answered with a symbol not listed in the key will be treated as a negative or non-response.

Code	Meaning
Y	Fully meets specification, out of the box.
A	Available in the next version (include the estimated date of release).
T	Specification is provided through third-party software.
M	Modifications are necessary to meet the specification.
W	Specification is not provided, but there is a reasonable work-around.
C	Customisation or change of source code is required to meet the specification.
N	Specification is not, and cannot be, provided.

22. FUNCTIONAL REQUIREMENTS — NIPS CORE PLATFORM

The proposed National Instant Payment System solution shall include, but not be limited to, the following functionalities. The detailed compliance matrix for the core platform is at Appendix B, which must be completed in full.

22.1 System-Wide Technical Specifications

Ref.	Requirement
A-01	The solution utilises a graphical user interface, preferably based on external entity and accessed via a standard browser or desktop application.
A-02	Where applicable, the solution includes drop-down menu lists or other look-up features, such as autocomplete, to ensure consistent and validated data entry.
A-03	The solution is ODBC compliant (does not require a third-party interface), providing the ability to access data without third-party products such as Microsoft Excel or Microsoft Access.
A-04	The solution is capable of running on Windows or Linux servers in a virtualised environment. Specify any other compatible operating systems or limitations.
A-05	Provide the minimum CPU, memory, storage, switching and bandwidth specifications required for the proposed solution to operate efficiently. Detail any specific hardware required.
A-06	The solution must support high transaction volumes during peak processing times. Indicate the supported volume per minute for the solution proposed.

Ref.	Requirement
A-07	The solution must keep a detailed audit of every user action and payment transaction. Audit details must include username, IP address, selected menu or screen, action taken, date and time.
A-08	The graphical user interface of the solution must be available in English and Arabic.

22.2 User Authentication and Authorisation

Ref.	Requirement
B-01	The solution must allow for user authentication against corporate directories.
B-02	The solution must support integration with third-party multifactor solutions such as Cisco DUO, Okta Auth0 and similar solutions.
B-03	The solution must provide support for third-party secure identity and access solutions.
B-04	The solution must provide role-based access controls (RBAC) for the granular definition of user privileges.

22.3 Administration and Management

Ref.	Requirement
C-01	The solution must support the creation and participation of both direct and indirect participation types.
C-02	The solution should allow administrators to specify an institution type for each participant on the NIPS, from a configurable list.
C-03	The solution should allow administrators to suspend participants from participating on the NIPS.
C-04	The solution should allow administrators to remove or disable participants from participating on the NIPS.
C-05	The solution should allow administrators to view the activity under selected user sessions.
C-06	The solution must allow administrators to view an audit of detailed user activity.
C-07	The solution must provide configurable alerts based on payment activity, liquidity levels, clearing and settlement failures, high transaction amounts and similar events.
C-08	The solution must support up to a six-eyed process for selected actions performed on the administrative interface.
C-09	The solution must allow participants to view only payment and other information pertaining to their own organisation.

22.4 Clearing and Settlement

Ref.	Requirement
D-01	The solution must finalise payments using a real-time settlement model, achieved via collateralisation using a specific account on the existing RTGS.
D-02	The solution must provide built-in liquidity management tools allowing participants to manage their liquidity on the NIPS efficiently.
D-03	The solution must provide built-in liquidity-related alerts triggered when liquidity thresholds are met or projected to be met.

Ref.	Requirement
D-04	The solution must provide support to execute participant intraday liquidity loans.
D-05	Payments made on the solution must be settled within a maximum average SLA of six seconds.
D-06	The solution must support concurrent transactions initiated through all digital channels from every participant.
D-07	The solution must support peak processing times.
D-08	The solution must include support for merchant payments and provide tools enabling seamless integration with point-of-sale devices and management of multiple payment types through a single connection.
D-09	The solution must provide a centralised proxy identifier (alias) database facilitating the addressing of aliases on a one-to-many design against user accounts.
D-10	The solution must support multiple types of proxy identifiers (aliases); specifically custom usernames or user handles, mobile numbers and email addresses.
D-11	The solution must allow payments to be made via standard bank account number and branch where applicable.
D-12	The solution must generate and support standardised QR codes.
D-13	The solution must provide support for merchant-presented static QR codes, merchant-presented dynamic QR codes and consumer-presented dynamic QR codes.
D-14	The solution should provide built-in tools allowing administrators to investigate failed or rejected transactions.
D-15	The solution should provide built-in tools allowing administrators to monitor and control pending message queues.
D-16	The solution should include a built-in refund and payment dispute review mechanism.
D-17	The system should include built-in fraud detection and prevention capabilities, able to flag and place on hold potentially fraudulent transactions for further review.

22.5 ISO 20022 Messaging

Ref.	Requirement
E-01	The solution must provide support for ISO 20022 Payments Clearing and Settlement (PACS) messages, specifically pacs.008.001, pacs.004.001 and pacs.002.001.
E-02	The solution must provide support for ISO 20022 Payment Initiation (PAIN) messages, specifically pain.013.001 and pain.014.001.
E-03	The solution must provide support for ISO 20022 Account Management (ACMT) messages, specifically acmt.023.001 and acmt.024.001.
E-04	The solution must provide support for ISO 20022 Cash Management (CAMT) messages, specifically camt.053.001, camt.052.001 and camt.054.001.

22.6 Interoperability and Integrations

Ref.	Requirement
F-01	The solution should be integrated with the national switch to perform its transactions.

Ref.	Requirement
F-02	The solution must be able to integrate with the existing Sudanese Pound (SDG) settlement arrangements.
F-03	The solution must be able to integrate with other existing on-premises and off-premises payment systems, and with payment networks, government services and fintech partners through API interfaces or adapters.
F-04	The solution should support client APIs over the HTTPS protocol.
F-05	The solution must support idempotency and must provide protection against replayed transactions across its integration interfaces.
F-06	The solution should support integration with Security Information and Event Management systems.

22.7 Cybersecurity

Ref.	Requirement
G-01	The solution must adhere to local and global financial regulations, including GDPR, GLBA and/or PSD2 where applicable, subject to REG-008.
G-02	The solution must align with ISO 27001 and other applicable industry standards, such as the relevant portions of NIST applicable to an instant payment system.
G-03	The solution should have redundancy to fail over in case the primary solution goes down, allowing for clustering and failover mechanisms to ensure continuous availability (99.99%).
G-04	The vendor shall provide specific requirements for data backup and recovery procedures to ensure efficient disaster preparedness.
G-05	The solution should support an active-active high availability infrastructure.
G-06	The solution must support adaptive authentication to allow risk-based authentication during high-risk transactions.
G-07	The solution must support Identity Assurance Level 2 (IAL2) in accordance with NIST SP 800-63A.
G-08	The solution must enforce the principle of least privilege, enforceable at the central bank (system ownership) level, and must utilise role-based access controls.
G-09	The solution must support secure audit trails and Write Once Read Many (WORM) storage capabilities.
G-10	The solution must be able to function in a Zero Trust Network Architecture.
G-11	The solution must support AES-256 encryption as a minimum standard of encryption.
G-12	The solution must utilise TLS version 1.3 for all internal and external communication.
G-13	The solution must be compatible with centralised authentication solutions and servers.
G-14	The solution must utilise token-based security for applications, API security and JSON Web Tokens.
G-15	The solution should employ DDoS mitigation technologies such as web application firewalls, traffic filtering and content delivery networks.

22.8 Reporting

Ref.	Requirement
H-01	The solution should provide standard out-of-the-box reports.
H-02	The solution must include built-in comprehensive reporting functions for compliance and anti-money laundering audits.
H-03	The solution must allow the Bank's administrators to create custom reports.
H-04	The solution must provide reports on user access.
H-05	The solution must provide built-in reports on participant activity and message flows.
H-06	The solution must provide detailed participant statements.
H-07	The solution should provide customisable payment-related dashboards.
H-08	Administrators should be able to integrate the solution with third-party reporting solutions, for example Tableau, Power BI or Cognos.
H-09	Users should be able to export all generated reports to PDF, CSV and XLSX files.

22.9 Billing

Ref.	Requirement
I-01	The solution must allow administrators to define billing rates based on message types, volumes and flow direction.
I-02	The solution must automatically create invoices based on selected billing cycles.
I-03	The solution must have mechanisms to automatically collect due invoices on specified charge dates and billing cycles.

22.10 Deliverables

Ref.	Requirement
M-01	A detailed design of the architecture of the solution must be provided, inclusive of data and network flows.
M-02	Detailed configurations of the implementation must be provided.
M-03	A day-to-day operation and maintenance manual must be provided.
M-04	End-user manuals must be provided.
M-05	Backup and recovery procedures to ensure recoverability in the event of data loss or corruption must be provided.

23. FUNCTIONAL REQUIREMENTS — PAYMENT APPLICATION AND USER CHANNELS

23.1 User Onboarding and Identity Management

Ref.	Requirement
FR-001	The system shall provide a multi-step onboarding process that collects and verifies: mobile number with OTP verification; national identification number or equivalent government-issued ID; biometric data (facial recognition or fingerprint) where supported by the device; and user consent for terms of service and data processing.
FR-002	The system shall integrate with the national eKYC infrastructure to perform real-time identity verification against government databases.
FR-003	The system shall support tiered KYC levels aligned with Central Bank regulations: Tier 1 — Basic registration with limited transaction thresholds for financial inclusion; Tier 2 — Full KYC with enhanced limits for verified users; Tier 3 — Enhanced due diligence for high-value merchant accounts.
FR-004	The system shall enable users to link multiple bank accounts and/or wallets from participating institutions with explicit user consent and bank confirmation.
FR-005	The system shall provide account management capabilities including add, remove, set primary account, and temporary account suspension.

