**KARANDAAZ PAKISTAN**

**Request for Proposal**

 **Financial Switch & Card Management Platform, implementation and support services**

**Issue Date: 29-January-2018**

**Deadline for Questions: 05-February-2018**

**Deadline for Karandaaz Pakistan Responses: 08-February-2018**

**Deadline for submission for proposals: 19-February-2018**

**Bid Opening: 20-February-2018**

**KARANDAAZ PAKISTAN**

**Request for Proposal**

**SECTION 1. LETTER OF INVITATION**

RFP No. 38

29-January-2018, Islamabad

1. The purpose of this RFP is to solicit bids from companies interested in providing a Financial Switch and Card Management Platform, along with related implementation and support services for CDNS (Central Directorate of National Savings). The RFP is designed to assess whether organizations are able to provide the services required, and through a competitive and fair assessment, select a winning vendor for implementation and a 3 to 5 year support contract.
2. Karandaaz Pakistan invites sealed proposals from interested and eligible organizations. More details on the Services required are provided in the Terms of Reference (Section 4 of RFP).
3. The company will be selected under open competitive procedures, in accordance with the procurement policies and procedures of Karandaaz Pakistan.
4. The full RFP is available at [**karandaaz.com.pk**](http://www.karandaaz.com.pk/).
5. Both financial and technical proposals must be submitted before 05:00 PM Pakistan Standard Time on 19th February 2018. Offerors must prepare four hard copies of the technical proposal and one hard copy of the cost proposals, and submit in separate **sealed** envelopes to the attention of ‘The Procurement Department’ 1-E, Ali Plaza, D Chowk, Mezzanine Floor, Nazimuddin Road, Blue Area, Islamabad .

The financial proposal and technical proposals (password protected) should also be sent in separate e-mails to the following email address: **procurement@karandaaz.com.pk** with the subject line: Responding to RFP for “TECHNICAL proposal - Financial Switch and Card Management platform, implementation and support services” and “FINANCIAL proposal - Financial Switch and Card Management platform, implementation and support services”. The password for the financial proposal shall be communicated upon request on the day the proposal is opened.

Yours sincerely,

**The Procurement Department**

Karandaaz Pakistan

**SECTION 2. INSTRUCTIONS TO FIRMS**

* 1. **General**
1. **Scope of Proposal**

Karandaaz Pakistan issues this Request for Proposal (RFP) for the following product & services:

“Financial Switch and Card Management Platform, with implementation and support services, for the Central Directorate of National Savings (CDNS)”

Throughout this RFP:

1. The term “in writing” means communicated in written form (e.g., by mail, e-mail, fax)
2. “Day” means calendar day
3. **Fraud and Corruption**

Firms shall comply with Karandaaz Pakistan’s policy regarding fraud and corruption given in Section 3 of the RFP.

1. **Eligibility**

Karandaaz Pakistan may specify certain minimum qualification criteria in the Terms of Reference e.g. minimum years of relevant experience.

The firm has an obligation to disclose to Karandaaz Pakistan any situation of actual or potential conflict that impacts its capacity to serve Karandaaz Pakistan’s best interests. Failure to disclose such situations may lead to the disqualification of the firm or the termination of its Contract. Karandaaz Pakistan’s policy with regard to conflict of interest is given Section 3 of the RFP.

Firms shall provide such evidence of their continued eligibility satisfactory to Karandaaz Pakistan, upon request.

1. **One Proposal Per Firm**

Each firm shall submit only one proposal, either individually or as a partner in a joint venture. A firm that submits or participates in more than one proposal shall cause all the proposals with the firm’s participation to be disqualified. However, this does not limit the participation of subcontractors and individual experts in more than one proposal.

1. **Cost of Preparation of Proposal**

The firm shall bear all costs associated with the preparation and submission of its proposal. Karandaaz Pakistan shall not be responsible or liable for those costs, regardless of the conduct or outcome of the bidding process.

* 1. **Request for Proposal**
1. **Contents of the RFP**

The RFP includes the documents listed below and any Addendum issued in pursuant to point 8 of this section ‘Amendment of RFP’.

Section 1 – Letter of Invitation

Section 2 – Instructions to firms

Section 3 – Procurement Policy – vendor conduct

Section 4 – Terms of Reference

Annexure A – Proposal Submission Form

1. **Clarification of RFP**

All questions and/or clarifications regarding this RFP must be submitted via email to Procurement@karandaaz.com.pk no later than 5:00PM local time on 05th February 2018. All correspondence and/or inquiries regarding this solicitation must reference the RFP number.  No phone calls or in-person inquiries will be entertained; all questions and inquiries must be in writing

Questions and requests for clarification—and the responses thereto—will be circulated to all RFP recipients who have indicated an interest in bidding by 5:00PM on 08th February 2018.

Only the written answers will be considered official and carry weight in the RFP process and subsequent evaluation. Any verbal information received from a Karandaaz employee or other entity should not be considered as an official response to any questions regarding this RFP.

1. **Amendment of RFP**

At any time prior to the deadline for submission of bids, Karandaaz Pakistan may amend the RFP by issuing an Addendum.

Any Addendum issued shall be part of the RFP and will be communicated via the Karandaaz Pakistan website. Firms are advised to monitor the site for updates.

To give prospective firms reasonable time in which to take an Addendum into account in preparing their bids, Karandaaz Pakistan may, at its discretion, extend the deadline for the submission of bids, pursuant to point 17 ‘Deadline for Submission of Proposals’ of this section.

* 1. **Preparation and Submission of Proposals**
1. **Language of proposal**

All documents relating to the proposal shall be written in the English language.

1. **Documents Comprising the Proposal**

The documents and the required information mentioned below must be provided with the respective technical and financial proposals.

1. **Technical Proposal**

**TECHNICAL PROPOSAL CHECKLIST**

|  |  |  |
| --- | --- | --- |
| **Sr. No** | **Required Documents** | **Checkbox** |
| 1 | Name, address and contact information of the company | ☐ |
| 23 | Website of the companyNumber and location of all offices (local and international) | ☐☐ |
| 4 | Year of incorporation or registration, and details of registration | ☐ |
| 5 | Tax registration number (if applicable) | ☐ |
| 6 | Letter of participation for request for proposal | ☐ |
| 7 | Client references (minimum 3, of which at least 2 local references) | ☐ |
| 8 | Brief of completed and on-going projects (local and international) | ☐ |
| 9 | Organogram of project team – List of staff with brief bios | ☐ |
| 10 | Management team – List of staff with brief bios | ☐ |
| 11 | Audited financial statement of last three years | ☐ |
| 1213 | Details of local partner including track-record, in case vendor does not have local presenceTechnical proposal includes the following | ☐ |
|  | a. Proposed implementation of work scope | ☐ |
|  | b. Software architecture and design | ☐ |
|  | c. Change management process | ☐ |
|  | d. Managed service methodology for CMS and financial switch | ☐ |
|  | e. Infrastructure Requirement with BOQ | ☐ |
|  | f. Security and stress testing methodology | ☐ |
| 14 | Filled compliance matrix | ☐ |
| 15 | Company has clearly defined in its introduction in the proposal of the lead vendor and whether the company is the principal Owner, authorized Partner or part of a consortium member | ☐ |
| 1617 | The firm’s strategy and performance in innovationAny other document attached, please specify | ☐☐ |

1. **Financial Proposal**

 **FINANCIAL PROPOSAL TO BE SUBMITED SEPERATELY IN A SEALED ENVELOPE**

**FINANCIAL PROPOSAL CHECKLIST**

|  |  |  |
| --- | --- | --- |
| **Sr. No** | **Required Financials** | **Checkbox** |
| 1 | Cost of licenses for the core application | ☐ |
| 2 | List of hardware and system software in the form of separate BOQ with itemized costs | ☐ |
| 3 | Cost of professional services for implementation of the scope of work. | ☐ |
| 4 | Cost of managed services / operations for a period of 3 and 5 years. | ☐ |
| 5 | In case of separate costs of annual software support for principal supplier and annual operational support for local partner, both need to be included and a split to be shared of their respective costs for a period of 3 and 5 years. | ☐ |
| 6 | Change management charging methodology with charge-out rates providing man-day rate for development of new functionality/features, development of reports, configuration and integrations, etc. | ☐ |
| 7 | Draft of the annual maintenance contract | ☐ |





TCO for 3 to 5 Years shall be submitted in the above format. However, Order duration shall be as per Karandaaz Pakistan’s discretion. All prices must be inclusive of all applicable taxes. These taxes shall be mentioned separately.

