

Ref No. E-SLTE JKB/T&D/DCMS/2026/1639

Dated 05-02-2026



**Special Limited Tender Enquiry (SLTE-RFP/SLTE) for selection of
Service Provider for ATM/Debit Switch
& Debit Card Management System (DCMS) on hosted model.**

Issued By	Dated: 05-02-2026
J&K Bank Technology & Development, 5 th Floor, Corporate Headquarters MA Road, Srinagar Phone No :+91- 9419042744 email id - mir.arif@jkmail.com	E-SLTE JKB/T&D/DCMS/2026/1639

SCHEDULE OF RFP/SLTE

S.No	Description	Details
1	RFP/SLTE Reference No.	E-SLTE JKB/T&D/DCMS/2026/1639
2	Date of Issue of RFP/SLTE	05-02-2026
3	RFP/SLTE Description	Selection of Service Provider for ATM/Debit Switch & Debit Card Management System (DCMS) on hosted model.
4	Issuer of the RFP/SLTE- Department	Technology & Development Department
5	Bank's Communication Details	J&K Bank Technology & Development, 5 th Floor, Corporate Headquarters, MA Road, Srinagar Mr Mir Arif Phone No :+91- 9419042744 email id – mir.arif@jkbmail.com
6	RFP/SLTE Application Fee (Non - Refundable)	Rs. 10,000/- (Rupees Ten Thousand Only)
7	Earnest Money Deposit (EMD)(Refundable)	Rs. 1,50,00,000/- (Rupees One Crore Fifty Lac Only)
8	Performance Bank Guarantee	5% of total contract Value
9	Bid Document Availability including changes/amendments, if any to be issued	RFP/SLTE may be downloaded from https://jkbank.abcprocure.com from: February 06, 2026, 16.00 Hrs. to February 20, 2026 17.00 Hrs.
10	Time & Date of Submission of RFP/SLTE Bid	February 06, 2026, 16.00 Hrs
11	Last Date of Submission of RFP/SLTE Bid	February 20, 2026 17.00 Hrs
12	Pre Bid Meeting Pre Bid Queries reply Date	February 11, 2026 17.00 Hrs February 16, 2026 17.00 Hrs
13	Submission of	As prescribed in Bank's online tender portal

	online Bids	https://jkbank.abcprocure.com										
14	Date and time of opening of technical bid	To be notified separately										
15	Corrigendum	All the Corrigendum will be uploaded on online tender portal https://jkbank.abcprocure.com only										
16	For E-Tender Related Queries	<p>Service Provider: M/s. E-procurement Technologies Limited (Auction Tiger) , B-705, Wall Street- II, Opp. Orient Club, Ellis Bridge, Near Gujarat College, Ahmedabad- 380006, Gujarat</p> <table border="1"> <thead> <tr> <th>Sr No</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Sandhya Vekariya - 6352631968</td> </tr> <tr> <td>2</td> <td>Suraj Gupta - 6352632310</td> </tr> <tr> <td>3</td> <td>Ijlalaehmad Pathan - 6352631902</td> </tr> <tr> <td>4</td> <td>Imran Sodagar - 9328931942</td> </tr> </tbody> </table>	Sr No	Name	1	Sandhya Vekariya - 6352631968	2	Suraj Gupta - 6352632310	3	Ijlalaehmad Pathan - 6352631902	4	Imran Sodagar - 9328931942
Sr No	Name											
1	Sandhya Vekariya - 6352631968											
2	Suraj Gupta - 6352632310											
3	Ijlalaehmad Pathan - 6352631902											
4	Imran Sodagar - 9328931942											

DISCLAIMER

The information contained in this RFP/SLTE document or any information provided subsequently to bidder(s) whether verbally or in documentary form/email by or on behalf of the J&K Bank is provided to the bidder(s) on the terms and conditions set out in this RFP/SLTE document and all other terms and conditions subject to which such information is provided. This RFP/SLTE is neither an agreement nor an offer and is only an invitation by the J&K Bank to the interested parties for submission of bids. The purpose of this RFP/SLTE is to provide the bidder(s) with information to assist the formulation of their proposals. While effort has been made to include all information and requirements of the Bank with respect to the solution requested, this RFP/SLTE does not claim to include all the information each bidder may require. Each bidder should conduct its own investigation and analysis and should check the accuracy, reliability and completeness of the information in this RFP/SLTE and wherever necessary obtain independent advices/clarifications. The Bank makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP/SLTE. The Bank may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP/SLTE. The Bank and its officers, employees, contractors, agents, and advisers disclaim all liability from any loss or damage (whether foreseeable or not) suffered by any person acting on or refraining from acting because of any information including forecasts, statements, estimates, or projections contained in this RFP/SLTE document or conduct ancillary to it whether or not the loss or damage arises in connection with any negligence, omission, default, lack of care or misrepresentation on it.

The Bank also accepts no liability of any nature whether resulting from negligence or otherwise, howsoever caused arising from reliance of any Bidder upon the statements contained in this RFP/SLTE. The Bidder is expected to examine all instructions, forms, terms and specifications in this RFP/SLTE. Failure to furnish all information required under this RFP/SLTE or to submit a Bid not substantially responsive to this RFP/SLTE in all respect will be at the Bidder's risk and may result in rejection of the Bid.

The issue of this RFP/SLTE does not imply that the Bank is bound to select a Bidder or to award the contract to the Selected Bidder, as the case may be, for the Project and the Bank reserves the right to reject all or any of the Bids or Bidders without assigning any reason whatsoever before issuance of purchase order and/or its acceptance thereof by the successful Bidder as defined in Award Criteria and Award of Contract in this RFP/SLTE.

The Bidder shall, by responding to the Bank with a bid/proposal, be deemed to have accepted the terms of this document in totality without any condition whatsoever and accepts the selection and evaluation process mentioned in this RFP/SLTE document. The Bidder ceases to have any option to object against any of these processes at any stage

subsequent to submission of its responses to this RFP/SLTE. All costs and expenses incurred by interested bidders in any way associated with the development, preparation, and submission of responses, including but not limited to the attendance at meetings, discussions, demonstrations, etc. and providing any additional information required by J&K BANK, will be borne entirely and exclusively by the Bidder.

The bidder shall not assign or outsource the works undertaken by them under this RFP/SLTE assignment awarded by the Bank without the written consent of the Bank. The Bidder hereby agrees and undertakes to Indemnify the Bank and keep it indemnified against any losses, damages suffered and claims, action/ suits brought against the Bank on account of any act or omission on part of the Bidder, its agent, representative, employees and sub-contractors in relation to the performance or otherwise of the Services to be provided under the RFP/SLTE. The bidders shall not assign or outsource the works undertaken by them under this RFP/SLTE awarded by the Bank, without the written consent of the Bank.

List of Abbreviations

DC	Data Centre
DR	Disaster Recovery
HA	High Availability
BG	Bank Guarantee
OEM	Original Equipment Manufacturer
PBG	Performance Bank Guarantee
SP	Service Provider
EMD	Earnest Money Deposit
SLA	Service Level Agreement
NDA	Non-Disclosure Agreement
SI	System Integrator
PO	Purchase Order
RFP	Request For Proposal
AMC	Annual Maintenance Contract
NEFT	National Electronic Fund Transfer
BCP	Business Continuity Plan
RPO	Recovery Point Objective
RTO	Recovery Time Objective
NPCI	National Payments Corporation of India
SSO	Single Sign On
IVR	Interactive Voice Response
ACS	Access Control Server
SMS	Short Message Service
API	Application Programming Interface
IAM	Identity and Access Management
SFTP	Secure Fund Transfer Protocol
TPA	Third Party Application

MIS	Management Information System
SOC	Security Operations Center
COFT	Card on File Tokenization
VAPT	Vulnerability Assessment Penetration Testing
DCMS	Debit Card Management System
SIEM	Security Incident Event Management
ITSM	Information Technology Service Management
ICCW	Interoperable Cardless Cash Withdrawal
ICCD	Interoperable Cardless Cash Deposit
ATM	Automated Teller Machine
TCS	Tax Collected at Source
PoS	Point of Sale
EMV	Europay Mastercard Visa
NFC	Near Field Communication
HSM	Hardware Security Module
CVV	Card Verification Value
CVC	Card Verification Code
ARQC	Authorization Request Cryptogram
ARPC	Authorization Response Cryptogram
CRM	Cash Recycler Machine
CDM	Cash Deposit Machine
SSH	Secure Shell
BIN	Bank Identification Number
MAC	Message Authentication Code
SAF	Store and Forward
TLS	Transport Layer Security
KYC	Know Your Customer

PCI DSS	Payment Card Industry-Data Security Standard
RBAC	Role Based Accessed Control
NTP	Network Time Protocol
DAM	Database Activity Monitoring
AML	Anti Money Laundering
RMM	Remote Monitoring and Management

CONTENTS

<u>SECTION A-INTRODUCTION</u>			
1	<u>Brief about Bank</u>	5	<u>Scope of Work</u>
2	<u>Purpose Of RFP/SLTE</u>	6	<u>Location of Work</u>
3	<u>Eligibility Criteria</u>	7	<u>Invitation for Tender Offer</u>
4	<u>Brief Scope of Work</u>	8	<u>Project Delivery Milestones</u>

<u>SECTION B-EVALUATION PROCESS</u>			
1	<u>Stage A-Evaluation of Eligibility</u>	3	<u>Stage C-Evaluation of Commercial Bid</u>
2	<u>Stage B-Evaluation of Technical Bid</u>		

<u>SECTION C-RFP/SLTE SUBMISSION</u>			
1	<u>e-tendering Process</u>	8	<u>Deadline for Submission of Bids</u>
2	<u>Service Provider</u>	9	<u>Bid Validity Period</u>
3	<u>RFP/SLTE Fees</u>	10	<u>Bid Integrity</u>
4	<u>Earnest Money Deposit</u>	11	<u>Cost of Bid Document</u>
5	<u>Performance Bank Guarantee</u>	12	<u>Contents of Bid Document</u>
6	<u>Tender Process</u>	13	<u>Modification and Withdrawal of Bids</u>
7	<u>Bidding Process</u>	14	<u>Payment Terms</u>

<u>SECTION D-GENERAL TERMS & CONDITIONS</u>			
---	--	--	--

1	Standard of Performance	16	No Agency
2	Indemnity	17	Project Risk Management
3	Cancellation of Contract and Compensation	18	Information Security
4	Liquidated Damages	19	No Set-Off, Counter-Claim and Cross Claims
5	Fixed Price	20	Statutory Requirements
6	Right to Audit	21	Bidder Utilization of Know-how
7	Force Majeure	22	Corrupt & Fraudulent Practices
8	Publicity	23	Solicitation of Employees
9	Amendments	24	Proposal Process Management
10	Assignment	25	Confidentiality Provision
11	Applicable law and jurisdictions of court	26	Sub-Contracting
12	Resolution of Disputes and Arbitration clause	27	Award Notification
13	Execution of Service Level Agreement (SLA)/ Non-Disclosure Agreement (NDA)	28	Suspension of Work
14	NO CLAIM Certificate	29	Taxes & Duties
15	Cost And Currency		

SECTION E-Annexures

1	Annexure A-Confirmation of Terms and Conditions	9	Annexure H: Performance Bank Guarantee Format
2	Annexure B: Tender Offer Cover Letter	10	Annexure I: Non-disclosure Agreement (NDA)
3	Annexure C: Details of Bidder	11	Annexure J: Service Level Agreement
4	Annexure D: Compliance to Eligibility Criteria	12	Annexure K: Undertaking

5	<u>Annexure E: Technical Bid Format</u>	13	<u>Annexure L: Know Your Employee</u>
6	<u>Annexure E1: Techno Functional Specification</u>	14	<u>Annexure M: Compliance Network</u>
7	<u>Annexure F: Commercial Bid Format</u>	15	<u>Annexure N: Hosting Assessment Checklist</u>
8	<u>Annexure G: Bank Guarantee Format</u>		

A-INTRODUCTION

1. Brief About Bank:

The Jammu and Kashmir Bank Limited(J&K Bank / Bank) having its Corporate Headquarters at M.A Road Srinagar, J&K -19001 has its presence throughout the country with 1000+ Branches and more than 1500 ATMs. The Bank uses Information Technology in all spheres of its functioning by connecting all its branches and offices through its WAN.J&K Bank functions as a universal Bank in Jammu & Kashmir and as a specialized Bank in the rest of the country. Bank functions as a leading bank in the Union Territories of Jammu & Kashmir and Ladakh and is designated by Reserve Bank of India as its exclusive agent for carrying out banking business for the Government of Jammu & Kashmir and Ladakh. J&K bank caters to banking requirements of various customer segments which includes Business enterprises, employees of government, semi-government and autonomous bodies, farmers, artisans, public sector organizations and corporate clients. The bank also offers a wide range of retail credit products, including home, personal loans, education loan, agriculture, trade credit and consumer lending, a number of unique financial products tailored to the needs of various customer segments. The Bank, incorporated in 1938, is listed on the NSE and the BSE. Further details of Bank including profile, products and services are available on Bank's website at <https://jkb.bank.in/>

2. Purpose of RFP/SLTE

The Jammu and Kashmir Bank Limited intends to onboard a reputed and experienced service provider for providing an end-to-end ATM/Debit Switch, Debit Card Management System (DCMS) and ATM Driving Solution on a hosted model from the bidder's Data Centre (DC) and Disaster Recovery (DR) sites located within India.

The proposed Software Solution/ service must integrate with Bank's existing infrastructure seamlessly wherever required. The solution should be having High availability, Scalability, Extensibility, Industry standard compliance (like ISO 8583,ISO 20022,https,XML,PA-DSS, PCI DSS & SSF) which supports IPv6 as well as IPv4),Fault-Tolerance, Configurability, High-capacity and throughput, Business Continuity Plan (BCP) which support RPO of zero and RTO of near to zero, Integration Capability, Platform independence, Modular structure, New Product-roll out and solution must have an adequate real-time Monitoring capabilities.

The selected service provider must deliver all requisite services for Debit cards issued under various networks, including but not limited to Visa, RuPay, and MasterCard. All associated processes must comply with industry best practices and receive certification from VISA, NPCI, MasterCard, or other relevant authorities wherever mandated. Furthermore, the bidder should possess the capability to issue chip-based contactless cards as well as any emerging card technologies that may develop in the future during the contract period.

The bidder shall also be responsible for the end-to-end migration of the existing setup including all data and for the design, development, hosting, integration, certification, operation, maintenance, monitoring, and support of the complete solution throughout the contract period.

3. Eligibility Criteria

J&K Bank shall scrutinize the Eligibility bid submitted by the bidder. A thorough examination of supporting documents to meet each eligibility criteria (Annexure D) shall be conducted to determine the Eligible bidders. Bidders not complying with the eligibility criteria are liable to be rejected and shall not be considered for Technical Evaluation.

The bidders meeting the Eligibility Criteria as per Annexure D will be considered for technical evaluation. Any credential/supporting detail mentioned in “Annexure D - Compliance to Eligibility Criteria” and not accompanied by relevant proof documents will not be considered for evaluation. All credential letters should be appropriately bound, labelled and segregated in the respective areas. There is no restriction on the number of credentials a bidder can provide.

4. Brief Scope of Work:

The selected Bidder's responsibility will include providing at minimum the below listed areas of the Bank's functions and requirements:

1. Debit Card end-to-end Hosting, Authorization and Operations.
2. Debit card product management, Card Generation & Processing.
3. Issuance of EMV Contactless Cards, virtual cards.
4. Card Issuance through Website, Internet Banking, Mobile banking, FI module etc.
5. End-to-End Transaction Processing.
6. The system should allow integration with Banks Reconciliation system for all network Associations like MasterCard, Rupay and Visa. (Settlement & Reconciliation.)
7. Customer Care Management Helpdesk portal for raising tickets/issues.
8. SDK/API integration with the Banks Mobile Banking application (iOS and Android).
9. SMS, email application alerts and notifications.
10. Dispute & Grievance Redressal System-UDIR.
11. Portal for Branches & Head Office with Integration to Bank's In-House System through SSO.
12. Integration with Bank's Core Banking system, Mobile app, Internet Banking, UPI onboarding, IVR, ACS, Si Hub, Schemes/Associations, WhatsApp, Chatbot, Loyalty Rewards, NACH,RECON, Transaction monitoring, EFRM Solution, Anti money laundering Solution, SMS, Email and others if required by bank or regulators through API/ ISO as required by bank during the agreement period.
13. Interface with MIS/ Analytics Systems/ Data Lake, Digital Marketing Service etc.
14. Interface with Anti Money Laundering System for alerts/report generation etc.

15. Interface with card embossing vendor through API/SFTP.
16. API integrations to communicate with different channels. The API exposed should have the security features as per the industry standard and best practices.
17. Integration with Call Center/ IVR (Both inbound - outbound).
18. Pin set/reset facility on Branch Portal/ATMs/Mbank/Internet banking/IVR.
19. Debit Card Instapin Printing / Green Pin Generation (with API implementation).
20. Connectivity with VISA/MasterCard/NPCI along with certification and related services.
21. Storage of Payment Data norms as set by RBI.
22. Integration with any Third Party Service provider
23. Implementation of Regulatory Requirements.
24. The system should support (COFT) Tokenization functionality along with push provisioning for Rupay MasterCard, VISA, etc.
25. Migration of existing inhouse DCMS to New DCMS (including Data Migration).
26. Data Analytics & MIS Dashboard.
27. Compliance & Information Data Security Measures.
28. Interface with InfoSec system e.g. SIEM/SOC/ITSM solution.
29. Compliance to all RBI, Regulatory, Association and statutory guidelines issued as on date of project implementation and those that shall be issued in future during the contract period.
30. Primary and Disaster Recovery Setup for the solution offered.
31. Integration with POS management system/switch and Onus routing of POS transactions.
32. Integration with FI (Kiosk Solution) and Multi-Functional kiosks.
33. Implementation of Interoperable Card Less Cash withdrawal/Deposit- (ICCW/ICD) along with any middleware requirements.
34. Implementation of Onus Cardless cash withdrawal on ATMs using MBank application.
35. Implementation of UDIR as Issuer and acquirer switch.
36. Remapping of Debit card with different account, linking of multiple accounts with single card and add-on card issuance.

37. Convert Debit Card Purchase to EMI, View EMI Details.
38. Geo tagging of ATM terminals, Multi language support on ATMs.
39. Aadhaar seeding on ATM terminals/ Mobile Banking Registration.
40. Tracking of issued debit card, option to select debit card delivery address (Branch or Registered Address with Bank).
41. Deduction of TCS on International usage of debit cards as per the regulatory guidelines.
42. Deduction of issuance, replacement and usage charges on monthly, quarterly, or yearly basis.
43. Deduction of mark-up charges on foreign currency as required by the Bank.
44. Implementation of TR31 Key Block for migration of Pin encryption from Variant method to key block method.
45. Support for DCC transactions and implementation of the charges on such transactions both issuing and acquiring.
46. Dynamic DES key injection for the ATM's and periodic DES key exchange/key change.
47. Support for MCC based restriction and Merchant specific restriction.
48. Support for MasterCard money send, Visa direct pay transactions, Pre-authorization and refund transactions.
49. Solution must have a load balancing capability.
50. Solution must provide interface to support Micro ATMs, Onus cash credit transactions and Onus POS transactions.
51. Support for cash withdrawal on POS.