23.2 Authentication and Security

Ref.	Requirement
FR-006	The system shall implement multi-factor authentication combining a knowledge factor (PIN or password), a possession factor (device binding and OTP), and an inherence factor (biometric authentication) where available.
FR-007	The system shall enforce adaptive authentication, requiring additional verification for: first-time device login; high-value transactions exceeding configured thresholds; sensitive operations (account linking, PIN change, beneficiary addition); and login from a new geographic location or suspicious patterns.
FR-008	The system shall implement device fingerprinting and binding to detect account takeover attempts.
FR-009	The system shall enforce automatic session timeout after a configurable period of inactivity (default: 5 minutes).
FR-010	The system shall provide a secure PIN/password reset mechanism with multi-step verification.

23.3 Person-to-Person Transfers

Ref.	Requirement
FR-011	The system shall enable instant transfers between users using the following identifiers: mobile number registered with the system; account number or IBAN; national ID number; unique user alias or handle; and QR code scan.
FR-012	The system shall perform beneficiary validation through NIPS before presenting the confirmation screen to the user.

Ref.	Requirement
FR-013	The system shall support own-account transfers across different banks and PSPs linked to the same user profile.
FR-014	The system shall enable users to save frequent beneficiaries for quick access.
FR-015	The system shall support scheduled and recurring transfers with configurable frequency.
FR-016	The system shall display a transaction preview including fees, exchange rates , status (completion, pending, reverse,cancelled) (if applicable) and estimated completion time before execution.

23.4 Merchant Payments

Ref.	Requirement
FR-017	The system shall support QR code-based merchant payments compliant with the EMVCo QR Code Specification or an equivalent national standard.
FR-018	The system shall distinguish between static QR (fixed merchant identifier, user enters amount) and dynamic QR (pre-populated transaction with amount, merchant details and optional invoice reference).
FR-019	Upon scanning a merchant QR, the system shall display merchant verification information including legal business name, trade licence number, merchant category code, transaction amount and description, and applicable fees.
FR-020	The system shall generate user-initiated payment QR codes for P2P collection scenarios.
FR-021	The system shall support contactless in-app payment links shared via messaging platforms.

23.5 Bill Payments and Top-Ups

Ref.	Requirement
FR-022	The system shall integrate with the national biller aggregation platform to present a categorised list of billers, including utilities (electricity, water, gas), telecommunications (post-paid, prepaid, data), government services (taxes, fees, fines), educational institutions, insurance providers and charitable organisations.
FR-023	The system shall support both ad-hoc and scheduled bill payments with payment reminders.
FR-024	The system shall enable bill inquiry to retrieve outstanding amounts before payment.
FR-025	The system shall support mobile airtime and data top-up with carrier selection and package options.
FR-026	The system shall allow users to store favourite biller accounts for quick access.

23.6 Account and Balance Management

Ref.	Requirement
FR-027	The system shall display an aggregated view of all linked accounts and wallets with current available balance, pending transactions, daily and monthly transaction limits and utilisation, and account status.
FR-028	The system shall support real-time balance inquiry through NIPS integration or direct bank API where available.

Ref.	Requirement
FR-029	The system shall cache balance information with a clear timestamp indication when real-time inquiry is unavailable.
FR-030	The system shall alert users when approaching configured transaction limits.

23.7 Transaction History and Statements

Ref.	Requirement
FR-031	The system shall provide comprehensive transaction history with a minimum 12-month retention period accessible within the application.
FR-032	The system shall support advanced filtering by date range, transaction type (send, receive, bill payment, top-up), counterparty, amount range and transaction status (successful, failed, pending, reversed).
FR-033	The system shall enable search functionality across transaction descriptions and reference numbers.
FR-034	The system shall provide a transaction detail view including date and time, amount and currency, fees and charges breakdown, counterparty information, transaction reference number, settlement status and a receipt download option.
FR-035	The system shall generate and email monthly account statements in PDF format upon user request.
FR-036	The system shall allow transaction history export in CSV format for financial management purposes.

23.8 Merchant Management

Ref.	Requirement
FR-037	The system shall provide a dedicated merchant onboarding workflow capturing business legal information and registration documents, business owner or authorised signatory KYC, business category and expected transaction volumes, settlement bank account details, tax identification numbers, and supporting documentation upload (trade licence, tax certificate).
FR-038	The system shall route merchant applications through a verification workflow with document review and approval stages.
FR-039	Merchants shall access a dedicated merchant portal displaying real-time transaction monitoring, daily/weekly/monthly sales summaries, expected settlement schedule and amounts, QR code generation and management, transaction dispute notifications, and customer ratings and feedback.
FR-040	The system shall enable merchants to generate and print static QR codes for in-store display.
FR-041	The system shall provide merchant transaction reporting with export functionality.
FR-042	The system shall support merchant sub-user management for businesses with multiple locations or staff.

23.9 Dispute Management and Consumer Protection

Ref.	Requirement
FR-043	The system shall enable users to raise disputes on completed transactions by selecting the transaction and providing a dispute category (unauthorised transaction, incorrect amount, service not received, and so on), a description with supporting evidence, and a preferred resolution (refund, reversal, investigation).
FR-044	The system shall generate a unique dispute reference number and communicate it via push notification and SMS.
FR-045	The system shall provide a dispute tracking interface showing current status and resolution timeline.
FR-046	The system shall route disputes to the appropriate resolution party (bank, PSP, merchant) based on transaction type and dispute category.
FR-047	The system shall support automatic refund processing for qualifying dispute types per Central Bank rules.
FR-048	The system shall maintain a comprehensive dispute audit trail accessible to Central Bank supervisors.

23.10 Notifications and Communication

Ref.	Requirement
FR-049	The system shall deliver real-time push notifications for transaction initiation and completion, transaction failure with reason, receipt of funds, dispute updates, security alerts (new device login, PIN change), and promotional offers and announcements.
FR-050	The system shall send SMS notifications or email for critical events including successful high-value transactions above a configurable threshold, account linking and delinking, PIN reset, and security incidents.
FR-051	The system shall maintain a notification centre within the application, preserving notification history.
FR-052	The system shall enable users to configure notification preferences by channel and event type.
FR-053	The system shall support in-app messaging for customer support communication.

23.11 Customer Support

Ref.	Requirement
FR-054	The system shall provide multi-channel support including an in-app FAQ and knowledge base with search capability, a chatbot for common inquiries with escalation to human agents, secure in-app messaging with support agents, support ticket creation and tracking, and call centre integration with screen-pop capability.
FR-055	The system shall enable screen sharing for remote support sessions with user consent and security controls.
FR-056	The system shall maintain customer support interaction history accessible to authorised agents.

24. NON-FUNCTIONAL REQUIREMENTS

24.1 Performance and Scalability

Ref.	Requirement
NFR-001	The system shall process 95% of instant payment transactions end-to-end within 2 seconds, measured from user confirmation to receipt notification. Payments must in all cases be settled within a maximum average SLA of six seconds, and the end-to-end consumer payment flow must complete in under 5 seconds.
NFR-002	The system shall support a peak throughput of a minimum of 1,000 transactions per second (TPS), with linear scalability to 5,000 TPS. Bidders must state the supported transaction volume per minute for the proposed solution.
NFR-003	The application shall launch and be ready for user interaction within 2 seconds on a cold start and 1 second on a warm start, on standard mid-range devices.
NFR-004	The system shall support concurrent active users scaling from 100,000 at launch to 5 million within three years, and shall be architected to support a registered user base of 10 million or more.
NFR-005	API response times shall not exceed 500 milliseconds for the 95th percentile of requests under normal load.
NFR-006	The system architecture shall support horizontal scaling without requiring application downtime.
NFR-006A	The proxy identifier (alias) directory shall be provisioned to support a minimum of 350,000 aliases at launch and shall scale to at least 10 million aliases without architectural change. Bidders must state the maximum supported alias volume.

24.2 Availability and Reliability

Ref.	Requirement
NFR-007	The NIPS core platform shall maintain a minimum uptime of 99.99% per annum. The payment application platform shall maintain a minimum of 99.9% availability measured annually, excluding planned maintenance windows.
NFR-008	Planned maintenance windows shall not exceed 4 hours per month and must be scheduled during low-traffic periods (02:00–06:00 local time).
NFR-009	The system shall implement automatic failover with a Recovery Time Objective (RTO) of 15 minutes.
NFR-010	The system shall implement continuous data replication with a Recovery Point Objective (RPO) of zero for transaction data.
NFR-011	The system shall maintain business continuity and disaster recovery capabilities with documented procedures and quarterly testing. The vendor shall provide specific requirements for data backup and recovery procedures to ensure efficient disaster preparedness, and shall state whether a cloud-based backup solution is offered.
NFR-011A	The solution shall support redundancy and failover in the event that the primary solution becomes unavailable, allowing clustering and failover mechanisms, and shall support an active-active high availability infrastructure. Bidders must describe, with network diagrams, how the desired availability is achieved.