1. **Currencies of Bid and Payment**

Firms may express the price only in PKR. Payment will be made in PKR only in the bidder’s account maintained in Pakistan.

1. **Proposal Validity**

Proposal shall remain valid for one hundred and eighty (180) days after the proposal submission deadline date established by Karandaaz Pakistan. A proposal valid for a shorter period shall be rejected as non-responsive.

In exceptional circumstances, prior to the expiration of the proposal validity period, Karandaaz Pakistan may request all firms who submitted their proposals to extend the period of validity of their proposal for a specified additional period. The request and the responses shall be made in writing. If the firm agrees to extend the validity of its proposal, it shall be done without any change in the original proposal and with the confirmation of the availability of the key experts. The firm has the right to refuse to extend the validity of its proposal in which case such proposal will not be further evaluated.

If any of the Key Experts become unavailable for the extended validity period, the firm shall provide a written adequate justification and evidence satisfactory to the Client together with the substitution request. In such case, a replacement Key Expert shall have equal or better qualifications and experience than those of the originally proposed Key Expert. The technical evaluation score, however, will remain to be based on the evaluation of the CV of the original Key Expert.

 If the firm fails to provide a replacement Key Expert with equal or better qualifications, or if the provided reasons for the replacement or justification are unacceptable to the Client, such Proposal will be rejected.

1. **Proposal Security**

In this procurement, a proposal security is not required.

1. **Alternative Proposals**

Alternative proposals shall not be considered.

1. **Format, Signing, and Submission of Proposals of Proposal**

The firm shall prepare and email a scanned copy of the documents comprising the Proposal as described in point 10 on official company letterhead. Each document shall be signed by a person duly authorized to sign on behalf of the firm. All pages of the proposal shall be initialed by the person or persons signing the proposal.

 Both financial and technical proposals must be submitted before 05:00 PM Pakistan Standard Time on February 19, 2018. Offerors must prepare four hard copies of the technical proposal and one hard copy of the cost proposals, and submit in separate **sealed** envelopes to the attention of ‘The Procurement Department’ 1-E, Ali Plaza, D Chowk, Mezzanine Floor, Nazimudin Road, Blue Area, Islamabad.

The financial proposal and technical proposals (password protected) should also be sent in separate e-mails to the following email address: **procurement@karandaaz.com.pk** with the subject line: Responding to RFP for “TECHNICAL proposal - Financial Switch and Card Management platform, implementation and support services” and “FINANCIAL proposal - Financial Switch and Card Management platform, implementation and support services”. The password for the financial proposal shall be communicated upon request on the day the proposal is opened.

 The Proposal shall contain no alterations or additions, except those to comply with instructions issued by Karandaaz Pakistan, or as necessary to correct errors made by the firm, in which case such corrections shall be initialled by the person or persons signing the Proposal.

1. **Deadline for Submission of Proposals**

Proposals must be received by Karandaaz Pakistan no later than 05:00 PM Pakistan Standard Time on **February 19, 2018.**

Karandaaz Pakistan may extend the deadline for submission of proposals by issuing an amendment in accordance with point 8 ‘Amendment of RFP’, in which case all rights and obligations of Karandaaz Pakistan and the firms previously subject to the original deadline shall then be subject to the new deadline.

1. **Late Proposals**

Any Proposal received late by Karandaaz Pakistan will be considered only at the discretion of the evaluation team.

1. **Withdrawal, Substitution, and Modification of Proposals**

Firms may withdraw, substitute or modify their proposals by giving notice in writing before the deadline for submission of proposals prescribed in point 16 ‘Deadline for Submission of Proposal’ of this section.

Each firm’s withdrawal, substitution or modification notice shall be prepared, sealed, marked, and delivered in accordance with point 15 ‘Format, Signing, and Submission of Proposals of Proposal’, with the subject line as: Responding to RFP for “Financial Switch and Card Management Platform, implementation and support services - “WITHDRAWAL,” SUBSTITUTION” or “MODIFICATION” as appropriate. No Proposal may be substituted or modified after the deadline for submission of proposals.

* 1. **Proposal Opening and Evaluation**
1. **Proposal Opening**

Karandaaz Pakistan shall open the proposals, including modifications made pursuant to point 18, on the business day following the deadline, as per point 16.

1. **Confidentiality**

Information relating to the examination, evaluation, comparison, and post-qualification of proposals, and recommendation of contract award, shall not be disclosed to firms or any other persons not officially concerned with such process until publication of the contract award. Any effort by a firm to influence Karandaaz Pakistan in the examination, evaluation, comparison, and post-qualification of the Proposals or contract award decisions may result in the rejection of its Bid. Notwithstanding the above, from the time of proposal opening to the time of contract award, if any firm wishes to contact Karandaaz Pakistan on any matter related to the bidding process, it should do so in writing at the address indicated in point 7 ‘Clarification of RFP’.

1. **Clarification of Bids**

To assist in the examination, evaluation, and comparison of proposals, Karandaaz Pakistan may, at its discretion, ask any firm for clarification of the firm’s proposal. The request for clarification and the response shall be in writing, but no change in the price or substance of the proposal shall be sought, offered, or permitted except as required to confirm the correction of arithmetic errors discovered by Karandaaz Pakistan in the evaluation of the proposals in accordance with point 25 ‘Correction of Errors’.

1. **Preliminary Examination of Proposals**

Prior to the detailed evaluation of proposals, Karandaaz Pakistan shall first review each Proposal and check the power of attorney or any other form demonstrating that the representative has been duly authorized to sign the proposal, initialization of all pages, etc.

1. **Determination of Firm’s Eligibility and Qualifications**

Karandaaz Pakistan shall determine whether the firm meets the eligibility and qualification requirements of the bidding documents. Firms failing to comply with the eligibility criteria indicated in point 3 ‘Eligibility’ shall be disqualified.

Further, Karandaaz Pakistan shall determine whether the proposal is substantially responsive to the requirements of the bidding documents.

Karandaaz Pakistan’s determination of a proposal’s responsiveness is to be based on the contents of the proposal itself. A substantially responsive proposal is one, which conforms to all the terms, conditions, and specifications of the RFP, without material deviation or reservation. A material deviation or reservation is one (a) which affects in any substantial way the scope, quality, or performance of the service; (b) which limits in any substantial way, inconsistent with the RFP, Karandaaz Pakistan’s rights or firm’s obligations under the contract; or (c) whose rectification would affect unfairly the competitive position of other firms presenting substantially responsive Proposals.

1. **Evaluation of Technical Proposal**

The procurement model that will be used is “Two Stage – Two Envelope bidding procedure”. The bid shall comprise of two separate envelopes – Technical and Financial. In Stage One, only the Technical Proposal shall be opened and reviewed.

As part of the Technical Evaluation, the suppliers will be invited for the presentation sessions. The presentations will be scheduled between 22nd February 2018 and 1st March 2018, and will be advised by 20th February 2018. Based on this, the technical evaluation will be finalized.

Minimum qualifying criteria for a firm to be considered for stage 2, i.e. financial evaluation, is to meet the minimum score in the technical evaluation. Technical Proposal has a weightage of 80% of total score. The vendors falling below 50% (40 Score) in the technical proposal will not be considered for financial evaluation.

 Technical Proposal

 The technical proposal will be evaluated on the following criteria:

* **Experience and profile of the company**
* **Scope of Work and approach**
* **Firm’s strategy and performance in innovation**
* **Compliance of non-functional requirements**
* **Financial strength, as reflected in audited financial statements of last three years**
1. **Correction of Errors**

Proposals determined to be substantially responsive shall be checked by Karandaaz Pakistan for any arithmetic errors. Errors shall be corrected by Karandaaz Pakistan as follows:

 Where there is a discrepancy between the amounts in figures and in words, the amount in words shall govern.

 The amount stated in the proposal shall be adjusted by Karandaaz Pakistan in accordance with the above procedure for the correction of errors and, with the concurrence of the firm, shall be considered as binding upon the firm. If the firm does not accept the corrected amount, the proposal shall be rejected.