5. Scope of Work

The scope of work should be read along with the technical specifications to ensure complete compliance to the scope of work. Successful bidder shall be responsible for end-to-end supply of solution including all modules, components, and services required for making the ATM Driving, ATM/Debit Switch and DCMS fully operational shall be deemed to be part of the scope, even if not explicitly mentioned, and shall be provided at no additional cost and a detailed design document needs to be submitted as part of the bid. The scope of assignment includes but not limited to the following:

A. Architecture:

1. The proposed solution should have an open architecture and a proven mature platform, in production at least for the last 5 years.
2. An Open architecture platform that is flexible and dynamic in nature and should provide APIs to interface with third party applications.
3. The solution should be modular and configurable for ease of change management and maintenance while providing the flexibility of accommodating new generation application.
4. The application architecture should be modular having plug and play capability to eliminate any development/ enhancement limitation and also for load balancing and fault tolerance.
5. The application should be cost-effective, flexible, efficient and dynamic in nature.
6. Ability to quickly and easily develop and implement new products in Payments area.
7. The solution must have adequate real-time monitoring capabilities for application, hardware and transactions.

B. Availability and Scalability:

1. High availability (99.99%) with fault tolerant design.
2. The system should have a RPO of zero and RTO of near to zero.
3. Should provide High Availability at the component level.
4. Should be up and running in DR environment in less than 30 minutes if the primary site fails in case of Active Passive --- Product shall also support active-active feature.
5. Should maintain switch data for at least 15 years in an easily retrievable form.
6. The system should provide horizontal, vertical and linear scalability without any bottleneck and core design changes.
7. The solution should also allow 100% scalability, by adding capacity to the current environment vertically and horizontally.
8. The solution should have provision to enhance key components with minimal changes and minimal disruption and support reusability.
9. The solution should have high throughput capacity and capable of processing 3000 TPS and ability to scale up further without any performance Degradation.

C. Security

1. The solution should support IPv4 and IPv6. Have encryption features such as AES and should be EMV compliant.

2. The Switching solution must have system security functionality in terms of user authentication, 2-factor authentication, access management, audit trails, data back-up, and encryption of data in motion and at rest.
3. Should support message level encryption (software and hardware based) for entire/critical elements in the message such as PIN, Track Data etc.
4. Support for latest security standards and EMV and NFC mandates. - RBI guidelines, NPCI and Association mandates and IT Act requirements to be complied with.
5. Support AES method of PIN verification.
6. Should support PKI based transactions.
7. Support PIN of variable length (in the range (4 to 11)
8. Supports encryption by interfacing with Host Security Module (HSM).
9. CVV/CVC and CVV2/CVC2/ICVV verification using HSM
10. ARQC/ARPC
11. Support for Hardware PIN verification using HSM.
12. Admin Card Generation and Admin card PIN verification for ATMs, CRMs/CDMs and other channels wherever necessary.
13. System should validate transactions allowed for the specific card / card type and linked account.
14. PIN/PAN and PIN/PAD methods of PIN block creation and decryption.
15. PIN offset and VISA PVV verification.
16. Expiry date verification.
17. Check Digit verification.
18. Active/ non active card checking.
19. Support Negative /Positive Bin /Prefix/card list / Hot listed Card.
20. Dynamic generation of terminal session key must be available (key management on AES technology to be made available)
21. Support for Masking the sensitive information partial & full.
22. Dynamic/ Static key exchange with interchanges.
23. User login passwords should be transmitted in encrypted format between client and server to prevent unauthorized access.

24. All the file/data transfers from/to Switch should be in secured manner (SFTP / or higher level of security is preferred).
25. Solution should support secure/encrypted sessions (SSH/ or higher level of security is preferred).
26. The solution should support secured PIN generation and printing (PIN must be in encrypted format from generation till printing).
27. Any other industry standard security requirement - Audit requirements.
28. The system should maintain a record of the users who have accessed the system, resources used and actions performed along with security violations.
29. Solution must have audit logs of each activity on the system.
30. Solution must have audit logs of the transaction throughout the system and each transaction should be uniquely identifiable in the system
31. Solution must provide audit trail for all user activities and provide exception report
32. The mode to access the system should be through passwords/smartcards/ to ensure that only authorized users gain access. Bank's password policy should be configurable on system. User passwords in the Switch (OS Level, DB Level and Application Level) must be encrypted using industry standard encryption algorithms. It must support complex passwords.
33. Solution should provide capabilities to enable biometric, Two Factor Authentication, Secure PIN Based and similar industry standard modes of authentication.
34. Solution should provide front end software for accessing the ATM Switch in a secure manner.

User rights management:

1. Solution should support configurable security controls over specific users or group of users.
2. Data access should be controlled based on individual profiles/roles.
3. Solution should provide for configuring privileges at user level and be able to set preferences based on rules/roles/groups.
4. Solution should provide facility for recording time-in, timeout of user from such device in ATM Switch database. Audit logs should be maintained and made available for the bank in case of need
5. Solution should provide adequate reports for these controls and should provide report/alert on unauthorized Access.

Operational Security:

1. Solution should have maker checker facility.

2. Mode to access the system should be through passwords /2FA to ensure that only authorized users gain access.
3. Solution should provide for configuration of complex passwords using algorithms and special characters.
4. Option to set life for the password in the system for forcing the user to change it once it expires.
5. Password history is to be maintained and validated so that the same password is not continued by the user.
6. The user rights on the system should be definable so that a user can perform only those tasks, which are assigned to them.
7. System must provide levels of security, which will include Add, Modify, Delete, Query etc.
8. It should be capable of maintaining audit logs of each activity on the system. Audit Trail of all changes made in the application, system Parameter, user role change etc. with details like user name, IP address, date and time, module name etc. System should maintain a record of the users who have accessed the system, resources used and actions performed along with security violations if any.
9. Type and nature of security violations should be configurable over & above what has been stated above.
10. Solution should provide and retain audit logs of transactions throughout the system and each transaction should be uniquely identifiable in the system.
11. The solution should be capable to send alerts on changes in system parameters as per configurations

D. Switching Services

1. The Switch Solution shall be PA-DSS, SSF compliant.
2. The Switch Solution shall support both single and dual message interfaces, Support for EMV Chip, Contactless and NCMC cards.
3. The Switch Solution shall support different makes of ATM, Cash Recyclers Cash Depositors that follows to NDC, NDC+ and DDC protocols.
4. The Switch Solution shall be compatible to interface with the Bank's CBS Solution.
5. Real time monitoring of the switching solution.
6. Limit checking based on card, product, on-line limit, BIN and frequency such as daily/ monthly, etc.

7. The Switch Solution shall have system security functionality in terms of user authentication, access management, audit trails, VAPT.
8. Switch Solution Transaction routing based on transactions type, issuer Bank Identification Number (BIN), schemes and services, merchant.
9. The mode to access the system should be through passwords to ensure that only authorized users gain access. User passwords in the environment (OS Level, DB Level and Application Level) must be secured using industry standard encryption.
10. The Switch Solution shall have comprehensive channel wise Controls to enable define number and value limits applied for window period, transaction type filters (ATM/ POS/ Ecommerce/ NFC) and transaction value thresholds.
11. The Switch Solution shall support PKI based transactions.
12. The Switch Solution shall support message authentication Code (MAC) as per the requirement of the card schemes.
13. Solution should support Bunch Note Acceptance (Single and bunch), cash recycler, cash deposit, cash dispenser for major OEM such as Diebold, NCR, Vortex, Wincor, OKI, Hitachi or equivalent.
14. Switch must handle any Message Level routing based on but not limited to Card Based, Account Based, Institution Code, BIN, Card Range, Message ID, Network ID, Transaction Type and any other ISO/XML field value.
15. The system should be capable enough to route online/offline transaction to different CBS, network providers, interchange, private interchange, billers, service providers, different Card Management System, etc based on different criteria.
16. Support up to 19 digit card number as well up to 16 digit card number (presently and any further variations introduced by VISA, MasterCard, NPCI or any other payment system association etc.) for routing.
17. Solution should be capable of acquiring, authenticating (issuer) and routing (acquirer) e-Commerce merchant transactions.
18. Should allow routing based on Source of transaction / Destination of transaction / Transaction Type / Account Type / Authentication Method (with PIN /without PIN /Aadhaar authentication).
19. Should support alternate path routing - Ability to block /unblock different types of transactions based on - Merchant Category Code (MCC) /Bin based /Domestic /International / Institution / Card Number based/ interchange/ ATMs /GEO LOCATION based/Currency based
20. Support Stand-in processing and Store and Forward (SAF) facility.
21. The Switch Solution shall support timeout and acquirer generated reversals. Partial reversals are supported as an issuer for remote onus scenarios.

22. The Switch Solution shall support various PIN block format like ANSI X 9.9 PIN formats, IBM 3624, ISO 9654 etc.
23. Switch Solution should support compliance to NFS, VISA, Master and RUPAY Standards. The Solution should support real time integration with systems using ISO 8583, XML and Web Services. The Switch Solution must support international networks / interchanges including but not limited to RUPAY, VISA, and MASTERCARD.
24. The Switch Solution should support transactions originating from Visa, MasterCard and NFS / RUPAY ATM's and supported POS Terminals.
25. Support daily Transaction Log Files to Bank post EOD LTS & TVS logs
26. Perform routine activities like addition of new BINs or IINs to the Switch at no additional cost to the Bank.
27. Support for Chip and Non-Chip based card.
28. Should support all variants of different Card brands like MasterCard, Maestro, VISA, VISA Plus, Rupay, Cirrus,etc.
29. All transactions should be identified by a unique transaction id generated by the Switch.

E. Switching Authorization

1. System should be capable of authorizing and routing based on multiple variables such as source profile of transaction, destination profile of transaction, transaction code, account type, auth method, etc.
2. System should support standing instructions & batch authorization.
3. Must have TLS 1.3 capability for full transaction flow (including Application level).
4. Switch must handle any Message Level Interface and should support all Industry standards message formats like ISO 8583, XML etc, for all major ATM machines and POS terminals
5. Support for multiple accounts on a card and multiple cards on an account.
6. Switch should support Full and Partial Reversal (Bank will decide whether to implement it or not) in compliance to NFS Rupay / MasterCard/ VISA guidelines.
7. Switch should support online addition/ modification of different devices, processes, interfaces etc.
8. Solution should support multicurrency (including but not limited to INR, USD, GBP, Euro, SAR ,Yen etc), multi-language, multiple-institutions, and multiple-time zones.
9. It should have tools for monitoring the application as well as devices/hardware.
10. Bank should have real time access to transactional and customer data (Web Based Dashboard to be provided for monitoring purpose) without any additional cost. The

dashboard should be made available to/from any bank location as and when desired by the bank.

11. Proposed Solution should have customized report generation capability based on configurable parameters as per banks requirement from time to time (Like user, time etc.). The bank should have the facility for remote generation of reports and online view/download facility along with the complete audit trail as per the requirement of bank.
12. To be mandatorily integrated with ESQ monitoring solution or any other new solution that Bank may procure during the contract period without any additional cost to the Bank.
13. Switch should support different cutover times for different institutions /interchanges.
14. Should be able to give alert at screen, through voice, through SMS and emails in case of problem
15. The solution should be scalable (linear, horizontally and vertically) and flexible to provide new service and interfaces in future.
16. The solution should be capable of integrating with Bank Payment Gateway (both in-house & outsourced) for 3D Secure transactions.
17. Application should be highly scalable, should have been enabled for parameterization and customizable as per need of the bank.
18. The product offered should be customizable, flexible and user friendly (preferably GUI based).
19. The Bidder to confirm that they would implement proposed End to end EFT switch /DCMS solution updates, patches & compliance to all Security Guidelines issued by regulatory bodies (like Ministry of Finance, RBI, IBA etc), Visa, MasterCard, NPCI from time to time without additional cost to the Bank. Bidder to submit the self-certificate along with this Bid. The requisite modules/ patches/ customizations if any required for the said purpose would also be provided by the bidder within the offered solution without any extra cost during the currency of contract.
20. Testing support for the entire integration of proposed End to End EFT switch/DCMS solution with Bank's existing setup, MasterCard, Visa, NPCI, Payment Gateway of the bank both in house and outsourced without any additional cost.
21. Should provide any other facility not mentioned in the scope of work but related to ATM switch/DCMS/ATM Driving functionalities.
22. Should support instant refresh of balances from the host to the Switch online.
23. Should support configuration of new Host parameters on the Switch/DCMS without stopping services.
24. Should be able to monitor and report status of Host, partner switches, ATMs, BNAs/CRs and all interfaces.

25. The application should have user-friendly and powerful querying mechanism and help effective data mining based on the Bank defined parameters, processing logic, rules and criteria.
26. The solution should have a strong Management Information /Decision Support System facility.
27. Maintain logs and offer report of all transactions coming in and going out of the Switch, including the application messages and communication messages without impacting on the performance at peak load condition.
28. Switch should have capabilities to offer seamless support and integration capabilities for Card Not Present (CNP) Transactions through Internet.
29. Real-time addition of New ATM/BNA/CR without bringing down the System / Switch network

F. Supported Interfaces

Standard Application Interfaces that have been implemented as a part of the Switch Solution for the Bank

1. Core Banking Solution
2. Mobile Banking
3. Enterprise Service Bus / API Module
4. Enterprise data warehouse
5. Interactive Voice Response System (IVRS)
6. Web Portal, Mobile Apps
7. ACS / SI-HUB / eNACH
8. Card Schemes (MasterCard, Visa, Rupay)
9. Online Interfaces with POS Switch.
10. Online Interfaces with Banks UPI Switch.
11. Online Interfaces with Credit Card Switch.
12. SMS/Email Gateway
13. Business Intelligence Applications
14. Document Management System
15. Enterprise Fraud Management System
16. Reconciliation system
17. Loyalty Management System
18. AML (Anti Money laundering)

19. Card Personalization vendor
20. CHATBOT / Whatsapp
21. Dispute Resolution System
22. Integrations with Mastercard/Visa/Rupay
23. Tokenization functionality interface with Mobile banking / Internet Banking
24. API interface with card sourcing partners (Including co-branded)
25. RUPAY & NFS
26. MasterCard.
27. Visa.
28. (Interfaces to be arranged/managed by Bidders without additional cost to the Bank).
29. Internet Banking Interface for banking channels
30. Interface for Point of Sale (On-Us)
31. Interface for Micro ATMs
32. Interface for Card Issuance, Maintenance, Linking, Delinking, Hotlisting etc
33. ATM Green PIN / One Time Password Solution
34. Extranet User Interface
35. ATM Device Status Feed Messaging Interface
36. Credit card interface for Green Pin and Onus routing.
37. Direct Integration with Bank's authorized service partner for ecommerce transactions
38. Interface with Bank's Financial Inclusion Server for driving Micro ATMs along with any regulatory and Bank specific changes required during the transition or in future.
39. Interface with NPCI / Bank's FI Gateway Server for UIDAI Aadhaar authentication as an alternative mechanism for PIN authentication on biometric ATMs whenever required by the Bank
40. ISO 8583 (87/93) relevant for Payment processing

Interchange Interfaces

1. The solution should comply to all requirements of MasterCard/ VISA/ Rupay/ NPCI or any other interchange
2. Solution must support international networks / interchanges including but not limited to Rupay, VISA, MASTERCARD, Amex, JCB, Dinners, DISCOVER, qSPARC etc.
3. Should automatically update from external Interchange Routing tables list refresh sources (VISA, MasterCard, Rupay etc)

G. Card Authorization Services

Switch Solution shall perform pre-authorization checks

1. Card verification in the database
2. Card Status Verification
3. Creation of Account Inquiry Response
4. Verify allowed transactions by processing code
5. Instant PIN verification and or standard PIN verification
6. Channel Validation (ATM, POS, ECOM, Contactless)
7. Geography Validation (Domestic, International)
8. PIN at POS shall be checked for all domestic transactions
9. Per transaction limit checks by merchant identifier
10. Deny transactions by country
11. Deny suspected fraud transactions
12. 3DSecure CAVV/AAV data checking
13. Chip Data Verification
14. CVV1 / CVV2 / ICVD validation
15. Expiry date validation
16. Validation as per transaction amount limit
17. Limit Verification and accumulation (Authorization and Reversals)
18. Card blocking, Hot listing verification

H. Switch Feed Service:

1. Provide on-line Switch Feed to Bank's ATM Vendors for State of Health, Cash balances etc. of their ATMs.
2. Provide services on demand for ATM download and such activities which need to be managed remotely from the Switch.
3. Provide various statistics, support, and query resolution to ATM Vendors like cash files at a frequency of 2 hours, transaction reports.
4. Support daily Transaction Log Files/EJs to Bank post EOD over secured SFTP.

5. System should automatically generate Daily transaction reports based on the scheduled time and should have the capability to export the same in different formats but not limited to CSV, xls/xlsx, xml, text, etc.
6. Should have the capability to generate any custom reports as per the Banks requirement.
7. Should have capability to initiate Bulk ATM download based on make, geo location etc.
8. Facility to push ATM screens including the ones meant for campaigns across terminals as required by the Bank.
9. Facility to deploy content (push, pull and execute files) on the terminals.

I. Web services:

1. Web services supplied for Internet Banking / Alternative Channels including maintenance and enhancements.
2. Web Application Programming interface- support for nonfinancial transactions
3. Card Verification for all delivery channels.
4. Card Hotlist, Blocking / Unblocking for banking channels.
5. PIN Verification from banking channels.
6. Set ATM PIN from banking channels.
7. Enable / Disable Domestic/International transactions (as per RBI Requirement)
8. Enable / Disable transactions by Channel (RBI Requirement)
9. Enable / Disable Channel wise Limits (RBI Requirement).
10. Set/reset ATM pin
11. Re-KYC
12. Integration with Banks KYC module.

J. Card Control:

1. Alert all transactions
2. My Location: Alert if device location is not in geographical proximity (zip/city/state) of transaction for card-present, card-holder present transactions that qualify.
3. My Region: Alert if transaction is not in specified geographical region for card-present, cardholder present transactions that qualify.

4. Alert if International transaction.
5. Alert for specified transaction types.
6. Alert for specific merchant types.
7. Alert if transaction exceeds threshold amount.
8. Alert if monthly spend exceeds threshold amount.
9. Alert on card and account status changes Set alert preferences on dependent cards.
10. All other alerts as per the Regulatory/Bank requirements.

K. NACH Integration

1. Debit Card seamless integration for eNach transactions.
2. API to manage the eNach and SI mandates through Mobile app/ebank etc.
3. Report generation.