24.3 Security and Compliance

Ref.	Requirement
NFR-012	All data transmission shall be encrypted using TLS 1.3 or higher with perfect forward secrecy, for all internal and external communication. No cleartext traffic shall be permitted.
NFR-013	All sensitive data at rest shall be encrypted using AES-256 encryption with hardware security module (HSM) key management. The solution shall support encryption of data at rest, in transit and in use.
NFR-014	The system shall implement a defence-in-depth security architecture including a web application firewall (WAF), DDoS protection, intrusion detection and prevention systems (IDS/IPS), security information and event management (SIEM), and regular penetration testing and vulnerability assessments.
NFR-015	The system shall comply with PCI DSS requirements where card data is processed or stored.
NFR-016	The system shall comply with the Central Bank cybersecurity framework and information security standards, and shall align with ISO 27001 and relevant portions of NIST applicable to an instant payment system.
NFR-017	The system shall implement comprehensive audit logging capturing all user authentication attempts, all financial transactions, all administrative actions, all system configuration changes, and all API calls with request and response payloads. Audit detail must include username, IP address, selected menu or screen, action taken, date and time.
NFR-018	Audit logs shall be tamper-proof, supported by Write Once Read Many (WORM) storage capability, retained for a minimum of 7 years, and accessible for regulatory examination.
NFR-019	The system shall comply with national data protection and privacy regulations, including data minimisation, purpose limitation and user consent management.
NFR-020	The system shall implement geographic data residency controls, ensuring all citizen financial data remains within national jurisdiction.
NFR-020A	The solution shall enforce the principle of least privilege, enforceable at the central bank (system ownership) level, using role-based access controls; shall support Identity Assurance Level 2 (IAL2) in accordance with NIST SP 800-63A; shall function within a Zero Trust Network Architecture; and shall use token-based security for applications, API security and JSON Web Tokens.
NFR-020B	The solution shall support adaptive, risk-based authentication for high-risk transactions, including amount thresholds, unusual login and location verification, and shall be compatible with centralised authentication solutions and servers.

24.4 Usability and Accessibility

Ref.	Requirement
NFR-021	The application shall provide an intuitive user interface following platform-specific design guidelines (Material Design for Android, Human Interface Guidelines for iOS). Administrative interfaces shall provide an intuitive user interface for administrators and other authorised users.
NFR-022	The application and all administrative graphical user interfaces shall support a minimum of two languages (Arabic and English) with in-app language switching capability.

Ref.	Requirement
NFR-023	The application shall implement right-to-left (RTL) language support for Arabic with culturally appropriate number formatting.
NFR-024	The application shall follow WCAG 2.1 Level AA accessibility guidelines, including minimum contrast ratios (4.5:1 for normal text), screen reader support, keyboard navigation support, scalable font sizes and alternative text for images.
NFR-025	The application shall function on devices with screen sizes ranging from 4.7 inches to 12.9 inches.
NFR-026	The application shall be optimised for low-bandwidth environments (2G/3G networks) with progressive loading and data compression.
NFR-027	The application shall provide clear error messages in user-friendly language with guidance on resolution steps.

24.5 Maintainability and Supportability

Ref.	Requirement
NFR-028	The system shall implement a microservices architecture enabling independent deployment and scaling of components.
NFR-029	The system shall provide comprehensive API documentation using the OpenAPI/Swagger specification.
NFR-030	The system shall implement centralised configuration management, enabling parameter changes without code deployment.
NFR-031	The system shall provide real-time monitoring dashboards displaying system health metrics, transaction success and failure rates, API performance metrics, user activity patterns, and security incidents and alerts.
NFR-032	The system shall implement automated alerting for anomalies, performance degradation and security events, with configurable thresholds.
NFR-033	The system shall support over-the-air (OTA) application updates with rollback capability.
NFR-034	The system shall maintain backward compatibility for API versions for a minimum of 12 months after a deprecation notice.
NFR-034A	The solution shall provide comprehensive documentation and training resources, and the vendor shall provide a detailed project management document outlining the timeline and resources required for implementation.

24.6 Interoperability

Ref.	Requirement
NFR-035	The system shall integrate with NIPS using ISO 20022 message standards or Central Bank-specified formats.
NFR-036	The system shall provide RESTful APIs for bank and PSP integration with OAuth 2.0 authentication, supporting client APIs over HTTPS.
NFR-037	The system shall support webhooks for real-time event notification to integrated parties.
NFR-038	The system shall implement message queuing for asynchronous processing and guaranteed delivery, and shall support idempotency with protection against replayed transactions across its integration interfaces.

25. INTEGRATION REQUIREMENTS

25.1 National Instant Payment System

Ref.	Requirement
INT-001	The solution shall integrate with the NIPS core switch for instant payment initiation and settlement.
INT-002	The integration shall support the following transaction types: credit transfers (P2P, P2B), payment requests, balance inquiries, beneficiary validation, transaction status queries, and reversals and refunds.
INT-003	The solution shall implement NIPS-mandated security protocols including message signing, encryption and mutual TLS authentication.
INT-004	The solution shall handle NIPS response codes and error conditions with appropriate user messaging and retry logic.
INT-004A	The core solution shall support ISO 20022 messages, specifically: PACS — pacs.008.001, pacs.004.001 and pacs.002.001; PAIN — pain.013.001 and pain.014.001; ACMT — acmt.023.001 and acmt.024.001; and CAMT — camt.053.001, camt.052.001 and camt.054.001.

25.2 Bank and Payment Service Provider Integration

Ref.	Requirement
INT-005	The solution shall provide standardised integration interfaces enabling banks and PSPs to receive account linking requests, validate account ownership, provide balance inquiries, receive debit authorisations, send credit notifications, and report transaction status.
INT-006	The solution shall support multiple integration patterns: synchronous API calls for real-time operations; asynchronous messaging for batch operations; and webhook notifications for status updates.
INT-007	The solution shall provide a test environment for bank and PSP testing and certification.
INT-007A	The solution shall be integrated with the national switch to perform its transactions, shall integrate with the existing Sudanese Pound (SDG) settlement arrangements, and shall integrate with other existing on-premises and off-premises payment systems, payment networks, government services and fintech partners through API interfaces or adapters.
INT-008	The system SHALL implement an automated, per-endpoint Circuit Breaker pattern across all external interfaces and participant bank integrations to prevent cascading performance degradation. The circuit breaker must support configurable failure thresholds (error rate, timeouts, latency) to automatically transition between Closed, Open, and Half-Open states

25.3 National Identity and KYC Systems

Ref.	Requirement
INT-008	The solution shall integrate with the national Civil Registry for identity verification using citizen national ID numbers.
INT-009	The solution shall integrate with the national biometric identification system, where available, for enhanced KYC verification.
INT-010	The solution shall support document verification services for trade licences, tax certificates and business registrations.

25.4 Biller Aggregation Platform

Ref.	Requirement
INT-011	The solution shall integrate with the national biller aggregation platform for bill presentation and payment posting.
INT-012	The integration shall support biller inquiry, bill fetch, payment posting and payment confirmation workflows.
INT-013	The solution shall handle multiple biller categories with category-specific data fields.

25.5 Telecommunications Integration

Ref.	Requirement
INT-014	The solution shall integrate with mobile network operators for OTP SMS delivery with delivery confirmation, airtime and data package top-up, and mobile number validation and portability checks.
INT-015	The solution shall implement SMS routing logic with fallback providers for high availability.
INT-015A	The solution shall support the USSD access channel described in Section 14, integrated with all national mobile network operators, with full Arabic and English menu support.

25.6 Card Schemes (Future Phase)

Ref.	Requirement
INT-016	The solution architecture shall accommodate future integration with international card schemes (Visa, Mastercard) for card-based funding and disbursement.

26. REGULATORY AND COMPLIANCE REQUIREMENTS

Ref.	Requirement
REG-001	The solution shall comply with the Central Bank Payment Systems and Services Law and all implementing regulations.
REG-002	The solution shall implement Anti-Money Laundering (AML) controls, including a transaction monitoring rules engine, suspicious activity detection and reporting, sanctions screening against national and international lists, and enhanced due diligence for high-risk customers.
REG-003	The solution shall implement Counter-Terrorism Financing (CTF) controls aligned with FATF recommendations.
REG-004	The solution shall enforce transaction limits as mandated by Central Bank regulations, with the ability to adjust limits through configuration.
REG-005	The solution shall generate regulatory reports including daily transaction volumes and values by type, monthly active users and growth metrics, failed transaction analysis, fraud and security incident reports, and customer complaint and dispute statistics.
REG-006	The solution shall comply with national data protection law, including lawful basis for data processing, user consent management, right to access personal data, right to rectification and erasure, data portability, and data breach notification within mandated timeframes.

Ref.	Requirement
REG-007	The solution shall implement consumer protection controls including clear and transparent fee disclosure, transaction confirmation before execution, transaction receipt generation, an accessible dispute resolution process, and customer data confidentiality.
REG-008	The solution shall adhere to applicable local and international financial regulations. Where the Bidder's product implements requirements derived from GDPR, GLBA or PSD2, the Bidder shall state how those controls map onto Sudanese law; Sudanese law prevails in the event of conflict.
REG-009	The solution shall include built-in fraud detection and prevention capabilities, able to flag and place on hold potentially fraudulent transactions for review. Bidders shall explain how potentially fraudulent transactions are handled and the tools available to assist in the recovery of funds should fraud occur.
REG-010	Bidders must describe any enhanced KYC and security controls for alias and QR code usage in the proposed solution, and how these controls address the risks identified with alias and QR code usage in global instant payment implementations.