1. **Currency for Price Evaluation**

For evaluation and comparison purposes, Karandaaz Pakistan shall convert all proposal prices expressed in US Dollars into an equivalent amount in PKR, using the selling exchange rates established by the State Bank of Pakistan on the date of proposal opening specified in point 19 ‘Proposal Opening’.

1. **Evaluation of Proposal Price and Ranking**

In Stage Two, the ranking from the technical evaluation will be shared with the Procurement team. Procurement will open the financial proposal of the technically qualified bidder(s).

Financial proposals submitted will be evaluated according to price reasonableness determination under full and open competition and known market conditions. Final scoring shall be done after negotiations with technically qualified suppliers.

Financial Proposal has a weightage of 20% of total score.

Evaluation of the financial proposal will consider, but will not be limited to, the following:

* Cost reasonableness;
* Consistency with the technical proposal;

20 points will be awarded to the lowest responsive bidder while rest of the bids will be allocated points according to following formula:

* Points of a Bidder = (P1/ P2) \* 20

Where:

* P1= Price of Lowest Responsive Bidder
* P2= Price of the Bidder
	1. **Award of Contract**
1. **Award Criteria**

Subject to 31 below, Karandaaz Pakistan shall award the contract to the firm whose proposal has been determined to be substantially responsive to the RFP and which has the highest score, provided that such firm has been determined to be eligible in accordance with point 3.

The weightage of the technical evaluation will be 80% while the financial will have a 20% weightage in the total score

1. **Karandaaz Pakistan’s right to accept any proposal and to reject any or all proposals**

Notwithstanding point 28 above, Karandaaz Pakistan reserves the right to accept or reject any proposal, and to cancel the bidding process and reject all bids, at any time prior to the award of contract, without thereby incurring any liability to the affected firm or firms or any obligation to inform the affected firm or firms of the grounds for Karandaaz Pakistan’s action.

1. **Notification of Award and Signing of Agreement**

The firm whose Proposal has been accepted shall be notified of the award by Karandaaz Pakistan prior to expiration of the proposal validity period in a written letter. This letter (hereinafter and in the contract called the “Letter of Acceptance”) shall state the sum that Karandaaz Pakistan shall pay the contractor in consideration of the services as prescribed by the contract.

The Agreement shall incorporate all agreements between Karandaaz Pakistan and the successful firm. It shall be signed by Karandaaz Pakistan and CDNS (Central Directorate of National Savings) and sent to the successful firm, within seven (7) days following the Letter of Acceptance’s date. Within seven (7) days of receipt, the successful firm shall sign the Form of Agreement and deliver it to Karandaaz Pakistan.

Karandaaz Pakistan will also promptly notify in writing each unsuccessful firm. After publication of the award, unsuccessful firms may request in writing to Karandaaz Pakistan seeking explanations of the grounds on which their Proposals were not selected. Also, Karandaaz Pakistan shall entertain a complaint from any firm that claims to have suffered or that may suffer, loss or injury due to a breach of a duty by the company in the conduct of this bidding process. Such requests shall be addressed and delivered in writing to:

Karandaaz Pakistan

Attention: Chief Executive Officer

Re: “Financial Switch and Card Management platform, implementation and support services”

1 E, Ali Plaza, Nazimuddin Road, D-Chowk, Islamabad

Any requests via email seeking this explanation will not be answered.

**SECTION 3. PROCUREMENT POLICY – VENDOR CONDUCT**

1. **Corrupt or fraudulent practices**

Bidders, suppliers, contractors and their agents (whether declared or not), sub-contractors, sub-consultants, firms or suppliers, and any personnel thereof, shall observe the highest standard of ethics during the procurement and execution of contracts.

Karandaaz Pakistan shall not award contract if it is determined that the bidder, or any of its personnel, or its agents, or its sub-consultants, sub-contractors, firms, suppliers and/or their employees, has, directly or indirectly, engaged in corrupt, fraudulent, collusive, coercive, or obstructive practices in competing for the contract in question. As part of bidding/ solicitation documents, Karandaaz Pakistan will seek declaration of ‘Non-collusive non-corrupt practices’ from each bidder. Format for such declaration is prescribed in section 3 of the standard bidding document. In pursuance of this policy, following terms are defined as follows:

1. “Corrupt practice” is the offering, giving, receiving, or soliciting, directly or indirectly, of anything of value to influence improperly the actions of another party;
2. “Fraudulent practice” is any act or omission, including a misrepresentation, that knowingly or recklessly misleads, or attempts to mislead, a party to obtain a financial or other benefit or to avoid an obligation;
3. “Collusive practice” is an arrangement between two or more parties designed to achieve an improper purpose, including to influence improperly the actions of another party;
4. “Coercive practice” is impairing or harming, or threatening to impair or harm, directly or indirectly, any party or the property of the party to influence improperly the actions of a party;
5. “Obstructive practice” is deliberately destroying, falsifying, altering, or concealing of evidence material to the investigation or making false statements to investigators in order to materially impede investigation into allegations of a corrupt, fraudulent, coercive or collusive practice; and/or threatening, harassing or intimidating any party to prevent it from disclosing its knowledge of matters relevant to the investigation or from pursuing the investigation.
6. **Avoidance of conflict of interest**

Any firm participating in the procurement process should disclose any actual or perceived conflict of interest situation/condition. Any firm found to have a conflict of interest shall be ineligible for award of a contract.

A firm shall be considered to have a conflict of interest in a procurement process if:

1. Such firm is providing goods, works, or non-consulting services resulting from or directly related to consulting services for the preparation or implementation of a project that it provided or were provided by any affiliate that directly or indirectly controls, is controlled by, or is under common control with that firm; or
2. Such firm submits more than one bid, either individually or as a joint venture partner in another bid, except for permitted alternative bids. This will result in the disqualification of all bids in which the bidder is involved. However, this does not limit the inclusion of a firm as a sub-contractor in more than one bid. Only for certain types of procurement, the participation of a bidder as a sub-contractor in another bid may be permitted subject to the company’s no objection and as allowed by the standard bidding documents applicable to such types of procurement; or
3. Such firm (including its personnel) has a close business or family relationship with a professional staff of the company who: (i) are directly or indirectly involved in the preparation of the bidding documents or specifications of the contract, and/or the bid evaluation process of such contract; or (ii) would be involved in the implementation or supervision of such contract unless the conflict stemming from such relationship has been resolved in a manner acceptable to the company throughout the procurement process and execution of the contract; or
4. Such firm does not comply with any other conflict of interest situation as specified in the standard bidding documents relevant to the specific procurement process.
5. **Duty of care**

The supplier in performance of services for Karandaaz Pakistan shall exercise duty of care. Duty of care holds the supplier responsible for the safety and well-being of its personnel and any third party affected by its activities.

**SECTION 4. TERMS OF REFERENCE**

**Thematic Area**:

**Project Title:** Financial switch and Card Management Platform, along with related implementation and support services for CDNS (Central Directorate of National Savings)

**Expected Start Date:**March, 2018

**Task Manager:                  Director DFS**

**About Karandaaz Pakistan**

KARANDAAZ PAKISTAN, a private company established in August 2014, promotes access to finance for small businesses through a commercially directed investment platform, and financial inclusion for individuals by employing technology enabled digital solutions. The Company has financial and institutional support from leading international development finance institutions; principally the United Kingdom Department for International Development (UKAid) and the Bill & Melinda Gates Foundation. The Consultative Group to Assist the Poor (CGAP), a member of the World Bank Group, provides technical support to Karandaaz Pakistan.

Karandaaz Pakistan has three core work streams:

* **Corporate Investment and Credit (CIC)** focuses on providing credit and capital to high impact small and medium-size businesses, and business models that have potential to generate sustainable employment and offer attractive risk-adjusted financial returns.
* **Digital Financial Services (DFS)** focuses on expanding the poor’s access to digital financial services in Pakistan by working across the ecosystem of local actors – policy-makers, regulators, government departments, businesses, researchers and academics. The DFS Unit facilitates digitization of government and other payment streams, encourages experimentation with businesses, and provides support to innovative DFS start-ups.
* **Knowledge Management and Communications** focuses developing and communicating credible data to inform the core themes of the Company, including DFS innovation, women’s empowerment and youth employment.

This work will fall under the Digital Financial Services department.

