



The Central Bank of Sudan

National Instant Payment System
(NIPS)Solution

Request for Proposal

Version 5.0
07st April 2026

TABLE OF CONTENTS

1.	Purpose and Background.....	1
1.1	Purpose.....	1
1.2	Background.....	1
1.3	Types of Proposals.....	3
1.4	Contract Terms.....	3
1.5	Contract Award.....	3
2.	Schedule of Events and Definition of Terms.....	4
2.1	Key Timelines Regarding Events Schedule.....	4
2.2	Definition of Terms.....	4
3.	Proposal Instructions, Content, and Format.....	6
3.1	Proposal Inquiries.....	6
3.2	Delivery of Proposal.....	6
3.3	Required Review.....	7
3.4	Errors and Omissions.....	7
3.5	Addenda.....	7
3.6	Amendments to Proposals.....	7
3.7	Right of Rejection.....	7
3.8	Subcontractors.....	8
3.9	Conflict of Interest.....	8
3.10	Bidders Certification.....	9
3.11	Non-collusion.....	9
3.12	Disclosure of Proposal Content.....	9
3.13	System Demonstrations.....	10
3.14	Proposal Format.....	10
3.15	Proposal Content.....	11
3.15.1	Cover Page.....	11
3.15.2	Transmittal Letter.....	11
3.15.3	Table of Contents.....	12
3.15.4	Executive Summary.....	12
3.15.5	Introduction, Bidder Background, Experience and References.....	12
3.15.6	Proposed Solution.....	12
3.15.7	Implementation Approach and Work Plan.....	13
3.15.8	Cost Proposal.....	14
3.15.9	Contract Payment Details.....	14

National Instant Payment System (NIPS) solution for proposals

4.	Scope of Work	14
4.1	Solution Scope	14
4.2	Background	15
4.2.1	Supply of Hardware and Software.....	16
4.2.2	Implementation & Integration Services.....	16
4.2.3	Vendor Risk Management Program	16
4.3	Solution Delivery	17
5.	Evaluation Criteria and Vendor Selection	17
5.1	Proposal Evaluation Weightings	17
5.2	Rating and Scoring	18
5.3	Planned Evaluation Steps.....	18
5.3.1	Initial Screening	18
5.3.2	Evaluation of Written Proposals.....	19
5.3.3	Final Evaluation.....	19
5.4	Proposal Evaluation	19
5.4.1	Converting Costs to Points	20
6.	Standard Proposal Information	21
6.1	Assignment	21
6.2	Disputes	21
6.3	Severability	21
6.4	Supplemental Terms and Conditions	21
6.5	Clarification of Offers.....	21
6.6	Discussion with Bidders	22
6.7	F.O.B. Point	22
6.8	Contract Negotiation	22
6.9	Failure to Negotiate	23
6.10	Notice of Intent to Award	23
7.	Standard Contract Information	23
7.1	Contract Approval.....	23
7.2	Proposals as Part of the Contract.....	23
7.3	Additional Terms and Conditions.....	23
7.4	Proposed Payment Procedures.....	24
7.5	Retainer	24
7.6	Contract Payment	24
7.7	Contract Personnel	24
7.8	Inspection and Modification	24
7.9	Termination for Default	25

National Instant Payment System (NIPS) solution for proposals

7.10	Schedule Delay Penalty.....	25
7.11	Contract Changes – Unanticipated Amendments.....	25
7.12	Contract Invalidation.....	26
8.	Appendix A: Pricing Worksheet	27
9.	Appendix B: Non-Functional Requirements	28
10.	Appendix C: Solution Technical and Functional Requirements and Specifications	29
10.1	Functional Requirements.....	29
10.2	Detailed Technical Specifications.....	31
10.3	Hardware and Networking Requirements	44
10.3.1	Architecture.....	44
10.3.2	Operating System and Related Software.....	44
10.3.3	Backup and Failover Solution	44
10.3.4	Capacity	44
10.3.5	Upgrades and Expansion	44
10.3.6	Server Functionality.....	45
11.	Appendix D: Bidder Comments to Technical Specifications	46

1. Purpose and Background

1.1 Purpose

This Request for Proposal (RFP) is issued by the Central Bank of Sudan (hereinafter referred to as the Bank or the Central Bank), inviting technical and commercial proposals from qualified Bidders for the design, supply, implementation, and ongoing support of a National Instant Payment System Solution.

The main objectives of this project are to:

- Implement a National Instant Payment System (NIPS) solution that enables real-time payments in the domestic payments space in The Sudan.
- Ensure that the implemented solution supports real-time or near real-time payment transmission and on as near to a 24-hour and seven-day (24x7) basis as possible.
- Guarantee interoperability with existing payments and settlements platforms in The Sudan, , Sudan Interbank Settlement System, Real Time Gross Settlement System (RTGS), and other Sudan payment methods.
- Facilitate both direct and indirect participation from commercial banks, credit unions and other payment services institutions operating in the domestic payments space.
- Develop user-friendly mobile applications enabling 10M+ users to conduct instant payments
- Ensure seamless integration with the core NIPS platform APIs
- Deliver exceptional user experience with sub-5-second payment flows
- Implement enterprise-grade security and compliance features
- Support financial inclusion through intuitive, accessible design

This RFP outlines the overall scope of the initiative, including the expected outcomes, required vendor qualifications, submission constraints and the evaluation process.

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.

1.2 Background

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”.

Central Bank of Sudan (CBOS) is willing to launch a project at National scheme for Instant payment at country level, to take over the lead with the digital transformation strategy announced by the Digital transformation ministry since 2025.

The project aims to facilitate national immediate transfer between parties with all categories i.e. person to person, person to government, and person to business and it's vice versa.

Therefore, the imminent NIPS is intended to further support the Bank's efforts to increase payments efficiency in The Sudan, by allowing for real-time payments, thereby, supporting commerce, the adoption of digital financial services (DFS), and—to a broader extent--financial inclusion.

The proposed NIPS 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 possible¹.
- The use of ISO20022 messaging standards, where applicable, for richer more structured data, enhancing customer insights and experience, better payment reconciliation, and faster processing.
- Utilization of a real-time settlement model between participants as opposed to a deferred net settlement model.
- The ability for end users to utilize multiple types of proxy identifiers (aliases) to perform payments.
- Application Programmable Interfaces (APIs) to allow for integration and interoperability. This includes interface with the central bank's digital currency.
- Configurable for high availability to allow for an uptime on as near to a 24x7 basis as possible.

Overall, the selected NIPS solution must meet the following requirements:

- Be a commercial off-the-shelf (COTS), real-time settlement solution that aligns with the functional requirements as defined in this RFP.
- Have been successfully implemented for at least one central bank in the last 18 months.
- Be configurable to meet the current and future operational needs of the Bank.
- Include standardized APIs to enable seamless integration with other existing payment systems.
- Be stable, secure and accessible, supporting continuous service delivery transparency and user trust.
- Be a solution that readily and or easily integrates with the Bank's Sudanese sdg for ease of payment and settlement in the domestic market.

1.3 Types of Proposals

Bidders are required to submit one proposal in the form of two proposal documents: a technical proposal document and a separate cost proposal document ([Section 3.15.8](#)). Bidders are limited to one proposal per Prime Bidder. Bidders shall be allowed to 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. 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. 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.

1.4 Contract Terms

The terms of service are anticipated to commence in two to four weeks of the contract agreement. A kickoff meeting to align objectives is required, followed by other key documents, including project scope, timeline for completion, among the required documents.

1.5 Contract Award

A contract awarded by the Bank will be based upon criteria, standards and weighting identified in this RFP as applied to the a 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 shall maintain full control and unequivocal rights to all data stored, created and developed as part of this contract and for a Fast Payments Solution.

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

A. Award a single contract to one Bidder for the entire solution and services, or

B. 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:

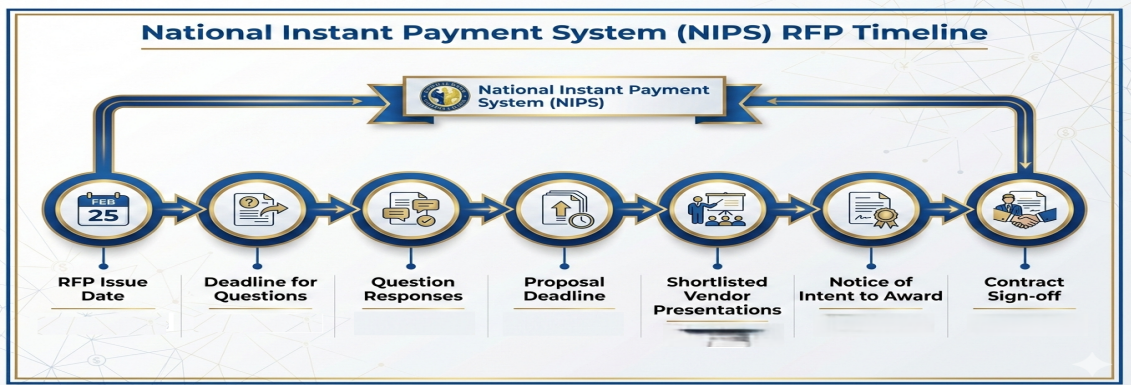
Splitting the contract between the core NIPS platform implementation and the development of end-user (mobile) applications.

Engaging two prime vendors to distribute the workload or project phases for redundancy and risk mitigation.

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.

2. Schedule of Events and Definition of Terms

2.1 Key Timelines Regarding Events Schedule



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		
Shortlisted Vendor Presentations		
Notice of Intent to Award		

2.2 Definition of Terms

This RFP uses the following terminology:

- **“Automation”** refers the technique of making a process or a system function operate automatically.
- **“Bidder”** refers to any recipient of this RFP who submits a proposal. All references that would normally use the words Firm, Vendor, Offeror, or Bidder and Respondent, have been changed to Bidder for consistency.
- **“The Central Bank”** or **“the Bank”** refers to the Central Bank of The Sudan and includes 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”** means 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”** or **“Agreement”** refers to a signed agreement for consulting services between the successful Bidder and the Bank.
- **“Contractor”** refers to the vendor selected as the Prime Bidder as a result of this RFP.
- **“Disaster Recovery”** refers to the ability to recover from the loss of a complete system or site, whether due to natural disaster, system failure or malicious intent. Disaster recovery strategies include replication and backup/restoration.
- **“EOL”** refers to End of Life.
- **“EOVS”** refers to End of Vendor Support.
- **“NIPS”** refers to a Fast Payment System solution.
- **“High Availability”** refers to the capability to maintain continuous operation and service delivery, minimizing downtime and ensuring users’ access even in the face of component failures or disruptions.
- **“Must”**, **“shall”**, **“mandatory”** or **“required”** means a requirement that must be met in substantially unaltered form for the proposal to receive consideration.
- **“Orchestration”** refers to the automation of linked workflows.
- **“On-premises”** refers to IT infrastructure hosted on an organization's premises, allowing full control over server management, security, and maintenance of networking equipment and data storage.
- **“Project”** refers to the objective of the contract, as a whole, the sum total of all elements of the contract.
- **“Proposal”** refers to the submission from a Bidder in response to the RFP for the design, development, implementation, licensing and software maintenance of the requested National Instant Payment System (NIPS) solution.
- **“RFP”** refers to this Request for Proposal.
- **“Role-Based Access Control (RBAC)”** refers to an access control method that assigns access rights based on user roles in the organization.
- **“Services”** refer to labor, resources and materials provided by the Contractor, as required to execute the Agreement.
- **“Should”** or **“desirable”** means a requirement having a significant degree of importance to the objectives of the Request for Proposal.

- **“Solicitation”** refers to the invitation by the Bank or proponents to submit formal quotations, bids, tenders, proposals or statements of qualifications in direct response to the invitation.
- **“Subcontractor”** refers to the party contracted with the Prime Bidder to deliver part of all of the solution and has no direct contractual relationship with the Bank.
- **“Successful”** or **“winning Bidder”** means the successful proponent to this Request for Proposal who enters into a written contract with the Bank.
- **“Supplier”** refers to an individual, Bidder, consultant, or group awarded an agreement under a Bank solicitation invitation.
- **“TBD”** refers to ‘To Be Determined’.

3. Proposal Instructions, Content, and Format

3.1 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 considered binding. Questions regarding any aspect of this RFP should be sent electronically to:

Tenders Committee

Central Bank of The Sudan

Subject Line: **CDNIPS202501 National Instant Payment System (NIPS) Solution Request for Proposals**

Via E-Mail: _____

3.2 Delivery of Proposal

Electronic copies of the proposal must be received by the dd/mm/yyyy at or before 00:00 Sudanese Time. Faxed, hardcopy or oral proposals will not be accepted and could result in disqualification.