L. Helpdesk

1. Help Desk Services.
2. Support to Bank for problem resolution.
3. Support for queries related to ATMs and transaction details.
4. Providing all types of MIS required by the Bank.
5. Help Desk services to Managed Service centres of various ATM Vendors with status of their ATMs in case of non-availability of Data Feed services due to network and / or hardware disasters

M. Infosec Requirements

i. Governance & Compliance Controls

- Compliance with RBI Cyber Security Framework & Payment Security Guidelines
- Compliance with PCI DSS v4.0
- Valid PCI DSS certificate
- Data localization - data hosted within India
- ISO 27001 certified.

ii. Cryptography & Encryption Controls

- TLS 1.2 minimum, TLS 1.3 preferred
- Only strong ciphers (AES-GCM, ECDHE, SHA-256+)

- AES-128 / AES-256 used for encryption

iii. HSM & Key Management Controls

- HSM mandatory for PIN, CVV, ARQC/ARPC
- HSM is PCI PTS / FIPS 140-2 Level 3+ certified.
- Dual control & split knowledge enforced
- Key rotation & expiry policy defined
- Key lifecycle policy defined
- No cryptographic keys stored outside HSM

iv. PIN, PAN & Card Data Protection

- PIN generated & verified only via HSM
- No storage of PIN or CVV post authorization
- PAN masked in logs, reports & dashboards

v. Application & API Security

- Secure API authentication (mTLS / OAuth where applicable)
- Input validation & schema enforcement
- Rate limiting & anti-abuse controls
- VAPT against TOP 10 OWASP (App + API)
- Secure SDLC & source code review

vi. Access Control & Identity Management

- Role-Based Access Control (RBAC)
- Privilege access to assets via Privileged Access Management (PAM)
- Quarterly user access review
- Passwords stored using strong hashing (bcrypt/Argon2/PBKDF2)

vii. Logging, Monitoring & SIEM Integration

- Centralized audit logging enabled and integrated with Vendor SIEM as well as bank SIEM
- 24/7 SOC Operation.
- Log retention for 03 Years.
- Logs protected from alteration, admin tampering.
- Time synchronization (NTP) enabled
- Alerts for admin actions & security violations
- 24x7 incident response support

viii. Infrastructure & Platform Security

- Secure configuration / hardening applied.
- Regular OS, DB, App patching.
- Endpoint security on servers.
- Firewall with security features, WAF/Anti-DDoS protection enabled

ix. Infosec Support

- Must follow Bank's internal Infosec and Cyber Security Policy
- Firewall policy governance and quarterly firewall rule review

- Exceptions and Risk Acceptance to be documented with RCA within 04 hours of incident
- Compliance reports to be shared with the Bank

x. Data Protection & Monitoring

- Database Activity Monitoring (DAM) solution
- End-user DLP implementation for protection of Bank/customer PII and proprietary data

xi. Backup, DR & Resilience

- Regular backups of data and configurations
- DR cutover and backup restoration testing as required by the Bank

xii. Integration & Operations

- Integration with ITSM tools (along with PAM and SIEM) and monitoring

xiii. Application Security & Code Management

- Version control for every code change with repository management and hash values
- Assurance of application code integrity and security (explicit requirement)

N. Secured File Transfer Protocol (SFTP)

- Bidder shall maintain the card lifecycle for Bank's issued cards.
- Bidder shall integrate with the Bank's card embossing bureau by API/over Secure File Transfer ("SFTP") / loyalty/RECON/AML.
- Bidder shall encrypt card data files using applicable encryption standard.

O. Monitoring:

1. GUI based with dashboard facility (configurable to user's need) at multiple locations, as required by the Bank.
2. Online status of ATMs, devices, interchanges, host, servers etc. connected to switch including reason in case of down/ problem in ATM and generation of alerts via SMS, email, whatsapp etc.
3. Online status of different components of Switch application like processes, interfaces, nodes, etc.
4. Online transactions surveillance giving information/analysis on TPS, transaction wise, interchange wise, type of transactions wise, successful/ decline ratio, reason for declining of transaction, abnormal transaction behaviour on particular device etc.
5. Hardware performance monitoring like CPU, memory, Disk I/O, other performance parameters etc.
6. Provision for defining the thresholds for different parameters.

7. Should be able to give alert at screen, through voice, SMS, whatsapp and emails in case of problem and abnormal network/transaction behaviour.
8. Customizable Dashboard for monitoring the live transactions on Debit Switch for Cards and ATM terminals with real-time transaction status.
9. Graphical representation of Business and Technical declines.

P. MIS and Documentation

1. It should provide all industry standard and Bank specific reports in desired format for reconciliation for Bank's current and future need.
2. MIS setup to be integrated with our data lake.
3. Auto scheduling of day to day reporting as per the Banks requirement.
4. Web interface for accessing standard reports / Adhoc reports.
5. Web-based Transaction details query to be configured based on card no. / account no. & transaction date for fast tracking transaction inquiry.
6. The selected bidder must provide all the documents and 'Manuals' related to the core product and the proposed solution respectively. The documentation must also include BCP /DR document in adherence to the Bank policies.
7. Technical Training to be provided to the Bank staff for managing the front end solution.
8. Migration of existing APIs to new solution without Bank required to do any changes in the corresponding setups.
9. Resource to be stationed at Bank premises.

Q. Limit Management :

1. Solution should handle all four limits i.e. Cash withdrawal, PoS, e-Commerce and contactless both domestic and international.
2. Limits must be variable - Option for card holders for personalized limits for different types of transactions through Mobile App / SMS/IVRS / Core Banking.
3. (Branch)/ebanking/ATM terminals or any other channel as required by the Bank.
4. Limits (Daily/ Weekly/ monthly etc) setting and checking at Global level, BIN level and Card number level, Product level, Type of Transaction level, online/ offline limits etc.
5. Changes in limits should be appropriately logged and alerted to relevant stakeholders.

6. Card limits shall be set to levels consistent with the Bank' risk appetite and compliance tolerance levels and should be easily configurable as per the Banks requirement.
7. Solution must support variable limits.
8. Setting up separate limits & velocity at Interchange level, Institution level, Transaction Type, Country level, MCC, Merchant and Terminal level.
9. Solution should allow monthly and annual capping on international usage of debit cards.

R. End to End switch solution deployment:

1. Like to Like DC and DR setup which must be in Sync.
2. Should have modular architecture and should support, load sharing and fault tolerance for switch solution and hardware failure.
3. The Switch Solution should be deployed in high availability mode at the DC (active - active load balanced within the site). The system architecture should be modular, with application level load balancing and fault tolerance for data recovery, hardware failure and site failure with built in redundancy. The Switch Solution should also allow scalability, by adding capacity to the current environment (vertical and horizontal).
4. The Switch Solution should support measures such as PIN Verification, AES Encryption, Key Management, MAC, Key encryption and Masking.

S. Test setup:

1. The set up should be able to support bank/Entity on behalf of bank in all the testing activities performed by the bank/authorized partner or scheme of Bank.
2. Service Provider to configure test environments (development, SIT, UAT)
3. Service provider to facilitate Simulators for UAT testing.
4. Any patch movement from UAT to production shall invariably be signed off by the Bank before production deployment.

T. Other capabilities:

1. EFT switch system should be designed to store and utilize other customer identification such as mobile number, email address, UID etc. and link these IDs to accounts to use these credentials for card less routing.
2. Switch should support online addition/ modification of different devices, processes, interfaces etc.
3. Solution should support multicurrency (including but not limited to INR, USD, GBP, Euro, SAR, Yen etc), multi-language, multiple-institutions, and multiple-time zones.

4. It should have tools for monitoring the application as well as devices/hardware.
5. Bank should have real time access to transactional and customer data (Web Based Dashboard to be provided for monitoring purpose) without any additional cost. The dashboard should be made available to/from any bank location as and when desired by the bank.
6. Proposed Solution should have customized report generation capability based on configurable parameters as per banks requirement from time to time (Like user, time etc.). The bank should have the facility for remote generation of reports and online view/download facility along with the complete audit trail as per the requirement of bank.
7. Switch should support different cutover times for different institutions /interchanges.
8. Should be able to give alert at screen, through voice, through SMS and emails in case of problem
9. Should provide any other facility not mentioned in the scope of work but related to ATM Driving/ATM switch/DCMS functionalities.
10. Should support configuration of new Host parameters on the Switch/DCMS without stopping services.
11. Should be able to monitor and report status of Host, partner switches, ATMs, BNAs/CRMs and all related interfaces.
12. The application should have user-friendly and powerful querying mechanism and help effective data mining based on the Bank defined parameters, processing logic, rules and criteria.
13. The solution should have a strong Management Information /Decision Support System facility.
14. Maintain logs and offer report of all transactions coming in and going out of the Switch, including the application messages and communication messages without impacting on the performance at peak load condition.
15. Switch should have capabilities to offer seamless support and integration capabilities for Card Not Present (CNP) Transactions through Internet.
16. Realtime addition of New ATM/CRM/any other interface without bringing down the System / Switch network.

U. Terminal Driving

1. The Switching solution must support capabilities such as ATMs/CRMs/CDMs terminal Driving.
2. Should support DDC, NDC, NDC +, Diebold emulate 911/912 as well as ISO 8583 etc. standard protocols and no additional license modules are required to connect any ATM /Cash Dispenser make & model (like NCR, Diebold, Wincor,OKI, Hitachi, AGS, Petro, Triton, Vortex, Hyosung or any other OEM as required by the Bank) with proposed debit Switch solution which supports any one of these standard protocols.

3. Support Biometric ATMs
4. Support ATMs for visually impaired persons with voice guidance.
5. Solution should support Note Acceptance (Single and bunch) and Cash recycler for makes such as OKI, Diebold, NCR, Vortex, Wincor, LIPI and all major terminals Available in the domestic/ global market.
6. Support NFC enabled transactions on any NFC supported terminals (in compliance to RBI guidelines).
7. Switch should be compatible with all standard Kiosks available in the market.
8. Switch should be compatible with all the existing agents like RMM, EJ Pulling, TSS, ITSM etc deployed on ATM/CRM terminals.

V. Debit Card Management Solution:

1. “End to End Debit Card Management System Solution” including issuance of all Card Products, solution & services as per the requirements of Bank.
2. Proposed solution should have capability to extract data from core banking system as an input source for Card Production & card related maintenance activities through automated process and event based activities.
3. Products Considered- Debit Cards (Physical / Virtual cards/Form Factors) or any other product as required by the bank
4. Schemes Considered for Issuance - VISA, MasterCard & RuPay or any other scheme as required by the bank.
5. Support for Virtual Cards/Form Factors
6. Support of converting Virtual to Physical.
7. Ease of integration & usage with an out of the box readily available API rich library
8. Support for Contact, Contactless and NCMC enabled EMV Cards both instant and personalized.
9. Card Lifecycle management, Renewal and Replacement of Debit Cards issued.
10. APIs: DCSM will expose APIs to Tellers, IVRS, Mobile Banking, Internet Banking, Core Banking.
11. Solution should have the capabilities to synchronize Card details in DCMS with Switch, CBS and other supporting systems in realtime.
12. Embossing files generation and sending the same to Bank Embossing Partners with the facility of API integration.

13. Standard Reports would be provided through reporting module such as card production, card renewals, card management reports (Card Issuance, Lost/stolen Cards reports).
14. Data matrix for card projections encompassing the number of cards that are due for renewal, issued cards, Acknowledged cards and pending for acknowledgement consolidated, Zone wise or Branch wise as per the Bank requirement.
15. Sending configurable alerts to customers about card renewals due, on activation of cards, activation or disabling of services across the channels, Business declines, etc.
16. Capability to generate Green PIN on ATMs/MBank/IVR/eBank /Branch or anyother delivery channel as per the Bank requirement.
17. Card data is encrypted in the platform.
18. As part of implementation Data migration of existing Cards from existing DCMS solution to new DCMS Solution will include Cards Data, Keys, card audits and any other related data.
19. Solution provided by the successful bidder should provide, generate relevant MIS, Dashboards & Reports as an automated, event driven, user driven process meeting the current & future requirements of Bank, RBI, any other regulatory authorities in the required format without any additional cost to the Bank. MIS, Dashboards & Reports should be configurable at the request of the bank based on banks requirements from time to time.
20. The Successful Bidder should provide an end-to-end Card Tracker System for maintenance of data related to Cards and PINs dispatch, inquiry, retrieval of data and acknowledgement of cards & PINs dispatch status at branches, processing centre, customers etc.
21. The proposed solution should have capability for configuring business rules for the issuance and maintenance of cards, linking of accounts to cards
22. The offered solution must be scalable for handling up to minimum 10 million cards on incremental basis.
23. Successful bidder should provide application with system security functionality in terms of user authentication, access management, audit trails of cards, user maintenance and activities performed by the users with no limitation on number of users.
24. The Successful Bidder should complete end to end migration of existing complete card database, Data conversion, Migration of keys, migration testing, and business processes, seamlessly into the proposed solution. Successful Bidder should share the migration plan along and migration process shall be finalized in consultation with the Bank.
25. Successful bidder should deliver mandates as and when required by Networks/ Card Schemes such as RuPay, VISA, MasterCard, Bank regulatory authorities etc. with no additional cost to Bank. The proposed Solution should comply with all the specifications and conditions set by NPCI, VISA and Master Card while issuing debit cards.
26. Bidder to ensure status of cards is in sync on Switch and DCMS.

27. The Bidder should generate card reports as per BIN/ IIN wise, card type wise, Network wise, branch wise, product wise, sub product wise, issuance wise, expiry wise dispatch wise, date wise or as per Bank's and Statutory requirement from time to time in the format as required by the Bank's and Statutory authority and send them by automated email/Branches /regional Offices
28. Future Technologies: Should be able to support all future technologies (Samsung Pay/Apple Pay/Tokenization etc.).
29. Manuals/Documentation - Should be provided for Users during and after implementation for all modules
30. Bidder shall provide DCMS with Compliance/Risk Management capabilities.
31. The Successful Bidder should have a proper UAT setup for testing all customizations/products which should integrate with Bank's/Entity's UAT environment. The Successful Bidder should also provide test cards (generated using UAT keys) for testing purpose as and when required by Bank during the contract period.
32. However, kindly note that the Bank reserves the right to finalize the scope of work, as decided by the Bank. The Bank's decision is FINAL in this regard.

W. Roles & Responsibility

1. The Successful Bidder will be responsible for migrating Switch/DCMS data from the existing Switch/DCMS to the proposed switch/DCMS, without causing any disruption to the existing services at the time of migration.
2. The vendor would be fully responsible for all data migration (with zero loss) related activities and the Bank would only facilitate a joint meeting of the existing service providers / vendors / interchange agencies.
3. The bidder is required to provide a detailed project plan as well as migration plan to the Bank and the progress of the project needs to be shared with the Bank on a regular basis at the frequency required by the Bank.
4. The bidder is required to interface with the bank's existing and future ecosystems at their own cost.
5. The Bidder shall be responsible for facilitating the middleware required to implement any functionality wrt to ATMs/Debit Switch/DCMS at no additional cost to the Bank..
6. Bidder should be able to provide 24x7 support
7. Have support team to follow up all incidents until closure and Report incident to bank team in timely manner.
8. Should have business continuity plan (BCP) in place in line with Banks BCP Plan.
9. Must perform DR drill as per Regulatory guidelines/ Bank requirement.

10. The bidder shall coordinate and ensure the required Certification for Mastercard, Visa & NPCI interchanges. Any cost incurred towards VISA/ NPCI/Mastercard certification will be borne by the Bidder.
11. Bidder shall be responsible for Implementation, integration, testing, migration of the Switch, ATMs, Card and all other data, hosting of the ATM Switch and associated services, training of bank staff and Online monitoring of all delivery channels/ hosts/interchanges operating through/interfaced with ATM Switch.
12. Bidder should have Simulators for all different channels for the purpose of testing during migration and production issue replication.
13. Equipment as required for ATM switch/DCMS solution to be implemented at the bidder's premises with High Availability (99.99%) and load balancing.
14. GUI based real-time user-friendly monitoring tool for devices accessible through laptops/desktops at banks premises wherever required.
15. The switch solution offered under hosted model by the bidder should be complied with EMV/PCI-DSS/PCI SSF standards. All necessary interfaces customizations, testing to be done by the bidder at their own cost.
16. Providing transaction routing, authentication and authorization services for Card based /non card based and Admin cards, biometric authentication and Aadhaar-based biometric authentication (when required).
17. Carrying- out the customization on the Debit switch/ DCMS/ ATMs to address the existing requirements from the Bank.
18. The Bidder shall be responsible for developing interfaces/customization of existing modules for various requirements of the Bank.
19. Bidder shall provide Interface for Bank's existing/future channels.
20. The bidder would be required to maintain (retention and archiving) Banks Card / ATM data/Transaction data for the entire contract period online.
21. The Bidder will also be required to provide post implementation support and maintenance during the contracted period from the date of successful commissioning and acceptance by the bank.
22. Bidder must share the detailed exit management process in case bank decide to migrate off from the bidder's solution.
23. Bidder to adhere to the RBI master direction on Storage of Payment System Data.
24. The bidder shall also implement value-added services on ATMs. Bidder should ensure that all existing services through ATMs should be available from day one of go-live in the hosted switch solution.
25. Bank will continue with existing Reconciliation system and the switch solution offered by the bidder should be compatible with that system. Any customization required for the above

purpose is to be done by the vendor without any additional cost to the Bank. Solution should facilitate out of the box end-to-end Reconciliation/Chargeback/Disputes module in case the Bank decides to use it.

26. If at any stage during the contract period, performance degrades due to any reasons, the selected bidder would be fully liable to take corrective steps with respect to hardware/software up-gradation, customization etc. without any additional cost to Bank.
27. The bidder must ensure compliance with all mandates, regulations, and features that are:
 - Live and operational with the bank at the time of implementation.
 - Guidelines Issued by the regulator/ Association/NPCI but not implemented/live at the time of the current implementation or any future guideline/mandate shall be provided at no additional cost to the Bank.
28. Provide mock/test environment for UAT, DR, and training
29. In case, the bidder has not indicated any component/module in their proposed solution and the same is required for implementation of solution, the successful bidder has to provide required peripherals/equipment's, within the contracted price at no additional cost to the Bank.
30. No changes will be carried out by the Bank in its existing Interfaces/Hosts/terminals for integrating the solution offered by the bidder. The bidder's solution should be compatible with all the systems integrated with Bank's existing ATM Switch/DCMS and it is the responsibility of the vendor to customize the same in case of need to meet the requirements of integration.
31. Connectivity/interface with the interchanges/Associations shall be responsibility of the bidder and shall be offered at no additional cost to the Bank.
32. The bidder shall be responsible for end to end support in case the Bank decides to migrate back to on prem model in future.
33. Bidder shall be responsible to follow the purging and archiving policy of the bank as applicable.

X. Robust Incident Management

1. 24 x 7 support for incident management.
2. Automated fault detection and resolution.
3. Automatic dispatching to avoid delays and automated messages to field engineers.
4. System to provide for automatic escalation in case of a problem not getting resolved.
5. Proactive management of all devices.
6. Remote resolution before actual dispatch.

7. Analysis of and recommendations on machine performance.
8. Back-up, storage and restoration of data related to the hosted ATM switch, DCMS and associated services, in a secure and reliable manner.
9. Restoration of backup should be done by the bidder as and when asked by the Bank for any requirement of historical data.
10. The vendor is responsible for any loss of data and any claim/penalty raised on the bank and non-submission of required data by any entity will be recovered from the vendor.
11. The vendor shall be responsible for Implementing and maintaining Business Continuity Planning and online DR readiness including data replication, for the proposed solution and associated services. Business continuity solution should support Real- time secured data replication between the primary and the DR site with Minimum impact on overall system performance. The connectivity between the Bank DC/DR site and Vendors DC/DR site for provisioning the services will be provided by the Bidder.
12. Facility Management on a 24 x 7 x 365 basis to be offered as a part of solution for entire contract period. End to End Service Support should be provided by the bidder.
13. The selected vendor would ensure the availability of dedicated personnel for the Bank at Bank premises on 24x7 basis during the contract period. The successful bidder should ensure that the personnel are available exclusively for entire solution.
14. Technical assistance to the Bank for logging, troubleshooting and managing the service requests for the entire solution.
15. Monitoring, alerting, troubleshooting and resolution of incidents / problems.
16. Monitoring and alerting on the health of the ATM network.
17. The selected vendor will have a telephone line(s) dedicated for the Bank service. The Bank will contact the Help desk using this telephone/mobile line. The Help desk should also be contactable using email and ticketing solution.