 **About the Project**

**National Savings,** as it stands today, is one of the primeval institutions in the country with a legacy of more than 140 years that came into existence with the promulgation of Government Savings Bank Act in 1873. In September 1960, it was decided to rejuvenate the structure of CDNS by declaring the status of an Attached Department of the Ministry of Finance with the powers to formulate policies and execute various**National Savings Schemes (NSS).**

The year 1972 came as a turning point in the long journey of National Savings whereby the organization was made responsible for all policy matters and execution of various NSS. **CDNS (Central Directorate of National Savings)** has not only remained successful in promoting financial savings in the economy but has also generated requisite funds for the Government to finance the budgetary deficit and infrastructure projects. As a custodian of the nation’s savings, today the National Savings is the largest investment and financial institution in Pakistan with a portfolio of over **Rs. 3.4 trillion** and more than**7 million** valued investors served through a large network of**376 branches** nationwide, controlled by **12 Regional Directorates** of National Savings (RDNS).

As part of digitalization effort of CDNS, Karandaaz Pakistan is supporting in implementing digital channels for the customers of CDNS. The financial switch enables CDNS to build a layer of digital channels for the customers of CDNS, to perform transactions and other services at their convenience from channels of their choice. The objective is for CDNS’ customers to be able to use their savings account to pay bills or even withdraw cash through debit cards from more than 12,000 ATMs across Pakistan.

For CDNS, it is a significant opportunity to improve public service delivery by digitalizing a range of investment products, savings account and even prize bonds ensuring digitalized profit or prize money payouts to its customers in their accounts, which could be utilized through a range of channels other than visiting a national savings center.

**Target Audience**

The effort is to facilitate existing CDNS customers and also provide an opportunity to the unbanked population to access and benefit from investment products of CDNS through digital channels. The digital channels would introduce savings product to the unbanked population in remote areas which could not be catered through the 376 National savings centers across Pakistan.

**Scope of Work**

**Provision of software licenses, implementation and managed services support for the following**

* Financial switch
* Card management system (including Card Management Suite that should be an end-to-end card life-cycle management solution for debit cards)

**Implementation Services**

1. **High level objectives:**

Following are the main objectives for implementation of the financial switch:

1. **Implementation of financial switch**
	1. General requirements for the financial switch
	2. Multiples interface protocols for interconnectivity interface (ISO 8583, Webservices, SOAP / REST APIs etc.) with ADC channels and consolidated generic interface with the CDNS Main Application (Vendors to list all supported protocols and details of consolidated generic interface with Main Application)
	3. Customizable reporting & business rules
	4. PCI complaint – PCI DSS / PA DSS certification/compliance
	5. Web based \ monitoring dashboards
	6. Connections and integrations of the financial switch
2. Integration with multiple channels and host application for transaction routing for systems internal to CDNS including but not limited to:
	1. CDNS main application (This serves the purpose of CDNS’ core banking application)
	2. Internet transactional channel
	3. Mobile application
	4. Card management system
	5. CRM application
3. Integrate with external ATM networks and payments switch like 1Link and PSO/PSP licensed entities against their standard specifications
4. Integrate with NADRA for biometric verification and customer information against CNIC against NADRA standard API packages for branchless and branch banking
5. Integration with multiple external organizations like bank / microfinance institution for funds transfer, agent based services such as cash in, cash out, instrument purchase and bilateral transactions
	1. Routing of card-based transactions
6. ATM transactions (cash withdrawal / balance enquiry / mini-statement) from bank account through local ATM acquiring network (1Link)
7. ATM transactions (cash withdrawal / balance enquiry) from bank account through international ATM network (International card scheme)
8. POS transactions with card schemes (local or international)
9. E-Commerce
	1. Routing of non-card based transactions
10. Utility bill payment
11. Mobile top-ups
12. Merchant payments
	1. Funds transfer
13. Within a single branch in CDNS main application
14. Third party funds transfer transactions within CDNS branches
15. External fund transfer (to and from other network) such as IBFT (via 1Link or direct integration with one or many financial institutions on standard protocols)
	1. Other transaction
16. Encashment of CDNS instruments
17. Transfer of CDNS instruments
18. Purchase of CDNS instruments
	1. Transactional authorizations

Financial switch should be able to consolidate transaction authorization from multiple systems such as CDNS main application and/or card management system, etc.

* 1. Financial requirements
1. Real-time settlement entries
2. Auto reversals
3. **Implementation of card management system**
	1. General requirements for the card management system
4. CMS should provide the option to maintain customer relationship based on unique identifier such as CNIC of each customer
5. Restrict the customers to have one active card per saving account.
6. Define transaction types and assign to different products
7. 4-eye principle for authorization of various card production activities
8. Open Application Programming Interface – API for interconnectivity to any institution
9. Easy Product Management Wizard must be available
10. Complete card life cycle management should be available
11. Customer 360-degree view (Cardholder) of any customer issued a card
12. System must be capable to issue both MagStrip and EMV cards
13. Capability to issue Domestic scheme card for transactions within Pakistan
14. Bulk upload (Import / export user data)
15. Reporting of card related activities
16. Integration to the host through financial switch on industry standard protocol (ISO 8583, Webservice SOAP / REST API)
17. Define card expiry of various products
	1. Processing of card-based transactions
18. ATM transactions (cash withdrawal / balance enquiry / mini-statement) from Bank Account through local ATM acquiring network (1Link)
19. ATM transactions (cash withdrawal / balance enquiry) from Bank Account through international ATM network (international card scheme)
20. POS transactions with card schemes (local or international)
	1. Card issuance / Batch Management Processing
		1. CMS to be able to support and schedule multiple events during the day, creating, generation and processing of card issuance requests
		2. Mechanism to get the card request file in a standard file format from a specified location and to process card creation request
		3. Generate card numbers against the card requests and sharing them in return file for the systems to be updated with the customer profile
		4. Card embossing file to be generated against each batch processed
		5. Stationary file generation
		6. Availability of different batch statuses indicating its process stage
	2. Limits
		1. Predefined transactional limits (self-authorization)
		2. Daily account limits
		3. Relationship limits
	3. Card expiry and renewal management
21. System should have the option to generate card renewal batch against cards expiring in 30 days (end of month)
22. Managing card status of existing and renewed card - upon processing of a renewal batch, new cards should be issued in an inactive state against the card batch while the existing cards (about to reach expiry) are active
23. Managing renewed cards - to be issued once card renewal fee is successfully collected (fee deduction transaction confirmation received from main application / core banking)
24. Managing card status - upon activation of the renewed card, old card should automatically be marked as expired
25. Managing expiry of old cards - on reaching expiry in case the new card is still not active, the expired card should automatically be blocked, marked expired
	1. PIN management
26. The card management system should be able to perform PIN authentication for transactional processing
27. The card management system should be able to reset PIN and provide for API for CRM to be able to send a real-time request
28. The card management system to provide option to generate card PIN real-time against input in an integrated model (via the IVR, mobile app, etc)
29. The card management should provide a configurable option to allow the number of re-tries (default set to 3) before which the PIN is exhausted. In case of exhaustion of invalid PIN attempts the card, status should be automatically changed to “warm”
30. It should provide an option to generate random card PINs against card batches for PIN Mailer printing
31. Transaction PIN encryption through industry standard hardware (Hardware Security Module (HSM) – 3DES)
	1. Card transactional authorization
32. The card management system should validate the PIN for the card based transactions where the PIN is mandatory in the integrations specifications
33. The card management system should be able to validate the card status before card transaction authorization
	1. Fee management
34. Dynamic Fee Management Wizard with Flat, percentage, min. max and range based fees
35. The card management system should be able to initiate periodic based fee deduction for renewal
36. The card management system should be able to deduct transactional fees (if any)
	1. Card status management
37. Offer various card status management both, from within the CMS native interface as well as in integration with an external application (CRM)
38. Card statuses required
39. Inactive (New / Fresh) Status
40. Active (Cold)
41. Temporary Block (Warm / Suspend)
42. Permanent Block (Hot)
43. Expired cards (Hot/Expired/Closed)
	1. Activity reports
44. The system should be able to provide reports for the following activities on daily basis for the operations of debit card
45. Customizable reports
46. Reconciliation and settlement
47. Card issuance batch processing
48. Card generation
49. Card embossing
50. Card fee deduction
51. Card expiry
52. Card renewal
53. Card pin generation
54. Card transactional report (transaction-wise)
55. Card status change
56. User activity
	1. User role management
57. CMS should provide UI option to create customizable roles and assign functions/screens. Initial roles will be assigned as part of the CMS deployment before go-live
58. CMS should provide UI option to create users and assign one or more role to a single user. Initial users will be created as part of the CMS deployment before go-live
59. **Testing requirements for both the systems**
	1. Penetration testing / vulnerability assessment from independent security testing vendor should be part of the proposal
	2. Proposal should include three options for the security testing vendor to choose from, which are approved by NTISB
	3. Benchmarking reports for stress testing, load testing, performance testing report with TPS and FTPS certification for the financial switch and card management system
60. **Support and services**
	1. Managed Services for the financial switch and card management system
61. Patch management and its support to the client for the financial switch and card management system is part of the managed services
62. The support to be provided in security management of the financial switch and card management system through tools and interfaces to the client is part of the managed services required in the solution
63. Proposal should include the support to be provided in application performance management for the financial switch and card management system through monitoring tools and interfaces to the client
64. 24x7 support of the financial switch and card management system is part of the service scope of the proposal
	1. Change Management
65. Complete process of change management to be included
66. Effort estimation methodology of change management has been provided, including the separate man-day rates with different skill classification of possible activities such as development activities, operational activities, configuration activities etc.