A Bidder’s failure to submit its proposal in the submission timeline will disqualify the proposal. Late proposals or amendments will not be accepted for evaluation.

All proposals submitted in response to this RFP must consist of a single electronic version of the proposal, including all required attachments (may be separate electronic documents but clearly identified), and be accompanied by a digitally signed transmittal

letter described in [Section 3.15.2: Transmittal Letter](#). The Cost Proposal ([Section 3.15.8](#)) must be submitted as a separate electronic document.

3.3 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. It will also help to prevent the opening of a defective solicitation and exposure of Bidders' proposals upon which award could not be made. 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.

3.4 Errors and Omissions

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

3.5 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.

3.6 Amendments to Proposals

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

3.7 Right of Rejection

Bidders must comply with all of the terms of the RFP and all applicable laws governing the republic of The Sudan.

The Bank may reject any proposal that does not comply with all of the material and substantial terms, conditions, and performance requirements of the RFP without

incurring any liability or obligation to inform the Bidder(s) 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; and
- 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.

3.8 Subcontractors

Subcontractors may be used to perform work under this contract. If a Bidder intends to use subcontractors, the Bidder must identify the following in the proposal:

- a. Complete name of the subcontractor;
- b. Complete address of the subcontractor;
- c. Type of work the subcontractor will be performing;
- d. Percentage of work the subcontractor will be providing;
- e. A written statement signed by each proposed subcontractor, that clearly verifies that the subcontractor agrees to the terms of this RFP and is committed to rendering the services required by the contract.

N.B. The subcontractor must also comply with [Section 3.10: Bidders Certification](#) as outlined in this document.

The substitution of one subcontractor for another may be made only at the discretion and prior written approval of the Bank. If subcontractors are used, the Prime Bidder retains all responsibility for full delivery of all requirements of this RFP.

3.9 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 (e.g., employed 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 questions of conflict of interest shall be final.

3.10 Bidders Certification

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

- a. the laws of the Republic of The Sudan, Value Added Tax (VAT) compliance and a valid Business License);
- b. all terms and conditions set out in this RFP;
- c. a condition that the proposal submitted was independently arrived at, without collusion, under penalty of perjury; and
- d. the requirement that the offers will remain open and valid for at least 90 days.

If a Bidder fails to comply with [a] through [d] of this paragraph, the Bank reserves the right to disregard the proposal, terminate the contract, or consider the contractor in default.

3.11 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.

3.12 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, in writing, that the Bank does so, and if the Bank agrees, in writing, to do so. Material considered confidential by the Bidder must be clearly identified and the Bidder must include a brief statement that sets out the reasons for confidentiality.

3.13 System Demonstrations

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

3.14 Proposal Format

Vendors must organize their proposals in the following format:

- Technical Proposal
 1. Cover Page
 2. Transmittal Letter
 3. Table of Contents
 4. Executive Summary (concise overview of solution proposed)
 5. Introduction, Bidder's Background, Experience and References
 6. General System Design, Functional Specifications, and Implementation Approach (including responses to the requirements outlined in [Section 4: Scope of Work](#), including the specifications outlined in [Appendix B](#), and [Appendix C](#), (including responses using [Appendix D](#)).
 7. Risk management program as outlined in [Section 4.2.3: Vendor Risk Management Program](#).
 8. Draft contract with the proposal based on information in the RFP, including confidentiality and non-disclosure clauses.
 9. Copy of a valid Tax Compliance Certificate
 10. Copy of National Insurance Board (NIB) Certificate, if applicable
 11. Copy of current Business License
 12. Attachments and supporting documentation
- Cost Proposal

The Bidder must provide a point-by-point technical response stating compliance 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 should 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.

The Bank will retain full ownership, governance, and operational oversight of the NIPS. Vendors must structure proposals to reflect the Bank as the system operator. Vendors should also note that legislative amendments to the Sudan Payments System Act or related statutes may be required. Proposals should therefore incorporate the flexibility to accommodate potential regulatory changes during implementation.

3.15 Proposal Content

Proposals **must** contain the following:

3.15.1 Cover Page

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

CENTRAL BANK OF THE SUDAN

Payment System 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, bank, state, country, zip code and e-mail address.

3.15.2 Transmittal Letter

The Bidder must submit a signed transmittal letter with its response that includes the items below.

- a. Bidder's legal name and any other name under which the Bidder does business; mailing address; street address (for courier mail services); name and title of individual who will sign the contract; name and title of the Bidder contact person (if different); and for each key person: direct telephone number, fax number (if applicable), and e-mail address;
- b. A statement that the individual who signs the transmittal letter is authorized to commit the Bidder;
- c. A statement that the proposal is effective for a period of **90 days**;
- d. A guarantee that prices quoted in the proposal were established without collusion with other Bidders and without effort to preclude the Bank from obtaining the best possible competitive price;

- e. Acknowledgement that the Bidder has read this RFP and subsequent amendments;
- f. A statement indicating whether or not the Bidder or any individual working on the contract has a possible conflict of interest;
- g. A statement identifying all subcontractor and joint venture partners.

3.15.3 Table of Contents

The Bidder must provide a table of contents with corresponding page numbers related to its proposal.

3.15.4 Executive Summary

The Executive Summary, which must not exceed five pages, must provide a concise overview of the Bidder's proposed solution and services, but must exclude pricing information. Bidders are encouraged to highlight those factors that they believe distinguish their proposals from their competitors.

3.15.5 Introduction, Bidder Background, Experience and References

The Bidder must provide an introduction, the background of the Bidder and details of the organization's experience with deploying similar solutions. As the Bank will evaluate qualifications of key staff proposed by the Bidder, this section should include:

- a. Proposed team organization and the designation and identification of key staff;
- b. Qualification of the candidate for project manager;
- c. Qualifications of candidates for key Bidder staff roles, i.e., solution design architects, solution engineers, etc.; and
- d. References: last three implementations for this proposed solution.

3.15.6 Proposed Solution

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

- a. Provide a brief solution overview of the various solution components, their release history, current release being proposed, and number of operational installations for the proposed software solution;
- b. Describe and illustrate the general system design of the proposed solution;
- c. Provide a narrative on how the proposed solution addresses the requirements outlined in [Section 4: Scope of Work](#), including the specifications outlined in [Appendix B](#) and [Appendix C](#) (including

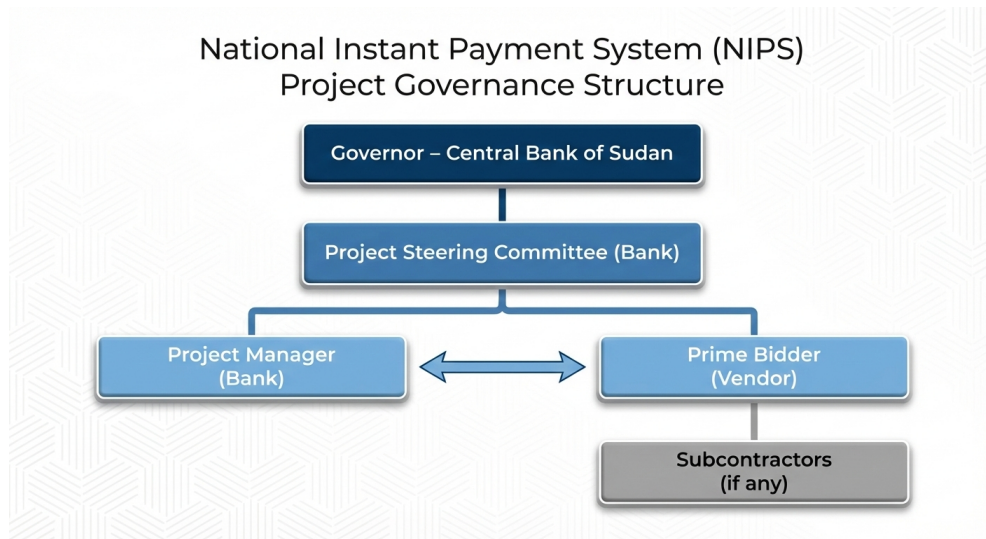
detailed explanations using [Appendix D](#)). Include all requested narrative responses.

- d. Identify any additional features, functionality, recommended solution components or services that were not outlined in [Section 4: Scope of Work](#) but that the Bidder recommends that the Bank consider. Include a description of the features and functions of each additional proposed module;
- e. Describe the security features of the proposed solution;
- f. Describe alternative service delivery models (i.e., Software-as-a-Service, Application Service Provider, Hosted, etc.) available to the Bank and indicate how these might impact the proposed solution; and
- g. Confirm ability to conform to the requirements in [Section 4: Scope of Work](#) and the related Appendices or clearly articulate proposed alternatives.
- h. Future abilities for the Solution:

The central bank of Sudan , would like you have an abilities to add more feature for the solution including but limited services or modules ..

- A) Remittance services .
- B) request to pay to other clients .
- C) Dynamic QR to pay to merchants.

3.15.7 Implementation Approach and Work Plan



Bidders are required to describe their proposed implementation approach, clearly identifying each phase, the timeline proposed, roles and responsibilities

to be performed by the Bidder and those to be performed by the Bank. The Bidder should clearly indicate the Bank's resource requirements needed to meet the Bidder's proposed schedule and:

- a. Describe your implementation and project management methodology and approach to ensure a successful implementation;
- b. Provide a project organization chart highlighting the key staff who will be assigned to the project. Provide names and resumes for the project manager and other key assigned resources;
- c. Provide a detailed work plan that identifies major activities, tasks, deliverables, and resources. The work plan should assume that project will kick-off in no more than three weeks of the approval of the contract by the Bank;
- d. Describe the roles and responsibilities of Bank staff during implementation. Include the minimal and optimal number of Bank staff members (with job category) and the expected role and level of effort during each phase of the project;
- e. Describe the roles and responsibilities of the Bank staff required to maintain and update the system during the first five years. Include the minimal and optimal number of Bank Staff members (with job category), the expected role and level of effort on an on-going basis;
- f. Describe your change management methodology and activities that will be performed during the implementation;

- g. Describe your user acceptance methodology and the responsibilities of Bank staff during testing;
- h. Describe your training methodology and approach; and
- i. Describe how the use of any alternative service delivery models would impact the proposed implementation approach, work plan and Bank staff level of effort.

3.15.8 Cost Proposal

As indicated in [Section 3.2: Delivery of 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. In this section, Bidders must itemize all costs inclusive of all shipping, taxes (e.g., Value Added Taxes 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. A sample of the worksheet can be found in [Appendix A: Pricing Worksheet](#).

3.15.9 Contract Payment Details

This section should outline, among other things specific to your firm, the following terms and conditions (for further details, see [Appendix A: Pricing Worksheet](#)):

1. Total contract sum (inclusive of all taxes and charges)
2. Mobilization deposit
3. Stage payments
4. Final payment
5. Retention terms

4. Scope of Work

4.1 Solution Scope

This section outlines the scope of work (SoW) for the implementation and deployment of a National Instant Payment System (NIPS) solution for the Bank. The purpose of this section is to provide prospective vendors with a clear understanding of the Bank's technical, operational, and strategic requirements and expectations related to the NIPS. The selected solution will serve as a foundational component of the Bank's ongoing efforts to modernize the domestic payments infrastructure and support real-time or near real-time payments on a near 24x7 operational basis. The NIPS must, either directly or indirectly, provide non-discriminatory access to all prospective participants, ensuring equitable participation and fostering financial inclusion. These may include licensed commercial banks, credit unions and approved non-bank payment service providers.

4.2 Background:

The Central Bank of Sudan Payments System) seeks to achieve improved outcomes for financial inclusion by advancing efficiencies in the domestic payments system to promote non-discriminatory access to financial services in The Sudan. In line with this objective, the Bank has progressed a several projects to drive increased payments efficiency, including the establishment of the Real Time Gross Settlement System (RTGS) and the introduction of legislation to license and oversee non-bank providers of electronic payment instruments, the simplification of requirements for account opening, and most recently, In addition, given the increased adoption of digital payment alternatives over the last five years, the Central Bank, through its Steering Committee on Cheque Reduction, has made steady progress toward a strategy for further reducing the usage of cheques in The Sudan by 2026, which runs parallel to the broader objectives of the country's digital transformation objectives.