Y. Compliance to Regulatory Circulars:

Bidder shall be responsible for implementation of all regulatory guidelines issued by various regulatory bodies like RBI, NPCI and Associations etc. as on date of Go live and issued during contract period without any additional cost to the Bank. The circular include but not limited to the following circulars which are mandatory to be complied with at the time of Go live and any coordination to be done with the entities to facilitate their implementation shall be sole responsibility of the Bidder:

1. Implementation of ICCW and ICD as per the regulatory guidelines.
2. Implement UDIR (Unified Dispute Issue Resolution) process for handling and resolving customer complaints for ATM transactions (incl. card+PIN transactions on Micro-ATMs)

3. Implementation of NPCI SecureNxt-Rupay EMV 3DS Transaction- As per latest NPCI Circular- ATM EFT SWITCH & DEBIT CARD MANAGEMENT SOLUTION NPCI/2024-25/Rupay/007 dated.20.06.2024
4. Implementation of Card-on-File Tokenisation (CoFT) - Enabling Tokenisation through Card Issuing Banks CO.DPSS.POLC.No.S-919/02-14-003/2023-24 dated December 20, 2023.
5. Migration of PIN encryption from variant to Key Block for Rupay and NFS Network- As per NPCI Circular-NPCI/2024-25/Rupay/006 dated. 03.06.2024.

Important Note: Bidder has to ensure that all the regulatory/Association circulars/Guidelines/mandates issued, are complied within the defined timelines, without any additional cost to the Bank. Bidder shall be liable to pay any penalty levied by the regulator/Association for any non-compliance of any regulatory/Association circulars/Guidelines issued from time to time during the period of contract.

- Z. The bidder has to comply with the Technical Functional Requirement (Annexure E1), Compliance Requirements (Annexure M), Hosting Assessment Checklist (Annexure N) and all the terms and conditions of this LTE-RFP/SLTE document.

6. Location of Work

The successful bidder shall be required to work in close co-ordination with Banks teams and may be required to work at locations prescribed by Bank such as Banks DC/DR and other offices as per requirement. All expenses (travelling/lodging, etc.) shall be borne by the successful bidder

1. **CHQ , Srinagar**
Jammu & Kashmir Bank Ltd.
Corporate Headquarters,
MA Road, Srinagar-190001
2. **Data Center Noida**
Jammu & Kashmir Bank Ltd.
Green Fort Data Center, Plot B7, Sector 132, Noida U.P.-201301
3. **DR Mumbai**
CtrlS Data Center,
Mahape, Navi Mumbai, Maharashtra, 400701

7. Invitation for Tender Offer

J&K Bank invites tenders for Technical bid (online) and Commercial bid (online) from suitable bidders. In this RFP/SLTE, the term “bidder” refers to the bidder delivering products / services mentioned in this RFP/SLTE.

The prospective bidders are advised to note the following: The interested bidders are required to submit the Non-refundable RFP/SLTE Application Fees of ₹10,000 by way of NEFT, details of which are mentioned at clause of Earnest Money Deposit in Part C.

1. Bidders are required to submit Earnest Money Deposit (EMD) for ₹1,50,00,000/- (Rupees One Crore Fifty Lac Only). The Bank may accept Bank guarantee in lieu of EMD for an equivalent amount valid for 180 days from the last date of bid submission and issued by any scheduled commercial Bank acceptable to the Bank. Offers made without EMD will be rejected.
2. Technical Specifications, Price Bid, Terms and Conditions and various formats for submitting the tender offer are described in the tender document and Annexures.

8. Project Delivery Milestones

The solution as per the required scope needs to be rolled out as per the delivery timelines mentioned. The phases of the Schedule are as follows:

PROJECT PHASES:

1. Project Plan
2. Delivery of Solution
3. User Acceptance Testing
4. Operationalization of Solution
5. Solution Review

1. PROJECT PLAN:

Successful Bidder shall submit the project plan for complete implementation of the solution as per the Scope of Work detailed in this RFP/SLTE along with Solution Architecture, DFD and other required documents. This plan should be submitted for review and bank's acceptance within two week after the issuance of PO to the successful bidder.

Bank shall issue a Project Plan signoff accepting the same. It shall be the responsibility of the successful bidder to submit and get the plan approved by the Bank authorities within the timelines mentioned above without any delay. Bank shall have the discretion to cancel the purchase order in lieu of delay in submission of the project plan.

2. PROJECT MILESTONES & DELIVERY

The solution must be implemented as per project scope within a period defined in this RFP/SLTE. Rollout of the solution has to be as per the below timelines:

S.No	Milestone	Timeline
1	Issuance of PO	Week 0
2	Signing of Agreement	4 Weeks from the Issuance of PO
3	Submission of Project Plan Documentation	6 Weeks from the Issuance of PO

4	Supply, Delivery, Integration, Installation & Implementation of Solution (UAT Delivery) as per SOW of RFP, including mock migration.	Within 22 Weeks from the acceptance of Project Plan by bank
5	Full project Go-Live, Migration of existing Data in Production and training	Within 6 Weeks from the UAT sign off by Bank

Successful bidder is expected to provide detailed project implementation status on weekly basis.

The bidder must strictly adhere to the project timeline schedule, as specified in the purchase contract executed between the Parties for performance of the obligations, arising out of the purchase contract and any delay in completion of the obligations by the bidder will enable Bank to resort to any or all of the following provided that the bidder is first given a 30 days" written cure period to remedy the breach/delay:

- a. Claiming Liquidated Damages
- b. Termination of the purchase agreement fully or partly and claim liquidated damages.
- c. Forfeiting of Earnest Money Deposit / Invoking EMD Bank Guarantee/Performance Guarantee.

However, Bank will have the absolute right to charge penalty and/or liquidated damages as per Tender /contract without giving any cure period, at its sole discretion besides taking any other appropriate action.

EXTENSION OF DELIVERY SCHEDULE:

If, at any time during performance of the Contract, the Bidder should encounter conditions impeding timely delivery, the Bidder shall promptly notify the Bank in writing of the fact of the delay, its likely duration and its cause(s). As soon as practicable after receipt of the Bidder's notice, the Bank shall evaluate the situation and may at its discretion may extend the Bidder's time for performance against suitable extension of the performance guarantee for delivery.

NON-DELIVERY:

Failure of the successful bidder to comply with the above delivery schedule, shall constitute sufficient grounds for the annulment of the award of contract and invocation of bank guarantee (delivery) besides taking appropriate action against the successful bidder including blacklisting such bidder from participating in future tenders.

3. USER ACCEPTANCE TESTING:

Successful bidder shall assist Bank in the User Acceptance Testing of the solution for the functionalities stated in this RFP/SLTE document. Bank shall issue a UAT signoff on successful completion of the UAT for all channels. If the UAT fails or there is undue delay of the completion of the UAT due to reasons attributable to the successful bidder, Bank may at its own discretion cancel the purchase order and invoke the Bank guarantee for implementation.

4. OPERATIONALIZATION OF SOLUTION:

Bank shall issue Go Live Signoff on successful operationalization of the solution. If there is delay in the operationalization of the solution, Bank reserves the right to cancel the purchase order and invoke the Bank guarantee submitted for implementation.

5. REVIEW:

The solution shall remain under review for a period of 3 months from the date of issuance of Go Live Certificate as stated above. The Successful bidder shall be readily available during the review phase for troubleshooting and other support. During the review phase, Bank may request changes to the application as per its requirement and no extra costs shall accrue to the bank for the effort involved in the same. Bank shall issue final acceptance signoff at the end of the review phase.

B-EVALUATION PROCESS

The endeavor of the evaluation process is to find the best fit Solutions as per the Bank's requirement at the best possible price. The evaluation shall be done by the Bank's internal committees formed for this purpose. Through this RFP/SLTE, Bank aims to select bidder(s) /Service provider(s) who would undertake **Selection of Service Provider for ATM/Debit Switch & Debit Card Management System (DCMS) on hosted model**. The bidder shall be entrusted with end to end responsibility for the execution of the project under the scope of this RFP/SLTE. The bidder is expected to commit for the delivery of services with performance levels set out in this RFP/SLTE.

Responses from Bidders will be evaluated in two stages, sequentially, as below:

Stage A. Evaluation of Eligibility

Stage B: Technical Evaluation

Stage C. Commercial Evaluation

The three stage evaluation shall be done sequentially on knock-out basis. This implies that those Bidders qualifying in Stage A will only be considered for Stage B and those bidders qualifying Stage B will be considered for Stage C. Please note that the criteria mentioned in this section are only indicative and Bank, at its discretion, may alter these criteria without assigning any reasons. Bank also reserves the right to reject any / all proposal(s) without providing any specific reasons. All deliberations and evaluations performed by Bank will be strictly confidential and will be maintained as property of Bank exclusively and will not be available for discussion to any Bidder of this RFP/SLTE.

Stage A-Evaluation of Eligibility

The Bidders of this RFP/SLTE will present their responses as detailed in this document. The Response includes details / evidences in respect of the Bidder for meeting the eligibility criteria, leading the Bank to evaluate the Bidder on eligibility criteria. The Bidder will meet the eligibility criteria mentioned in Annexure D in this document individually. Bank will evaluate the Bidders on each criterion severally and satisfy itself beyond doubt on the Bidders ability / position to meet the criteria. Those Bidders who qualify on all the criteria will only be considered as "Qualified under Stage A" of evaluation and will be considered for evaluation under Stage B. Those Bidders who do not qualify at this Stage A will not be considered for any further processing. The EMD money in respect of such Bidders will be returned on completion of the Stage A evaluation. Bank, therefore, requests that only those Bidders who are sure of meeting all the eligibility criteria only need to respond to this RFP/SLTE process.

Stage B-Evaluation of Technical Bid

All technical bids of bidders who have Qualified Stage A will be evaluated in this stage and a technical score would be arrived at. The bidder should meet the technical requirements as mentioned in the Annexure E1. The Bank will scrutinize the offers to determine their completeness (including signatures from the relevant personnel), errors, omissions in the technical & commercial offers of respective bidders. The Bank plans to, at its sole discretion, waive any minor non-conformity or any minor deficiency in an offer. The Bank reserves the right for such waivers and the Bank's decision in the matter will be final.

Bidders scoring at-least overall score of 70% marks or more ,as per Technical Bid Format in Annexure E ,will be declared technically qualified.

Bank may seek clarifications from the any or each bidder as a part of technical evaluation. All clarifications received within stipulated time shall be considered for evaluation. In case a clarification is not received within the stipulated time, the respective technical parameter would be treated as non-compliant and decision to qualify the bidder shall be accordingly taken by the Bank. Those Bidders who meet the threshold score of 70% or more will be considered as "Qualified under Stage B" and will be considered for evaluation under Stage C. Those who do not meet the above threshold will not be considered for further evaluation and their EMD will be returned. However, Bank reserves the right to relax the criteria.

The bidders will submit the Technical Bid in the format as per Annexure E. A copy of board resolution or power of attorney showing that the signatory has been duly authorized to sign the tender document.

Stage C-Evaluation of Commercial Bid

Cost Evaluation under Combined Quality cum Cost Based System (CQCCBS)

- i. Under CQCCBS, the technical proposals will be allotted weightage of 70% while the financial proposals will be allotted weightages of 30%.
- ii. Proposal with the lowest cost may be given a financial score of 100 and other proposals given financial scores that are inversely proportional to their prices.
- iii. Similarly Proposal with the Highest Technical Score may be given a technical score of 100 and other proposals given technical scores that are proportional to their scores.
- iv. The total score, both technical and financial, shall be obtained by weighing the quality and cost scores and adding them up. The proposed weightages for quality and cost shall be specified in the RFP/SLTE.

Highest point's basis:

On the basis of the combined weighted score for quality and cost, the bidder shall be ranked in terms of the total score obtained. The proposal obtaining the highest total combined score in evaluation of quality and cost will be ranked as L-1 followed by the proposals securing lesser marks as L-2, L-3 etc. The proposal securing the highest combined marks and ranked L-1 will be invited for negotiations, if required and shall be recommended for award of contract.

As an example, the following procedure can be followed. In a particular case of selection of bidder, it was decided to have minimum qualifying marks for technical qualifications as 70 and the

weightage of the technical bids and financial bids was kept as 70 : 30. In response to the RFP/SLTE, 3 proposals, A, B & C were received. The technical evaluation committee awarded them 75, 80 and 90 marks respectively. The minimum qualifying marks were 70. All the 3 proposals were, therefore, found technically suitable and their financial proposals were opened after notifying the date and time of bid opening to the successful participants.

The evaluation committee examined the proposals and evaluated shall take place as under:

Proposal	Technical Score	Highest Technical Score	Commerci als Quoted	Lowest Confirmed Commercial	Final Combined Score	Final Rank
A	80	90	Rs.100.	Rs.100	$[(80/90) \times 70] + [(100/100) \times 30] = 92.22$	L2
B	75	90	Rs.110	Rs.100	$[(75/90) \times 70] + [(100/110) \times 30] = 85.6$	L3
C	90	90	Rs.120.	Rs.100	$[(90/90) \times 70] + [(100/120) \times 30] = 95.00$	L1

Proposal C at the evaluated cost of Rs.120 was, therefore, declared as winner and recommended for negotiations/approval, to the competent authority.

Under CQCCBS method, the bidder who has secured first rank in technical evaluation shall be called for further negotiation after opening and evaluation of its financial proposals.

The Name of the successful bidder along with details of cost etc. shall be posted on the bank's website after the award to the successful bidder has been made and communicated to him in writing.

C-RFP/SLTE SUBMISSION

1. e-Tendering Process

This RFP/SLTE will follow e-Tendering Process (e-Bids) as under which will be conducted by Bank's authorized e-Tendering Vendor M/s. e-Procurement Technologies Ltd. through the website <https://jkbank.abcprocure.com>

- a) Publishing of RFP/SLTE
- b) Vendor Registration
- c) Pre Bid Queries
- d) Online Response of Pre-Bid Queries
- e) Corrigendum/Amendment (if required)
- f) Bid Submission
- g) Bids Opening
- h) Pre-Qualification
- i) Bids Evaluation
- j) Commercial Evaluation
- k) Contract Award

Representative of bidder may contact the Help Desk of e-Tendering agency M/s. e-Procurement Technologies Ltd for clarifications on e-Tendering process:

2. Service Provider:

M/s. E-procurement Technologies Limited
(Auction Tiger), B-705, Wall Street- II, Opp. Orient Club, Ellis
Bridge, Near Gujarat College,
Ahmedabad- 380006, Gujarat

Help Desk:

Contact Persons: Nandan Velara
Mobile No.: 9081000427 / 9904407997
Landline: 079-68136831/ 6857 / 6820 / 6843 / 6853 / 6829 /
6835 / 6863 / 6852 / 6840

No consideration will be given to e-Bids received after the date and time stipulated in this RFP/SLTE and no extension of time will normally be permitted for submission of e-Bids.

Bank reserves the right to accept in part or in full or extend or reject the bids received from the bidders participating in the RFP/SLTE.

Bidders will have to abide by e-Business Rules framed by the Bank in consultation with M/s. e-Procurement Technologies Ltd.

3. RFP/SLTE Fees

The non- refundable RFP/SLTE application fee of Rs.10,000/- is required to be paid by the prospective bidders through NEFT as per the following details:

Bank Details for RFP/SLTE Fees	
Account Number	9931530300000001
Account Name	Tender Fee / Cost Account
Bank Name	The J&K Bank Ltd
Branch Name	Corporate Headquarters MA Road Srinagar J&K - 190001
IFSC Code	JAKA0HRDCHQ
Amount	INR 10,000/=

The Bidder shall solely bear all expenses whatsoever associated with or incidental to the preparation and submission of its Bid and the Bank shall in no case be held responsible or liable for such expenses, regardless of the conduct or outcome of the bidding process including but not limited to cancellation / abandonment / annulment of the bidding process.

4. Earnest Money Deposit

Prospective bidders are required to submit Earnest Money Deposit (EMD) of INR 1,50,00,000 (Rupees One Crore Fifty Lac Only). The Bank may accept Bank guarantee in lieu of EMD for an equivalent amount valid for 180 days from the last date of bid submission and issued by any scheduled commercial Bank in India (other than Jammu & Kashmir Bank). The Bank will not pay any interest on the EMD. The bidder can also submit the EMD through NEFT as per the following details:

Bank Details for Earnest Money Deposit	
Account Number	9931070690000001
Account Name	Earnest Money Deposit (EMD)
Bank Name	The J&K Bank Ltd
Branch Name	Corporate Headquarters MA Road Srinagar J&K - 190001
IFSC Code	JAKA0HRDCHQ
Amount	INR 1,50,00,000/=

In case of a Bank Guarantee from a Foreign Bank, prior permission of the Bank is essential. The format of Bank Guarantee is enclosed in Annexure G.

EMD submitted through Bank Guarantee/Demand Draft should be physically send in an envelope mentioning the RFP/SLTE Subject, RFP/SLTE No. and date to the following address:

Address:	Technology & Development Department, J&K Bank Ltd. 5 th Floor Corporate Headquarters, MA Road Srinagar, J&K Pin- 190001
-----------------	---

Note: EMD is exempted for all Start-ups as recognized by DPIIT/DIPP. In case of such exemption, relevant documents/proof is to be submitted with Bid.

The EMD made by the bidder will be forfeited if:

- a. The bidder withdraws his tender before processing of the same.
- b. The bidder withdraws his tender after processing but before acceptance of the PO issued by Bank.
- c. The selected bidder withdraws his tender before furnishing an unconditional and irrevocable Performance Bank Guarantee.
- d. The bidder violates any of the provisions of the terms and conditions of this tender specification.

The EMD will be refunded to:

- a. The Successful Bidder, only after furnishing an unconditional and irrevocable Performance Bank Guarantee (other than Jammu & Kashmir Bank) from any scheduled commercial bank in India for 5% of the total project cost for 5 years and valid for 5 year+6 months including claim period of 6 months, validity starting from its date of issuance. The PBG shall be submitted within 30 days of the PO issued from the Bank.
- b. The Unsuccessful Bidder, only after acceptance of the PO by the selected bidder.

5. Performance Bank Guarantee (PBG)

The successful bidder will furnish unconditional performance bank guarantees (other than Jammu & Kashmir Bank) from any scheduled commercial bank in India, for 5% of the total Purchase order cost for a period 5 years + 6 months. The format of the PBG is given as per Annexure H .The PBG shall be submitted within 30 days from the date of issuance of Purchase order by the Bank. The PBG shall be denominated in Indian Rupees. All charges whatsoever such as premium, commission etc. with respect to the PBG shall be borne by the Successful Bidder. The PBG so applicable must be duly accompanied by a forwarding letter issued by the issuing Bank on the printed letterhead of the issuing Bank. Such forwarding letter shall state that the PBG has been signed by the lawfully constituted authority legally competent to sign and execute such legal instruments. The executor (BG issuing Bank Authorities) is required to mention the Power of Attorney number and date of execution in his / her favour with authorization to sign the documents. Each page of the PBG must

bear the signature and seal of the BG issuing Bank and PBG number. In the event of delays by Successful Bidder in implementation of project beyond the schedules given in the RFP/SLTE, the Bank may invoke the PBG. Notwithstanding and without prejudice to any rights whatsoever of the Bank under the contract in the matter, the proceeds of the PBG shall be payable to Bank as compensation by the Successful Bidder for its failure to complete its obligations under the contract. The Bank shall also be entitled to make recoveries from the Successful Bidder's bills, Performance Bank Guarantee, or any other amount due to him, the equivalent value of any payment made to him by the Bank due to inadvertence, error, collusion, misconstruction or misstatement. The PBG may be discharged / returned by Bank upon being satisfied that there has been due performance of the obligations of the Successful Bidder under the contract. However, no interest shall be payable on the PBG.