**Compliance Matrix**

**Definitions:**

Mandatory requirements: The mandatory requirements need to be complied by the vendors bidding for the RFP. Non-compliance to these requirements may lead to disqualification at the sole discretion of Karandaaz

FC: Fully Compliant means that platform fully meets the requirement out of the box

PC: Partially Compliant means that some customization would be required to meet the requirement

NC: Non-Compliant means that this requirement cannot be met by the platform

|  |  |  |
| --- | --- | --- |
| **Mandatory Requirements** | **Compliant (Yes / No)** | **Vendor Remarks / Comments** |
| Vendor has technical capabilities on the proposed components to provide support services / assistance during active period of Contract from the date of signing of operations, maintenance and support services to cover SLA period |   |   |
| Certificate/Letter from the principal to confirm that the local vendor is a licensed implementation partner of application offered. (If the principal is participating themselves in the RFP then this is not needed) |   |   |
| Maintenance and Professional Services fee by Principal / Manufacturer (if any) are part of the cost of services in the proposal |   |   |
| Representation through partner or local office in any one of major city in Pakistan (Karachi, Lahore, Islamabad) |   |   |
| Card management system and the financial switch comply with all existing regulatory and statutory guidelines including but not limited to the SBP card payment security guidelines issued in 2016, SBP enterprise technology governance & risk management framework for financial institutions and card scheme guidelines for EMV compliance |   |   |
| The platforms must have been implemented by the implementation vendor (principal or SI partner as in this proposal) successfully in at least 2 instances with customers having more than 200,000 active card holders.  |   |   |
| PCI Compliant – PCI DSS / PA DSS Certification/Compliance. Vendor to mention clearly if compliant or certified |   |   |
| The audited financial statement or auditor statement does not have concerns on the going concern of the vendor |   |   |
| Affidavit for not being blacklisted in any Public Tender/RFP |   |   |
| **Functional Requirements** | **Compliance (Fully =2, Partially=1, Not compliant=0)** | **Vendor Remarks / Comments** |
| **Financial Switch** |
| **General Requirement for Financial switch** |
| Multiple interface protocols for interconnectivity interface (ISO 8583, Webservices, SOAP / REST APIs etc.) with ADC channels and consolidated interface with the CDNS Main Application (Vendors to list all supported protocols and details of consolidated interface with Main Application) |   |   |
| Customizable Reporting & Business rules |   |   |
| Web Based \ Monitoring Dashboards |   |   |
| **Connections for a financial switch** |
| Integration with multiple channels and host application for transaction routing for systems internal to CDNS including but not limited to CDNS main application, Card management system, Mobile Application, Internet banking and CRM |   |   |
| Integration with multiple external organizations like bank / microfinance institution for funds transfer, agent based services such as cash in, cash out, instrument purchase and bilateral transactions |   |   |
| Integrate with external ATM networks and payments switch like 1Link and PSO/PSP licensed entities against their standard specifications |   |   |
| Integrate with NADRA for biometric verification and customer information against CNIC against NADRA standard API packages for branchless and branch banking |   |   |
| Financial Switch must have successful experience of integrations with: |
| 1-     Domestic ATM Switch (1Link) |   |   |
| 2-    Domestic Bill Payment Aggregators (1Link, Telenor Bank, Nadra) |   |   |
| 3-   Existing Integration specification types supported with multiple Core Banking Solutions (Mention the names of all the current integrations specifications supported in the proposed solution) |   |   |
| System should have active / active implementation on Application and database level for supporting the DR Site. |   |   |
| **Routing of card based transactions** |
| ATM transactions (Cash Withdrawal / Balance Inquiry / Mini Statement) from Bank Account through local ATM acquiring network(1link) |   |   |
| ATM transactions (cash Withdrawal / Balance Inquiry) from Bank Account through international ATM network (International card scheme) |   |   |
| POS Transactions with card schemes (local or international) |   |   |
| **Routing of Non-card based transaction** |
| **Non-financial transaction** |
| Balance inquiry |   |   |
| Mini-statement |   |   |
| Account opening through digital interfaces |   |   |
| Service/ CRM calls for customer profile management |   |   |
| **Financial transactions** |
| Utility bill payment |   |   |
| Mobile Top ups |   |   |
| Merchant payments |   |   |
| **Funds transfer** |
| Within a single branch in CDNS main application and also third-party funds transfer transactions from one branch to the other within CDNS main application |   |   |
| External fund transfer (to and from other network) such as IBFT (via 1Link or Direct integration with CDNS on standard protocols)  |   |   |
| **Other transaction** |
| Encashment of CDNS instruments |   |   |
| Transfer of CDNS instruments |   |   |
| Purchase of CDNS instruments |   |   |
| Any other transactions supported by the system to be listed |   |   |
| **Transactional Authorizations** |
| Financial switch should be able to manage transaction authorization from multiple systems such as CDNS main application and/or card management system etc. |   |   |
| **Financial Requirements** |
| Settlement entries |   |   |
| Auto reversal (scenario based management of auto reversal) |   |   |
| **Transactional reports** |
| The system should be able to provide the reports for all activities and transactions on daily basis for the transactions and the proposal to include the list of the reports provided by the system along with formats for these reports |   |   |
| **Card Management System** |
| **General Requirement for CMS** |
| CMS should provide the option to maintain customer relationship based on unique identifier such as CNIC of each customer in sync with the CDNS main application |   |   |
| Restrict the customers to have one active card on a single customer profile/product/account |   |   |
| Allow issuance of one or more cards for different products against single unique identifier such as CNIC  |   |   |
| Define transaction types and assign to different products |   |   |
| 4-eye principle for authorization of back-end manual card production activities |   |   |
| Open Application Programming Interface – API for interconnectivity to any institution.  |   |   |
| Easy Product Management Wizard must be available |   |   |
| Complete card life cycle management of card should be available. |   |   |
| Customer 360 View (Cardholder) of any customer issued a card |   |   |
| System must be capable to issue both MagStrip and EMV Cards. The cost to include both implementation |   |   |
| Capability to issue Domestic scheme card for transactions within Pakistan. |  |  |
| Bulk Upload (Import / Export user data) |   |   |
| Connected to host through financial switch on industry standard protocol (ISO 8583, Webservice SOAP / REST API). |   |   |
| Define different card expiry of different products |   |   |
| **Processing of card based transactions** |
| ATM transactions (Cash Withdrawal / Balance Inquiry / Mini Statement) from Bank Account through local ATM acquiring network(1link) |   |   |
| ATM transactions (cash Withdrawal / Balance Inquiry) from Bank Account through international ATM network (International card scheme) |   |   |
| POS Transactions with card schemes (local or international) |   |   |
| E-commerce transaction |  |  |
| **Card issuance / Batch Management Processing** |
| CMS to be able to support and schedule multiple events during the day creating, generation and processing of card issuance requests |   |   |
| Mechanism to get the card request file in a standard encrypted file format from a specified location and to process card creation request. (proposal to mention with encryption method) |   |   |
| Generate card numbers against the card requests and sharing them in encrypted return file for the systems to be updated with the customer profile. (proposal to mention with encryption method) |   |   |
| Card embossing file to be generated against each batch processed |   |   |
| Stationery file generation |   |   |
| Availability of different batch statuses indicating its process stage |   |   |
| **Defining limits on card management system** |
| Card management system is able to set predefined transactional limits (self-authorization) |   |   |
| Card management system is able to set daily account limits |   |   |
| Card management system is able to set limits based on relationship/product type |   |   |
| **Card Expiry & Renewal Management** |
| System should be option to generate card renewal batch against cards expiring in 30 days (end of month). |   |   |
| **Managing card status of existing and renewed card** - Upon processing of a renewal batch new cards should be issued in an inactive state against the card batch while the existing cards (about to reach expiry) are active. |   |   |
| **Managing renewed cards** - to be issued once card renewal fee set (if any) is successfully collected (fee deduction transaction confirmation received from core banking) |   |   |
| **Managing card status -** Upon activation of the renewed card, old card should automatically be marked expired |   |   |
| **Managing expiry of old cards -** On reaching expiry incase the new card is still not active, the expired card should automatically be blocked, marked expired and the new card remains in a fresh |   |   |
| **PIN management** |
| The card management system should be able to perform PIN authentication for transactional processing |   |   |
| The card management system should be able to reset PIN and provide for API for CRM to be able to send a real-time request |   |   |
| The card management system to provide option to generate card PIN real-time against input in an integrated model (via the IVR, mobile app, etc.) |   |   |
| The card management should provide a configurable to allow the number of re-tries (default set to 3) allowed before which the PIN is exhausted. In case of exhaustion of invalid PIN attempts the card, status should be automatically changed to Warm |   |   |
| It should provide an option to generate random card PINs against card batches for PIN Mailer printing |   |   |
| Transaction PIN encryption through industry standard hardware (Hardware Security Module (HSM) – 3DES) |   |   |
| **Card Transactional Authorization** |
| The card management system should be able to validate the PIN for the card based transactions where the PIN is mandatory in the integrations specifications |   |   |
| The card management system should be able to validate the card status before card transaction authorization |   |   |
| **Fee Management** |
| Dynamic Fee Management Wizard with Flat, percentage, min. max and range based fees. |   |   |
| The card management system should be able to initiate periodic based fee deduction for renewal and integrate with core to automatically deduct the charges in real time |   |   |
| The card management system should be able to deduct transactional fees (if any)  |   |   |
| **Card Status Management** |
| Offer various card state management both from within the CMS native interface as well as in integration with an external application (CRM) |   |   |
| Card statuses required: |
| o   Inactive (New / Fresh) Status |   |   |
| o    Active (Cold) |   |   |
| o   Temporary Block (Warm / Suspend) |   |   |
| o    Permanent Block (Hot) |   |   |
| o    Expired cards (Hot/Expired/Closed) |   |   |
| **Activity Reports** |
| The system should be able to provide the reports for the activities listed on daily basis for the operations of debit card and the proposal to include any additional reports provided by the system along with formats for all reports |   |   |
| Customizable reports for reconciliation and settlement |
| -          Card issuance batch processing |   |   |
| -          Card generation  |   |   |
| -          Card embossing  |   |   |
| -          Card fee deduction |   |   |
| -          Card expiry |   |   |
| -          Card renewal |   |   |
| -          Card pin generation |   |   |
| Card transactional report (transaction wise) |   |   |
| Card status change |   |   |
| Reconciliation files |   |   |
| User activity |   |   |
| **User Role Management** |