In an effort to continue its efforts toward modernizing the domestic payments system, the Bank intends to launch a National Instant Payment System (NIPS), which will allow for faster payments that settle in real time, or as near to a real-time basis as possible, Utilizing indirect (passing clearing file through national switch clearing mechanism OR NIPS will have it's own clearing modules) real- time gross settlement model as the primary settlement mechanism. This should be achieved by either utilizing dedicated prefunded RTGS accounts for each participant or by collateralized NIPS-level settlement accounts.

This is a natural next step to the milestones achieved under the current PSD, and is aligned with the Bank's broader strategic goals for a more efficient and modern payments system.

The goals of the PSD are closely linked to the objectives of the NIPS solution, which include:

- To support enhanced commerce by facilitating timely payments;
- To foster innovation in the domestic payments landscape;
- To ensure 100 percent of the population has universal access to digital financial services;
- To promote a reduction in the size of legitimate but unrecorded economic activities that take place in the informal sector;
- To allow for improved security and an enhanced end-user experience; and
- To promote financial inclusion.

Given these objectives, the implementation of a secure NIPS solution that is interoperable with existing local payment platforms is imperative to The Sudan' PSD.

The solution requirement is detailed in [Appendix B](#) and [Appendix C](#) for the proposed NIPS solution. The Bidder must specify whether they comply with these specifications with necessary clarifications in the 'Comments' column. The scope will broadly include:

4.2.1 Supply of Software

The Bidder will supply the required licenses as it relates to the supply and support of a NIPS solution, as per Bank's specifications.

4.2.2 Implementation & Integration Services

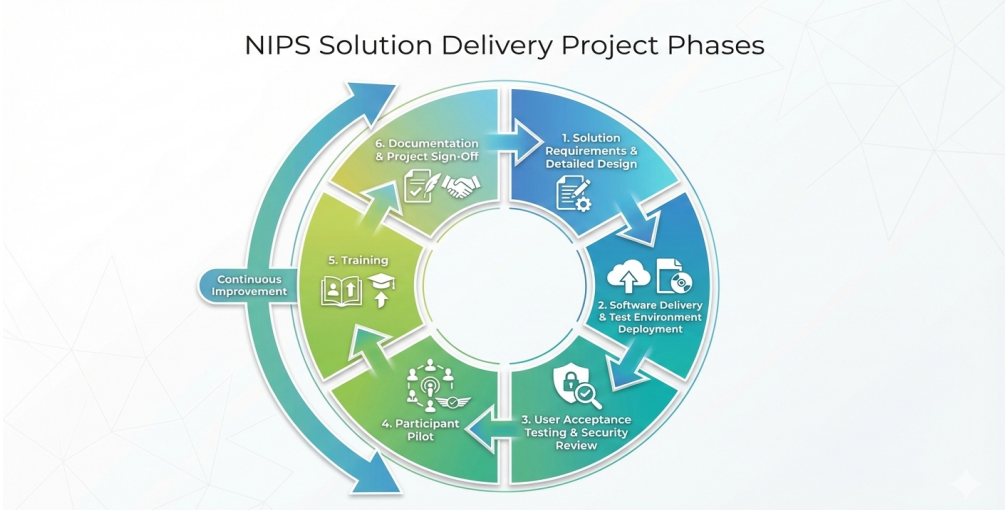
The Bidder will be responsible for the installation and commissioning of the entire solution. The installation and commissioning services will include, but not be limited to the following:

- Installing the Fast Payment System solution at the Bank's primary and secondary datacenters.
- Configuring high availability for the solution.
- Operationalize and optimizing the NIPS solution.
- Configuration of all features included in this RFP.
- Project documentation.
- Project hand-over inclusive of user and administrator training.
- Completion of the project end-to-end.
- Stepwise documentation for all administrative activity.
- Post-implementation support for 60 days.

4.2.3 Vendor Risk Management Program

The Bidder shall maintain a documented risk management program consistent with recognized frameworks, along with establishing strategies. The program must cover technology, operations, information security, fraud, privacy, third-party and supply chain risk, and must be applied to the NIPS through implementation and steady state operations.

4.3 Solution Delivery

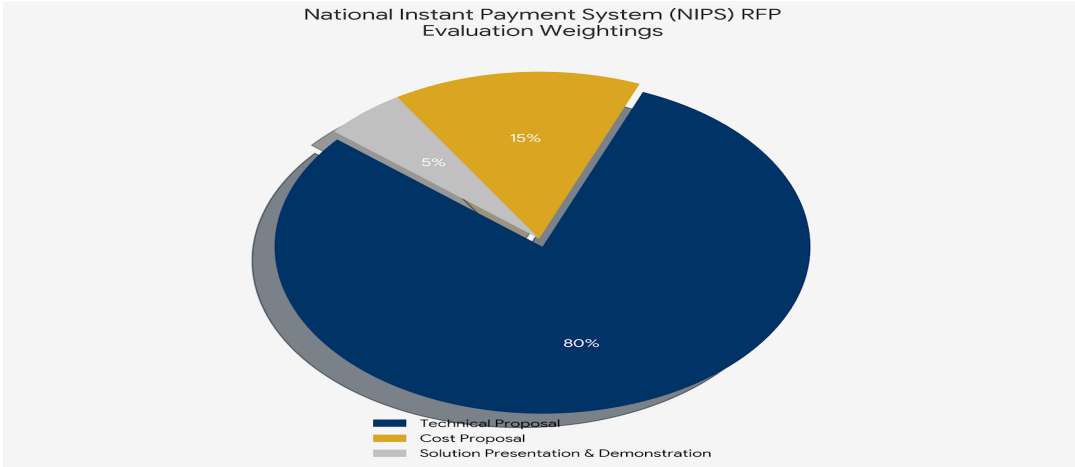


The Bank seeks to implement the proposal NIPS solution in phases with an overall completion in 40 to 44 weeks from the firm order date. To accomplish this, the Bank envisages the following initial milestones that will be further developed and agreed with the selected vendor.

Number	Milestones	Week
1	Solution Requirements Specification and Detailed Design	
2	Software Delivery and Test Environment Deployment	
3	User Acceptance Testing and Security Review	
4	Participant Pilot	
5	Training	
6	Documentation and Project Completion Sign-Off	

5. Evaluation Criteria and Vendor Selection

5.1 Proposal Evaluation Weightings



National Instant Payment System (NIPS) solution for proposals

Proposals will be evaluated based on the following weights (100%):

- Technical Proposal – 80 percent
- Financial Proposal – 15 percent
- Solution presentation and demonstration – 5 percent

The Technical Proposal will be evaluated based of the following attributes.

Attribute	Weight
Adherence to RFP submission requirements.	5
Solution design and compliance with the technical, functional, and non-functional requirements of the delivered solution.	20
Relevant knowledge, experience, and qualifications of Bidder and team members, including an established record of success in similar projects.	20
Documented risk management program that covers technology, operations, information security, supply chain, and other risks, as they relate to a successful delivery of the proposed solution.	5
Vendor and Solution References.	15
Implementation Methodology and Approach.	15
Timeline for the recommended solution to be implemented.	10
Training, documentation, service, support, product warranty and maintenance.	10
Total	100

The Bidder with the highest combined total points will be selected.

5.2 Rating and Scoring

Proposals will be evaluated and ranked according to the outline below. The evaluation will be based on a 0 to 10 scale. The score of each criterion will be determined by multiplying the criteria weight by the rating. The sum of all scores will be the total score.

Rating	Description
10	Exceeds expectations; Proposal clearly addresses and exceeds requirements, excellent probability of success.
8	Somewhat exceeds expectations; the proposal addresses all requirements, with a very good probability of success.
6	Meets expectations; Proposal addresses basic requirements, good probability of success.
4	Somewhat meets expectations; minor weakness or deficiencies, 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.

5.3 Planned Evaluation Steps

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

- Initial screening; see [Section 5.3.1](#).
- Preliminary evaluation of the written proposals and reference checks.
- Final evaluation of proposals.

5.3.1 Initial Screening

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 nonresponsive and disqualified from the proposal evaluation process.

Bidders must meet all the mandatory minimum requirements in this section by providing a written, affirmative response to each of the criteria stated below.

- a. By submitting a response, the Prime Bidder accepts the terms of this request for proposal.
- b. Proposals must be submitted in the form of two separate documents; a technical proposal and a cost proposal.
- c. The proposed solution must currently be in production.

- d. The Prime Bidder must be an authorized solution provider for the proposal solution.
- e. The Prime Bidder must fully support the proposed solution throughout the life of the contract, including but not limited to: bug fixes, replacement parts, support, etc.
- f. The Bidder and their subcontractors must agree to protect the privacy and security of the Bank's data at all times and further agrees not to use or disclose such data other than to accomplish the objectives of the project.
- g. The Prime Bidder has a minimum of three years of experience providing NIPS solutions for central banks and other financial institutions.
- h. The Prime Bidder will ensure that adequate and expert staffing is assigned for the duration of the project.

5.3.2 Evaluation of Written Proposals

The Bank will establish a Proposal Evaluation Committee composed of Bank employees and inclusive of subject matter experts to evaluate proposals received in response to this RFP.

5.3.3 Final Evaluation

The Bank will conduct final evaluations as a culmination of the entire process of reviewing Bidder proposals and information gathering.

5.4 Proposal Evaluation

In evaluating the proposals submitted in response to the RFP, the Bank will apply the "Best Value" standard. Evaluations will be based upon the criteria and standards contained in this RFP and from applying the weightings listed in [Section 5.1](#) above as well as the qualitative factors listed below. Purchase price is not the only criteria that will be used in the evaluation process. Any award resulting from this RFP will be made to that vendor whose offer conforms to the RFP and it is determined to be the most advantageous, of "best value" to the Bank, in the sole judgment of the Bank.

- 1. The quality and range of services the Bidder proposes to provide.
- 2. Degree of alignment with the Bank's technical and operational requirements, including interoperability with existing system.
- 3. The Bidder's overall experience, reputation, expertise, stability and financial responsibility.
- 4. The Bidder's past relationship with the Bank, if any.

5. The experience and qualifications of the staff that will be assigned to implement the solution and service the Bank's account. This should be accompanied with evidence of the relevant industry certifications.
6. The ability to provide service in an expedient and efficient manner.
7. Quality and range of management and performance reports.
8. Vendor's financial terms offered to the Bank.
9. The training options available and the supported delivery formats.
10. The total, long-term cost to the Bank to acquire the vendor's goods and services.
11. Clarity and credibility of the vendor's approach to meeting the stated requirements.
12. Service Level Agreement (Triage and Response Times), if applicable.
13. Any other relevant factor that the Bank would consider in selecting a supplier.

Reference checks will be used to refine and finalize preliminary scores.

6. Standard Proposal Information

6.1 Assignment

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

6.2 Disputes

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

6.3 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.

6.4 Supplemental Terms and Conditions

Proposals must comply with [Section 3.7: Right of Rejection](#). However, if the Bank fails to identify or detect supplemental terms or conditions that conflict with those contained in this RFP or that diminishes the Bank's rights under any contract resulting from the RFP, the term(s) or condition(s) will be considered null and void.

After award of contract:

- a. If 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.
- b. If the Bank's rights would be diminished as a result of the application of a supplemental term or condition included in the proposal, the supplemental term or condition will be considered null and void.

6.5 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 by the Bank or the Proposal Evaluation Committee may be adjusted as a result of a clarification under this section.

6.6 Discussion with Bidders

The Bank may conduct discussions with Bidders for the purpose of ensuring full understanding of the requirements of the RFP and proposal. Discussions will be limited to specific sections of the RFP or proposal identified by the Bank. Discussions will only be held with Bidders who have submitted a proposal deemed reasonably susceptible for award by the Bank. Discussions, if held, will be after initial evaluation of proposals by the Proposal Evaluation Committee. 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 reevaluated after receipt of best and final proposal submissions.

If a Bidder does not submit a best and final proposal or a notice of withdrawal, the Bidder's immediate previous proposal is considered the Bidder's best and final proposal.

Any oral modification of a proposal must be made 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.

6.7 Contract Negotiation

After final evaluation, the Bank may negotiate with the Bidder of the highest-ranked proposal. Negotiations, if held, shall be in the scope of the request for proposal and limited to those items, which would not have an effect on the ranking of proposals. If the highest-ranked Bidder fails to provide necessary information for negotiations in a timely manner, or fails to negotiate in good faith, the Bank may terminate negotiations and negotiate with the Bidder of the next highest-ranked proposal. If contract negotiations are commenced, they may be held at the Bank's main office in Portsudan, The Sudan.

If the contract negotiations take place in Portsudan, The Sudan, the Bidder will be responsible for their own travel and per diem expenses.