6. Tender Process

- i. Three-stage bidding process will be followed. The response to the tender should be submitted in three parts: Eligibility, Technical and Commercial Bid through online e-tendering portal with a tender document fee and EMD details mentioned above.
- ii. The Bidder shall submit their offers strictly in accordance with the terms and conditions of the RFP/SLTE. Any Bid, which stipulates conditions contrary to the terms and conditions given in the RFP/SLTE, is liable for rejection. Any decision of Bank in this regard shall be final, conclusive and binding on the Vendor.
- iii. Bank reserves the right to call the successful bidder for a price negotiation.
- iv. Successful Bidder (L1) shall submit to the Bank the price breakup for the bid amount in the format as provided by the Bank. If the price breakup is not submitted to the Bank, the Bank reserve the right to reject the L1 Bidder's Bid and make procurement from the L2 or L3 Bidder.
- v. Bank will enter in to contract with the L1 bidder(s) (in normal cases). Rates fixed at the time of contract will be non-negotiable for the whole contract/SLA period and no revision will be permitted subject to Bank review. This includes changes in taxes or similar government decisions.
- vi. If the service provided by the vendor is found to be unsatisfactory or if at any time it is found that the information provided by the vendor is false, the Bank reserves the right to revoke the awarded contract without giving any notice to the vendor. Bank's decision in this regard will be final.
- vii. If any of the shortlisted Vendors are unable to fulfil the orders within the stipulated period, Bank will have the right to allot those unfulfilled orders to other participating vendors, after giving 15-days" notice to the defaulting Vendor, provided the next vendor (L2) matches the rate fixed. Also during the period of the contract due to unsatisfactory service, Bank will have the right to cancel the contract and award the contract to other participating vendors.

7. Bidding Process

- i. **The bids in response to this RFP/SLTE must be submitted in three parts:**

- a. Confirmation of Eligibility Criteria
- b. Technical Bid
- c. Commercial Bid" (CB).
 - i. The mode of submission of Confirmation of Eligibility, Technical Criteria and Commercial Bid (CB) shall be online.
 - ii. The Bidders who qualify the Eligibility Criteria will be qualified for commercial bid evaluation.
 - iii. Bidders are permitted to submit only one Bid and relevant Commercial Bid. More than one Bid should not be submitted.
 - iv. Receipt of the bids shall be closed as mentioned in the bid schedule. Bid received after the scheduled closing time will not be accepted by the Bank under any circumstances.
 - v. Earnest Money Deposit must accompany all tender offers as specified in this tender document. EMD amount / Bank Guarantee in lieu of the same should accompany the Bid. Bidders, who have not paid Cost of RFP/SLTE and Security Deposit (EMD amount) will not be permitted to participate in the bid and bid shall be summarily rejected.
 - vi. All Schedules, Formats, Forms and Annexures should be stamped and signed by an authorized official of the bidder'
 - vii. The bidder is expected to examine all instructions, forms, terms and conditions and technical specifications in the bidding documents. Failure to furnish all information required by the bidding documents or submission of a bid not substantially responsive to the bidding documents in every respect will be at the bidder's risk and may result in rejection of the bid.
 - viii. No rows or columns of the tender should be left blank. Offers with insufficient information are liable to rejection.
 - ix. The bid should contain no interlineations, erasures or over-writings except as necessary to correct errors made by the bidder. In such cases, the person/s signing the bid should initial such corrections.
 - x. Bank reserves the right to re-issue / re-commence the entire bid process in case of any anomaly, irregularity or discrepancy in regard thereof. Any decision of the Bank in this regard shall be final, conclusive and binding on the Bidder.
 - xi. Modification to the Bid Document, if any, will be made available as an addendum/corrigendum on the Bank's website and Online tendering portal.
 - xii. All notices regarding corrigenda, addenda, amendments, time-extension, clarification, response to bidders' queries etc., if any to this RFP/SLTE, will not be published through any advertisement in newspapers or any other mass media. Prospective bidders shall regularly visit Bank's website or online tendering portal to get themselves updated on changes / development in relation to this RFP/SLTE.
 - xiii. Prices quoted should be exclusive of GST.
 - xiv. Applicable taxes would be deducted at source, if any, as per prevailing rates.
 - xv. The price ("Bid Price") quoted by the Bidder cannot be altered or changed due to escalation on account of any variation in taxes, levies, and cost of material.
 - xvi. During the period of evaluation, Bidders may be asked to provide more details and explanations about information they have provided in the proposals. Bidders should respond

to such requests within the time frame indicated in the letter/e-mail seeking the explanation.

- xvii. The Bank's decision in respect to evaluation methodology and short-listing Bidders will be final and no claims whatsoever in this respect will be entertained.
- xviii. The Bidder shall bear all the costs associated with the preparation and submission of its bid and the bank, will in no case be responsible or liable for these costs, regardless of the conduct or outcome of the bidding process.

8. Deadline for Submission of Bids:

- i. Bids must be received at the portal and by the date and time mentioned in the "Schedule of Events".
- ii. In case the Bank extends the scheduled date of submission of Bid document, the Bids shall be submitted at the portal by the time and date rescheduled. All rights and obligations of the Bank and Bidders will remain the same.
- iii. Any Bid received after the deadline for submission of Bids prescribed at the portal, will be rejected.

9. Bid Validity Period

- i. Bid shall remain valid for duration of 06 calendar months from Bid submission date.
- ii. Price quoted by the Bidder shall remain valid for duration of 06 calendar months from the date of conclusion of RFP.
- iii. Once Purchase Order or Letter of Intent is issued by the Bank, the said price will remain fixed for the entire Contract period and shall not be subjected to variation on any account, including exchange rate fluctuations and custom duty. A Bid submitted with an adjustable price quotation will be treated as non-responsive and will be rejected.

10. Bid Integrity

Willful misrepresentation of any fact within the Bid will lead to the cancellation of the contract without prejudice to other actions that the Bank may take. All the submissions, including any accompanying documents, will become property of the Bank. The Bidders shall be deemed to license, and grant all rights to the Bank, to reproduce the whole or any portion of their Bid document for the purpose of evaluation and to disclose the contents of submission for regulatory and legal requirements.

11. Cost of Bid Document

The participating Bidders shall bear all the costs associated with or relating to the preparation and submission of their Bids including but not limited to preparation, copying, postage, delivery fees, expenses associated with any demonstration or presentations which may be required by the Bank or any other costs incurred in connection with or relating to their Bid. The Bank shall not be liable in any manner whatsoever for the same or for any other costs or other expenses incurred by a Bidder regardless of the conduct or outcome of the bidding process.

12. Contents of Bid Document

- i. The Bidder must thoroughly study/analyse and properly understand the contents of this RFP/SLTE, its meaning and impact of the information contained therein.
- ii. Failure to furnish all information required in this RFP/SLTE or submission of Bid not responsive to this RFP/SLTE in any respect will be at the Bidder's risk and responsibility of Bidders and shall be summarily rejected
- iii. The information provided by the Bidders in response to this RFP/SLTE will become the property of the Bank and will not be returned. Incomplete information in Bid document may lead to non-consideration of the proposal.
- iv. The Bid prepared by the Bidder, as well as all correspondences and documents relating to the Bid exchanged by the Bidder and the Bank and supporting documents and printed literature shall be submitted in **English**.

13. Modification and Withdrawal of Bids

- i. The Bidder may modify or withdraw its Bid after the Bid's submission, provided that written notice of the modification, including substitution or withdrawal of the Bids, is received at the portal, prior to the deadline prescribed for submission of Bids.
- ii. No modification in the Bid shall be allowed, after the deadline for submission of Bids.
- iii. No Bid shall be withdrawn in the interval between the deadline for submission of Bids and the expiration of the period of Bid validity specified in this RFP/SLTE. Withdrawal of a Bid during this interval may result in the forfeiture of EMD submitted by the Bidder.

14. Payment Terms

The Bidder must accept the payment terms proposed by the Bank as proposed in this section.

- a) The Payments shall be made on the achievement of the following project milestones:

S.No	Project Milestone	Payment (Incl. Of applicable taxes)
1	Submission of Project Plan Documentation	10% of One Time Cost
2	Supply, Delivery, Integration, Installation & Implementation of Solution (UAT Delivery) as per SOW of RFP, including mock migration.	30% of One Time Cost
3	Final Migration, Go-Live, Trainings and Production Sign-off by Bank.	40 % of one Time Cost
4	3 months after complete go-live and bug free operations	20 % of One-Time Cost

5	Monthly Card Hosting Fee per Active Debit Card	Monthly In Arrears subject to submission of transaction reports (As per actuals)
6	Transaction processing Fee-Financial and Non-Financial (Switching and debit card management system with 24x7 support)	Monthly In Arrears subject to submission of transaction reports (As per actuals)
7	Monthly Charges per ATM for ATM Driving with 24x7 support.	Monthly In Arrears subject to submission of reports(As per actuals)
8	Monthly Scheme connectivity (DC & DR) for Visa, MasterCard and NPCI.	Monthly In Arrears
9	Man-day cost for any additional Customization	As per actuals

Payments shall be released on acceptance of the purchase order with following pre-requisites:

- i) Post Signing of Service Level Agreement (SLA) between Bank and Successful bidder.
- ii) Post Signing of Non-Disclosure Agreement (NDA) between Bank and Successful bidder.
- iii) No advance payment will be made on award of the contract.
- iv) All taxes, if any, applicable shall be deducted at source as per current rate while making any payment.
- v) Payments will be withheld in case of Non-compliance of the terms and condition of this RFP/SLTE.

D-GENERAL TERMS & CONDITIONS

1. Standard of Performance

The bidder shall perform the service(s) and carry out its obligations under the Contract with due diligence, efficiency and economy, in accordance with generally accepted techniques and practices used in industry and with professional engineering standards recognized by the international professional bodies and shall observe sound management, technical and engineering practices. It shall employ appropriate advanced technologies, procedures and methods. The Bidder shall always act, in respect of any matter relating to the Contract, as faithful advisors to J&K Bank and shall, at all times, support and safeguard J&K Bank's legitimate interests.

2. Indemnity

The Successful bidder shall indemnify and hold the Bank harmless from and against all claims, losses, costs, damages, expenses, action suits and other proceedings (including attorney fees), relating to or resulting from:-

- i. Intellectual Property infringement or misappropriation of any third party trade secrets or infringement of any patent, trademarks, copyrights etc. or such other statutory infringements in respect of all components provided to fulfil the scope of this project.
- ii. Claims made by the employees who are deployed by the Successful bidder.
- iii. Breach of confidentiality obligations by the Successful bidder,
- iv. Negligence (including but not limited to any acts or omissions of the Successful bidder, its officers, principals or employees) or misconduct attributable to the Successful bidder or any of the employees deployed for the purpose of any or all of the its obligations,
- v. Any loss or damage arising out of loss of data;
- vi. Bonafide use of deliverables and or services provided by the successful bidder;
- vii. Non-compliance by the Successful bidder with applicable Laws/Governmental/Regulatory Requirements.

The Successful bidder shall be responsible for any loss of data, loss of life etc. due to acts of its representatives, and not just arising out of negligence or misconduct, as such liabilities pose significant risk. It is hereby agreed that the above said indemnity obligations shall apply notwithstanding anything to the contrary contained in this Tender document and subsequent Agreement and shall survive the termination of the agreement for any reason whatsoever. The Successful bidder will have sole control of its defence and all related settlement negotiations

3. Cancellation of Contract and Compensation

The Bank reserves the right to cancel the contract of the selected Bidder and recover expenditure incurred by the Bank on the following circumstances. The Bank would provide 30 days' notice to rectify any breach/ unsatisfactory progress:

- a. The selected Bidder commits a breach of any of the terms and conditions of the RFP/SLTE/contract.
- b. The selected Bidder becomes insolvent or goes into liquidation voluntarily or otherwise.
- c. Delay in completion of Supply, Installation of Project Deliverables.

- d. Serious discrepancies noted in the inspection.
- e. Breaches in the terms and conditions of the Order.
- f. Non submission of acceptance of order within 7 days of order.
- g. Excessive delay in execution of order placed by the Bank.
- h. The progress regarding execution of the contract, made by the selected Bidder is found to be unsatisfactory.
- i. If the selected Bidder fails to complete the due performance of the contract in accordance with the agreed terms and conditions.

4. Liquidated Damages

If bidder fails to make delivery or perform services within stipulated time schedule, the Bank shall, without prejudice to its other remedies under the contract, deduct from the contract price, as liquidated damages, a sum equivalent to 0.5% of the total project cost for delay of every 1 week or part thereof maximum up to 5% of contract price. Once the maximum is reached, Bank may consider termination of Contract pursuant to the conditions of contract. However, the bank reserves the right to impose / waive any such penalty.

5. Fixed Price

The Commercial Offer shall be on a fixed price basis, inclusive of all taxes and levies (excluding GST). No price increase due to increases in customs duty, excise, tax, dollar price variation etc. will be permitted.

6. Right to Audit

“Bank reserves the right to conduct an audit/ ongoing audit of the Company/Service Provider(including its sub-contractors).The Company shall be subject to annual audit by internal/ external Auditors appointed by the Bank / inspecting official from the RBI or the persons authorized by RBI or any regulatory authority, covering the risk parameters finalized by the Bank/ such auditors in the areas of products (IT hardware/ Software) and services etc. provided to the Bank and company is required to submit such certification by such Auditors to the Bank

Company shall allow the Bank and RBI or persons authorized by it to access Bank documents, records or transactions or any other information given to, stored or processed by Company within a reasonable time failing which Company will be liable to pay any charges/ penalty levied by the Bank without prejudice to the other rights of the Bank. Company shall allow the Bank to conduct audits or inspection of its Books and account with regard to Bank’s documents by one or more officials or employees or other persons duly authorized by the Bank.”

7. Force Majeure

- i. The Selected Bidder shall not be liable for forfeiture of its performance security, Liquidated damages or termination for default, if any to the extent that its delay in performance or other failure to perform its obligations under the contract is the result of an event of Force Majeure.

- ii. For purposes of this Clause, "Force Majeure" means an event explicitly beyond the reasonable control of the Contractor and not involving the contractor's fault or negligence and not foreseeable. Such events may be due to or as a result of or caused by act of God, wars, insurrections, riots, earth quake and fire, revolutions, civil commotion, floods, epidemics, pandemics, quarantine restrictions, trade embargos, declared general strikes in relevant industries, events not foreseeable but does not include any fault or negligence or carelessness on the part of the parties, resulting in such a situation. In the event of any such intervening Force Majeure, either party shall notify the other in writing of such circumstances or the cause thereof immediately within five calendar days.
- iii. Unless otherwise directed by the Bank in writing, the selected contractor shall continue to perform its obligations under the Contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.
- iv. In such a case the time for performance shall be extended by a period(s) not less than duration of such delay. If the duration of delay continues beyond a period of three months, the Bank and the contractor shall hold consultations in an endeavor to find a solution to the problem.
- v. Notwithstanding above, the decision of the Bank shall be final and binding on the successful bidder regarding termination of contract or otherwise.

8. Publicity

Bidders, either by itself or through its group companies or Associates, shall not use the name and/or trademark/logo of Bank, in any sales or marketing publication or advertisement, or in any other manner.

9. Amendments

Any provision of hereof may be amended or waived if, and only if such amendment or waiver is in writing and signed, in the case of an amendment by each Party, or in the case of a waiver, by the Party against whom the waiver is to be effective.

10. Assignment

The Selected Bidder shall not assign, in whole or in part, the benefits or obligations of the contract to any other person. However, the Bank may assign any of its rights and obligations under the Contract to any of its affiliates without prior consent of Bidder.

11. Applicable law and jurisdictions of court

The Contract with the selected Bidder shall be governed in accordance with the Laws of UT Of J&K read with laws of India so far as they are applicable to the UT of J&K for the time being enforced and will be subject to the exclusive jurisdiction of Courts at Srinagar (with the exclusion of all other Courts). However, the services from the bidder during the period of dispute or pending resolution shall continue as far as is reasonably practical.

12. Resolution of Disputes and Arbitration clause

The Bank and the Bidder shall make every effort to resolve any disagreement or dispute amicably, arising in connection with the Contract, by direct and informal negotiation between the designated Officer of the Bank for **Selection of Service Provider for ATM/Debit Switch & Debit Card Management System (DCMS) on hosted model** and designated representative of the Bidder. If designated Officer of the Bank and representative of Bidder are unable to resolve the dispute within reasonable period, which in any case shall not exceed 30 days, they shall immediately escalate the dispute to the senior authorized personnel designated by the Bank and Bidder respectively. If even after elapse of reasonable period, which in any case shall not exceed 30 days, the senior authorized personnel designated by the Bank and Bidder are unable to resolve the dispute amicably OR any party fails to designate its officer/representative/ senior authorized personnel within 30 days from the date of request in writing for the same by the other party for amicable settlement of dispute, the same shall be referred to a sole arbitrator to be appointed by Bank. The Arbitration and Conciliation Act, 1996 will be applicable to the arbitration proceeding and the venue of the arbitration shall be at Srinagar. The language of the arbitration proceedings shall be in English. The award of the arbitrator shall be final and binding. The courts at Srinagar shall have exclusive jurisdiction at Srinagar.

13. Execution of Service Level Agreement (SLA)/ Non-Disclosure Agreement (NDA)

The Successful Bidder shall have to execute service level agreement for deliverables and successful execution of the projects to meet Banks requirement to its satisfaction. The Bank would stipulate strict penalty clauses for nonperformance or any failure in the implementation/efficient performance of the project .The Bidder should execute the Agreement within 30 days from the date of acceptance of Work Order. The date of agreement shall be treated as date of engagement and the time-line for completion of the assignment shall be worked out in reference to this date. The Bidder hereby acknowledges and undertakes that terms and conditions of this RFP/SLTE may be varied by the Bank in its absolute and sole discretion. The SLA/NDA to be executed with the successful bidder shall accordingly be executed in accordance with such varied terms.

14. 'NO CLAIM' Certificate

The Bidder shall not be entitled to make any claim(s) whatsoever, against J&K Bank, under or by virtue of or arising out of, the Contract/Agreement, nor shall J&K Bank entertain or consider any such claim, if made by the Bidder after he has signed a 'No Claim' Certificate in favor of J&K Bank in such form as shall be required by J&K Bank after the works are finally accepted.

15. Cost and Currency

The Offer must be made in Indian Rupees only, including the following:

- a) Cost of the equipment/software/licenses specified
- b) Installation, commissioning, maintenance, migration charges, hosting charges, if any,
- c) Comprehensive on-site software support.
- d) Packing, Forwarding and Transportation charges up to the sites to be inclusive.
- e) All taxes and levies are for Destinations.
- f) Bidder have to make their own arrangements for obtaining road permits wherever needed.

16. No Agency

The Service(s) of the Bidder herein shall not be construed as any agency of J&K Bank and there shall be no Principal - Agency relationship between J&K Bank and the Bidder in this regard.

17. Project Risk Management

The selected bidder shall develop a process & help Bank to identify various risks, threats & opportunities within the project. This includes identifying, analyzing & planning for potential risks, both positive & negative, that might impact the project & minimizing the probability of & impact of positive risks so that project performance is improved for attainment of business goals.