| CMS should provide UI option to create customizable roles and assign functions/screens. Initial roles will be assigned as part of the CMS deployment before go-live |   |   |
| CMS should provide UI option to create users and assign one or more role to a single user. Initial users will be created as part of the CMS deployment before go-live |   |   |
| **General Requirements (Subsequent sections are applicable to both the card management and financial switch)** | **Compliance (Fully =2, Partially=1, Not compliant=0)** | **Vendor Remarks / Comments** |
| Core switching system and card management system to be hardware platform independent. Should not be a particular hardware brand specific. Bidders could propose alternatives; however, the application will be hosted at the site specified by the client |   |   |
| Core switching system and card management system to be compatible with virtualized environment |   |   |
| Core switching system and card management system should support multiple databases. Recommendations can be provided but should not be limitations |   |   |
| Security policies, user permissions, user grouping and hierarchies to be managed centrally over the entire system |   |   |
| Creation of generic profiles for users, roles, transactions, limits, permissions etc. and the ability to do bulk assignments rather than individual one-by-one assignments |   |   |
| Proposal should include three options for the security testing vendor to choose from for penetration testing / vulnerability assessment of the deployed systems. The bidder will include cost of PT/VA from these vendors in the proposal. The client will decide which vendor to choose from the three proposed choices |   |   |
| Enter system to be manageable through a browser based interface. |   |   |
| Solution to provide REST Based Open API(s) that enable end users to create additional services or to add additional delivery channels without requiring vendor's service |   |   |
| Vendor must have local representation and support in Pakistan |   |   |
| Wide variety of HSM Module to be supported for proposed solution. Names of all HSM modules to be mentioned. |   |   |
| Multi HSM Support should also be available. |   |   |
| Vendor must provide product roadmap of both the systems for assessment |   |   |
| Bidirectional support for file adds and updates, card bulk request etc. [Bulk Card printing and activation] |   |   |
| System to have feature to allow activation of cards through various mechanisms such as IVR / Call Center or Internet, mobile app etc. |   |   |
| System should support OTP based PIN generation without having a dependency on IVR |   |   |
| System has integration with an Analysis tool that has reporting wizard and allows analysis on large amount of data |   |   |
| System must have following alert management support:·   Personalization alerts.·   Transaction alerts·   Network Monitoring alerts·   Push Alerts |   |   |
| Acceptance testing Test Pack to be provided  |   |   |
| **Testing requirements** |
| Stress testing report of the systems (Financial switch and card management system) with maximum TPS and FTPS certification. System must support highest level of transaction processing with minimum requirement of more than 500 transactions per second which should be supported by formal benchmark report. |   |   |
| Penetration testing / Vulnerability assessment from independent security testing vendor is part of the proposal |   |   |
| Proposal includes three options to choose from for the security testing vendor approved by NTISB |   |   |
| User acceptance testing support should be included in the proposal |   |   |
| Testing environment will be setup by the vendor |   |   |
| **Roles & Responsibilities** |
| Systems should be configured to provide a dedicated Access Control Administration [ACA] function that is only used to perform account management. |   |   |
| Systems should provide the Security Administration role that is only used to perform security duties. [e.g. event log auditing, incident reviewing]. |   |   |
| Accesses to system resources must be based on job function, where rights are granted on a need to have basis. |   |   |
| The system must enforce the two people [dual control] rule and/or segregation of duties for manual/offline transactions/activities. Proposal should include the list of such activities and transactions |   |   |
| Authentication credentials for this application must be generated securely, issued following formal procedures and distributed through secure channels. Credentials must be generated with best industry practices using secure algorithms. Mention the details of the algorithms and the standards complied.  |   |   |
| Dual control must be implemented in the ACA process for rights that give access to critical systems or functions. User creation rights, credential management. [Maker / Checker] |   |   |
| Every assigned ID must be linked to a department to ensure that a responsible manager can be identified. This is just a departmental hierarchy |   |   |
| The application’s security administration should be capable of reporting on an application’s user rights |   |   |
| The application’s security administration should be capable of generating application user status [e.g. active, inactive] |   |   |
| Scripts to be provided to perform several conversion-test cycles before actually going live with new system batch processing of request on the test portal so the testing results could be obtained promptly. |   |   |
| Generic accounts with access to the application must have an auditable activity trail for all access to these accounts. |   |   |
| **Access Control** |
| The application's passwords must be encrypted during storage and transport. |   |   |
| The application's passwords must be checked against unwanted password values [e.g. all the same characters]. |   |   |
| The application's passwords must NEVER be displayed, logged or printed in plain text. |   |   |
| The application's passwords must be confirmed by the user after a password change. |   |   |
| The application must enforce password change at first usage of the initial password. |   |   |
| The application must enforce a change of passwords that have not been changed for a specified number of days. The number of days must be configurable. |   |   |
| The application must disable initial passwords that have not been used within specified duration of creation. The specified duration must be configurable. |   |   |
| The application must disable any user id that has not been used for a specific number of days. The number of days must be configurable |   |   |
| The application should enforce passwords that are not the same as any of the previous predefined number of passwords used. The number of passwords should be configurable. |   |   |
| When the login is performed by systems or applications which use either a system or application ID, the minimum authentication mechanism is a password. |   |   |
| Passwords should not be stored in plain text. |   |   |
| If passwords are stored encrypted, there must be a process to prevent a single person from knowing the entire password, for example by the implementation of a system generated password or by a password composed from dual control input. |   |   |
| There must be a process to change a password when it is suspected of being compromised. (Regular enforced password change is not required). |   |   |
| System/application IDs must be disabled for interactive logon, for example, disabled for use on consoles. Like saved password in browser cookies / multiple instance should not be enable on single user |   |   |
| All access to the system must be based upon a valid ID. |   |   |
| Access must be limited to authenticated IDs in accordance with their granted access rights. The access control system must check the access request against the rights of the application as defined in the access control administration. |   |   |
| Access rights must be grouped in roles aligned with business functions to enable effective management. |   |   |
| After access, the date and time of the last successful login should be reported to the user. |   |   |
| Details of unsuccessful login attempts since the last successful login should be displayed to the user. |   |   |
| There must be a session lock provided either by the system/application or through workstation time-out that can be either manually activated by the user or automatically activated after a pre-defined time of session inactivity. The predefined time to be configurable. |   |   |
| The reason for failed authentication must not be communicated by the system to the user, to prevent giving clues to the user about which aspect of the login process failed. |   |   |
| After a maximum predefined number of failed login attempts there must be either a time delay enforced before a new attempt is permitted or a temporary block of the user ID that can be automatically de-blocked. The predefined number needs to be configurable |   |   |
| After a maximum predefined number of failed login attempts the user ID must be blocked where after it must be manually de-blocked by security administration or a self-service facility. Predefined number of attempts are to be configurable in the system. |   |   |
| All actions on the systems must be linked to a user ID which uniquely identifies an individual user. |   |   |
| **Card Account Management** |
| Solution must be able to link all type of payment instruments with a card like Accounts |   |   |
| Solution to provide statistical information about customer, account and transaction instrument. |   |   |
| Solution to provide comprehensive report about customers relationships |   |   |
| System to support issuance of cards through file based requests |   |   |
| Individual renewal in exceptional situations, replacements and reissue of lost and stolen cards through batch files and online or GUI capture. |   |   |
| Manual blocking of the cards for renewal, reissue and replacement. |   |   |
| **Security** |
| Application password related to an individual [i.e. not with terminal] |   |   |
| Application user password to be stored and transmitted in encrypted format. |   |   |
| Password to change with manageable frequency. |   |   |
| Application interface to deactivate after non-use of specific time. |   |   |
| Important input to the system to require up to two levels of authority. Also mention the list of activities where 4 eye principle is implemented. |   |   |
| Application logs & saves each individual activity. |   |   |
| System to produce reports on user actions as log-on attempts, data removal addition and update. |   |   |
| Security policies, user permissions, user grouping and hierarchies are managed centrally over the entire system. |   |   |
| **Management Information System Reports** |
| Realtime system interface and reports for all transactions with segregation of approved transactions and declined transactions with the reasons for decline. |   |   |
| Realtime system interface and reports for the card holder activities. |   |   |
| User operational activity and attempts made to modify and account etc. [with account logging along with date and time] |   |   |
| Certify that all statutory and regulatory reports are available and will be provided in future at no additional cost |   |   |
| System has ability to run scheduled reports weekly, monthly, quarterly, annually and as required [scheduled]. |   |   |
| Reporting interface to be web based so that branches can produce their required reports themselves. |
| Mechanism in the system exists for the report/activity data extraction to an external system or to be emailed to authorized ids. |   |   |
| **Backup & Recovery** |
| Successful experience of at least two critical advance disaster recovery site implementation for proposed solution.  |   |   |
| Detail of Backup solution to be explained |   |   |
| Detail of backup Support Mechanism to be explained. |   |   |
| Disaster Recovery [DR] solution to be explained. |   |   |
| Auditing for Transactions and Configuration change to be explained. |   |   |
| System to provide transaction logs to assist in case of recovery of data. |   |   |
| Single site single server contingency support without high availability systems to be confirmed and explained. |   |   |
| Total system recovery as a backup within 2 hours. |   |   |
| System to have procedure to place historical data on archiving system. Procedure to be explained. |   |   |
| Procedure on automation of data protection of media management to be provided. |   |   |
| Strategy to access to archived data in a time not exceeding than 3 hours to be defined If stand-alone than restoration should be in 3 hours. |   |   |