6.8 Failure to Negotiate

If the selected Bidder:

- a. fails to provide information required to begin negotiations in a timely manner.
- b. fails to negotiate in good faith.
- c. indicates they cannot perform the contract in the budgeted funds available for the project.
- d. and 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.

6.9 Notice of Intent to Award

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

7. Standard Contract Information

7.1 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, in accordance with internal procedures approves the contract. 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.

7.2 Proposals as Part of the Contract

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

7.3 Additional Terms and Conditions

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

7.4 Proposed Payment Procedures

The Bank will make payments based on a negotiated payment schedule. The agreed payment terms will be final and no amendments in the payment terms are permissible.

Each billing must consist of an invoice and progress report. The Bidder must include all costs including travel and living expenses incurred during the project life cycle as a part of the Bill of Materials and the Bank will not bear any additional costs on these.

7.5 Retainer

A withholding (retainer) of 15 percent (15%), will be taken off every invoice amount paid to the supplier under this contract. This accumulated balance will be paid at the end of the project, as defined in the final contract.

7.6 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 SDG plus other curacies if need it.

7.7 Contract Personnel

Any change of 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.

7.8 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 its

intent; the Bank's project manager may direct the contractor to make such changes. The contractor will not unreasonably withhold such changes.

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.

7.9 Termination for Default

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.

7.10 Schedule Delay Penalty

In the event of a delay in delivering the proposed solution beyond the agreed-upon timeline without justifiable cause, a penalty of one percent (1%) per week of delay or part thereof, subject to a maximum of five percent (5%) of the contract value shall be deducted from the final contract payment after the successful installation and commissioning of the solution.

The vendor must promptly notify the Bank in writing of any foreseen delays, providing a detailed explanation and revised delivery schedule. Failure to notify in advance may impact penalty calculations.

Extensions to the delivery schedule may be considered under exceptional circumstances, such as force majeure events, provided that the vendor provides documented evidence supporting the delay.

7.11 Contract Changes – Unanticipated Amendments

During the course of this contract, the contractor may be required to perform additional work that is not currently included in this RFP. That work will be in the general scope of the initial contract. When additional work is required, the Bank's project manager will provide the contractor a written description of the additional work and request the contractor to submit a time schedule for accomplishing the additional work and a price for the additional work. 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 necessary for the amendment and issued a written

contract amendment approved by the Governor of the Central Bank or the Governor's designee.

7.12 Contract Invalidation

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

8. Appendix A: Pricing Worksheet

For all available deployment models, Bidders must provide a software and services required to meet the specifications outlined in this request for proposal. Costs must include any and all taxes (e.g., Value Added Tax), shipping and duties. Additionally, Bidders must provide a 3-year cost summary using the table displayed below.

Price Description	Non-Recurring (Base)	Recurring (Annual)	3-Yr Extended Cost
Product Costs			
Software Licensing			
Another Licensing & Per Feature Cost			
Maintenance/Support			
Implementation Services			
Project Management			
Documentation & Training			
Additional Costs (Attach description)			
TOTAL			

Software: List, describe, and record the licensing, implementation, maintenance, support and training fees associated with your proposed solution.

Documentation & Training: List, describe, and record the cost of developing/delivering the required technical, administrative and end-user documentation for the proposed solution. Please also include all training fees associated with your proposed solution.

Support/Maintenance: List, describe and record the ongoing costs associated with the maintenance, support and operation of your proposed solution.

Implementation: Describe any labor, equipment, supplies, or other costs associated with installing your proposed solution.

Project Management: If there are project management fees associated with your proposed solution, list and describe them here.

Miscellaneous: List and describe any other costs associated with your proposed solution.



9. Appendix B: Non-Functional Requirements

The proposed Fast Payment System solution should meet or exceed the following non-functional requirements. Bidders must indicate in their proposal how each requirement will be satisfied.

- Scalability:
 - The solution should scale with increased user adoption, supporting payments amongst at least 350,000 aliases.
 - Availability:
 - The solution should have a minimum uptime of 99.99% per annum.
 - Security:
 - The solution must have built in compliance with industry-standard encryption protocols.
 - The solution must have strong access controls and encryption to protect sensitive data.
 - The solution must be able to comply with the Bank's retention policies for transactional data and audit logs.
 - Usability:
 - The solution should have an intuitive user interface for administrators and other authorized users.
 - The solution must have comprehensive documentation and training resources.
 - Implementation:
 - The vendor must provide a detailed project management document outlining the timeline and resources required to implement the proposed solution.
-



10. Appendix C: Solution Technical and Functional Requirements and Specifications

10.1 Functional Requirements

The proposed National Instant Payment System (NIPS) solution should include, but not be limited to, the following functionalities:

- User Authentication and Authorization:
 - a. Centralized user authentication and authorization mechanism.
 - b. Role-based access control (RBAC) for defining user privileges.
 - c. User authentication against corporate directories (e.g., Active Directory).
 - d. Support for and integration with third-party multifactor authentication and secure identity and access solutions.
 - Administration and Management:
 - a. Creation and management of participants across access type and participant type.
 - b. Comprehensive proxy identifier (alias) database.
 - Clearing and Settlement:

A file format agreed on with bilateral or multilateral complying with RTGS format.
 - Interoperability and Integrations:
 - a. Interoperability with the existing central switch.
 - b. Integration with other existing payment systems in the domestic payments space in The Sudan.
-

- c. APIs for participant access and the transmission of messages.
- d. Integration with third-party security and fraud monitoring tools.
- e. Integration with Security Information and Event Management (SIEM) system.
- Cybersecurity:
 - a. Adherence to local and global financial regulations.
 - b. Alignment with ISO27001 and other applicable industry standards.
 - c. Supports Adaptive Authentication.
 - d. Support Identity Proofing.
 - e. Secure access control implementation.
 - f. Supports advanced logging and auditing features.
 - g. Compatible with Zero Trust Network Architecture.
 - h. Supports encryption of data at rest, in transit and in-use.
 - i. Supports the latest TLS encryption standards.
 - j. Secure and encrypted API gateways and interfaces.
 - k. Configurable for redundancy and an active-active high availability infrastructure.
 - l. DDoS mitigation technologies (e.g., Application Firewalls, Traffic Filtering, Content Delivery Networks).
- Audit and Reporting:
 - a. Logging of every transaction processed by the NIPS.
 - b. Comprehensive reporting functionalities for compliance and AML audits.
 - c. Customizable reports on user access, message flows and usage patterns.
 - d. Customizable dashboards.
 - e. Performance monitoring.
- Billing Module:
 - a. Custom billing rate creation.
 - b. Automatic invoice creation with the flexibility to set billing cycles and invoice dates.
 - c. Mechanisms to automatically collect invoices on due dates against participant accounts.

USSD Service Overview

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 (e.g., *0123#) and provides an interactive, menu-driven interface accessible to any mobile phone user.

Key characteristics of USSD:

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 numeric keypad
Arabic & English support	Full bilingual capability as required by the Central Bank

Why USSD for NIPS?

Based on prior approvals from the MDTT and all telecom operators in Sudan, USSD serves as an approved and essential access channel for the National Instant Payment System (NIPS). 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.

Propose Supported transactions via USSD channel:

- a. Wallet account opening (onboarding)
- b. Balance inquiry
- c. Instant person-to-person (P2P) transfers
- d. Bill payments (utilities, telecom, etc.)
- e. Mobile airtime recharge
- f. PIN change and wallet blocking
- g. Transaction history inquiry



10.2 Detailed Technical Specifications

In addition to the minimum specifications listed above, the proposed solution must meet the following specific requirements. The following answer key should be used when responding to the specifications:

Y = Fully meets specification, “out-of-the box”.

A = Available in the next version (include estimated date of release).

T = Specification is provided through third-party software.

M = Modifications necessary to meet specification.

W = Specification is not provided, but there is a reasonable work-around.

C = Customization/change of source code required to meet specification.

N = Specification is not, and cannot, be provided.

If any symbol other than “Y” or “A” is the response for a specification, the Bidder must complete [Appendix D: Bidder Comments to Technical Specifications Sheet](#). Any specification that is answered with a symbol other than what is listed above will be treated as a negative/non-response.

10.2.1 NIPS Requirements

No.	Requirements	Response Code	Comments
System-wide Technical Specifications			
A	1		The solution utilizes a graphical user interface, preferably based on external entity and accessed via a standard browser or Desktop Application
A	2		Where applicable, the solution includes drop-down menus lists, or other look-up features, such as autocomplete, to ensure consistent and validated data entry.

No.		Requirements	Response Code	Comments
A	3	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, Microsoft Access, etc.		
A	4	The solution is capable of running on Windows or Linux servers in a virtualised environment. Specify any other compatible OS or limitations. If your software does not run-on Microsoft or Linux operating systems, please specify which operating systems it supports.		
A	5	Provide the minimum CPU, memory, storage, switching and bandwidth, specifications that would be required for the proposed solution to operate efficiently. Also detail if any specific hardware is required to run the proposed solution.		
A	6	The solution must support high transaction volumes during peak processing times. Please indicate the supported volume per minute for the solution proposed.		
A	7	The solution must keep a detailed audit of every user action and payment transaction. Audit details must include username, IP address, selected menu\screen, action taken, date, time.		
A	8	The GUI of the solution must be available in the English , Arabic language.		
User Authentication and Authorization				
B	1	The solution must allow for user authentication against corporate directories.		

No.		Requirements	Response Code	Comments
B	2	The solution must support integration with third-party multifactor solutions such as Cisco DUO, Okta's Auth0 and similar solutions.		
B	3	The solution must provide support for third-party secure identity and access solutions.		
B	4	The solution must provide role-based access controls (RBAC) for the granular definition of user privileges. Briefly explain how role-based access is achieved.		
Administration and Management				
C	1	The solution must support the creation and participation of both direct and indirect participation types.		
C	2	The solution should allow administrators to specify an institution type for each participant on the NIPS, from a configurable list.		
C	3	The solution should allow administrators to suspend participants from participating on the NIPS.		
C	4	The solution should allow administrators to remove or disable participants from participating on the NIPS.		
C	5	The solution should allow administrators to view the activity under select user sessions.		
C	6	The solution must allow administrators to view an audit of detailed user activity.		
C	7	The solution must provide configurable alerts based on payment activity, liquidity levels, clearing and settlement failures, high transaction amounts etc. Provide more details on the alerts available on your proposed solution and their presentation types.		

No.		Requirements	Response Code	Comments
C	8	The solution must support up to a six-eyed process for select actions performed on the solutions administrative interface. Administrators should be able to configure which action requires four to six eyed levels of review.		
C	9	The solution must allow participants to only view payment and other information pertaining to their organization. Participants should not be allowed to view the information of other participants on the NIPS.		
Clearing and Settlement				
D	1	The solution must finalize payments by utilizing a real-time settlement model. This should be achieved via collateralization using either a technical account held on the NIPS itself or via a specific account on the existing RTGS. Explain how real-time settlement is achievable in the proposed solution.		
D	2	The solution must provide built-in liquidity management tools allowing participants to efficiently manage their liquidity on the NIPS.		
D	3	The solution must provide built in liquidity related alerts that are triggered when liquidity thresholds are met or projected to be met.		
D	4	The solution must provide support to execute participant intraday liquidity loans.		
D	5	Payments made on the solution must be settled in a maximum average SLA of six seconds.		

No.		Requirements	Response Code	Comments
D	6	The solution must be able to support concurrent transactions initiated through all digital channels from every participant. Provide brief details on whether the proposed solution handles concurrent transactions, once the minimum computing requirements are met.		
D	7	The solution must be able to support peak processing times. Provide more details on the peak transaction processing figures that the proposed solution is able to facilitate once the minimum computing requirements are met.		
D	8	The solution must include support for merchant payments, provide tools to enable a seamless integration with point-of-sale devices and to manage multiple payment types through a single connection.		
D	9	The solution must provide a centralized proxy identifier (alias) database that facilitates the addressing of aliases based on a one-to-many design, against user accounts. Provide brief details on capabilities of the proposed solution's one-to-many proxy identifier (alias) database design.		
D	10	The solution must support multiple types of proxy identifiers (aliases). Specifically custom usernames or user handles, mobile numbers and email addresses must be supported.		
D	11	The solution must allow payments to also be made via standard bank account number and branch when applicable.		