26.1 Data Protection Compliance

Ref.	Requirement
REG-006A	The solution shall comply with Sudan Data Protection Law and international standards. Implement data minimisation, purpose limitation, and consent management. Data must remain within Sudan jurisdiction.
REG-006B	Foreign bidders must demonstrate local presence or partnership with a Sudanese-licensed entity. Submit license applications within 30 days of award.
REG-006C	All costs inclusive of VAT (15%), withholding tax (5% on services), and other applicable taxes. Clarify tax treatment for foreign vendors.
REG-006D	Comply with PCI DSS for card data, FATF recommendations for AML/CFT, and international sanctions lists. Document compliance approach for each standard.

27. DATA ANALYTICS AND REPORTING

Ref.	Requirement
DA-001	The solution shall capture and analyse user behaviour metrics including user acquisition and retention rates, feature adoption and usage patterns, user journey and drop-off points, session duration and frequency, and geographic distribution.
DA-002	The solution shall provide real-time and historical transaction analytics including transaction volumes and values by type, channel and time period; success and failure rates with root cause analysis; average transaction value and frequency per user segment; peak usage patterns and capacity planning metrics; and transaction routing and settlement analytics.
DA-003	The solution shall generate financial reporting including revenue recognition by fee type and counterparty, settlement reconciliation reports, merchant discount rate calculations, and cost allocation and profitability analysis.
DA-004	The solution shall generate automated regulatory reports as required by the Central Bank, including payment systems oversight returns, financial inclusion metrics, consumer complaint statistics, security incident reports, and AML/CFT suspicious activity reports.

Ref.	Requirement
DA-005	The solution shall provide business intelligence capabilities including interactive dashboards with drill-down capability, ad-hoc query and reporting tools, data export functionality, predictive analytics for demand forecasting, and customer segmentation and cohort analysis.
DA-006	The solution shall provide standard out-of-the-box reports (which the Bidder must list), allow Bank administrators to create custom reports, provide reports on user access and participant activity and message flows, provide detailed participant statements generated by date range and other filters, support integration with third-party reporting tools (for example Tableau, Power BI, Cognos), and allow export of all generated reports to PDF, CSV and XLSX.

28. DISPUTE MANAGEMENT AND RESOLUTION SYSTEM

The Bidder shall design, supply, configure, test, deploy, document and support a complete Dispute Management and Resolution System (DMS) as an integral part of the solution. The DMS is a mandatory deliverable of this RFP and shall be priced within the solution; it shall not be offered as an optional module, a future-phase item or a chargeable extra. The dispute functionality shall cover every element of the solution and shall expose the interfaces necessary for end-to-end dispute handling across the national scheme.

The DMS shall manage the complete lifecycle of every dispute, claim, complaint, investigation, reversal, recall and chargeable exception arising from transactions processed through the national instant payment infrastructure, whichever channel the transaction originated from (mobile application, USSD, merchant point of sale, QR, participant channel or bulk file). The Central Bank is the owner of the scheme dispute rules and the final arbiter; the DMS shall enforce those rules through configuration, not through code changes.

28.1 Scope of the Dispute Management System

Ref.	Scope Element
DMS-S01	Disputes raised by end users against their own transactions, whether sent or received
DMS-S02	Disputes and claims raised by merchants, including claims relating to settlement, non-receipt of funds and payment reversals
DMS-S03	Claims raised between participants (banks, payment service providers and wallet operators) against one another in respect of scheme transactions
DMS-S04	Complaints and escalations received by the Central Bank directly from the public and referred into the system for handling and adjudication
DMS-S05	Exceptions detected by the system itself, including unmatched settlement entries, timed-out transactions, duplicate postings and suspected fraudulent transactions placed on hold

28.2 Functional Requirements

A. Case Intake and Registration

Ref.	Requirement
DMS-001	The system shall accept dispute cases from all of the following intake channels: the mobile payment application; the USSD channel; the Progressive Web Application; the merchant portal; the participant (bank and PSP) portal and API; the Central Bank supervisory console; the call centre and support agent console; and bulk upload for cases originated outside the platform.
DMS-002	The system shall generate a unique, non-reusable case reference for every dispute at the point of registration and shall communicate it to the raising party through the channel used, and additionally by push notification and SMS where the raising party is a registered user.
DMS-003	The system shall support a configurable dispute categorisation taxonomy maintained by the Central Bank, covering at minimum: unauthorised or fraudulent transaction; transaction not received by beneficiary; duplicate transaction; incorrect amount debited; funds sent to the wrong beneficiary (including through an incorrect alias or QR code); goods or services not received; merchant refund not processed; technical failure or timeout with uncertain status; settlement discrepancy; fee or charge dispute; and reversal or recall request.
DMS-004	On registration, the system shall automatically retrieve and attach the complete transaction record from the core platform, including the full message trail (ISO 20022 messages exchanged), timestamps, participant identifiers, channel, device information, alias or QR data used, settlement status and any prior related cases involving the same parties or instruments.
DMS-005	The system shall enforce configurable eligibility rules at intake, including the maximum permitted period from transaction date within which a case of each category may be raised, minimum and maximum disputable amounts, and the number of open cases permitted per user.
DMS-006	The system shall detect and link duplicate or related cases arising from the same transaction or the same underlying incident, and shall support the merging and splitting of cases with a full audit trail.

B. Workflow, Routing and Case Handling

Ref.	Requirement
DMS-007	The system shall provide a configurable workflow engine allowing the Central Bank to define, without code modification, the stages, actions, mandatory fields, permitted outcomes and participant obligations applicable to each dispute category.
DMS-008	The system shall route each case automatically to the responsible party or parties (sending participant, receiving participant, merchant, third-party service provider or the Central Bank) on the basis of dispute category, transaction type and the scheme liability rules.
DMS-009	The system shall support multi-party cases in which more than one participant must respond, and shall track the status and response of each party independently within the single case.
DMS-010	The system shall support case reassignment, delegation, supervisor override, maker-checker approval for financially impactful actions, and configurable four-eye or six-eye authorisation for high-value refunds, reversals and write-offs.
DMS-011	The system shall provide a structured request-for-information mechanism enabling handling parties to request additional evidence from the raising party or from another participant, with the ability to pause the applicable service-level clock while awaiting a response and to auto-close or auto-decide where the response is not received within the configured period.

Ref.	Requirement
DMS-012	The system shall support the following claim responses between participants: accept in full; accept in part; reject with reason code; counterclaim; request further information; and escalate to Central Bank adjudication.
DMS-013	The system shall maintain a configurable reason-code set for acceptance, rejection and closure, aligned with the scheme rules and usable for analytics and regulatory reporting.

C. Financial Resolution

Ref.	Requirement
DMS-014	The system shall execute approved refunds, reversals, returns and recalls automatically through the core platform, generating the corresponding payment and settlement instructions, and shall reflect the resulting settlement postings against the correct participant accounts.
DMS-015	The system shall support provisional (temporary) credit to the disputing customer where the scheme rules require it, together with automatic reversal of that provisional credit if the dispute is subsequently decided against the customer.
DMS-016	The system shall support the placing of holds on funds, the freezing of beneficiary accounts or wallets in coordination with the receiving participant, and funds-recall requests, in cases of suspected fraud, in accordance with Central Bank rules.
DMS-017	The system shall apply the scheme liability matrix to apportion loss between the parties, calculate any dispute-handling fees, penalties or interest payable between participants, and post them through the billing module.
DMS-018	The system shall support partial resolutions, instalment recoveries, and write-off of irrecoverable amounts under configurable approval authority.
DMS-019	The system shall guarantee that no financial adjustment can be executed without an approved case decision, and that every financial adjustment is permanently linked to the case that authorised it.

D. Merchant Disputes and Chargebacks

Ref.	Requirement
DMS-020	The system shall provide a merchant dispute workflow supporting notification of a claim, submission of merchant defence and evidence (representment), acceptance of the claim, and automatic debit of the merchant settlement account where the claim is upheld.
DMS-021	The system shall track merchant dispute ratios and automatically flag merchants exceeding configurable dispute or fraud thresholds for supervisory review, enhanced monitoring or suspension.

E. Evidence, Communication and Transparency

Ref.	Requirement
DMS-022	The system shall provide secure evidence management, allowing the upload of documents, images and transaction records, with configurable file type and size controls, malware scanning, encryption at rest, and controlled access according to party role.
DMS-023	The system shall provide the raising party with a dispute tracking interface showing the current status, the stage reached, the expected resolution date and the outcome, in Arabic and English.

Ref.	Requirement
DMS-024	The system shall issue automatic status notifications at registration, at each material change of status, on request for further information, and at final resolution, through push notification, SMS, e-mail and in-app messaging according to the user's notification preferences.
DMS-025	The system shall generate a formal case outcome statement, downloadable in PDF, setting out the decision, the reasoning, the amounts involved and the right of escalation.

F. Escalation and Adjudication by the Central Bank

Ref.	Requirement
DMS-026	The system shall provide a Central Bank adjudication function through which unresolved or contested cases are escalated with the complete case file, evidence and message trail presented in a single view.
DMS-027	The system shall record Central Bank decisions as binding scheme outcomes, execute them automatically against the participants concerned, and prevent further amendment of the case except through a formal reopening with supervisory authorisation.
DMS-028	The system shall maintain a searchable repository of adjudicated precedents and scheme rulings, accessible to authorised Central Bank users and, where the Bank permits, to participants.
DMS-029	The system shall support the reopening of closed cases within a configurable period, with full traceability of the original and revised outcomes.