18. Information Security:

- a. The Successful Bidder and its personnel shall not carry any written material, layout, diagrams, hard disk, flash / pen drives, storage tapes or any other media out of J&K Bank's premises without written permission from J&K Bank.
- b. The Successful Bidder's personnel shall follow J&K Bank's information security policy and instructions in this regard.
- c. The Successful Bidder acknowledges that J&K Bank 's business data and other proprietary information or materials, whether developed by J&K Bank or being used by J&K Bank pursuant to a license agreement with a third party (the foregoing collectively referred to herein as "proprietary information") are confidential and proprietary to J&K Bank; and the Successful Bidder agrees to use reasonable care to safeguard the proprietary information and to prevent the unauthorized use or disclosure thereof, which care shall not be less than that used by Successful Bidder to protect its own proprietary information. Successful Bidder recognizes that the goodwill of J&K Bank depends, among other things, upon the Successful Bidder keeping such proprietary information confidential and that unauthorized disclosure of the same by Successful Bidder could damage J&K Bank. By reason of Successful Bidder's duties and obligations hereunder, Successful Bidder may come into possession of such proprietary information, even though the Successful Bidder does not take any direct part in or furnish the Service(s) performed for the creation of said proprietary information and shall limit access thereto to employees with a need to such access to perform the Services required by the Contract/Agreement. Successful Bidder shall use such information only for the purpose of performing the Service(s) under the Contract/Agreement.
- d. Successful Bidder shall, upon termination of the Contract/Agreement for any reason, or upon demand by J&K Bank, whichever is earliest, return any and all information provided to

Successful Bidder by J&K Bank, including any copies or reproductions, both hardcopy and electronic.

- e. That the Successful Bidder and each of its subsidiaries have taken all technical and organizational measures necessary to protect the information technology systems and Data used in connection with the operation of the Successful Bidder's and its subsidiaries' businesses. Without limiting the foregoing, the Successful Bidder and its subsidiaries have used reasonable efforts to establish and maintain, and have established, maintained, implemented and complied with, reasonable information technology, information security, cyber security and data protection controls, policies and procedures, including oversight, access controls, encryption, technological and physical safeguards and business continuity/disaster recovery and security plans that are designed to protect against and prevent breach, destruction, loss, unauthorized distribution, use, access, disablement, misappropriation or modification, or other compromise or misuse of or relating to any information technology system or Data used in connection with the operation of the Successful Bidder's and its subsidiaries' businesses.
- f. The Successful Bidder shall certify that to the knowledge of the Successful Bidder, there has been no security breach or other compromise of or relating to any information technology and computer systems, networks, hardware, software, data, or equipment owned by the Successful Bidder or its subsidiaries or of any data of the Successful Bidder's, the Operating Partnership's or the Subsidiaries' respective customers, employees, suppliers, vendors that they maintain or that, to their knowledge, any third party maintains on their behalf (collectively, "IT Systems and Data") that had, or would reasonably be expected to have had, individually or in the aggregate, a Material Adverse Effect, and
- g. That the Successful Bidder has not been notified of, and has no knowledge of any event or condition that would reasonably be expected to result in, any security breach or other compromise to its IT Systems and Data;
- h. That the Successful Bidder is presently in compliance with all applicable laws, statutes, rules or regulations relating to the privacy and security of IT Systems and Data and to the protection of such IT Systems and Data from unauthorized use, access, misappropriation or modification. Besides the Successful Bidder confirms the compliance with Banks Supplier Security Policy.
- i. That the Successful Bidder has implemented backup and disaster recovery technology consistent with generally accepted industry standards and practices.
- j. That the Successful Bidder and its subsidiaries IT Assets and equipment, computers, Systems, Software's, Networks, hardware, websites, applications and Databases (Collectively called IT systems) are adequate for, and operate and perform in all material respects as required in connection with the operation of business of the Successful Bidder and its subsidiaries as currently conducted, free and clear of all material bugs, errors, defects, Trojan horses, time bombs, malware and other corruptants.
- k. That the Successful Bidder shall be responsible for establishing and maintaining an information security program that is designed to:
 - o Ensure the security and confidentiality of Customer Data, Protect against any anticipated threats or hazards to the security or integrity of Customer Data, and
 - o That the Successful Bidder will notify Customer of breaches in Successful Bidder's security

that materially affect Customer or Customer's customers. Either party may change its security procedures from time to time as commercially reasonable to address operations risks and concerns in compliance with the requirements of this section.

- l. The Successful Bidder shall establish, employ and at all times maintain physical, technical and administrative security safeguards and procedures sufficient to prevent any unauthorized processing of Personal Data and/or use, access, copying, exhibition, transmission or removal of Bank's Confidential Information from Companies facilities. Successful Bidder shall promptly provide Bank with written descriptions of such procedures and policies upon request. Bank shall have the right, upon reasonable prior written notice to Successful Bidder and during normal business hours, to conduct on-site security audits or otherwise inspect Companies facilities to confirm compliance with such security requirements.
- m. That Successful Bidder shall establish and maintain environmental, safety and facility procedures, data security procedures and other safeguards against the destruction, corruption, loss or alteration of the Client Data, and to prevent access, intrusion, alteration or other interference by any unauthorized third parties of the same, that are no less rigorous than those maintained by Successful Bidder for its own information or the information of its customers of a similar nature.
- n. That the Successful Bidder shall perform, at its own expense, a security audit no less frequently than annually. This audit shall test the compliance with the agreed-upon security standards and procedures. If the audit shows any matter that may adversely affect Bank, Successful Bidder shall disclose such matter to Bank and provide a detailed plan to remedy such matter. If the audit does not show any matter that may adversely affect Bank, Bidder shall provide the audit or a reasonable summary thereof to Bank. Any such summary may be limited to the extent necessary to avoid a breach of Successful Bidder's security by virtue of providing such summary.
- o. That Bank may use a third party or its own internal staff for an independent audit or to monitor the Successful Bidder's audit. If Bank chooses to conduct its own security audit, such audit shall be at its own expense. Successful Bidder shall promptly correct any deficiency found in a security audit.
- p. That after providing 30 days prior notice to Successful Bidder, Bank shall have the right to conduct a security audit during normal business hours to ensure compliance with the foregoing security provisions no more frequently than once per year. Notwithstanding the foregoing, if Bank has a good faith belief that there may have been a material breach of the agreed security protections, Bank shall meet with Successful Bidder to discuss the perceived breach and attempt to resolve the matter as soon as reasonably possible. If the matter cannot be resolved within a thirty (30) day period, the parties may initiate an audit to be conducted and completed within thirty (30) days thereafter. A report of the audit findings shall be issued within such thirty (30) day period, or as soon thereafter as is practicable. Such audit shall be conducted by Successful Bidder's auditors, or the successors to their role in the event of a corporate reorganization, at Successful Bidder's cost.
- q. Successful Bidders are liable for not meeting the security standards or desired security aspects of all the ICT resources as per Bank's IT/Information Security / Cyber Security Policy. The IT /Information Security/ Cyber Security Policy will be shared with successful Bidder. Successful Bidders should ensure Data Security and protection of facilities/application managed by them.

- r. The deputed persons should aware about Bank's IT/IS/Cyber security policy and have to maintain the utmost secrecy & confidentiality of the bank's data including process performed at the Bank premises. At any time, if it comes to the notice of the bank that data has been compromised / disclosed/ misused/misappropriated then bank would take suitable action as deemed fit and selected vendor would be required to compensate the bank to the fullest extent of loss incurred by the bank. Besides bank will be at liberty to blacklist the bidder and take appropriate legal action against bidder.
- s. The Bank shall evaluate, assess, approve, review, control and monitor the risks and materiality of vendor/outsourcing activities and Successful Bidder shall ensure to support baseline system security configuration standards. The Bank shall also conduct effective due diligence, oversight and management of third party vendors/service providers & partners.
- t. Vendor criticality assessment shall be conducted for all partners & vendors. Appropriate management and assurance on security risks in outsources and partner arrangements shall be ensured.

19. No Set-Off, Counter-Claim and Cross Claims:

In case the Bidder has any other business relationship(s) with J&K Bank, no right of set-off, counter-claim and cross-claim and or otherwise will be available under this Contract/Agreement to the Bidder for any payments receivable under and in accordance with that business.

20. Statutory Requirements

During the tenure of the Contract/Agreement nothing shall be done by the Bidder in contravention of any law, act and/ or rules/regulations, there under or any amendment thereof governing inter-alia customs, foreign exchange, etc., and the Bidder shall keep J&K Bank, its directors, officers, employees, representatives, agents and consultants indemnified in this regard.

21. Bidder Utilization of Know-how:

J&K Bank will request a clause that prohibits the finally selected bidder from using any information or know-how gained in this contract for another organization whose business activities are similar in part or in whole to any of those of the Bank anywhere in the world without prior written consent of the Bank during the period of the contract and one year thereafter.

22. Corrupt and Fraudulent practice:

- i. It is required that Successful Bidder observe the highest standard of ethics during the procurement and execution of such contracts and not to indulge in any corrupt and fraudulent practice.
- ii. "Corrupt Practice" means the offering, giving, receiving or soliciting of anything of value to influence the action of an official in the procurement process or in contract execution.
- iii. "Fraudulent Practice" means a misrepresentation of facts in order to influence a procurement process or the execution of contract to the detriment of the Bank and includes collusive practice among bidders (prior to or after bid submission) designed to establish bid prices at

artificial non-competitive levels and to deprive the Bank of the benefits of free and open competition.

- iv. The Bank reserves the right to reject a proposal for award if it determines that the Successful Bidder recommended for award has engaged in corrupt or fraudulent practices in competing for the contract in question.
- v. The Bank reserves the right to declare a bidder ineligible, either indefinitely or for a stated period of time, to be awarded a contract if at any time it becomes known that the firm has engaged in corrupt or fraudulent practices in competing for or in executing the contract.

23. Solicitation of Employees

Bidder will not hire employees of J&K Bank or solicit or accept solicitation (either directly, indirectly, or through a third party) from employees of the J&K Bank directly involved in this contract during the period of the contract and one year thereafter.

24. Proposal Process Management

The Bank reserves the right to accept or reject any/all proposal/ to revise the RFP/SLTE, to request one or more re-submissions or clarifications from one or more BIDDERS, or to cancel the process in part or whole. No bidder is obligated to respond to or to continue to respond to the RFP/SLTE. Additionally, the Bank reserves the right to alter the requirements, in part or whole, during the RFP/SLTE process. Each party shall be entirely responsible for its own costs and expenses that are incurred while participating in the RFP/SLTE, subsequent presentation and contract negotiation processes.

25. Confidentiality Provision

- a) The bidder shall hold in confidence all the information, documentation ,etc which shall come to their knowledge (Confidential Information) and shall not disclose or divulge confidential information to any third party or use Confidential Information or any part thereof without written consent of the Bank.
- b) Confidential Information means information which is by its nature confidential or is designated by the bank and confidential information and includes:
 - i. All information marked or otherwise designated as confident.
 - ii. Information which relates to the financial position, the internal management structure , the Personnel , policies and strategies of the Bank
 - iii. Data of the bank, customer lists, customer information, account information, and business information regarding business planning and operation of the Bank or otherwise information or data whether such data is permanent or otherwise

The restriction imposed in this clause does not apply to any disclosure or information:

- i. Which at the material time was in public domain other than breach of this clause; or

- ii. Which is required to be disclosed on account of order of any competent court or tribunal provided that while disclosing any information, Bank shall be informed about the same vide prior notice unless such notice is prohibited by applicable law.

26. Sub-Contracting

The services offered to be undertaken in response to this RFP/SLTE shall be undertaken to be provided by the bidder/ directly employing their employees, and there shall not be any sub-contracting without written permission of the Bank. All the resources deployed by the bidder should be on the bidder's payroll.

27. Award Notification

The Bank will award the contract to the successful Bidder, out of the Bidders who have responded to Bank's tender as referred above, who has been determined to qualify to perform the contract satisfactorily, and whose Bid has been determined to be substantially responsive, and is the lowest commercial Bid.

The Bank reserves the right at the time of award of contract to increase or decrease of the quantity or change in location where services are required from what was originally specified while floating the tender without any change in unit price or any other terms and conditions.

28. Suspension of Work:

The Bank reserves the right to suspend and reinstate execution of the whole or any part of the work without invalidating the provisions of the contract. The Bank will issue orders for suspension or reinstatement of the work to the Successful Bidder in writing. The time for completion of the work will be extended suitably to account for duration of the suspension.

29. Taxes and Duties:

- i. Successful Bidder will be entirely responsible for all duties, levies, imposts, costs, charges, license fees, road permit etc., in connection with delivery of equipment at site including incidental services and commissioning.
- ii. Income/Corporate taxes in India: The Successful Bidder shall be liable to pay all corporate taxes and income tax that shall be levied according to the laws and regulations applicable from time to time in India
- iii. Tax Deduction at Source: Wherever the laws and regulations require deduction of such taxes at source of payment, Bank shall effect such deductions from the payment due to the Successful Bidder. The remittance of amounts so deducted and issuance of certificate for such deductions shall be made by Bank as per the laws and regulations in force. Nothing in the Contract shall relieve the Successful Bidder from his responsibility to pay any tax that may be levied in India on income and profits made by Bidder in respect of this contract.
- iv. The Bank shall if so required by applicable laws in force, at the time of payment, deduct income tax payable by the Successful Bidder at the rates in force, from the amount due to the Successful Bidder and pay to the concerned tax authority directly.

Annexure A: Confirmation of Terms and Conditions

The General Manager
Strategy & IT
Corporate Headquarters
Jammu & Kashmir Bank MA Road, Srinagar

Dear Sir,

Sub: RFP/SLTE No for Selection of Service Provider for ATM/Debit Switch & Debit Card Management System (DCMS) on hosted model, dated

Further to our proposal dated, in response to the **Request for Proposal for Selection of Service Provider for ATM/Debit Switch & Debit Card Management System (DCMS) on hosted model**(hereinafter referred to as “RFP/SLTE”) issued by Jammu & Kashmir Bank (J&K BANK) we hereby covenant, warrant and confirm as follows:

We hereby agree to comply with all the terms and conditions / stipulations, payment terms, scope, SLAs etc. as contained in the RFP/SLTE and the related addendums and other documents issued by the Bank.

Place:

Date: Seal and signature of the bidder

Annexure B: Tender Offer Cover Letter

The General Manager
Strategy & IT
Corporate Headquarters
Jammu & Kashmir Bank M.A Road, Srinagar

Dear Sir,

Sub: RFP/SLTE no: _____ for Selection of Service Provider for ATM/Debit Switch & Debit Card Management System (DCMS) on hosted model dated _____

Having examined the tender documents including all annexures the receipt of which is hereby duly acknowledged, we, the undersigned, offer **ATM/Debit Switch & Debit Card Management System (DCMS) on hosted model** to Bank as mentioned in RFP/SLTE document in conformity with the said tender documents in accordance with the Commercial bid and made part of this tender.

We understand that the RFP/SLTE provides generic specifications about all the items and it has not been prepared by keeping in view any specific bidder.

We understand that the RFP/SLTE floated by the Bank is a confidential document and we shall not disclose, reproduce, transmit or made available it to any other person.

We have read, understood and accepted the terms/ conditions/ rules mentioned in the RFP/SLTE, proposed to be followed by the Bank.

Until a formal contract is prepared and executed, this tender offer, together with the Bank's written acceptance thereof and the Bank's notification of award, shall constitute a binding contract between us.

We undertake that in competing for and if the award is made to us, in executing the subject Contract, we will strictly observe the laws against fraud and corruption in force in India and the UT of J&K.

We have never been barred/black-listed by any regulatory / statutory authority in India.

We understand that the Bank is not bound to accept the lowest or any offer the Bank may receive.

This Bid, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract between us.

We certify that we have provided all the information requested by the Bank in the format requested for. We also understand that the Bank has the exclusive right to reject this offer in case the Bank is of the opinion that the required information is not provided or is provided in a different format.

Page **66** of **154**

It is also confirmed that the information submitted is true to our knowledge and the Bank reserves the right to reject the offer if anything is found incorrect.

Place:

Date:

Seal and signature of the bidder

Annexure C: Details of Bidder

Details filled in this form must be accompanied by sufficient documentary evidence, in order to facilitate the Bank to verify the correctness of the information.

S. No.	PARTICULARS	DETAILS
1	Name of the Company	
2	Postal Address	
3	Telephone / Mobile / Fax Numbers	
4	Constitution of Company	
5	Name & Designation of the Person Authorized to make commitments to the Bank	
6	Email Address	
7	Year of Commencement of Business	
8	Sales Tax Registration No	
9	Income Tax PAN No	
10	Service Tax / GST Registration No	
11	Whether OEM or System Integrator	
12	Name & Address of OEM/s.	
13	Brief Description of after sales services facilities available with the SI/OEM	
14	Web Site address of the Company	

Date:

Seal and signature of the bidder

Annexure D: Compliance to Eligibility Criteria

The bidder needs to comply with all the eligibility criteria mentioned below. Non-compliance to any of these criteria would result in outright rejection of the Bidder's proposal. The bidder is expected to provide proof for each of the points for eligibility evaluation criteria. Any credential detail not accompanied by required relevant proof documents will not be considered for evaluation. All credential letters should be appropriately bound, labelled and segregated in the respective areas. There is no restriction on the number of credentials a bidder can provide.

The decision of the Bank would be final and binding on all the Bidders to this document. The Bank may accept or reject an offer without assigning any reason what so ever.

The bidder must meet the following criteria to become eligible for bidding:

S.No.	Eligibility Criteria	Supporting Documents to be submitted	Compliance (Y/N)
1.	Bidder should be a Registered Private/Public Limited Company in India as per Indian Companies Act, 1956 or Indian Companies Act, 2013 having its legal existence in India for the last 5 years	Bidder to submit - Certified copy of the registration certificate	
2.	Bidder should be in business of providing ATM Driving, Switching & Debit card processing services on hosted platform from the last 5 years in India	Bidder to submit self-attested letter	
3.	Bidder must be certified and possessing a valid PCI-DSS, PCI-SSF & ISO 27001 Certifications.	Bidder to submit certified copy of the PCI-SSF, PCI DSS & ISO27001	
4.	The Bidder's hosted Switch should have currently interfaced with Visa, MasterCard, NFS and RuPay	Bidder to submit self-declaration on company letterhead and relevant documents wherever applicable.	
5.	Visa, MasterCard & Rupay gateways must be hosted in the same environment from where bidder is offering switch solution	Bidder to submit self-declaration on company letterhead	
6	Bidders proposed solution should be currently live with at least two scheduled commercial Banks in India providing ATM driving, Debit Card Management System and Switching services.	Copy of the purchase / work order and Certificate/ Letter (Signed by by Authorized Signatory) of satisfactory completion and management of the work including product, integration & running successfully, by the authorized official of the Bank served.	