No.		Requirements	Response Code	Comments
D	12	The solution must generate and support standardized QR codes. Provide details on the standards adhered to by the proposed solution as it relates to QR code generation.		
D	13	The solution must provide support for: <ul style="list-style-type: none">• Merchant-presented static QR codes.• Merchant-presented dynamic QR codes.• Consumer-presented dynamic QR codes.		
D	14	The solution should provide built-in tools that would allow administrators to investigate failed or rejected transactions, providing details on the reason for failure or rejection.		
D	15	The solution should provide built-in tools that would allow administrators to monitor and control pending message queues.		
D	16	The solution should include a built-in refund and payment dispute review mechanism. Briefly explain how the proposed solution handles payment disputes and refunds.		
D	17	The system should include built in fraud detection and prevention capabilities. The proposed solution should be able to flag and place on hold, potentially fraudulent transactions for further review. Briefly explain how the proposed solution handles potentially fraudulent transactions and the tools available to assist in the recovery of funds should fraud occur.		

No.		Requirements	Response Code	Comments
D	18	Bidders must describe any enhanced KYC and security controls for alias and QR code usage in the proposed solution. Briefly describe how this enhanced controls should address the risks identified with alias and QR code usage in global NIPS implementations.		
ISO20022 messaging				
E	1	The solution must provide support for ISO20022 Payments Clearing and Settlement (PACS) messages specifically pacs.008.001, pacs.004.001 and pacs.002.001.		
E	2	The solution must provide support for ISO20022 Payment Initiation (PAIN) messages specifically pain.013.001 and pain.014.001.		
E	3	The solution must provide support for ISO20022 Account Management (ACMT) messages specifically acmt.023.001 and acmt.024.001.		
E	4	The solution must provide support for ISO20022 Cash Management (CAMT) messages specifically camt.053.001, camt.052.001 and camt.054.001.		
Interoperability and Integrations				
F	1	The solution should be integrated with the national switch to perform it's transaction		
F	2	The solution must be able to integrate with the existing Sudanese ginee SDG		

No.		Requirements	Response Code	Comments
		interface options are available for the proposed solution to achieve this.		
F	3	The solution must be able to integrate with other existing on and off premises payment systems. Briefly details the interface options and channels available for integration with other payment systems.		
		The solution must be able to integrate with like payment networks, Government services, fintech partners etc. through API interface or adapters		
F	4	The solution should support client APIs over HTTPS protocol. Provide more details on the API architectures supported by your proposed solution (REST, SOAP etc.).		
F	5	The solution must support idempotency and must provide protections against replay transactions across its integration interfaces.		
F	6	The solution should support integration with Security Information and Event Management systems.		
Cybersecurity				
G	1	The solution must adhere to local and global financial regulations including GDPR, GLBA, and/or PSD2 where applicable.		
G	2	The solution must align with ISO27001 and other applicable industry standards such as relevant portions NIST to an NIPS.		
G	3	The solution should have redundancy to failover in case the primary solution goes down. The solution should allow for clustering and failover mechanisms to ensure continuous availability (99.99%) of the NIPS solution. Describe how the desired availability can be achieved.		

No.		Requirements	Response Code	Comments
G	4	The vendor shall provide specific requirements for data backup and recovery procedures to ensure efficient disaster preparedness.		
G	5	The solution should support an active-active high availability infrastructure. Provide details, including network diagrams, on how the proposed solution can be configured to support this.		
G	6	The solution must support Adaptive Authentication to allow for risk-based authentication during high-risk transactions such as amount thresholds, unusual login, location verification.		
G	7	The solution must support Identity Assurance Level 2 (IAL2) in accordance with NIST SP 800-63A.		
G	8	The solution must enforce the principle of least privilege. This should also be enforceable at the central bank (system ownership) level and must utilize role-based access controls (RBAC).		
G	9	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 at a minimum standard of encryption.		
G	12	The solution must utilize TLS version 1.3 for all internal and external communication.		
G	13	The solution must be compatible with centralized authentication solutions/servers.		

No.		Requirements	Response Code	Comments
G	14	The solution must utilize 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 (WAF), Traffic Filtering, Content Delivery Networks (CDN). Provide more details on how the proposed solution employs DDoS mitigation or is capable of integrating with DDoS solutions.		
Reporting				
H	1	The solution should provide standard out-of-the-box reports. Please list the standard reports included in the proposed solution.		
H	2	The solution must include built in comprehensive reporting functions for compliance and anti-money laundering (AML) audits.		
H	3	The solution must allow the Bank's administrators the ability to create custom reports. Define how custom reporting can be achieved in the proposed solution.		
H	4	The solution must provide reports on user access. Provide a listing of user access reports available on the proposed system. Auditing controls to track and measure user activity, access, etc.		
H	5	The solution must provide built in reports on participant activity, message flows. Provide a listing of participant activity and message flow reports available on the proposed solution.		
H	6	The solution must provide detailed participant statements. Participants should be able to generate statement reports via date range and other filters.		

No.		Requirements	Response Code	Comments
H	7	The solution must allow the Bank's administrators the ability to create custom reports. Define how custom reporting can be achieved in the proposed solution.		
H	8	The solution should provide customizable payment related dashboards. Briefly describe the dashboard options available on the proposed system.		
H	9	Administrators should be able to integrate the solution with third party reporting solutions e.g., Tableau, Power BI, Cognos etc.		
H	10	Users should be able to export all generated reports to .pdf, .csv and .xlsx files. Indicate if any other files types are supported.		
Billing				
I	1	The solution must allow administrators to define billing rates. Rates should be configurable primarily based on message types with additional options on volumes and flow direction (sender, receiver). Briefly explain how billing is managed in the proposed solution.		
I	2	The solution must automatically create invoices based on select billing cycles.		
I	3	The solution must have mechanisms to automatically collect due invoices on specified charge dates and billing cycles.		

--

User and Administrator Training				
L	1	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 and incorporate certified training material and delivered by a certified trainer for an efficient operation of the system. The trainer should have at least two years of experience and have delivered training on the specific domain on which training is being delivered. The training programme should be well-defined and scoped. The outcome of the training should be first and second level certified users.		
L	2	A detailed training plan with specifications for training courses, schedules, site and requirements must be defined and delivered.		
Deliverables				
M	1	A detailed design of architecture of the solution must be provided, inclusive of data and network flows.		
M	2	Detailed configurations of the implementation must be provided.		
M	3	Day to Day operation of maintenance manual must be provided.		
M	4	End-user manuals must be provided.		
M	5	Backup and recovery procedures to ensure recoverability in the event of data loss or corruption.		

10.2.2 Consumer Application Requirements

No.	Requirements	Response Code	Comments
1	Onboarding OCR-based KYC, biometric setup, guided tutorial		
2	Dashboard Real-time balance, quick actions, transaction history		
3	Send Money Multiple channels (phone, QR, email, bank, contacts)		
4	Request Money Payment request creation, shareable links		
5	QR Payments Scan-to-pay, personal QR codes, dynamic QR, NFC Scan-to-Pay		
6	Bill Payments Utilities, mobile top-up, subscription management		
7	Government Payments Taxes, Traffic fines		
8	Private Sectors education fees, Airline fees, NEC		
9	Transaction Management Search, filter, export, digital receipts		



--

10	Security 2FA, device management, transaction PIN		
11	Profile Management Aliases, linked accounts, preferences		
12	Beneficiary Management Add, update, view and delete beneficiary		
13	Notifications Real-time push, SMS, email alerts		
14	Dispute Management Built-in dispute reporting, case tracking		
15	language support English Arabic		

Performance Requirements

No.	Requirements	Response Code	Comments
1	App Launch Time < 2s (cold), < 1s (warm)		
2	Payment Flow Time < 5s end-to-end		
3	QR Scan Time < 500ms		



--

4	Application Size < 30MB (Android), < 50MB (iOS)		
5	Frame Rate Consistent 60 NIPS		
6	Memory Usage < 150MB during active use		
7	Battery Impact < 5% per hour of active use		

Security Requirements

NO	Requirement	Details	Response Code	Comments
1.	Data Security	AES-256 encryption for all locally stored data RSA encryption for API communications Certificate pinning to prevent MITM attacks Secure key management using platform keychains		
2.	Authentication & Authorization	Biometric authentication (Face ID, Touch ID, Android Biometric) Transaction PIN for payment authorization Two-factor authentication for sensitive operations JWT tokens with automatic refresh mechanism Session management with automatic timeout		
3.	Network Security	TLS 1.3 for all network communications No cleartext traffic allowed		

--

		VPN and proxy detection capabilities Network security configuration for Android App Transport Security for iOS		
4.	Application Security	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 & Remote Lock Device fingerprint and Anti-tampering mechanisms		
5.	Compliance Requirements	PCI DSS compliance for payment processing GDPR/data privacy compliance Local financial regulations compliance App Store and Play Store security guidelines		



10.3 Hardware and Networking Requirements

10.3.1 Architecture

Provide an introductory narrative of how the proposed system architecture aligns with the overarching objectives and functional requirements of the NIPS. It should cover the main features and benefits that distinguish your system. Your response should include a solution diagram, including network data flows, that depicts the overall design as well as hardware specifications if proposing an on-premises solution.

10.3.2 Operating System and Related Software

All proposals must specify the name and version number of the proposed operating system(s). In addition to the operating system(s), the following software packages, complete with any necessary licenses, must be specified with this proposal. The Bidder must state the application that is being used for each of the following:

- Desktop and server application update solution.
- Industry standard relational database management system.
- System and application backup and high availability.

10.3.3 Backup and Failover Solution

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

10.3.4 Capacity

Bidders must specify optimal server and storage capacity for the proposed solution, if offering an on-premise solution. Performance must be able to scale to meet the Bank's anticipated growth of 5% annually for at least 5 years. Identify exceptions.

10.3.5 Upgrades and Expansion

The proposed system must operate at no more than 35% of capacity (for CPU, memory, and I/O performance). It must have the capability to have a field upgrade to projected capacity without changing the initial CPU/disk equipment or other peripherals. Bidders must describe the expandability of their proposed solution in terms of processors, memory, I/O, disk drives, and peripheral devices for both the on premise.



10.3.6 Server Functionality

The Bank will provision all required hardware based on the Bidder's specifications and recommendation. Therefore, it is 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 NIPS Solution.

--



11. Appendix D: Bidder Comments to Technical Specifications

Item	Comment

ADDENDUM TO REQUEST FOR PROPOSAL

RFP Reference:	National Instant Payment System (NIPS) Implementation
Addendum Number:	A-01
Issue	National Unified Payment Application (NUPA)
Issuing Authority:	Central Bank of Sudan

Executive Summary

This Addendum supplements the main Request for Proposal (RFP) for the National Instant Payment System (NIPS) and defines the specific requirements for the design, development, deployment, and maintenance of the **National Unified Payment Application (NUPA)**—a Central Bank-owned and governed mobile payment application that will serve as the primary consumer and merchant interface to the national instant payment infrastructure.

The NUPA project represents a strategic initiative to consolidate fragmented digital payment channels, enhance financial inclusion, and provide the Central Bank with comprehensive oversight and supervisory capabilities over retail payment activities.

Bidders responding to the main NIPS RFP are invited to submit proposals for NUPA either as:

- **Option A:** An integrated solution delivered by the same vendor providing the NIPS core infrastructure
- **Option B:** A standalone solution with clearly defined integration touchpoints to the NIPS platform

This Addendum must be read in conjunction with the main NIPS RFP document. In case of conflict between this Addendum and the main RFP, the provisions of this Addendum shall take precedence for NUPA-related requirements.