G. Service Levels and Escalation Timers

Ref.	Requirement
DMS-030	The system shall apply a configurable service-level clock to each stage of each dispute category, measuring acknowledgement time, participant response time, information-request response time and total resolution time.
DMS-031	The system shall automatically escalate cases on breach of a service-level threshold, notify the responsible party and its supervisor, and record the breach for reporting and for the application of scheme penalties.
DMS-032	The system shall provide ageing views and early-warning alerts for cases approaching their service-level limits, by participant, category, channel and handler.

H. Supervision, Reporting and Analytics

Ref.	Requirement
DMS-033	The system shall provide the Central Bank with a supervisory dashboard offering read-only access to every case, with drill-down to the transaction and message level, and filtering by participant, category, channel, status, amount, ageing and outcome.
DMS-034	The system shall produce operational and regulatory reporting including: dispute volumes and values by category, participant, channel and period; acceptance, rejection and overturn rates; service-level compliance by participant; average and median resolution times; ageing and backlog analysis; provisional credit exposure; fraud-related losses and recoveries; and repeat-complainant and repeat-respondent analysis.
DMS-035	The system shall feed the consumer complaint statistics and dispute statistics required under REG-005 and DA-004 automatically, without manual compilation.
DMS-036	The system shall support ad-hoc query, export to PDF, CSV and XLSX, and integration with third-party business intelligence tools.

I. Controls, Audit and Integration

Ref.	Requirement
DMS-037	The system shall maintain a complete, tamper-evident audit trail of every action taken on every case, including the identity of the actor, the role used, the timestamp, the previous and new values, and the justification where required; audit records shall be retained for a minimum of 7 years on Write Once Read Many storage.
DMS-038	The system shall enforce role-based access control such that each participant can view only its own cases and the information pertaining to its own customers, while the Central Bank retains full visibility.
DMS-039	The system shall expose secure APIs enabling participants to raise, respond to, query and close cases directly from their own case management or core banking systems, using the same rules and service levels as the portal.
DMS-040	Where the underlying messaging standard supports it, inter-participant exception handling shall use ISO 20022 exceptions and investigations messages, including camt.056 (request to cancel payment), camt.029 (resolution of investigation), camt.026, camt.027, camt.028 and camt.087, in addition to any national message formats specified by the Bank.
DMS-041	The system shall integrate with the fraud detection and monitoring capability so that cases categorised as fraudulent automatically create or update the corresponding fraud record, and so that confirmed fraud outcomes feed back into the fraud rules and watchlists.
DMS-042	The system shall integrate with the customer support function (FR-054 to FR-056) so that support agents can view, create and update cases within the support console without switching systems.
DMS-043	The full dispute interface shall be available in Arabic and English, with right-to-left layout for Arabic, and case correspondence shall be issued in the language selected by the raising party.
DMS-044	The system shall meet the availability, performance, security and data residency requirements set out in Section 24 and shall be included within the disaster recovery and business continuity arrangements for the solution.

28.3 Indicative Dispute Service Levels

The following service levels shall be configurable within the system and shall be applied as the initial scheme defaults unless the Central Bank directs otherwise. Bidders must confirm that these values are configurable by the Bank without vendor intervention.

Stage	Standard Cases	Suspected Fraud Cases
Acknowledgement to the raising party	Immediate (system generated)	Immediate (system generated)
Routing to the responsible party	Within 1 hour	Within 15 minutes
First response by the responsible participant	2 business days	4 hours
Response to a request for further information	3 business days	1 business day
Provisional credit, where applicable	Within 3 business days	Within 1 business day
Final resolution and customer notification	10 business days	5 business days

Stage	Standard Cases	Suspected Fraud Cases
Escalation to Central Bank adjudication	On breach or on contested outcome	On breach or on contested outcome
Central Bank adjudication decision	15 business days	10 business days

29. TECHNICAL SPECIFICATIONS

29.1 Mobile Application Requirements

A. Platform Support

Ref.	Requirement
MA-01	Android: minimum API level 26 (Android 8.0), targeting the latest stable version
MA-02	iOS: minimum iOS 13.0, targeting the latest stable version
MA-03	PWA: support for modern browsers (Chrome, Safari, Firefox) on desktop and mobile

B. Development Framework

Bidders shall specify the proposed development framework with justification, covering native development (Swift/Kotlin), cross-platform frameworks (React Native, Flutter) or hybrid approaches.

C. Application Size and Updates

Ref.	Requirement
MA-04	Initial application download size shall not exceed 30 MB for Android and 50 MB for iOS
MA-05	Updates shall use delta patching to minimise data consumption

D. Device Permissions

The application shall request only necessary permissions, with clear user explanation:

Permission	Purpose
Camera	QR scanning and document capture
Location	Optional, for merchant proximity features
Biometrics	Authentication
Notifications	Transaction alerts
Contacts	Optional, for beneficiary selection

E. Device-Level Performance Targets

Metric	Target
Application launch time	Under 2 seconds (cold start); under 1 second (warm start)
Payment flow time	Under 5 seconds end to end
QR scan time	Under 500 milliseconds

Metric	Target
Application size	Under 30 MB (Android); under 50 MB (iOS)
Frame rate	Consistent 60 frames per second
Memory usage	Under 150 MB during active use
Battery impact	Under 5% per hour of active use

29.2 Back-End Architecture

A. Technology Stack

Bidders shall propose a comprehensive technology stack including:

Ref.	Component
TS-01	Programming languages and frameworks
TS-02	Database systems (relational and NoSQL)
TS-03	Message brokers and queuing systems
TS-04	API gateway and service mesh
TS-05	Container orchestration platform
TS-06	Monitoring and observability tools

Technology Preferences:

Ref.	Preference
TS-P01	The solution shall be compatible with Oracle Database as the preferred platform. Alternatives must be justified with clear technical and cost benefits.
TS-P02	The solution shall operate on Linux-based infrastructure (RHEL or Ubuntu LTS). Windows-based solutions must be justified.
TS-P03	The solution must be ODBC compliant, providing the ability to access data without third-party products.
TS-P04	The solution must be capable of running on Windows or Linux servers in a virtualised environment.

B. Deployment and Infrastructure

The NIPS core platform is to be installed at the Bank's primary and secondary data centres. For the payment application platform and its supporting services, the solution may be deployed on:

Ref.	Deployment Option
DP-01	Public cloud (AWS, Azure, GCP) with data residency controls
DP-02	Private cloud infrastructure
DP-03	Hybrid cloud architecture
DP-04	On-premises data centre

Any deployment model proposed must satisfy NFR-020 (data residency within national jurisdiction). Bidders shall provide a detailed infrastructure design with cost projections for a three-year growth trajectory.

C. Data Management

Ref.	Requirement
DM-01	Transaction data retention: minimum 7 years, with an archival strategy
DM-02	User data retention: active account lifetime plus the regulatory retention period
DM-03	Database backup: continuous replication with point-in-time recovery
DM-04	Data archival: automated archival of historical data to cost-effective storage

29.3 Security Architecture

A. Authentication and Authorisation

Ref.	Requirement
SA-01	Multi-factor authentication framework
SA-02	OAuth 2.0 / OpenID Connect for partner integration
SA-03	Role-based access control (RBAC) for administrative functions, including support for up to a six-eyed review process on configurable administrative actions
SA-04	JWT or equivalent token-based session management
SA-05	Certificate pinning for mobile applications

B. Cryptography

Ref.	Requirement
SA-06	Hardware Security Module (HSM) for key management
SA-07	Secure key generation and rotation procedures
SA-08	End-to-end encryption for sensitive operations
SA-09	Digital signatures for non-repudiation

C. Fraud Prevention

Ref.	Requirement
SA-10	Real-time fraud detection rules engine
SA-11	Machine learning-based anomaly detection
SA-12	Device fingerprinting and behavioural biometrics
SA-13	Velocity checks and transaction pattern analysis
SA-14	Geo-location verification and impossible travel detection

D. Mobile Application Security

Ref.	Requirement
SA-15	AES-256 encryption for all locally stored data; RSA encryption for API communications; secure key management using platform keychains
SA-16	Biometric authentication (Face ID, Touch ID, Android Biometric); transaction PIN for payment authorisation; two-factor authentication for sensitive operations; JWT tokens with automatic refresh; session management with automatic timeout
SA-17	VPN and proxy detection capabilities; network security configuration for Android; App Transport Security for iOS

Ref.	Requirement
SA-18	Code obfuscation using ProGuard/R8 for Android; jailbreak and root detection with appropriate responses; anti-tampering mechanisms; regular security updates and patches; secure code review and penetration testing; lost mode and remote lock; device fingerprinting
SA-19	Compliance with PCI DSS for payment processing, data privacy requirements, local financial regulations, and App Store and Play Store security guidelines

29.4 API Specifications

The solution shall provide RESTful APIs with the following characteristics:

Ref.	Requirement
API-01	JSON request and response format
API-02	OAuth 2.0 authentication
API-03	Rate limiting and throttling
API-04	Comprehensive error codes and messages
API-05	Request and response logging
API-06	API versioning strategy
API-07	Interactive API documentation (Swagger/OpenAPI)

Bidders must state the API architectures supported (REST, SOAP, and so on).

29.5 Hardware, Capacity and Networking Requirements

A. Architecture

Bidders must provide an introductory narrative of how the proposed system architecture aligns with the overarching objectives and functional requirements of the solution, covering the main features and benefits that distinguish the system. The response must include a solution diagram, including network data flows, depicting the overall design, as well as hardware specifications where an on-premises solution is proposed.