7.	<p>The Bidder should have both primary Data Center and DR center in India (Tier III and above or Rated 4) located within different seismic zones, with full back up arrangement and the Data Center should be ISO 27001 certified.</p> <p>The bidder shall comply with the storage of Payment Data norms issued by RBI.</p>	Copy of relevant certificate / Documentary proofs to be submitted.	
8.	The bidder should be "OEM or authorized partner/ License holder of the proposed solution offering for ATM driving switch & Debit card Management system.	Copy of relevant certificate / OEM Authorization Letter/ Documentary proofs to be submitted.	
9.	Bidder should be having an annual turnover of minimum 400 crores, for the past 3 years	Bidder to submit letter from statutory auditor	
10.	The bidder should have 24x7 operations team to manage the proposed solution	Bidder to submit self-declaration on company letterhead	
11.	The bidder should be currently managing and driving minimum of 5,000 ATMs on the proposed Hosted Solution.	Copy of the purchase / work order and Certificate/ Letter of satisfactory completion and management by the authorized official of the Bank served.	
12.	The bidder must be currently hosting a minimum of 80 Lacs Debit/Prepaid cards from the proposed hosted DCMS solution.	Copy of the purchase / work order and Certificate/ Letter of satisfactory completion and management by the authorized official of the Bank served.	
13.	The bidder must have experience of migrating at least two scheduled commercial banks under hosted model.	Copy of the purchase / work order and Certificate/ Letter of satisfactory completion and management by the authorized official of the Bank served.	
14.	ATM driving solution should support multivendor solution and bidder should have licence of the proposed multivendor solution.	Bidder to submit self-declaration on company letterhead.	
15.	The bidder should provide VISA/MasterCard/NPCI Connectivity to the Bank through its own/hosted Connectivity.	Self-Declaration along with relevant details on bidder's letter head	
16.	Bidder must warrant that key project personnel (solution experts) are deployed in this project who have been	Self-Declaration along with relevant details on bidder's letter head	

	involved in similar projects in last two years.		
17.	The Bidder to provide an undertaking on his letter head that all the technical requirements highlighted as part of Technical Scope are covered in totality in the proposal submitted by the bidder.	Self-Declaration along with relevant details on bidder's letter head	
18.	The bidder should not be involved in any Bankruptcy filing or for protection from it.	Undertakings from the bidder in this regard should be enclosed.	
19.	The Bidder should not be blacklisted/ debarred /banned by Government / Government agency / Banks / Financial Institutions / PSUs in India as on bid submission date.	Undertakings from the bidder in this regard should be enclosed.	
20.	The Bidder should not be involved in any legal case that may affect the solvency / existence of firm or in any other way affect the bidder's Capability to provide / continue the services to Bank.	Self-declaration confirming the Criteria.	
21	Bidder must provide information that any of its subsidiary or associate or holding company or companies having common director/s or companies in the same group of Promoters/ management or partnership firms/LLPs having common partners have not participated in the bid process.	Letter of confirmation on company letter head duly signed by authorized official to be submitted	

Please enclose documentary proof for all the above criteria. In absence of these, the bids will not be considered for further evaluation. No further correspondence will be entertained in this case. The Bank reserves the right to verify/evaluate the claims made by the vendor independently. Any misrepresentation will entail rejection of the offer.

1. Bidders need to ensure compliance to all the eligibility criteria points.
2. Purchase orders without relevant organization confirmation through a credential letter will not be considered as credentials.
3. Documentary evidence must be furnished against each of the above criteria along with an index. All documents must be signed by the authorized signatory of the Bidder. Relevant portions, in the documents submitted in pursuance of eligibility criteria, should be highlighted.
4. Bank shall not consider the bids of bidders having poor or unsatisfactory past experience in execution or providing support to any project in past.
5. Providing any wrong information by the bidder will result in disqualification of the bidder. The Bank may cross check above parameters by any means / during site visit.
6. All Annexures must be on the letter head of the Bidder, except those which are to be provided by OEM/CA/third party.

7. All third party documents must be signed by their authorized signatory and his/her designation, Official E-mail ID and Mobile no. should also be evident. Bidder is also required to substantiate whether the person signing the document is authorized to do so on behalf of his company.

Annexure E: Technical Bid Format

S.No	Proposal Bid Evaluation	Evaluation Parameters	Max Marks
1	The number of Implementations of proposed solution carried out in India (during the last 5 years as on date of issuance of RFP/SLTE).	2 Implementations -10 Marks 3-4 Implementations -12 Marks >4 Implementations -15 Marks	15 Marks
2	Number of Scheduled Commercial Bank (SCB) currently live on the proposed Debit Card solution on hosted model, in India	2 SCB: 10 marks 3-4 SCB: 12 marks More than 4 : 15 marks	15 Marks
3	Total Number of Active Debit Cards being managed on Hosted Model	80 lacs upto 1 Crore : 10 marks Above 1 crore to 1.2 Crore : 12 marks Above 1.2 Crore to 1.5 Crore: 15 marks Above 1.5 crore cards: 20 marks.	20 Marks
4	Total transactions currently being processed on the proposed hosted solution per month.	50 Lacs to 1 crore transactions: 10 marks Above 1 crore upto 2 crore: 12 marks Above 2 crore upto 3 crore: 15 marks Above 3 Crore : 20 marks	20 Marks
5	Total number of Debit Card Solution and Switch Migrations handled by Bidder on hosted model for Scheduled Commercial Bank in India	2 migration: 10 marks 3-4 migration: 15 marks Above 4 migrations: 20 marks	20 Marks
6	Techno Functional Requirements	Techno Functional Requirement (As per Annexure E1) Total marks shall be converted to equivalent of 30 marks	30 Marks
7	Solution Features and Capability/Product Demonstration/Technical Presentation/ Project Team Experience.	Committee Evaluation	50 Marks
8	Feedback from existing clients (References to be provided by bidder)Either through mail/on-site visit/ remotely as per banks discretion.	Committee Evaluation Excellent=20 Good=15 Average=10 Poor=5 Very Poor=0	20 Marks
9	Compliance to Hosting Assessment Checklist	As per Annexure N (Total marks shall be converted to equivalent of 10 marks)	10 Marks
		Total	200 Marks

We hereby confirm that our proposed Solution meet all the specifications as mentioned above and have submitted the supporting documents against each point claimed. The bank reserves the right to ask the bidder to furnish any such document as required during technical evaluation.

Signature and Seal of Company

Annexure E1: Techno Functional Requirements

Bidder is required to provide compliance as shown in below table, against each specification mentioned in below sections. The bidder has to do self-evaluation, provide compliance response and assign marks accordingly. The symbols and their description can be referred as follows:

S.No.	Description	Symbol	Marks
1	Available as a part of solution / readily available (The feature is already supported and included in the out-of-the-box solution)	A	3
2	Will be provided as customization (Can be developed / customized and delivered along with the solution, prior to go-live at no extra cost.)	C	2
3	Will be provided as Integration (This capability can be provided by integrating with other systems / service providers)	I	1
4	Not Feasible / Not Supported / Unavailable (This capability is neither supported nor available with this Solution.)	N	0

S.No	Feature/Requirement	Bidder's Response (A/C/I/N)	Bidder's Comment
A-Architecture and Technology			
	Solution should offer following deployment models:		
1	a) On-Premise deployment at bidder's Data Center and Disaster Recovery		
2	b) Solution should support Cloud deployment		
3	c) Hybrid Cloud		
	Proposed solution should support following deployment capabilities:		
4	Active-Passive setup across DC-DR		
6	Proposed solution must have microservices based architecture		
7	Proposed Switch Solution should be cloud native.		
	Proposed solution must be agnostic to following:		
8	a) Hardware		
10	b) Operating System		
11	c) Database		
12	Solution should provide higher uptime on commodity hardware (such as x86) and databases such as MySQL, PostGreSQL, MariaDB in addition to Oracle		
13	Switch should not have "business downtime" during general upgrades such as OS patch, security patch,		

	hardware memory etc. Customer transactions should continue to process.		
14	The system architecture should be modular and solution should also allow high scalability, by adding capacity to the current environment (vertical and horizontal)		
15	Proposed solution should have benching marking report of minimum 3000 TPS, share the bench-mark report.		
B-ATM Driving and Switch Solution			
B1-Switch Solution			
16	Bidder's Switch Solution must be PCISSS / SSF certified		
17	Bidder must be ISO27001 certified		
18	Bidder must be ISO22302 certified		
19	Bidder hosting environment must be PCIDSS certified.		
20	Solution should be compliant to all existing regulatory guidelines GOI/IBA/RBI/NPCI etc.		
21	Solution should be compliant with standards and guidelines issued by major interchanges such as Rupay, VISA, MasterCard		
22	Should support EMV (Chip & PIN) compliant with contact and contact-less, for ATM Transactions		
23	Should be AES compliant		
24	Should support message level encryption for entire or select critical elements in the message such as PIN, Track Data etc.		
25	Transaction Security - The system should support measures such as PIN Verification, AES Encryption, Key Management, MACing, Key encryption		
26	Solution should provide capabilities to enable biometric, Secure PIN Based and similar industry standard modes of authentication.		
27	Switch must handle Message Level Interface and should support all Industry standards message formats like ISO 8583, XML, Restful, ISO20022 etc.		
28	The bidder's data centers must be in India and should explain its DC and DR site Architecture in detail		
29	Should regularly update interchange BIN routing tables list (VISA, MasterCard, Rupay etc.)		
30	Should support instant Refresh of balances from the host to the Switch online, if bank decide to support stand-in transactions		
31	Should maintain switch data for at least 15 years in an easily retrievable form		
32	All transactions should be identified by a unique transaction id.		
33	The solution should have capability to provide feed to bank's data ware house system, if and when bank is ready with the same		

34	Maintain logs and offer report of all transactions coming in and going out of the Switch, including the application messages and communication messages without impacting on the performance at peak load condition		
35	Switch should have capabilities to offer seamless support and integration capabilities for Card Not Present (CNP)		
36	Online addition of New ATM/Recycler without bringing down the System / Switch network		
37	Proposed solution should provide multi-institutional and configurable business logic		
38	Solution should provide for dynamic generation of terminal session key		
39	System should automatically generate Daily transaction reports based on the scheduled time and should have the capability to export the same in CSV/xls/xlsx/xml/text, etc.		
40	Switch should have capability to drive all standard ATMs including DIEBOLD,NCR, Wincor, Hitachi,OKI etc		
41	Solution should support all leading brands of ATM and Cash recycler		
42	The system should support ATM access fee based on Terminal ID, ATM Location, BIN, Country Code, etc		
43	The solution should have a strong Management information facility - instead solution should provide real-time interface to send information data ware housing solution for generation of MIS, adhoc reports regulatory reports on faster TAT basis		
B2-ATM Driving			
44	Solution should support all leading brands (viz AGS, OKI, NCR, Hitachi, Diebold) of ATM and Cash recycler over native protocols as well as Multi-vendor Standard in same application		
45	Solution must provide processing of Card & PIN as well as biometric based ATMs with NDC/NDC+ / DDC message formats		
	Services through ATMs:		
46	Cash Withdrawal along with display of available denominations.		
47	ICCW		
48	Balance Enquiry		
49	Fast Cash		
50	Mini Statement;		
51	MBank Registration		
52	PIN Change and Green pin module		
53	Aadhaar seeding		
54	Debit Card Limit and Service Management Module.		
	Services for CRMs:		

55	Cash withdrawal; Balance Enquiry (with card)		
56	Cash Deposit (with and without card)		
57	PIN Change (with card); Green Pin		
58	Mini Statement (with card)		
59	Transactions without Card-ICD and ICCW		
60	Should be able to monitor and report status of Host, ATMs, CRMs, and all interfaces.		
61	Proposed solution must support Multi-vendor Solution (MVS) capability for ATM driving.		
62	ATM driving capability should support NDC / DDC as well as XFS based communication with the devices.		
63	For MVS, ATM driving solution must provide real time EJ. EJ must be available for download as soon as transaction on bank's ATM is completed.		
64	Solution must have capability to download ATM transaction details from front end GUI.		
65	ATM driving solution must allow fetching Technical logs from ATM Terminal.		
66	Capabilities to allow Addition/Deletion/Modification of ATM/CRM screen flow & its contents centrally		
67	Should be able to centrally manage ATM Terminals like pushing screens or sending/executing update packages		
68	Bank must be able to send commands to the terminals using web based GUI or schedule the command to a certain date or time.		
69	Bank should be able to define Dynamic TPK refresh interval based on number of transactions or number of minutes/hours.		
70	Proposed solution should allow Bank to define cash-in or cash-out cassettes along with denominations for a specific terminal.		
71	Web based GUI in UAT/DC/DR env for ATM Monitoring based on: - Various Terminal components (status of Card Reader/Dispenser/Retain BIN etc.) - Cash availability on cassettes - Transaction search - Others as per bank requirement.		
72	Solution should provide detailed Audit report.		
73	Provide feed to bank's ATM managed services vendor for them to perform ATM monitoring and incident related activities		
74	Cash Management & Forecasting , Cash replenishment tracking		
C-Security control			
75	Solution should support configurable security controls over specific users or group of users		

76	Data access should be controlled based on individual profiles/roles.		
77	Solution should provide for configuring privileges at user level and be able to set preferences based on rules/roles/groups- Role based access controls, entitlement reviews.		
78	Solution should provide reports with time-in, time- out of user from such device in ATM Switch database. Audit logs should be maintained and made available for the bank in case of need		
79	Solution should provide adequate reports for these controls and should provide report/ alert on unauthorized access		
80	Should have maker/checker concept implemented		
81	Audit Logs for any user, parameter, and configuration changes. Access logs for minimum 3 yrs or as per the Bank requirement.		
82	Solution must allow for “read-only” and “audit” roles in user permissions.		
83	Access control, privileges at user/group level, login/audit reporting		
84	Two-factor authentication, secure PIN, two-step device login		
85	Support for configurable user workflows, approval hierarchies		
D-Authorization and PIN Verification			
86	Capable of handling minimum 16-digit to 19-digit card number (PAN) presently and any further variations introduced by VISA, MasterCard, NPCI and any other payment system association, etc.		
87	PIN number to be supported should be in the range of 4 to 11 digits		
88	Support for PIN verification using Hardware Security Modules		
89	Should be configurable with Host/Interchange for Authorization/PIN verification		
90	Admin Card Generation and Admin card PIN verification for ATMs, CRMs and other channels wherever necessary		
91	System should validate transactions allowed for the specific card / card type and linked account.		
92	Setting up separate limits & velocity at a Transaction level		
93	Capability to setup limits based on channel of initiation, country, online limits, off-line limits, scripts to control limits based on product needs - Daily/monthly/per transaction limit on amount and frequency		

94	Personalized card limits by cardholder for withdrawal, purchase transactions.		
95	Key Management for Dynamic (master/slave) and constant key DES, with support for dynamic key exchanges based on time, date, transaction volume		
96	Verification of the validity of the card (whether active or Inactive)		
97	Expiration date verification		
98	Checking for Hot listed or Closed cards		
99	Supports Card verification by Host / Interchange		
	Value Add Services:		
100	a) Solution must support numberless cards and vanity card numbers		
101	b) Solution must support network tokenization and must be live with Applepay, Samsungpay...etc		
102	c) Solution must give option to customer to select card image if customer wants to convert virtual card to physical card		
103	Solution should support push provisioning for Rupay MasterCard, VISA, etc.		
104	System should support following mechanisms for authorization control:		
105	PIN		
106	CVV/CVC, CVV2/ CVC2/ ICVV		
107	ARQC/ ARPC		
108	Expiration date		
109	Check Digit		
110	Personalized card limits by cardholder for withdrawal & POS transactions.		
E-Transaction Routing			
111	Offer reliable and flexible routing schemes to support flow of transactions. The system should be capable enough to route online/offline transaction to different bank's host and network i.e. CBS, network providers, interchange, private interchange, billers, service providers, different Card Management System, etc based on different criteria, some of which are: <ul style="list-style-type: none"> • Card Number • BIN Number • Institute • Network ID etc 		
112	Supports Stand-in Authorization.		
113	All transactions authorized in stand-in-mode are to be stored and then forwarded to the host authorizer when it becomes available automatically.		
114	Routing of on-us transactions to the Bank's Core banking system as well as other partner banks, Routing of on-us/ off-us/VISA/MasterCard transactions to single or multiple hosts.		

115	Routing of off-us card ATM withdrawals (SMS Transactions) advice message to the bank's core banking system.		
116	Capability to interface with any card schemes provided by the Bank		
117	Routing of Onus POS transactions to Banks CBS		
F-Operational Security			
118	Mode to access the system should be through passwords to ensure that only authorized users gain access and 2FA shall be in place.		
119	Solution should provide for configuration of complex passwords using algorithms and special characters		
120	Option to set life for the password in the system for forcing the user to change it once it expires		
121	Password history is to be maintained and validated so that the same password is not continued by the user		
122	The user rights on the system should be definable so that a user can perform only those tasks, which are assigned to them.		
123	Switch solution should be capable of maintaining audit logs of each activity on the system. Audit Trail of all changes made in the application, system Parameter, user role change etc. with details like user name, IP address, date and time, module name etc.		
124	Type and nature of security checks should be configurable over & above what has been stated above.		
125	Solution should provide and retain audit logs of transactions throughout the system and each transaction should be uniquely identifiable in the system		
126	The solution should be capable to send alerts on changes in system parameters as per configurations		
G- Debit Card Management System			
G-1 DCMS Features			
127	DCMS should be integral part of Switch solution		
128	Bidder must Provide GUI for DCMS access.		
129	All CMS functions including master setup, card lifecycle management, card control should be available on APIs		
130	System should be able to define multiple products using single BIN. 6 & 8 digit BIN should be defined in the system.		
131	Solution should support parameter definition at product level setup that can be overridden in the card level.		
132	DCMS should allow for Card Activation on the following events. a. Card Activation at the time of card issuance b. Card Activation on first successful transaction		
133	Renewal/Re-issue/Replacement a. Support Card Replacement/re-issue		

	b. Support both Manual and Automatic card renewal functionality for existing cards in the database. c. One to one and bulk functionality to be supported.		
134	Should have a Rule Engine through GUI which shall allow applying of rules easily on at card level for MCC, Merchant, Country, Transaction Code etc		
G2-Card Issuance			
135	Card and Client data Capture: a. Manual Data Entry: System should support manual entry of new card data and should generate card number for that customer. b. Card File Upload (File received from HOST), The system can upload customer information given in batch upload format into DCMS. Card and Account linkage records will be created based on the file. c. Bulk Card: DCMS to support batch option to generate cards in bulk		
136	Besides batch upload for new card creation, system to also support batch upload for modification of existing data and deletion of existing data in bulk.		
137	Card Production: DCMS should provide a batch operation for the generation of embossing files for the cards newly produced/replaced.		
138	PIN Production/Generation: a. Support PIN generation using HSM b. Support Green PIN option		
G3-Card Maintenance activities			
139	Restoration of backups for providing switch logs relating to transactions beyond 120 days for addressing customer complaints or as required by the Bank.		
140	Generating embossa for Admin Cards for terminals		
141	Monitor the status of ATMs for Link down, Cash out, Cash Handler/ Dispenser problems, Card reader issues etc		
142	Preparation of terminals down/Cash out status report for updating to Bank officials		
143	Sending ATM/CRM Downs/Cash Out report to Bank		
144	DCMS to support same card number or new card number for renewal		
145	Auto renewal/manual renewal option for existing cards on the database.		
146	Hot Listing of card ;		
147	Un-blocking of temporary blocked Card.		
148	Card Closure changes the status of the card to closed status.		
149	Attaching/removing accounts to a card.		
150	Ability to close the debit cards of the accounts that have been closed by the customers automatically.		
151	Any other related feature as required by the Bank.		