1. Project Background and Strategic Context

1.1 Current Payment Landscape

The national payment ecosystem currently exhibits the following characteristics:

- Multiple bank-operated and third-party payment applications with limited interoperability
- Fragmented customer experience requiring multiple app installations
- High cash dependency for retail transactions
- Limited Central Bank visibility into end-user payment behavior and patterns
- Inconsistent security and consumer protection standards across platforms

1.2 Strategic Objectives

The Central Bank seeks to address these challenges through NUPA by achieving the following strategic objectives:

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

1.3 Governance Model

NUPA will operate under the following governance framework:

- **Ownership:** Central Bank of Sudan retains full ownership of the application, brand, and user data
- **Licensing:** NUPA operates under the Central Bank of Sudan license with direct regulatory oversight
- **Governance:** Central Bank Payment Systems Committee provides strategic direction
- **Operations:** May be delegated to a qualified service provider under a strict SLA and oversight regime
- **Revenue Model:** Transaction fees, merchant discount rates, and value-added services as determined by Central Bank policy

2. Scope of Work

2.1 In-Scope Deliverables

Bidders shall provide comprehensive solutions covering the following components:

2.1.1 Mobile Applications

- Native mobile applications for Android (version 8.0 and above) and iOS (version 13.0 and above)
- Progressive Web Application (PWA) for broader accessibility
- Tablet-optimized interfaces for merchant point-of-sale scenarios
- Offline capability for transaction queuing and balance viewing

2.1.2 Back-End Platform

- Application server infrastructure with microservices architecture
- API gateway for secure communication with NIPS, banks, PSPs, and third-party services
- User identity and access management system
- Transaction processing and routing engine
- Real-time notification and messaging service
- Comprehensive logging, monitoring, and analytics platform

2.1.3 Merchant Solutions

- Merchant onboarding portal (web and mobile)
- Static and dynamic QR code generation and management
- Merchant transaction dashboard and reporting tools
- Settlement reporting and reconciliation interface

2.1.4 Administrative and Supervisory Tools

- Central Bank supervisory dashboard with real-time transaction monitoring
- Risk management and fraud detection system
- Regulatory reporting and analytics module
- User support and dispute management system
- Configuration and parameter management console

2.1.5 Integration Layer

- Secure APIs and messaging interfaces to the NIPS core switch
- Integration adapters for bank core banking systems and wallet platforms
- Biller aggregation platform for utilities, government services, and telecom operators
- National identity verification system integration (KYC/eKYC)
- SMS gateway and push notification services integration

2.2 Out-of-Scope (Initial Phase)

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

- Cross-border remittance services
- Credit origination and lending products
- Investment and wealth management features
- Cryptocurrency or digital currency wallet functionality
- E-commerce marketplace integration beyond payment processing

3. Functional Requirements

3.1 User Onboarding and Identity Management

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
- 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, enabling:

- **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

3.2 Authentication and Security

FR-006: The system shall implement multi-factor authentication combining:

- Knowledge factor: PIN or password
- Possession factor: Device binding and OTP
- Inherence factor: Biometric authentication (fingerprint, face recognition) 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)
- 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

3.3 Payment and Transfer Services

3.3.1 Person-to-Person (P2P) Transfers

FR-011: The system shall enable instant transfers between users using the following identifiers:

- Mobile number registered with NUPA
- Account number or IBAN
- National ID number
- Unique user alias/handle
- QR code scan

FR-012: The system shall perform beneficiary validation through NIPS before presenting the confirmation screen to the user

FR-013: The system shall support own-account transfers across different banks/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 transaction preview, including fees, exchange rates (if applicable), and estimated completion time before execution

3.3.2 Merchant Payments

FR-017: The system shall support QR code-based merchant payments compliant with EMVCo QR Code Specification or equivalent national standard

FR-018: The system shall distinguish between:

- **Static QR:** Fixed merchant identifier, user enters amount
- **Dynamic QR:** Pre-populated transaction with amount, merchant details, and optional invoice reference

FR-019: Upon scanning the merchant QR, the system shall display merchant verification information, including:

- Legal business name
- Trade license number
- Merchant category code
- Transaction amount and description
- 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

3.3.3 Bill Payments and Top-Ups

FR-022: The system shall integrate with the national biller aggregation platform to present a categorized list of billers, including:

- Utilities (electricity, water, gas)
- Telecommunications (postpaid, prepaid, data)
- Government services (taxes, fees, fines)
- Educational institutions
- Insurance providers
- Charitable organizations

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 favorite biller accounts for quick access

3.4 Account and Balance Management

FR-027: The system shall display an aggregated view of all linked accounts/wallets with:

- Current available balance
- Pending transactions
- Daily/monthly transaction limits and utilization
- Account status

FR-028: The system shall support real-time balance inquiry through NIPS integration or direct bank API, where available

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

3.5 Transaction History and Statements

FR-031: The system shall provide a 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
- 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
- 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

3.6 Merchant Management

FR-037: The system shall provide a dedicated merchant onboarding workflow capturing:

- Business legal information and registration documents
- Business owner/authorized signatory KYC
- Business category and expected transaction volumes
- Settlement bank account details
- Tax identification numbers
- Supporting documentation upload (trade license, 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 the 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
- 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

3.7 Dispute Management and Customer Protection

FR-043: The system shall enable users to raise disputes on completed transactions by selecting the transaction and providing:

- Dispute category (unauthorized transaction, incorrect amount, service not received, etc.)
- Description and supporting evidence
- Preferred resolution (refund, reversal, investigation)

FR-044: The system shall generate a unique dispute reference number and communicate via push notification and SMS.

FR-045: The system shall provide a dispute tracking interface showing the 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.

3.8 Notifications and Communication

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)
- Promotional offers and announcements

FR-050: The system shall send SMS notifications for critical events, including:

- Successful high-value transactions (above configurable threshold)
- Account linking/delinking
- PIN reset
- Security incidents

FR-051: The system shall maintain a notification center 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

3.9 Customer Support

FR-054: The system shall provide multi-channel support, including:

- In-app FAQ and knowledge base with search capability
- Chatbot for common inquiries with escalation to human agents
- Secure in-app messaging with support agents
- Support ticket creation and tracking

- Call center 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 authorized agents

4. Non-Functional Requirements

4.1 Performance and Scalability

NFR-001: The system shall process 95% of instant payment transactions end-to-end within 2 seconds, measured from user confirmation to receipt notification

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

NFR-003: The application shall launch and be ready for user interaction within 3 seconds 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

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

4.2 Availability and Reliability

NFR-007: The system shall maintain 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 (2:00 AM - 6:00 AM local time)

NFR-009: The system shall implement automatic failovers 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.

4.3 Security and Compliance

NFR-012: All data transmission shall be encrypted using TLS 1.3 or higher with perfect forward secrecy

NFR-013: All sensitive data at rest shall be encrypted using AES-256 encryption with hardware security module (HSM) key management

NFR-014: The system shall implement defense-in-depth security architecture including:

- Web application firewall (WAF)
- DDoS protection
- Intrusion detection and prevention systems (IDS/IPS)
- Security information and event management (SIEM)
- 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

NFR-017: The system shall implement comprehensive audit logging capturing:

- All user authentication attempts
- All financial transactions
- All administrative actions
- All system configuration changes
- All API calls with request/response payloads

NFR-018: Audit logs shall be tamper-proof, 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 minimization, 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

4.4 Usability and Accessibility

NFR-021: The application shall provide an intuitive user interface following platform-specific design guidelines (Material Design for Android, Human Interface Guidelines for iOS)

NFR-022: The application shall support a minimum of two languages (Arabic and English) with in-app language switching capability

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)
- Support for screen readers
- Keyboard navigation support
- Scalable font sizes
- 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 optimized 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

4.5 Maintainability and Supportability

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 OpenAPI/Swagger specification

NFR-030: The system shall implement centralized configuration management, enabling parameter changes without code deployment

NFR-031: The system shall provide real-time monitoring dashboards displaying:

- System health metrics
- Transaction success/failure rates
- API performance metrics
- User activity patterns
- 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 the deprecation notice

4.6 Interoperability

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

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

5. Integration Requirements

5.1 National Instant Payment System (NIPS)

INT-001: The solution shall integrate with 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
- 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

5.2 Bank and Payment Service Provider Integration

INT-005: The solution shall provide standardized integration interfaces enabling banks and PSPs to:

- Receive account linking requests
- Validate account ownership
- Provide balance inquiries
- Receive debit authorizations

- Send credit notifications
- Report transaction status

INT-006: The solution shall support multiple integration patterns:

- Synchronous API calls for real-time operations
- Asynchronous messaging for batch operations
- Webhook notifications for status updates

INT-007: The solution shall provide integration of a sandbox environment for bank/PSP testing and certification.

5.3 National Identity and KYC Systems

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 licenses, tax certificates, and business registrations

5.4 Biller Aggregation Platform

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

5.5 Telecommunications Integration

INT-014: The solution shall integrate with mobile network operators for:

- OTP SMS delivery with delivery confirmation
- Airtime and data package top-up
- Mobile number validation and portability checks

INT-015: The solution shall implement SMS routing logic with fallback providers for high availability

5.6 Card Schemes (Future Phase)

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

6. Regulatory and Compliance Requirements

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:

- Transaction monitoring rules engine
- Suspicious activity detection and reporting
- Sanctions screening against national and international lists
- 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
- 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
- Data breach notification within mandated timeframes

REG-007: The solution shall implement consumer protection controls, including:

- Clear and transparent fee disclosure
- Transaction confirmation before execution
- Transaction receipt generation
- Accessible dispute resolution process
- Customer data confidentiality

7. Technical Specifications

7.1 Mobile Application Requirements

7.1.1 Platform Support

- **Android:** Minimum API level 26 (Android 8.0), target the latest stable version
- **iOS:** Minimum iOS 13.0, target the latest stable version
- **PWA:** Support for modern browsers (Chrome, Safari, Firefox) on desktop and mobile

7.1.2 Development Framework

Bidders shall specify proposed development framework with justification including:

- Native development (Swift/Kotlin)
- Cross-platform frameworks (React Native, Flutter)
- Hybrid approaches

7.1.3 Application Size

- Initial application download size shall not exceed 50 MB
- Updates shall utilize delta patching to minimize data consumption

7.1.4 Device Permissions

Application shall request only necessary permissions with a clear user explanation:

- Camera (for QR scanning and document capture)
- Location (optional, for merchant proximity features)
- Biometrics (for authentication)
- Notifications (for transaction alerts)
- Contacts (optional, for beneficiary selection)

7.2 Back-End Architecture

7.2.1 Technology Stack

Bidders shall propose a comprehensive technology stack including:

- Programming languages and frameworks
- Database systems (relational and NoSQL)
- Message brokers and queuing systems

- API gateway and service mesh
- Container orchestration platform
- Monitoring and observability tools

7.2.2 Cloud Infrastructure

The solution may be deployed on:

- Public cloud (AWS, Azure, GCP) with data residency controls
- Private cloud infrastructure
- Hybrid cloud architecture
- On-premises data center

Bidders shall provide detailed infrastructure design with cost projections for 3-year growth trajectory.

7.2.3 Data Management

- Transaction data retention: Minimum 7 years with archival strategy
- User data retention: Active account lifetime plus regulatory retention period
- Database backup: Continuous replication with point-in-time recovery
- Data archival: Automated archival of historical data to cost-effective storage

7.3 Security Architecture

7.3.1 Authentication and Authorization

- Multi-factor authentication framework
- OAuth 2.0 / OpenID Connect for partner integration
- Role-based access control (RBAC) for administrative functions
- JWT or equivalent token-based session management
- Certificate pinning for mobile applications

7.3.2 Cryptography

- Hardware Security Module (HSM) for key management
- Secure key generation and rotation procedures
- End-to-end encryption for sensitive operations
- Digital signatures for non-repudiation

7.3.3 Fraud Prevention

- Real-time fraud detection rules engine
- Machine learning-based anomaly detection

- Device fingerprinting and behavioral biometrics
- Velocity checks and transaction pattern analysis
- Geo-location verification and impossible travel detection

7.4 API Specifications

The solution shall provide RESTful APIs with the following characteristics:

- JSON request/response format
- OAuth 2.0 authentication
- Rate limiting and throttling
- Comprehensive error codes and messages
- Request/response logging
- API versioning strategy
- Interactive API documentation (Swagger/OpenAPI)

8. Data Analytics and Reporting

8.1 User Analytics

DA-001: The solution shall capture and analyze user behavior metrics, including:

- User acquisition and retention rates
- Feature adoption and usage patterns
- User journey and drop-off points
- Session duration and frequency
- Geographic distribution

8.2 Transaction Analytics

DA-002: The solution shall provide real-time and historical transaction analytics, including:

- Transaction volumes and values by type, channel, 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
- Transaction routing and settlement analytics

8.3 Financial Analytics

DA-003: The solution shall generate financial reporting, including:

- Revenue recognition by fee type and counterparty
- Settlement reconciliation reports
- Merchant discount rate calculations
- Cost allocation and profitability analysis

8.4 Regulatory Reporting

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
- AML/CFT suspicious activity reports

8.5 Business Intelligence

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
- Customer segmentation and cohort analysis

9. Project Delivery Requirements

9.1 Implementation Phases

Bidders shall propose an implementation plan structured in phases:

Phase 1: Foundation (Months 1-6)

- Requirements finalization and solution design
- Infrastructure setup and environment provisioning
- Core platform development (user management, authentication)
- NIPS integration development
- Security implementation and testing

Phase 2: Core Features (Months 7-12)

- P2P transfer functionality
- QR payment implementation
- Bill payment integration
- Merchant onboarding portal
- Administrative and supervisory tools
- User acceptance testing

Phase 3: Pilot Launch (Months 13-15)

- Soft launch with limited user base (10,000-50,000 users)
- Bank and PSP integration with pilot institutions
- Performance testing and optimization
- Issue resolution and refinement