B. Operating System and Related Software

All proposals must specify the name and version number of the proposed operating system(s). In addition, the Bidder must state the application used for each of the following:

Ref.	Requirement
HW-01	Desktop and server application update solution
HW-02	Industry-standard relational database management system
HW-03	System and application backup and high availability

C. Backup and Failover

Bidders must specify the type of backup and solution redundancy they can provide. If the Bank hosts the systems, the Bank will provide the backup solution as part of its standardised backup strategy. The Bidder must specify whether it offers a cloud-based backup solution.

D. Capacity, Upgrades and Expansion

Ref.	Requirement
HW-04	Bidders must specify optimal server and storage capacity for the proposed solution where an on-premises solution is offered. Performance must scale to meet the Bank's anticipated growth of 5% annually for at least 5 years; exceptions must be identified.
HW-05	The proposed system must operate at no more than 35% of capacity (for CPU, memory and I/O performance), and must be capable of field upgrade to projected capacity without changing the initial CPU/disk equipment or other peripherals.
HW-06	Bidders must describe the expandability of the proposed solution in terms of processors, memory, I/O, disk drives and peripheral devices.
HW-07	Bidders must state the minimum CPU, memory, storage, switching and bandwidth specifications required for the proposed solution to operate efficiently, and detail any specific hardware required.

E. Server Functionality

The Bank will provision all required hardware based on the Bidder's specifications and recommendation. It is therefore essential that Bidders provide a comprehensive outline of the server sizing and specifications required to support the optimal performance, scalability and availability of the proposed solution.

PART V: VENDOR QUALIFICATION AND EVALUATION

30. VENDOR QUALIFICATION REQUIREMENTS

30.1 Mandatory Qualifications

Ref.	Requirement
QUAL-001	The Bidder must demonstrate a minimum of 7 years of experience in payment systems implementation, of which a minimum of 3 years must be in providing instant payment system solutions to central banks or other financial institutions.
QUAL-002	The Bidder must have successfully delivered a minimum of 2 instant payment or mobile wallet solutions for financial institutions or central banks, and the proposed core solution must have been successfully implemented for at least one central bank in the last 18 months.
QUAL-003	The Bidder must demonstrate ISO 27001 certification for information security management.
QUAL-004	The Bidder must demonstrate ISO 20000 or ITIL certification for IT service management.
QUAL-005	The Bidder must have, or be able to establish, a local presence in Sudan for the duration of the project.
QUAL-006	The Bidder must demonstrate expertise in: mobile application development (native or cross-platform); payment systems integration (ISO 8583, ISO 20022); cloud-native architecture and microservices; API design and management; security architecture and cryptography; and DevOps and continuous deployment.
QUAL-007	The Bidder must provide CVs of proposed key personnel, including a Project Manager (PMP or equivalent, 10+ years of experience), a Solution Architect (payment systems experience mandatory), a Security Architect (CISSP or equivalent), a Mobile Development Lead, a Backend Development Lead, and a QA/Test Manager.
QUAL-008	The Bidder must submit audited financial statements for the last 3 years demonstrating financial stability.
QUAL-009	The Bidder must provide evidence of professional indemnity insurance with minimum coverage of USD 5 million.
QUAL-010	The Bidder must provide evidence of cyber insurance with minimum coverage of USD 3 million.
QUAL-011	The Bidder must provide evidence of general liability insurance with minimum coverage of USD 2 million.

30.2 Initial Screening — Minimum Standards

The Bank will conduct an initial screening step to verify Bidder compliance with submission requirements. A proposal that fails to satisfy the minimum standards shall be considered non-responsive and disqualified from the evaluation process. Bidders must provide a written, affirmative response to each of the following:

Ref.	Screening Requirement
SCR-01	By submitting a response, the Prime Bidder accepts the terms of this Request for Proposal
SCR-02	Proposals must be submitted in the form of two separate documents: a technical proposal and a cost proposal
SCR-03	The proposed solution must currently be in production
SCR-04	The Prime Bidder must be an authorised solution provider for the proposed solution
SCR-05	The Prime Bidder must fully support the proposed solution throughout the life of the contract, including bug fixes, replacement parts and support
SCR-06	The Bidder and its subcontractors must agree to protect the privacy and security of the Bank's data at all times, and further agree not to use or disclose such data other than to accomplish the objectives of the project
SCR-07	The Prime Bidder must meet the experience thresholds in QUAL-001 and QUAL-002
SCR-08	The Prime Bidder must ensure that adequate and expert staffing is assigned for the duration of the project

30.3 Reference Projects

Ref.	Requirement
EVAL-001	Bidders must provide a minimum of 3 reference projects of similar scope, including client name and contact details, project scope and objectives, technologies used, project duration and team size, challenges faced and how they were overcome, and current operational status and metrics (users, transactions).
EVAL-002	The Central Bank reserves the right to contact reference clients for verification. Reference checks will be used to refine and finalise preliminary scores.

31. EVALUATION CRITERIA AND VENDOR SELECTION

31.1 Overall Weightings

Proposals will be evaluated based on the following weightings, totalling 100%:

Evaluation Component	Weight
Technical proposal	80%
Financial / cost proposal	15%
Solution presentation and demonstration	5%
Total	100%

31.2 Technical Proposal Attributes

The technical proposal will be evaluated on the following attributes, which are scored out of 100 and then weighted at 80% of the total:

Attribute	Weight
Adherence to RFP submission requirements	5%

Attribute	Weight
Solution design and compliance with the technical, functional and non-functional requirements of the delivered solution (Parts III and IV), including architecture, functional completeness, usability and user experience, and innovation and future-readiness	20%
Relevant knowledge, experience and qualifications of the Bidder and team members, including an established record of success in similar projects	20%
Documented risk management programme covering technology, operations, information security, supply chain and other risks as they relate to successful delivery	5%
Vendor and solution references	15%
Implementation methodology and approach, including knowledge transfer	15%
Timeline for the recommended solution to be implemented	10%
Training, documentation, service, support, product warranty and maintenance	10%
Total	100%

31.3 Rating and Scoring

Proposals will be evaluated and ranked using a 0 to 10 scale. The score for each criterion is determined by multiplying the criterion weight by the rating; the sum of all scores is the total score.

Rating	Description
10	Exceeds expectations. The proposal clearly addresses and exceeds requirements; excellent probability of success.
8	Somewhat exceeds expectations. The proposal addresses all requirements; very good probability of success.
6	Meets expectations. The proposal addresses basic requirements; good probability of success.
4	Somewhat meets expectations. Minor weaknesses or deficiencies; the proposal partially addresses requirements; fair probability of success.
2	Does not meet expectations or demonstrate understanding of the requirements; low probability of success.
0	Lack of response or complete misunderstanding of the requirements; no probability of success.

31.4 Evaluation Steps

The Bank plans to use the following multi-tiered process:

Step	Activity
Step 1	Initial screening (Section 30.2)
Step 2	Preliminary evaluation of the written proposals and reference checks
Step 3	Final evaluation

The Bank will establish a Proposal Evaluation Committee composed of Bank employees and including subject matter experts. The final evaluation is the culmination of the entire process of reviewing Bidder proposals and information gathering.

31.5 Best Value Standard

In evaluating proposals, the Bank will apply the "Best Value" standard. Evaluations will be based upon the criteria and standards contained in this RFP and the weightings in Section 31.1, as well as the qualitative factors listed below. Purchase price is not the only criterion used. Any award will be made to the vendor whose offer conforms to the RFP and is determined to be the most advantageous, or of best value, to the Bank, in the sole judgement of the Bank.

Qualitative factors include:

Ref.	Qualitative Factor
QF-01	The quality and range of services the Bidder proposes to provide
QF-02	Degree of alignment with the Bank's technical and operational requirements, including interoperability with existing systems
QF-03	The Bidder's overall experience, reputation, expertise, stability and financial responsibility
QF-04	The Bidder's past relationship with the Bank, if any
QF-05	The experience and qualifications of the staff assigned to implement the solution and service the Bank's account, accompanied by evidence of relevant industry certifications
QF-06	The ability to provide service in an expedient and efficient manner
QF-07	Quality and range of management and performance reports
QF-08	The vendor's financial terms offered to the Bank
QF-09	The training options available and the supported delivery formats
QF-10	The total, long-term cost to the Bank of acquiring the vendor's goods and services
QF-11	Clarity and credibility of the vendor's approach to meeting the stated requirements
QF-12	Service level agreement (triage and response times), if applicable
QF-13	Any other relevant factor the Bank would consider in selecting a supplier

PART VI: STANDARD PROPOSAL AND CONTRACT INFORMATION

32. STANDARD PROPOSAL INFORMATION

32.1 Assignment

The contractor may not transfer or assign any portion of the contract without prior written approval from the Bank.

32.2 Disputes

Any dispute arising out of this agreement will be resolved under the laws of the Republic of Sudan. Any appeal of an administrative order, or any original action to enforce any provision of this agreement or to obtain relief or a remedy in connection with it, may be brought only in the Supreme Court for the Republic of Sudan.

32.3 Severability

If any provision of the contract or agreement is declared by a court to be illegal or in conflict with any law, the validity of the remaining terms and provisions will not be affected, and the rights and obligations of the parties will be construed and enforced as if the contract did not contain the particular provision held to be invalid.