| A successful and full Disaster Recovery [DR] test of all technology components of the system must take place on an annual basis or whenever a major change in the organization occurs. |   |   |
| The technology recovery procedures for this system must be embedded in or referred to from the business continuity plan that applies to the business area involved. |   |   |
| Application backup / restore data must be stored in a protected and access-controlled site that is separate from the Production site, for a period of 7 years [or as defined by local regulatory requirements]. |   |   |
| The system should support clustering or failover to ensure high availability. |   |   |
| **Software Architecture** |
| Describe proposed solution support for configuration management. |   |   |
| System has to be fault tolerant by design for application process. |   |   |
| Integration protocols ISO 8583, Webservices (SOAP/REST), File, FTP, SFTP, SMTP, APIs |   |   |
| Detail of system Architecture for complete proposed solution has been provided. |   |   |
| Solution to integrate Switching, Routing, Card Management, Monitoring and Authorization. |   |   |
| Integrated solution between different channels |   |   |
| All remote administration tools used for connectivity between the applications should be proven software. |   |   |
| The application security should NOT rely upon user configurable security parameters on the client side at any time. |   |   |
| System should check for the data integrity & confirmation before proceeding for input and output. |   |   |
| A real-time alerting mechanism must ensure that immediate action is taken in the event of partial (temporary) unavailability or disruption of services while the application is up. |   |   |
| Access to directories and files must be secured by proper authorization settings that provide only the minimal access required for correct operation. |   |   |
| The overall architecture must utilize a corporate Network Time Source (NTS) (unless regulations stipulate the use of another time source). |   |   |
| The system should be able to automatically synchronize to the time source |   |   |
| The list of open source softwares utilized in the system should be mentioned. |   |   |
| The application's architecture must NOT contain any direct external-internal connections (including dial-in via a modem) or any connection from a wireless network device |   |   |
| There must be appropriate segregation, both technically and procedurally, between the development/maintenance, acceptance testing and production environments. |   |   |
| The system must ensure data confidentiality between the host server (application or web servers) and the client desktop irrespective of whether the data is traversing within the organization or through a 3rd party network. |   |   |
| Vendor to provide support to ensure that the information processing and storage facilities that support these information systems must be securely housed, with protection from unauthorized physical access and environmental hazards. |   |   |
| The system must securely log all relevant application events, including but not limited to user id, field changed, time stamps, new value and old value to provide a reliable audit trail. |   |   |
| The system must record the associated user IDs and date and time of each application event/transaction. |   |   |
| The system should record the type of “event” (e.g. verification, authorization) and its status (i.e. success/failure) |   |   |
| The system must strongly secure audit logs (e.g. read-only to authorized personnel). |   |   |
| Security events, such as an exceptional number of unsuccessful access attempts to the application, must trigger an alert, either on the host or on an intrusion detection system. |   |   |
| All log files must be retained for a period that is appropriate to local legislation and audit requirements.  |   |   |
| Confidentiality critical data must be encrypted when transported over an external or wireless connection or when stored on mobile devices. |   |   |
| The vendor must define the minimum key length used for symmetric algorithms in the response. |   |   |
| The vendor must define the minimum key length used for asymmetric algorithms in the response. |   |   |
| The vendor must define the minimum length for hash values in the response. |   |   |
| The application must use the following relevant algorithms for its cryptographic functions: Symmetric algorithms (Triple DES, AES, or RC4), Asymmetric algorithms (RSA or DSA), and Hash functions (SHA-1). Please specify the cryptographic functions used for both the symmetric and asymmetric algorithms |   |   |
| When using RSA to protect the secrecy of cryptographic keys, the minimum key length must be defined by the vendor in the response. |   |   |
| When origin authentication must have the property of non-repudiation, an asymmetric algorithm must be used. |   |   |
| The cryptographic hardware must be tamper-resistant, for example certified against FIPS 140-2 or validated by a recognized institution, to prevent the disclosure of secret keys. |   |   |
| The cryptographic hardware should be tamper-evident to provide indications that someone has attempted to attack the hardware. |   |   |
| The cryptographic hardware must contain functions that cannot be used separately, or in combination, that could compromise private or secret keys. |   |   |
| When encryption and authentication of information are both required, the information must be authenticated prior to being encrypted. |   |   |
| Critical key management operations must only be allowed to be carried out by specifically authorized personnel. |   |   |
| The key management procedures must describe when and why they are executed, the key management actions, sequence of actions, tools to be used, people involved, responsibilities, controls and logging of actions. |   |   |
| Key management procedures must be formally agreed and accepted by the party responsible for the operations. |   |   |
| Records of relevant key management activities must be maintained for at least seven years. |   |   |
| The application's secret key(s) should only be permitted to be used for one cryptographic function. |   |   |
| A process must exist so that secret or private keys which have been compromised (or are suspected of being compromised) are revoked as soon as possible or in any case within one week. |   |   |
| Keys which have been revoked or become invalid must no longer be used. |   |   |
| If the application requires the use of digital certificates, the certificate(s) must have been acquired and/or approved from a bank approved Certificate Authority. |   |   |
| Have email and / Or SMS alerts modules. |   |   |
| **Authorization & Routing** |
| Offer flexible routing mechanism to support a variety of acquirer requirements. All options to be mentioned. |   |   |
| System allows acquirer side authorization  |   |   |
| System allows issuer side authorization |   |   |
| System to Support flexible & user configurable authorization processing. |   |   |
| System to Operate as a full authorization engine supporting negative, positive, online, offline, stand-in, etc. |   |   |
| **Interfaces** |
| Integrations with Bank directly or via 1Link |   |   |
| Integration with CDNS main application through single uniform interface consolidating the requirements of multiple channels |   |   |
| Extract interfaces in solutions is to provide a near-real time transaction data of switch for supporting various reporting, monitoring and decision support systems, to be mentioned. |   |   |
| **Monitoring & Management** |
| Support for graphical based analysis and browser based interface for monitoring to be provided. |   |   |
| Network Management/Monitoring module to be provided. |   |   |
| Proposed system to support hierarchical display by regions, groups, owners, devices, host etc. |   |   |
| Support Monitoring of Host interface state and External Switch interface state. |   |   |
| System must support sign-on, sign-off, key exchange capability and provide details. |   |   |
| **Fraud Detection** |
| System to Capable to generate MIS and reports to gauge the efficiency of rules, analysis and overall effectiveness |   |   |
| System should have built-in transaction blocking module capable to configure rule directly from UI block transactions on real-time basis without any downtime for rule to apply. Vendor should state capability of integration with Fraud Detection Systems or whether the Fraud Detection System is available within the solution proposed. |   |   |
| System must provide Source and Destination channel configuration along with Incoming data elements configuration to block any transaction.  |   |   |
| **Advance modules** |
| System must be modular, new modules can be plugged without any major development and requirement of additional hardware. |   |   |
| System should be capable to offer ATM Management, POS and Merchant management as a module |   |   |
| System should be capable to offer Bill Payment system as a module |   |   |
| System must be capable to offer ticket management for issues reporting as a module. |   |   |
| System must be able to provide customization layer using which National Savings can build interfaces and transactions by themselves. |   |   |
| System must provide built-in CRM modules with following Financial and Non-Financial features: |
| ·         Card Block/Unblock |   |   |
| ·         Customer Demographic update |   |   |
| ·         PIN generation and validation |   |   |
| ·         Funds transfer |   |   |
| ·         Bill Payments |   |   |
| ·         Transaction Inquiry |   |   |
| **Managed services and change management** |
| **Requirements for managed services** | **Compliance (Fully =2, Partially=1, Not compliant=0)** | **Vendor Remarks / Comments** |
| 24x7 support of the financial switch and card management system is part of the service scope of the proposal |   |   |
| The following services are part of the proposal  |
| Proposal includes the support to be provided in application performance management for the financial switch and card management system through monitoring tools and interfaces to the client |   |   |
| Proposal includes the support to be provided in security management of the financial switch and card management system through tools and interfaces to the client |   |   |
| Patch management and its support to the client for the financial switch and card management system is part of the managed services  |   |   |
| Release management methodology has been shared with clear steps, roles and responsibility for every patch |  |  |
| Level 1, 2 and 3 supports for financial switch and card management services is part of the managed services**Level-1 support**: Basic level support for ensuring the system are up running. Escalation of issues which are not due to any apparent reasons such as power outage, netwok disconnection etc.**Level-2 support:** Intermediate level support which could involve configurational changes, investigating issues and running routine protocols to fix an issue that is identified**Level-3 support:** Issues which are not fixed through level 2 support are escalated to level-3 where developer level support may be needed and some changes needs to be made in the application. |   |   |
| Definition of services and their service levels with classification of service and incident management process and reporting along with TATs are part of the proposal. The vendor should also comment on penalties in event of breach of agreed service levels  |   |   |
| Process for change management is documented in the proposal |   |   |
| Effort estimation methodology of change management has been provided including the manned day rates with different skill classification of possible activities  |   |   |
| **Firm's strategy and performance in innovation** |
| **Strategy and innovation** | **Compliance (Fully =2, Partially=1, Not compliant=0)** | **Vendor Remarks / Comments** |
| Vendor has submitted the strategy relevant to the card management system and financial switch platforms |   |   |
| Vendor strategy is in line with market needs |   |   |
| The vendor has been able to define innovative ideas relevant to the card management system and financial switch |   |   |
| The innovation addresses practical problems that exist in the market |   |   |
| The innovation is unique and did not already exist as a solution in the market |   |   |
| The innovation been implemented successfully in the market |   |   |
| The company has a separate research and development budget and staff that works on innovation |   |   |
| The company has demonstrated a new line of revenue added in the last 2 years |   |   |