Phase 4: National Rollout (Months 16-18)

- Staged national rollout by region
- Marketing and user education campaigns
- Merchant acquisition programs
- Full bank/PSP ecosystem integration
- Ongoing optimization and support

9.2 Deliverables

Bidders shall provide the following deliverables:

9.2.1 Design Phase

- Business requirements document (updated)
- System design document
- Security architecture document
- Integration specifications
- User experience design and wireframes
- Data model and database design
- Infrastructure architecture diagram

9.2.2 Development Phase

- Source code with comprehensive inline documentation
- API documentation and integration guides
- Database schema and migration scripts
- Deployment automation scripts

- Test plans and test cases
- User manuals and training materials

9.2.3 Testing Phase

- Unit test reports
- Integration test reports
- Performance test reports
- Security test reports (penetration testing, vulnerability assessment)
- User acceptance test reports

9.2.4 Deployment Phase

- Deployment runbooks and procedures
- Operations and maintenance manuals
- Disaster recovery and business continuity plans
- Monitoring and alerting configurations
- Capacity planning documentation

9.3 Knowledge Transfer

KT-001: Bidder shall conduct a 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)
- Security administration training (3 days)

KT-002: Bidder shall provide train-the-trainer programs for customer support and merchant support teams

KT-003: All training shall include hands-on exercises and documentation in English and Arabic

9.4 Testing Requirements

TEST-001: Bidder shall conduct the following testing activities:

- Unit testing with a minimum 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 AA standards
- Localization testing for Arabic and English interfaces

TEST-002: Test environments shall mirror production configuration and be maintained throughout the solution lifecycle

10. Support and Maintenance

10.1 Warranty Period

SUP-001: Bidder shall provide a comprehensive warranty covering defects, bugs, and performance issues for a minimum of 12 months from production acceptance

SUP-002: During the warranty period, the bidder shall provide bug fixes and patches at no additional cost with the following 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 significant 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

10.2 Post-Warranty Support

SUP-003: 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

- Performance optimization services

SUP-004: Support proposal shall include:

- Support team structure and location
- Escalation procedures
- SLA commitments
- Pricing model (annual fixed fee or time and materials)

10.3 Enhancements and Evolution

SUP-005: Bidder shall describe the process for handling post-launch enhancements, including:

- Change request procedures
- Impact assessment and estimation methodology
- Development and deployment processes
- Pricing models for enhancements

11. Licensing and Intellectual Property

11.1 Software Licensing

LIC-001: Bidder shall provide perpetual, irrevocable licenses for all custom-developed software components, with full source code ownership transferred to Central Bank

LIC-002: For third-party commercial software components, the bidder shall:

- Disclose all third-party components and licensing terms
- Secure perpetual licenses with unlimited user/transaction rights where possible
- Provide alternatives to subscription-based components with vendor lock-in risks
- Ensure license transferability in case of vendor change

LIC-003: For open-source components, the bidder shall:

- Disclose all open-source components and licenses
- Ensure compliance with license obligations
- Avoid copyleft licenses (GPL, AGPL) that could restrict Central Bank rights
- Provide vulnerability monitoring for open-source dependencies

11.2 Intellectual Property Rights

IPR-001: All custom code, designs, documentation, and artifacts developed under this project shall be owned exclusively by Central Bank with full intellectual property rights

IPR-002: Bidder shall not reuse project-specific code or designs in other projects without explicit written permission from Central Bank

IPR-003: Bidder may retain ownership of pre-existing frameworks and tools brought to the project, provided such tools are licensed to Central Bank for perpetual use

12. Commercial and Pricing Requirements

12.1 Cost Breakdown

Bidders shall provide a detailed cost breakdown, including:

12.1.1 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

12.1.2 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

12.1.3 Transaction-Based Pricing

If proposing a transaction-based pricing model, provide:

- Price per transaction by transaction type
- Volume discounts and tier structure
- Minimum monthly commitments
- Price escalation terms

12.2 Payment Terms

PAY-001: Payment shall be milestone-based, tied to delivery and acceptance of specified deliverables

PAY-002: Bidders shall propose a payment schedule aligned with the implementation phases

PAY-003: Final payment (minimum 10% of total contract value) shall be released upon successful completion of the warranty period

12.3 Price Validity

PAY-004: Pricing shall remain valid for a minimum of 180 days from the proposal submission deadline

13. Vendor Qualification Requirements

13.1 Mandatory Qualifications

QUAL-001: Bidder must demonstrate a minimum of 7 years of experience in payment systems implementation

QUAL-002: Bidder must have successfully delivered a minimum of 2 instant payment or mobile wallet solutions for financial institutions or central banks

QUAL-003: Bidder must demonstrate ISO 27001 certification for information security management

QUAL-004: Bidder must demonstrate ISO 20000 or ITIL certification for IT service management

QUAL-005: Bidder must have presence or ability to establish local presence in Sudan for the project duration

13.2 Technical Qualifications

QUAL-006: 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
- DevOps and continuous deployment

QUAL-007: Bidder must provide CVs of proposed key personnel, including:

- Project Manager (PMP or equivalent, 10+ years experience)
- Solution Architect (payment systems experience mandatory)

- Security Architect (CISSP or equivalent)
- Mobile Development Lead
- Backend Development Lead
- QA/Test Manager

13.3 Financial Qualifications

QUAL-008: Bidder must submit audited financial statements for the last 3 years demonstrating financial stability

QUAL-009: Bidder must provide evidence of professional indemnity insurance with minimum coverage of \$5 million USD

14. Evaluation Criteria

Proposals for NUPA will be evaluated using the following weighted criteria:

Evaluation Criteria	Weight	Sub-Criteria
Technical Solution	35%	Architecture and design (10%) Functional completeness (10%) Innovation and future-readiness (8%) Usability and user experience (7%)
Implementation Approach	20%	Methodology and project plan (8%) Risk management (6%) Knowledge transfer approach (6%)
Vendor Qualifications	20%	Corporate experience (8%) Team qualifications (7%) Reference projects (5%)
Security and Compliance	15%	Security architecture (8%) Regulatory compliance (7%)
Commercial	10%	Total cost of ownership (5%) Pricing model transparency (3%) Value for money (2%)
TOTAL	100%	

14.1 Technical Evaluation

Proposals will be assessed on:

- Alignment with functional and non-functional requirements
- Scalability and performance characteristics
- Integration capabilities with NIPS and ecosystem partners

- Security posture and compliance approach
- Technology choices and architecture decisions
- User experience design quality
- Innovation and differentiation factors

14.2 Reference Projects

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 overcome
- Current operational status and metrics (users, transactions)

EVAL-002: Central Bank reserves the right to contact reference clients for verification

15. Proposal Submission Requirements

15.1 Proposal Structure

Bidders shall structure their proposals as follows:

Volume 1: Executive Summary

- Company profile and experience
- Understanding of project objectives
- Proposed solution overview (maximum 10 pages)

Volume 2: Technical Proposal

- Solution architecture and design
- Functional requirements response matrix
- Non-functional requirements response matrix
- Integration approach
- Security architecture
- Technology stack justification
- Innovation and value-added features

Volume 3: Implementation Plan

- Project methodology and governance
- Detailed work plan with milestones
- Resource plan and team structure
- Risk register and mitigation strategies
- Testing strategy
- Training and knowledge transfer plan

Volume 4: Commercial Proposal

- Detailed cost breakdown
- Payment schedule proposal
- Licensing and subscription terms
- Pricing assumptions and exclusions
- Post-warranty support options

Volume 5: Compliance and Qualifications

- Compliance matrix for mandatory requirements
- Company registrations and certifications
- Financial statements
- Insurance certificates
- Reference project details
- Key personnel CVs

15.2 Proposal Format

FORMAT-001: Proposals shall be submitted in PDF format with searchable text

FORMAT-002: All cost information must be provided in both USD and local currency, with the exchange rate clearly stated

FORMAT-003: Page limits (excluding appendices):

- Executive Summary: 10 pages
- Technical Proposal: 75 pages
- Implementation Plan: 40 pages
- Commercial Proposal: 20 pages
- Compliance: No limit

15.3 Submission Deadline and Method

SUB-001: Proposals must be submitted electronically to [procurement@centralbank.sd] by [Date to be announced] at 14:00 CAT

SUB-002: Subject line must read: "NUPA RFP Proposal - [Bidder Name]."

SUB-003: Proposals shall be encrypted with a password to be provided separately

SUB-004: Bidders must submit a signed non-disclosure agreement prior to receiving confidential RFP annexures

16. Terms and Conditions

16.1 RFP Process

TC-001: Central Bank reserves the right to:

- Amend this RFP through written addenda
- Extend submission deadlines
- Request clarifications or additional information from bidders
- Conduct site visits and bidder presentations
- Conduct proof-of-concept evaluations
- Negotiate with selected bidder(s)
- Cancel or reissue this RFP
- Award contract to other than the lowest bidder
- Split the award between multiple vendors

TC-002: Submission of proposal constitutes acceptance of these terms and conditions

TC-003: All costs incurred in preparing and submitting proposals are the bidder's responsibility

16.2 Confidentiality

TC-004: Bidders shall treat all RFP information as confidential and shall not disclose to third parties without written permission

TC-005: Bidders shall not use RFP information for purposes other than preparing and submitting a proposal

16.3 Validity Period

TC-006: Proposals shall remain valid for 180 days from the submission deadline

16.4 Questions and Clarifications

TC-007: All questions regarding this RFP must be submitted in writing to [procurement@centralbank.sd] by **[Date - typically 14 days before submission deadline]**

TC-008: Responses to all questions will be published as an RFP addendum to all registered bidders

TC-009: No verbal clarifications or commitments are binding

17. Contract Terms (Indicative)

The following contract terms will be negotiated with the selected bidder:

17.1 Contract Duration

- Initial term: 3 years from production go-live
- Renewable for an additional 2-year term by mutual agreement

17.2 Performance Guarantees

- Bank guarantee or performance bond: 10% of contract value
- Valid for contract duration plus 3 months

17.3 Liquidated Damages

- Delay in delivery: 0.5% of contract value per week, maximum 10%
- SLA breaches: As defined in the service level agreement

17.4 Liability and Indemnification

- Bidder shall indemnify Central Bank against third-party claims arising from solution operation
- Liability cap to be negotiated (typically 100-200% of annual contract value)

17.5 Termination

- Termination for convenience: 90 days written notice by either party
- Termination for cause: Immediate upon material breach
- Transition assistance: 6 months at agreed rates

18. Appendices (To Be Provided)

Appendix A: NIPS Integration Specifications

- NIPS API documentation
- Message formats and data dictionaries
- Security and authentication requirements
- Testing and certification procedures

Appendix B: Current System Landscape

- Existing payment infrastructure diagram
- Bank and PSP connectivity status
- Current transaction volumes and projections

Appendix C: Regulatory Framework Documents

- Payment Systems Law
- Payment Service Provider Regulations
- Data Protection Law extracts
- AML/CFT Guidelines

Appendix D: User Research and Personas

- User research findings
- Customer journey maps
- Persona definitions

Appendix E: Brand Guidelines

- Central Bank visual identity
- NUPA brand assets and usage guidelines
- Messaging and communication guidelines

19. Contact Information

Project Authority:
Central Bank of Sudan
Payment Systems Department
[Address]

RFP Coordinators:

Name: [To be provided]

Email: [To be provided]

Phone: [To be provided]

Submission Portal:

[URL if electronic submission platform used]

Acknowledgment of Addendum

By signing below, the bidder acknowledges receipt and understanding of this Addendum and agrees to comply with all requirements contained herein.

Bidder Name: _____

Authorized Signatory: _____

Title: _____

Date: _____

Company Stamp:

END OF ADDENDUM

NIPS PROJECT REQUIREMENTS: CENTRAL DISPUTE MANAGEMENT SYSTEM (CDMS) – FUNCTIONAL AND NON-FUNCTIONAL REQUIREMENTS

A Central Dispute Management System (CDMS) is required to integrate with NIPS to ensure the consumer Trust and Financial Inclusion:

For users to trust a digital system over physical cash, they need a clear path to recovery if they lose money for a technical glitch.

Without a reliable Dispute system to resolve issues, users may revert to cash, undermining national financial inclusion goals.

Dispute Management System is required to enforcing the Regulatory SLA compliance and mandatory Dispute Resolution Mechanism.

1. System Overview

The Central Dispute Management System (CDMS) shall provide a centralized platform to automate the management, tracking, and resolving of disputes related to electronic payment transactions and to integrate seamlessly with NIPS and other digital Payment systems.