32.4 Supplemental Terms and Conditions

Proposals must comply with Section 8.7. However, if the Bank fails to identify or detect supplemental terms or conditions that conflict with those contained in this RFP, or that diminish the Bank's rights under any resulting contract, the term or condition will be considered null and void. After award of contract: if a conflict arises between a supplemental term or condition included in the proposal and a term or condition of the RFP, the term or condition of the RFP will prevail; and if the Bank's rights would be diminished as a result of a supplemental term or condition included in the proposal, that term or condition will be considered null and void.

32.5 Clarification of Offers

To determine if a proposal is reasonably susceptible to award, communications to clarify uncertainties or eliminate confusion concerning the contents of a proposal are permitted between the Bank or the Proposal Evaluation Committee and a Bidder. Clarifications may not result in a material or substantive change to the proposal. The evaluation may be adjusted as a result of a clarification under this section.

32.6 Discussions with Bidders

The Bank may conduct discussions with Bidders to ensure full understanding of the requirements of the RFP and of the proposal. Discussions will be limited to specific sections of the RFP or proposal identified by the Bank, and will only be held with Bidders whose proposals are deemed reasonably susceptible for award. Discussions, if held, will follow the initial evaluation of proposals. If modifications are made as a result of these discussions, they will be put in writing. Following discussions, the Bank may set a time for best and final proposal submissions from those Bidders with whom discussions were held; proposals may be re-evaluated after receipt. If a Bidder does not submit a best and final proposal or a notice of withdrawal, the Bidder's immediate previous proposal is considered its best and final proposal. Any oral modification of a proposal must be confirmed in writing by the Bidder. Bidders with a disability needing accommodation should contact the Bank prior to the date set for discussions so that reasonable accommodation can be made.

32.7 Contract Negotiation and Failure to Negotiate

After final evaluation, the Bank may negotiate with the Bidder of the highest-ranked proposal. Negotiations, if held, shall be within the scope of this RFP and limited to items that would not affect the ranking of proposals. If contract negotiations are commenced, they may be held at the Bank's main office in Khartoum; the Bidder will be responsible for its own travel and per diem expenses.

If the selected Bidder fails to provide information required to begin negotiations in a timely manner, fails to negotiate in good faith, indicates that it cannot perform the contract within the budgeted funds available for the project, or if the Bank, after a good faith effort, simply cannot come to terms, then the Bank may terminate negotiations with the Bidder initially selected and commence negotiations with the next highest-ranked Bidder.

32.8 Notice of Intent to Award

After the completion of contract negotiation, the Bank will issue a written Notice of Intent to Award to the successful Bidder and send copies to all Bidders. The Notice will set out the names of all Bidders and identify the proposal and supplier selected for award.

32.9 Costs of Proposal Preparation

All costs incurred in preparing and submitting proposals are the Bidder's responsibility. Submission of a proposal constitutes acceptance of the terms and conditions of this RFP.

33. STANDARD CONTRACT INFORMATION

33.1 Contract Approval

This RFP does not by itself obligate the Bank. The Bank's obligation will commence when the Governor of the Central Bank, or the Governor's designee, approves the contract in accordance with internal procedures. Upon written notice to the Contractor, the Bank may set a different starting date for the contract. The Bank will not be responsible for any work done by the contractor, even work done in good faith, if it occurs prior to the contract start date set by the Bank.

33.2 Proposals as Part of the Contract

This RFP and the successful proposal may be incorporated into the contract agreement.

33.3 Additional Terms and Conditions

The Bank reserves the right to add terms and conditions during contract negotiations. These terms and conditions will be within the scope of this RFP and will not affect the proposal evaluations.

33.4 Proposed Payment Procedures

The Bank will make payments based on a negotiated, milestone-based payment schedule tied to the delivery and acceptance of specified deliverables. The agreed payment terms will be final and no amendments to the payment terms are permissible. Each billing must consist of an invoice and a progress report. The Bidder must include all costs, including travel and living expenses incurred during the project life cycle, as part of the Bill of Materials; the Bank will not bear any additional costs on these.

33.5 Retainer and Final Payment

A withholding (retainer) of 15 percent will be taken from every invoice amount paid to the supplier under this contract. The accumulated balance will be released as follows: ten percentage points of the contract value upon documented project completion sign-off and acceptance; and the remaining five percentage points upon successful completion of the warranty period defined in Section 19.1.

33.6 Contract Payment

No payment will be made until the contract is approved by the Governor of the Central Bank or the Governor's designee. Under no conditions will the Bank be liable for the payment of any interest charges associated with the cost of the contract. The Bank is not responsible for and will not pay taxes. All costs associated with the contract must be stated in Sudanese Pounds (SDG), plus other currencies if required.

33.7 Contract Personnel

Any change to the project team members named in the proposal must be approved by the Bank's project manager, two weeks in advance and in writing. Personnel changes that are not approved by the Bank may be grounds for the Bank to terminate the contract.

33.8 Inspection and Modification

The contractor is responsible for the completion of all work set out in the contract. All work is subject to inspection, evaluation and approval by the Bank's project manager. The Bank may employ all reasonable means to ensure that the work is progressing and being performed in compliance with the contract. Should the Bank's project manager determine that corrections or modifications are necessary in order to accomplish the Bank's intent, the project manager may direct the contractor to make such changes, and the contractor will not unreasonably withhold them. Substantial failure of the contractor to perform the contract may cause the Bank to terminate the contract; in this event, the Bank may require the contractor to reimburse monies paid by the Bank, based on the identified portion of unacceptable work received, and may seek associated damages.

33.9 Termination

If the Bank's project manager determines that the contractor has refused to perform the work, or has failed to perform the work with such diligence as to ensure its timely and accurate completion, the Bank may, by providing written notice to the contractor, terminate the contractor's right to proceed with part or all of the remaining work.

In addition, the indicative contract will provide for termination for convenience on 90 days' written notice by either party; termination for cause with immediate effect upon material breach; and transition assistance for 6 months at agreed rates.

33.10 Schedule Delay Penalty and Liquidated Damages

In the event of a delay in delivering the proposed solution beyond the agreed timeline without justifiable cause, a penalty of one percent (1%) of the contract value per week of delay, or part thereof, subject to a maximum of ten percent (10%) of the contract value, shall be deducted from the final contract payment after successful installation and commissioning of the solution. Penalties for breaches of service levels will be as defined in the service level agreement.

The vendor must promptly notify the Bank in writing of any foreseen delay, providing a detailed explanation and a revised delivery schedule. Failure to notify in advance may affect penalty calculations. Extensions to the delivery schedule may be considered under exceptional circumstances, such as force majeure events, provided the vendor supplies documented evidence supporting the delay.

33.11 Contract Changes — Unanticipated Amendments

During the course of this contract, the contractor may be required to perform additional work not currently included in this RFP but within the general scope of the initial contract. When additional work is required, the Bank's project manager will provide the contractor with a written description of the additional work and request a time schedule and price for it. Cost and pricing data must be provided to justify the cost of such amendments. The contractor will not commence additional work until the Bank's project manager has secured any required Bank approvals and issued a written contract amendment approved by the Governor of the Central Bank or the Governor's designee.

33.12 Contract Invalidation

If any provision of this contract is found to be invalid, such invalidation will not be construed to invalidate the entire contract.

34. INDICATIVE CONTRACT TERMS

Term	Indicative Provision
Contract duration	Initial term of 3 years from production go-live, renewable for an additional 2-year term by mutual agreement
Performance guarantee	Bank guarantee or performance bond of 10% of contract value, valid for the contract duration plus 3 months
Liquidated damages	Delay in delivery as per Section 33.10; SLA breaches as defined in the service level agreement
Liability and indemnification	The Bidder shall indemnify the Central Bank against third-party claims arising from solution operation. The liability cap is to be negotiated, typically 100–200% of the annual contract value
Termination	For convenience: 90 days' written notice by either party. For cause: immediate upon material breach. Transition assistance: 6 months at agreed rates
Governing law	The laws of the Republic of Sudan

APPENDIX A: PRICING WORKSHEET

For all available deployment models, Bidders must provide the software and services required to meet the specifications outlined in this Request for Proposal. Costs must include any and all taxes (for example Value Added Tax), shipping and duties. Bidders must complete the three-year cost summary below for the complete solution, showing the cost of each solution element (core platform; payment application and channels; dispute management and resolution system) and a consolidated total.

Price Description	Non-Recurring (Base)	Recurring (Annual)	3-Year Extended Cost
Product Costs			
Software licensing			
Other licensing and per-feature cost			
Maintenance / support			
Implementation Services			
Project management			
Documentation and training			
Additional Costs (attach description)			
TOTAL			

Notes:

- **Software:** List, describe and record the licensing, implementation, maintenance, support and training fees associated with the proposed solution.
- **Documentation and Training:** List, describe and record the cost of developing and delivering the required technical, administrative and end-user documentation, and all training fees.
- **Support and Maintenance:** List, describe and record the ongoing costs associated with the maintenance, support and operation of the proposed solution.
- **Implementation:** Describe any labour, equipment, supplies or other costs associated with installing the proposed solution.
- **Project Management:** List and describe any project management fees associated with the proposed solution.
- **Miscellaneous:** List and describe any other costs associated with the proposed solution.

APPENDIX B: NIPS CORE PLATFORM COMPLIANCE MATRIX

Bidders must complete the Response Code column for every line using the key in Section 21, and must complete Appendix E for any response other than "Y" or "A".