**Ownership/Control of Work and Product/Publication**

The ownership of all copyright and other intellectual property rights in respect of any data compilations, research, spreadsheets, graphs, reports, diagrams, designs, work products, software, or any other documents, developed in connection with this Contract will exclusively vest in and remain with Karandaaz which shall have all proprietary rights therein, notwithstanding that the Contractor or its employees may be the author of the intellectual property. All documents relating to the intellectual property or otherwise connected with this Contract, the services, or duties must be returned or delivered to Karandaaz at the time of the expiration or termination of this Contract. The Contractor agrees not to publish or make use of any of the intellectual property, or documents relating thereto, without the prior written approval of Karandaaz, and where approval is granted, without proper attribution to Karandaaz.

**Task Manager/Reporting**

**Reporting Line:                                Director DFS**

**Location:                                             Islamabad**

**Duration:                                             from 42 to 66 months (6 months implementation / 3-5 years post implementation Services), order duration shall be subject to Karandaaz discretion**

**Project:                                                Financial Switch and Card Management Platform, along with related implementation and support services**

**Payment**

Karandaaz will pay the Contractor’s invoice within thirty (30) business days after a) Karandaaz’ approval of the Contractor’s Deliverables, or b) Karandaaz’ receipt of the Contractor’s invoice, whichever is later.  Payment will be made in PKR or USD, as agreed, to the account specified in the Contractor’s invoice.

**PROPOSAL SUBMISSION FORM**

Dear Sir/Madam,

Having examined the Solicitation Documents, the receipt of which is hereby duly acknowledged, “THE FIRM NAME” undersigned, offer to provide consulting for “INSERT REFERENCE NUMBER” to Karandaaz Pakistan in accordance with the Price Schedule attached herewith and made part of this proposal. “THE FIRM NAME” undertake, if our proposal is accepted, to commence and complete delivery of all services specified in the contract within the time frame stipulated.

“THE FIRM NAME” agree to abide by this proposal for a period of 90 days from date fixed for opening of proposal in the invitation for proposal, and it shall remain binding upon us and may be accepted at any time before the expiration of that period.

We understand that you are not bound to accept any proposal you may receive.

Dated: this——day of ——-2018