The platform shall enable automated dispute lifecycle management between participating entities including:

- NIPS Participating Banks.
- Issuing Banks
- Acquiring Banks
- Payment Service Providers
- Mobile Wallet Providers
- Card Issuers
- Merchant
- ATM Operators

The system shall facilitate end-to-end dispute handling, reducing the manual turnaround Time for transaction status queries and “Funds Return” requests, ensuring compliance with national payment regulations, international rules, and service-level agreements (SLAs).

2. System Objectives

The Central Dispute Management System shall fulfill providing the following:

- Centralize dispute handling across the national payment ecosystem.
- Automate dispute lifecycle workflows.
- Reduce dispute resolution time.
- Ensure compliance with international card scheme dispute processes.
- Provide transparency and tracking of disputes.
- Facilitate communication between participating Banks, Fintech companies and the Central Bank Payment systems.
- Provide analytics and reporting for regulatory oversight.

3. Core Functional Capabilities

- The system shall provide Automated Case Creation: The system must automatically trigger a dispute case when a NIPS "Transaction Status Query" (TSQ) returns a failed or timed-out status but funds are debited.
- The system shall provide Integration (API Layer): Direct integration with NIPS and other digital payments systems using ISO 20022 message standards.

NIPS PROJECT REQUIREMENTS: CENTRAL DISPUTE MANAGEMENT SYSTEM (CDMS) – FUNCTIONAL AND NON-FUNCTIONAL REQUIREMENTS

Connectivity with the Core Banking System (CBS) for automated ledger reversal once a dispute is validated.

- Workflow Engine: Support for standard dispute types:
 - Failed Transaction/Debit Error: Automated refund logic.
 - Fraud/Unauthorized Transaction: Fraud tagging and communication with the receiving institution.
 - Duplicate Debit: Matching logic to identify identical RRNs (Retrieval Reference Numbers).

3.1 Dispute Case Management

The system shall provide a centralized case management module enabling financial institutions to initiate, manage, and resolve disputes.

Key capabilities:

- Create dispute tickets through a web portal.
- Automatic generation of unique dispute reference numbers.
- Ability to attach transaction details automatically from payment systems.
- Upload supporting documents and evidence.
- Assign dispute category and subcategory.
- Track dispute status throughout its lifecycle.
- Support multi-stage dispute processes.

Supported dispute types include:

- Cardholder transaction disputes
- Merchant chargebacks
- ATM surplus/shortage claims
- POS transaction disputes
- Wallet transaction disputes
- Interbank settlement disputes

3.2 Dispute Lifecycle Management

The system must manage the complete dispute lifecycle across participating institutions.

Lifecycle stages may include:

1. Dispute initiation
2. Validation
3. Issuer investigation
4. Acquirer response
5. Evidence submission
6. Arbitration
7. Resolution
8. Settlement
9. Closure

The system must:

- Track each stage automatically.
- Maintain a complete audit trail.
- Notify relevant parties during each stage.
- Allow escalation to the Central Bank when required.

NIPS PROJECT REQUIREMENTS: CENTRAL DISPUTE MANAGEMENT SYSTEM (CDMS) – FUNCTIONAL AND NON-FUNCTIONAL REQUIREMENTS

3.3 Interbank Workflow Automation

The platform must support automated workflow management:

The system shall be able to provide Automated Evidence Collector.

The system shall be able to provide configurable Business Rules Engine to enable:

- Automation of threshold-based dynamic Routing.
- Risk scoring, by automatically flagged for suspicious high-level review.
- Automated validation for failed transaction and trigger an automatic reversal.

Capabilities include:

- Automatic routing of dispute cases to the appropriate bank or financial institution.
- Workflow rules based on dispute type.
- Escalation mechanisms.
- Escalation Logic and Automated reminders for pending responses.
- Automatic closure of expired cases.

The system must support dispute flows including:

- Issuer → Acquirer
- Acquirer → Issuer
- Issuer → Central Bank
- Acquirer → Central Bank

3.4 Service Level Agreement (SLA) Management

The system must support configurable SLA management for dispute processing.

Capabilities include:

- SLA definition per dispute type.
- SLA definition per transaction channel.
- SLA definition per participant type.
- Automatic SLA timers.
- Alerts for SLA breaches.
- Escalation rules.
- SLA performance reporting.

Examples:

- Issuer response deadlines
- Acquirer evidence submission deadlines
- Arbitration deadlines

3.5 Regional and International Compliance

The platform must support dispute management requirements defined by international card networks including:

- Visa
- Mastercard

NIPS PROJECT REQUIREMENTS: CENTRAL DISPUTE MANAGEMENT SYSTEM (CDMS) – FUNCTIONAL AND NON-FUNCTIONAL REQUIREMENTS

Capabilities must include:

- Support for chargeback reason codes
- Compliance with scheme dispute timeframes
- Evidence submission requirements
- Arbitration workflows
- Representment processing
- Pre-arbitration handling
- Chargeback tracking

The system must allow configuration of card scheme rules to accommodate future updates.

3.6 Central Bank Oversight and Arbitration

The Central Bank must have supervisory access to all disputes across the ecosystem.

Capabilities include:

- Monitoring of disputes across all banks.
- Arbitration capabilities.
- Dispute escalation management.
- Regulatory intervention workflows.
- Audit trail of dispute actions.
- Ability to impose resolution decisions.

The system must allow the Central Bank to:

- Intervene in unresolved disputes.
- Issue binding decisions.
- Generate regulatory reports.

4. Web Portal for Banks and Financial Institutions

The system shall provide a secure web-based portal accessible by all participating financial institutions.

Each institution must have:

- Dedicated organizational accounts
- Role-based access control
- Multi-user access

Portal capabilities:

- Create and manage disputes
- Upload evidence documents
- Respond to dispute requests
- Track dispute progress
- Receive notifications
- Access dashboards and reports

5. Integration with Contact Center Systems

The platform must support integration with the Central Bank Contact Center platform.

Capabilities include:

- Automatic dispute ticket creation via:
- IVR
- Omnichannel chat
- AI agents
- Customer service agents

NIPS PROJECT REQUIREMENTS: CENTRAL DISPUTE MANAGEMENT SYSTEM (CDMS) – FUNCTIONAL AND NON-FUNCTIONAL REQUIREMENTS

- API integration with contact center platforms.
- Capture customer complaints directly into the dispute system.
- Auto-populate transaction data when available.
- Link customer interaction history to dispute records.

6. Notification and Communication Management

The system must provide real-time notification mechanisms for dispute events.

Supported notification channels:

- Email
- SMS
- System alerts
- API notifications

Notifications must be triggered for:

- New dispute creation
- Evidence requests
- SLA reminders
- Dispute resolution
- Escalations

7. Dashboards and Analytics

The platform must provide role-based dashboards.

Bank/FI Dashboard

Each bank must be able to view:

- Total disputes submitted
- Disputes pending response
- Disputes under investigation
- Resolved disputes
- SLA compliance metrics
- Dispute volume by type

Central Bank Dashboard

The Central Bank must have access to:

- System-wide dispute statistics
- Disputes by bank
- Disputes by transaction type
- SLA compliance across institutions
- Escalated disputes
- Dispute resolution performance

8. Reporting Capabilities

The system must support advanced reporting features.

Standard reports include:

- Disputes by bank
- Disputes by transaction channel
- Disputes by reason code
- Disputes by status

NIPS PROJECT REQUIREMENTS: CENTRAL DISPUTE MANAGEMENT SYSTEM (CDMS) – FUNCTIONAL AND NON-FUNCTIONAL REQUIREMENTS

- SLA compliance reports
- Dispute aging reports
- ATM surplus and shortage reports

Reports must support:

- Export to Excel
- Export to PDF
- Scheduled reporting
- Custom report creation

9. Security and Access Control

The platform must implement strong security mechanisms including:

- Role-Based Access Control (RBAC)
- Multi-Factor Authentication
- Secure user authentication
- Data encryption
- Audit logging
- Activity tracking

The system must support institution-level data segregation to ensure each bank can only access its own disputes.

10. Audit and Compliance

The system must maintain a complete audit trail including:

- Dispute creation
- Evidence submission
- Workflow transitions
- User actions
- Decision history

Audit records must be immutable and retained according to regulatory requirements.

The system must be configurable to adhere to the NIPS resolution Time.

11. API and System Integration

The platform must provide APIs for integration with:

- NIPS
- National payment switch
- Card management systems
- Core banking systems
- ATM switch
- Wallet platforms
- Merchant systems
- Contact center platform

The system should be able to enable the following:

- Raise Dispute API
- Provide Evidence API
- Dispute Status API

NIPS PROJECT REQUIREMENTS: CENTRAL DISPUTE MANAGEMENT SYSTEM (CDMS) – FUNCTIONAL AND NON-FUNCTIONAL REQUIREMENTS

- Settlement Integration

Supported standards:

- REST APIs
- JSON/XML
- Secure API authentication

12. Document and Evidence Management

The system must support secure document management including:

- Upload of supporting evidence
- File versioning
- Secure storage
- Document access control
- Large file support

13. Scalability and Performance Requirements

The system must support:

- Multiple banks and financial institutions
- Large volumes of disputes
- High availability
- Real-time processing
- Concurrent users.
- Real-Time Dashboard (a centralized portal for dispute officers to view the lifecycle of a claim).

14. Deployment Model

The system may be deployed as:

- On-premise within Central Bank infrastructure
- Private cloud
- Hybrid architecture

The solution must support:

- High availability
- Disaster recovery
- Data backup
- Business continuity.

14/4/2026

Presented by: Electronic Banking Services Company (EBS)

NIPS Request for Proposal (RFP): Fraud Management Requirements

1. Project Overview

The NIPS project requires a robust, high-performance **Fraud Risk Management (FRM)** solution capable of providing instant security for real-time payments. The selected vendor must demonstrate the ability to balance ultra-low latency with sophisticated detection capabilities.

2. Technical Scope of Requirements

2.1 Real-Time Monitoring & Intervention

The solution must provide immediate detection and prevention capabilities. Please detail your capabilities regarding:

- **Latency Caps:** Define your guaranteed processing time in milliseconds (ms) for a single transaction scoring event.
- **Automated Blocking:** Describe the mechanism for real-time automated transaction rejection based on risk scores.
- **Velocity Checks:** Detail how the system monitors transaction frequency and volume across the entire network to identify "smurfing" or rapid-fire fraud attacks.

2.2 Advanced Analytics & Machine Learning

- Describe your use of supervised and unsupervised ML models.
- Detail how the system handles adaptive learning to recognize emerging fraud patterns without manual intervention.

2.3 Case Management and Investigation

The vendor must provide a comprehensive UI for fraud analysts including:

- **Alert Prioritization:** Intelligent queuing based on risk severity.
- **Workflow Automation:** Ability to automate repetitive investigative steps.
- **Audit Trails:** Full, immutable logging of all analyst actions and system decisions for regulatory compliance.

2.4 Integration and Interoperability

- **API-First Architecture:** Detail your RESTful API capabilities for seamless integration into the NIPS ecosystem.
- **ISO-20022 Compliance:** Confirm native support for ISO-20022 messaging standards.

- **Blacklist Sharing:** Ability to ingest and contribute to shared industry blacklists in real-time.

3. High-Availability & Geo-Redundancy

As a critical national infrastructure component, the Fraud Engine must support geographically separated sites.

No.	Requirement	Vendor Specification/Response
1	Architectural Configuration	Describe support for Active-Active vs. Active-Passive setups.
2	Data Synchronization	Detail how low-latency sync is maintained between sites to avoid "double-spending" or "stale-rule" issues.
3	Distributed Rule Management	How are rule updates pushed across all sites simultaneously?
4	DR & Failover	Detail the RTO/RPO for automatic failover and how state persistence is maintained during a site crash.
5	Compliance & Sovereignty	Outline how the solution ensures data residency compliance and support cross-site auditing

4. Key Requirements Checklist (Response Required)

Vendors must complete the following table indicating "Met," "Partially Met," or "Not Met," along with comments.

No.	Category	Requirement
1	Throughput	Ability to handle peak loads (e.g., 5,000+ transactions per second).
2	Rule Engine	User-friendly "No-Code" interface for analysts to create new rules on the fly.
3	Reporting	Automated SAR (Suspicious Activity Report) generation for the Central Bank.
4	Security	Role-based access control (RBAC) and data encryption at rest and in transit.

5. Submission Instructions

Please ensure all responses address the Instant Security nature of this project. Responses should be quantitative where possible (e.g., specific millisecond counts, throughput figures, and recovery times).