Ref.	Requirement	Response Code	Bidder Comments
System-Wide Technical Specifications			
A-01	The solution utilises a graphical user interface, preferably based on external entity and accessed via a standard browser or desktop application.		
A-02	Where applicable, the solution includes drop-down menu lists or other look-up features, such as autocomplete, to ensure consistent and validated data entry.		
A-03	The solution is ODBC compliant (does not require a third-party interface), providing the ability to access data without third-party products such as Microsoft Excel or Microsoft Access.		
A-04	The solution is capable of running on Windows or Linux servers in a virtualised environment.		
A-05	Provide the minimum CPU, memory, storage, switching and bandwidth specifications required for the proposed solution to operate efficiently.		
A-06	The solution must support high transaction volumes during peak processing times.		
A-07	The solution must keep a detailed audit of every user action and payment transaction.		
A-08	The graphical user interface of the solution must be available in English and Arabic.		
User Authentication and Authorisation			
B-01	The solution must allow for user authentication against corporate directories.		
B-02	The solution must support integration with third-party multifactor solutions.		
B-03	The solution must provide support for third-party secure identity and access solutions.		
B-04	The solution must provide role-based access controls (RBAC) for the granular definition of user privileges.		
Administration and Management			
C-01	The solution must support the creation and participation of both direct and indirect participation types.		
C-02	The solution should allow administrators to specify an institution type for each participant on the NIPS.		

Ref.	Requirement	Response Code	Bidder Comments
C-03	The solution should allow administrators to suspend participants from participating on the NIPS.		
C-04	The solution should allow administrators to remove or disable participants from participating on the NIPS.		
C-05	The solution should allow administrators to view the activity under selected user sessions.		
C-06	The solution must allow administrators to view an audit of detailed user activity.		
C-07	The solution must provide configurable alerts based on payment activity, liquidity levels, clearing and settlement failures, high transaction amounts and similar events.		
C-08	The solution must support up to a six-eyed process for selected actions performed on the administrative interface.		
C-09	The solution must allow participants to view only payment and other information pertaining to their own organisation.		
Clearing and Settlement			
D-01	The solution must finalise payments using a real-time settlement model, achieved via collateralisation.		
D-02	The solution must provide built-in liquidity management tools.		
D-03	The solution must provide built-in liquidity-related alerts.		
D-04	The solution must provide support to execute participant intraday liquidity loans.		
D-05	Payments made on the solution must be settled within a maximum average SLA of six seconds.		
D-06	The solution must support concurrent transactions initiated through all digital channels from every participant.		
D-07	The solution must support peak processing times.		
D-08	The solution must include support for merchant payments.		
D-09	The solution must provide a centralised proxy identifier (alias) database on a one-to-many design.		
D-10	The solution must support multiple types of proxy identifiers (aliases).		
D-11	The solution must allow payments to be made via standard bank account number and branch.		
D-12	The solution must generate and support standardised QR codes.		
D-13	The solution must provide support for merchant-presented static QR codes, merchant-presented dynamic QR codes and consumer-presented dynamic QR codes.		
D-14	The solution should provide built-in tools allowing administrators to investigate failed or rejected transactions.		
D-15	The solution should provide built-in tools allowing administrators to monitor and control pending message queues.		

Ref.	Requirement	Response Code	Bidder Comments
D-16	The solution should include a built-in refund and payment dispute review mechanism.		
D-17	The system should include built-in fraud detection and prevention capabilities.		
ISO 20022 Messaging			
E-01	Support for ISO 20022 PACS messages: pacs.008.001, pacs.004.001, pacs.002.001		
E-02	Support for ISO 20022 PAIN messages: pain.013.001, pain.014.001		
E-03	Support for ISO 20022 ACMT messages: acmt.023.001, acmt.024.001		
E-04	Support for ISO 20022 CAMT messages: camt.053.001, camt.052.001, camt.054.001		
Interoperability and Integrations			
F-01	Integration with the national switch		
F-02	Integration with the existing Sudanese Pound (SDG) settlement arrangements		
F-03	Integration with other existing on-premises and off-premises payment systems		
F-04	Support for client APIs over the HTTPS protocol		
F-05	Support for idempotency and protection against replayed transactions		
F-06	Support for integration with Security Information and Event Management systems		
Cybersecurity			
G-01	Adherence to local and global financial regulations		
G-02	Alignment with ISO 27001 and other applicable industry standards		
G-03	Redundancy and failover mechanisms for continuous availability (99.99%)		
G-04	Specific requirements for data backup and recovery procedures		
G-05	Support for active-active high availability infrastructure		
G-06	Support for adaptive authentication		
G-07	Support for Identity Assurance Level 2 (IAL2)		
G-08	Enforcement of least privilege principle with RBAC		
G-09	Support for secure audit trails and WORM storage		
G-10	Function within a Zero Trust Network Architecture		
G-11	Support for AES-256 encryption minimum		
G-12	Utilisation of TLS version 1.3 for all communication		

Ref.	Requirement	Response Code	Bidder Comments
G-13	Compatibility with centralised authentication solutions		
G-14	Utilisation of token-based security for applications and APIs		
G-15	DDoS mitigation technologies		
Reporting			
H-01	Standard out-of-the-box reports		
H-02	Built-in comprehensive reporting functions for compliance and AML audits		
H-03	Ability to create custom reports		
H-04	Reports on user access		
H-05	Reports on participant activity and message flows		
H-06	Detailed participant statements		
H-07	Customisable payment-related dashboards		
H-08	Integration with third-party reporting solutions		
H-09	Export of reports to PDF, CSV and XLSX		
Billing			
I-01	Define billing rates based on message types, volumes and flow direction		
I-02	Automatic invoice creation based on selected billing cycles		
I-03	Automatic collection of due invoices on specified charge dates		
Deliverables			
M-01	Detailed design of the architecture inclusive of data and network flows		
M-02	Detailed configurations of the implementation		
M-03	Day-to-day operation and maintenance manual		
M-04	End-user manuals		
M-05	Backup and recovery procedures		

APPENDIX C: CONSUMER APPLICATION COMPLIANCE MATRIX

This matrix summarises the consumer-facing capability set. It is complementary to, and does not replace, the detailed requirements in Section 23.

Ref.	Requirement	Response Code	Bidder Comments
Consumer Application Requirements			
C-01	Onboarding: OCR-based KYC, biometric setup, guided tutorial		
C-02	Dashboard: real-time balance, quick actions, transaction history		
C-03	Send money: multiple channels (phone, QR, email, bank account, contacts)		
C-04	Request money: payment request creation, shareable links		
C-05	QR payments: scan-to-pay, personal QR codes, dynamic QR, NFC scan-to-pay		
C-06	Bill payments: utilities, mobile top-up, subscription management		
C-07	Government payments: taxes, traffic fines		
C-08	Private sector payments: education fees, airline fees, and similar		
C-09	Transaction management: search, filter, export, digital receipts		
C-10	Security: two-factor authentication, device management, transaction PIN		
C-11	Profile management: aliases, linked accounts, preferences		
C-12	Beneficiary management: add, update, view and delete beneficiary		
C-13	Notifications: real-time push, SMS and email alerts		
C-14	Dispute management: built-in dispute reporting, case tracking		
C-15	Language support: English and Arabic, with right-to-left layout for Arabic		
Performance Requirements			
P-01	Application launch time: under 2 seconds cold start, under 1 second warm start		
P-02	Payment flow time: under 5 seconds end to end		
P-03	QR scan time: under 500 milliseconds		
P-04	Application size: under 30 MB (Android), under 50 MB (iOS)		

Ref.	Requirement	Response Code	Bidder Comments
P-05	Frame rate: consistent 60 frames per second		
P-06	Memory usage: under 150 MB during active use		
P-07	Battery impact: under 5% per hour of active use		
Security Requirements			
S-01	Data security: AES-256 encryption for locally stored data; RSA encryption for API communications; certificate pinning; secure key management		
S-02	Authentication: biometric authentication, transaction PIN, two-factor authentication, JWT tokens with auto-refresh, session management with timeout		
S-03	Network security: TLS 1.3, no cleartext traffic, VPN/proxy detection, network security configuration		
S-04	Application security: code obfuscation, jailbreak/root detection, anti-tampering, regular security updates, penetration testing, lost mode, device fingerprinting		
S-05	Compliance: PCI DSS, data privacy, local financial regulations, App Store and Play Store guidelines		

APPENDIX D: REFERENCE DOCUMENTS TO BE PROVIDED BY THE BANK

The following annexures will be made available to registered bidders upon execution of a non-disclosure agreement:

Annexure	Content
D-A	NIPS Integration Specifications: NIPS API documentation; message formats and data dictionaries; security and authentication requirements; testing and certification procedures
D-B	Current System Landscape: existing payment infrastructure diagram; bank and PSP connectivity status; current transaction volumes and projections
D-C	Regulatory Framework Documents: Payment Systems Law; Payment Service Provider Regulations; extracts from the Data Protection Law; AML/CFT guidelines
D-D	User Research and Personas: user research findings; customer journey maps; persona definitions
D-E	Brand Guidelines: Central Bank visual identity; payment application brand assets and usage guidelines; messaging and communication guidelines

APPENDIX E: BIDDER COMMENTS TO TECHNICAL SPECIFICATIONS

Bidders must complete this sheet for every requirement answered with a code other than "Y" or "A". Add rows as required.

Item Reference	Comment

APPENDIX F: BIDDER'S ACKNOWLEDGEMENT

By signing below, the Bidder acknowledges receipt and understanding of this Request for Proposal, including all appendices, and agrees to comply with all requirements contained herein.

Item	Details
Bidder name	
Authorised signatory	
Title	
Date	
Company stamp	