G4-Limit Checks			
152	The system should have the capability to set up Various Limits [offline, per transaction, per day, daily, monthly at the Product Level that can be overridden at card level if bank wishes to alter the product level limit for certain cards.		
153	It should be able to setup Domestic and International Limit		
154	System to allow setup of Transaction Limit control by MCC code; Merchant based. Geo location etc.		
155	It should have the capability to configure channel wise transaction limit.		
156	System should have a capability to configure VIP profile for specific users		
157	Allow temporary enhancement of any card product limit for a specified time and automatic restoration of the limits on expiry of specified date.		
158	Solution should allow monthly and annual capping on international usage of debit cards.		
H-Interface to Bidder Solution			
	Bidder should be able to integrate with :		
159	CBS		
160	Bank FRM		
161	Internet Banking		
162	Mobile Banking		
163	Financial Inclusion Gateway		
164	IVR		
165	Email and SMS Gateway		
166	Whatsapp Banking		
167	Bank UPI		
168	ACS		
169	Branch Portal		
170	CRM		
171	Credit Card, POS		
172	UDIR		
173	eNACH		
174	KYCAML		
175	Interchanges/Schemes		
176	SI Hub		
177	Support for Micro ATMs :		
178	Balance Inquiry; Mini Statement		

179	Support transactions with PIN,OTP, Biometric- IRIS, Face Authentication based transactions		
180	PIN Change, Reset.		
181	Interface with FI solution for MATM transactions		
182	Any other existing or new interface as per Banks requirement		
I-Technical Support			
183	Monitoring the health of the ATM Switch, DCMS and Terminals.		
184	Processor Status Monitoring		
185	System Cut Over Monitoring		
186	System Backup - Daily, Weekly & Monthly		
187	Monitoring the status of various host stations and interchanges integrated with ATM Switch and coordinating with respective entity for problem resolution in case of any issues		
188	Configuring new processes depending on the increase in transaction volume without bringing Switch down		
189	Addition/Deletion/Modification of ATM/Host Configurations.		
190	Generation of Embossa for Card personalization/instant cards and printing of PINs/insta pins.		
191	Any other functionality as per the Bank's requirement.		
J-Monitoring			
192	GUI based with dashboard facility.		
193	Online status of ATM Terminals, and connectivity with interchanges, host, servers etc. connected to switch including reason in case of down/ problem in ATM and generation of alerts via SMS, email etc.		
194	Online status of different components of Switch application like processes, interfaces nodes, etc.		
195	Hardware performance monitoring like CPU, memory, Disk I/O, other performance parameters etc.		
196	Provision for defining the thresholds for different parameters.		
197	The system should be able to provide history of ATM status and should be able to generate and export report whenever and wherever necessary		
198	Dashboard for Transaction monitoring with customizable filters.		
199	Graphical representation/Report generation of technical/business declines for ATM transactions/ debit card transactions for customized time intervals.		
K-Reconciliation			
200	Solution shall seamlessly integrate with Banks existing Recon solution.		

201	The Solution shall also facilitate end to end reconciliation, chargeback and Dispute management in case Banks wishes to use it.		
L-MIS / Reporting			
202	Solution must provide MIS that can be customized in future as per bank requirement.		
203	MIS portal must be accessible to the Bank and also automatically share reports with bank on daily basis		
204	Solution should be able to provide reports in standard formats such as xls/xml/csv, etc.		
	Solution should be able to generate any related reports but not limited to:		
205	Daily Institution/Interchange/Network Settlement Report		
206	Daily Transactions Log report		
207	Daily TLF/PTLF Extract		
208	Daily Report on Reversal Transactions sent to Host.		
209	ATM down-time summary		
210	ATM down-time detail		
211	Cash position of ATMs - cassette wise		
212	Cash dispensed by ATMs - cassette wise		
213	Admin transactions reports		
214	Admin dispense vs Cash available report		
215	Reports on financial, non-financial and reversal/suspected transactions.		
216	Report of unsuccessful transactions with reasons for failure		
217	Location-wise transaction report		
218	Terminal-wise transaction report		
219	Report on income earned through interchange		
220	Usage by customer type (Onus Vs Offus)		
221	Similar reports are to be provided for Cash Recycler, issuing transactions or any other transactions that are processed through the vendors switch.		
222	Monthly Reports - ATMs average hits report on monthly basis		
223	Monthly Reports - ATMs hits analysis report covering financial/non-financial hits, cash disbursed, our bank vs other bank transactions, income earned by the ATM etc		
224	Monthly Reports - ATM Down time percentage		
225	Monthly Reports - ATM Down time details		
226	Monthly Reports - Down time analysis basing on reasons for downtime		
227	Monthly Report - Card Base		

228	Monthly Report - Migration of current reports and generation of new reports as per banks requirement.		
229	Solution must provide Interchange reports transaction wise.		
230	Any other reports as per the Banks requirement.		

Annexure F: Commercial Bid Format

1. Please be guided by RFP/SLTE terms, subsequent amendments and replies to pre-bid queries (if any) while quoting.
2. No counter condition/assumption in response to commercial bid will be accepted. Bank has a right to reject such bid.

The Commercial Bid shall be submitted in the following format:

Description	Unit Price	Multiplication Factor (Tentative Qty)	Amount
One time cost for end to end switching, debit card management system and ATM Driving -DC and DR (Implementation, Customization, Integration, Migration, Testing, Go-live, post go live support etc).	a	1	A=a
Monthly Card Hosting Fee per Active Debit Card <i>* Active cards means all cards excluding expired, hot listed, temporary blocked, unacknowledged, Not yet issued etc.</i>	b	55,00,000 Cardsx5 Yearsx12 months	B=bx55,00,000x5x1 2
Financial Transaction processing Fee Per Transaction (switching and debit card management system with 24x7 support)	c	10,00,00,000 Txns x5 Years	C=cx10,00,00,000x 5
Non-Financial Transaction processing Fee Per Transaction (switching and debit card management system with 24x7 support)	d	5,00,00,000 Txns x 5 Years	D=dx5,00,00,000x 5
Monthly Charges per ATM for ATM Driving with 24x7 support.	e	1600 ATM/CRM x 5 Yearsx12 months	E=ex1600x5x12
Monthly Scheme connectivity Fee (DC & DR) for Visa, Mastercard and NPCI.	f	12monthsx5 Years	F=fx12x5
Manday cost for any additional Bank specific Customizations (other than Regulatory/Association mandates) in addition to the scope mentioned in the RFP/SLTE	g	100 Mandays	G=gx100
Total Cost for 5 Years			A+B+C+D+E+F+G

The quantity mentioned is tentative and is calculated on current yearly average for calculation purpose only, actual numbers may vary during the contract period.

Annexure G: Bank Guarantee Format

Bank Guarantee No: _____

Dated: _____

Bank: _____

To

**Jammu & Kashmir Bank M.A. Road, Srinagar,
190 001 J&K.**

WHEREAS..... (Company Name) and having its Registered Office at..... India (hereinafter referred to as “the Bidder”) proposes to respond to RFP/SLTE No, dated of Jammu and Kashmir Bank Ltd for **Selection of Service Provider for ATM/Debit Switch & Debit Card Management System (DCMS) on hosted model** (Herein after called the “RFP/SLTE”) AND

WHEREAS, in terms of the conditions as stipulated in the RFP/SLTE, the bidder is required to furnish a Bank Guarantee in lieu of the Earnest Money Deposit (EMD), issued by a scheduled commercial bank in India in your favour to secure the order under the RFP/SLTE Document (which guarantee is hereinafter called as “BANK GUARANTEE”) AND WHEREAS the bidder has approached us, for providing the BANK GUARANTEE.

AND WHEREAS at the request of the bidder and in consideration of the proposed RFP/SLTE to you, We ,.....having Branch Office/Unit amongst others at....., India and registered office/Headquarter at.....have agreed to issue the BANK GUARANTEE.

THEREFORE, We,....., through our local office at..... India furnish you the Bank GUARANTEE in manner hereinafter contained and agree with you as follows:

1. We....., undertake to pay the amounts due and payable under this Guarantee without any demur, merely on demand from you and undertake to indemnify you and keep you indemnified from time to time to the extent of Rs.....(Rupeesonly) an amount equivalent to the EMD against any loss or damage caused to or suffered by or that may be caused to or suffered by you on account of any breach or breaches on the part of the bidder of any of the terms and conditions contained in the RFP/SLTE and in the event of the bidder commits default or defaults in carrying out any of the work or discharging any obligation in relation thereto under the RFP/SLTE or otherwise in the observance and performance of any of the terms and conditions relating thereto in accordance

with the true intent and meaning thereof, we shall forthwith on demand pay to you such sum or sums not exceeding the sum of Rs.....(Rupees..... only) as may be claimed by you on account of breach on the part of the bidder of their obligations in terms of the RFP/SLTE. Any such demand made on the Bank shall be conclusive as regards amount due and payable by the Bank under this guarantee.

2. Notwithstanding anything to the contrary contained herein or elsewhere, we agree that your decision as to whether the bidder has committed any such default or defaults and the amount or amounts to which you are entitled by reasons thereof will be binding on us and we shall not be entitled to ask you to establish your claim or claims under Bank Guarantee but will pay the same forthwith on your demand without any protest or demur.
3. This Bank Guarantee shall continue and hold good until it is released by you on the application by the bidder after expiry of the relative guarantee period of the RFP/SLTE and after the bidder had discharged all his obligations under the RFP/SLTE and produced a certificate of due completion of work under the said RFP/SLTE and submitted a “ No Demand Certificate “ provided always that the guarantee shall in no event remain in force after the day ofwithout prejudice to your claim or claims arisen and demanded from or otherwise notified to us in writing before the expiry of the said date which will be enforceable against us notwithstanding that the same is or are enforced after the said date.
4. Should it be necessary to extend Bank Guarantee on account of any reason whatsoever, we undertake to extend the period of Bank Guarantee on your request under intimation to the SI/OEM till such time as may be required by you. Your decision in this respect shall be final and binding on us.
5. You will have the fullest liberty without affecting Bank Guarantee from time to time to vary any of the terms and conditions of the RFP/SLTE or extend the time of performance of the RFP/SLTE or to postpone any time or from time to time any of your rights or powers against the bidder and either to enforce or forbear to enforce any of the terms and conditions of the said RFP/SLTE and we shall not be released from our liability under Bank Guarantee by exercise of your liberty with reference to matters aforesaid or by reason of any time being given to the bidder or any other forbearance, act or omission on your part or any indulgence by you to the bidder or by any variation or modification of the RFP/SLTE or any other act, matter or things whatsoever which under law relating to sureties, would but for the provisions hereof have the effect of so releasing us from our liability hereunder provided always that nothing herein contained will enlarge our liability hereunder beyond the limit of Rs.....(Rupees.....only) as aforesaid or extend the period of the guarantee beyond the said day of unless expressly agreed to by us in writing.
6. The Bank Guarantee shall not in any way be affected by your taking or giving up any securities from the bidder or any other person, firm or company on its behalf or by the winding up, dissolution, insolvency or death as the case may be of the bidder

7. In order to give full effect to the guarantee herein contained, you shall be entitled to act as if we were your principal debtors in respect of all your claims against the bidder hereby guaranteed by us as aforesaid and we hereby expressly waive all our rights of surety ship and other rights, if any, which are in any way inconsistent with any of the provisions of Bank Guarantee.
8. Subject to the maximum limit of our liability as aforesaid, Bank Guarantee will cover all your claim or claims against the bidder from time to time arising out of or in relation to the said RFP/SLTE and in respect of which your claim in writing is lodged on us before expiry of Bank Guarantee.
9. Any notice by way of demand or otherwise hereunder may be sent by special courier, telex, fax or registered post to our local address as aforesaid and if sent accordingly it shall be deemed to have been given when the same has been posted.
10. The Bank Guarantee and the powers and provisions herein contained are in addition to and not by way of limitation of or substitution for any other guarantee or guarantees here before given to you by us (whether jointly with others or alone) and that Bank Guarantee is not intended to and shall not revoke or limit such guarantee or guarantees.
11. The Bank Guarantee shall not be affected by any change in the constitution of the bidder or us nor shall it be affected by any change in your constitution or by any amalgamation or absorption thereof or therewith but will ensure to the benefit of and be available to and be enforceable by the absorbing or amalgamated company or concern.
12. The Bank Guarantee shall come into force from the date of its execution and shall not be revoked by us any time during its currency without your previous consent in writing.
13. We undertake to pay to you any money so demanded notwithstanding any dispute or disputes raised by the bidder in any suit or proceeding pending before any court or Tribunal relating thereto our liability under this present being absolute and unequivocal.
14. The Bank Guarantee needs to be submitted in online form also via SFMS Application.
15. Notwithstanding anything contained herein above;
 - i. our liability under this Guarantee shall not exceed Rs.....(Rupees.....only) ;
 - ii. this Bank Guarantee shall be valid up to and including the date and claim period shall be upto_____ ; and
 - iii. We are liable to pay the guaranteed amount or any part thereof under this Bank Guarantee only and only if you serve upon us a written claim or demand on or before the expiry of the claim period.

16. We have the power to issue this Bank Guarantee in your favour under the Memorandum and Articles of Association of our Bank and the undersigned has full power to execute this Bank Guarantee under the Power of Attorney issued by the Bank.

For and on behalf of BANK

Authorized Signatory

Seal

Address

Annexure H: Performance Bank Guarantee Format

To
Jammu & Kashmir Bank M.A. Road, Srinagar,
190 001 J&K.

WHEREAS..... (Company Name) registered under the Indian Companies Act 1956 and having its Registered Office at, hereinafter referred to as the Bidder has for taken up for **ATM/Debit Switch & Debit Card Management System (DCMS) on hosted model** in terms of the Purchase Order bearing No..... Dated, hereinafter referred to as the Contract. And Whereas in terms of the Conditions stipulated in the said Contract, the bidder is required to furnish, performance Bank Guarantee issued by a Scheduled Commercial Bank in your favor to secure due and satisfactory compliance of the obligations of the Bidder in accordance with the Contract; Therefore, We,, through our local office at Furnish you this Performance Guarantee in the manner hereinafter contained and agree with you as follows:

1. We,do hereby undertake to pay the amounts of ₹ and payable under this Guarantee without any demur, merely on a demand, which has to be served on us before the expiry of this guarantee, time being essence of the contract, from you stating that the amount claimed is due by way of loss or damage caused to or would be caused to or suffered by you by reason of breach by the said Bidder of any of the terms and conditions contained in the Contract or by reason of the vendor's failure to perform the said contract. Any such demand made on us within the time stipulated above shall be conclusive as regards the amount due and payable by us under this guarantee. However, our liability under this guarantee shall be restricted to an amount not exceeding..... (Rupees Only).
2. We undertake to pay to you any money so demanded notwithstanding any dispute/s raised by the Bidder in any suit or proceeding before any Court or Tribunal relating thereto, our liability under these presents being absolute and unequivocal. The payment so made by us under this guarantee shall be a valid discharge of our liability for payment there under and the Bidder shall have no claim against us for making such payment.
3. We further agree that, if demand, as stated above, is made on us within the stipulated period, the guarantee herein contained shall remain in full force and effect and that it shall continue to be enforceable till all your dues under or by virtue of the said contract have been fully paid and your claims satisfied or discharged or till you certify that the terms and conditions of the said contract have been fully and properly carried out by the said Bidder and accordingly discharge this guarantee. Provided, however, serving of a written claim / demand in terms hereof on us for payment under this guarantee on or before the stipulated

period , time being the essence of contract, shall be a condition precedent for accrual of our liability / your rights under this guarantee.

4. We further agree with you that you shall have the fullest liberty without our consent and without affecting in any manner our obligations hereunder, to vary any of the terms and conditions of the said Contract or to extend time for performance by the said vendor from time to time or to postpone for any time or from time to time any of the powers exercisable by us against the said Bidder and to forbear or enforce any of the terms and conditions relating to the said Contract and we shall not be relieved from our liability by reason of such variation, or extension being granted to the said Vendor or for any forbearance, act or omission on our part or any indulgence by us to the said Bidder or by any such matter or thing whatsoever which under the law relating to sureties would, but for this provision, have effect of so relieving us.

5. This Guarantee will not be discharged due to the change in the constitution of our Bank or the Bidder

6. We further agree and undertake unconditionally without demur and protest to pay you the amount demanded by you in writing irrespective of any dispute or controversy between you and the Bidder

7. We lastly undertake not to revoke this guarantee during its currency except with your written Consent. Notwithstanding anything contained herein above;
 - (i) Our liability under this Guarantee shall not exceed.....Rupees.....
..only);

 - (ii) This Guarantee shall be valid up to; and claim period of this Bank Guarantee shall be year/s after expiry of the validity period i.e., up to.....; and

 - (iii) We are liable to pay the guaranteed amount or any part thereof under this Bank Guarantee only and only if you serve upon us a written claim or demand on or before the expiry of the claim period.

Dated the..... Day of2026.

For.....

BANK Authorized Signatory

[Annexure I: Non-disclosure Agreement \(NDA\)](#)

THIS NON DISCLOSURE AGREEMENT (the “Agreement”) is made and entered into as of (____/____/2026) by and between

_____, a company incorporated under the laws of India, having its registered address at _____ (the “Receiving party/Company”) and

“Jammu and Kashmir Bank Ltd, a Banking Company under Indian Companies Act,2013 having corporate and registered office at M.A.Road,Srinagar,J&K,India-190001 represented herein by Authorized Signatory (hereinafter referred as Bank/Disclosing Party which unless the context requires include its successors in interests and permitted assigns). (the “Bank/Disclosing Party”).

The Company/Receiving party and Bank/Disclosing Party are hereinafter collectively referred to as parties and individually as a party.

Whereas the parties have entered into contract and for performance of contract, the parties may share/disclose certain proprietary/confidential information to each other. To protect the confidentiality of the confidential information shared/disclosed, the parties hereto have entered into this NDA.

NOW THEREFORE THIS AGREEMENT WITNESSETH AS FOLLOWS:

1. Purpose J&K Bank/Disclosing Party has engaged or wishes to engage the Company/Receiving party for undertaking the project of **Selection of Service Provider for ATM/Debit Switch & Debit Card Management System (DCMS) on hosted model** and each party may disclose or may come to know during the course of the project certain confidential technical and business information which the disclosing party desires the receiving party to treat as confidential.

2. Confidential Information means any information disclosed or acquired by other party during the course of the projects, either directly or indirectly, in writing, orally or by inspection of tangible objects (including without limitation documents, prototypes, samples, technical data, trade secrets, know-how, research, product plans, services, customers, markets, software, inventions, processes, designs, drawings, marketing plans, financial condition and the Company’s plant and equipment), which is designated as “Confidential,” “Proprietary” or some similar designation. Information communicated orally shall be considered Confidential Information if such information is confirmed in writing as being Confidential Information within a reasonable time after the initial disclosure. Confidential Information may also include information disclosed to a disclosing party by third parties. Confidential Information shall not, however, include any information which

- i. was publicly known and made generally available in the public domain prior to the time of disclosure by the disclosing party;
- ii. becomes publicly known and made generally available after disclosure by the disclosing party to the receiving party through no action or inaction of the receiving party;
- iii. is already in the possession of the receiving party at the time of disclosure by the disclosing part as shown by the receiving party’s files and records immediately prior to the time of disclosure;

- iv. is obtained by the receiving party from a third party without a breach of such third party's obligations of confidentiality;
- v. is independently developed by the receiving party without use of or reference to the disclosing party's Confidential Information, as shown by documents and other competent evidence in the receiving party's possession; or
- vi. Is required by law to be disclosed by the receiving party, provided that the receiving party gives the disclosing party prompt written notice of such requirement prior to such disclosure and assistance in obtaining an order protecting the information from public disclosure.

3. Non-use and Non-disclosure. Each party agrees not to use any Confidential Information of the other party for any purpose except to evaluate and engage in discussions concerning a potential business relationship between the parties. Each party agrees not to disclose any Confidential Information of the other party to third parties or to such party's employees, except to those employees of the receiving party who are required to have the information in order to evaluate or engage in discussions concerning the contemplated business relationship. Neither party shall reverse engineer, disassemble, or decompile any prototypes, software or other tangible objects which embody the other party's Confidential Information and which are provided to the party hereunder.

4. Maintenance of Confidentiality. Each party agrees that it shall take reasonable measures to protect the secrecy of and avoid disclosure and unauthorized use of the Confidential Information of the other party. Each party shall take at least those measures that it takes to protect its own most highly confidential information and shall ensure that its employees who have access to Confidential Information of the other party have signed a non-use and non-disclosures agreement in content similar to the provisions hereof, prior to any disclosure of Confidential Information to such employees. Neither party shall make any copies of the Confidential Information of the other party unless the same are previously approved in writing by the other party. Each party shall reproduce the other party's proprietary rights notices on any such approved copies, in the same manner in which such notices were set forth in or on the original. Each party shall immediately notify the other party in the event of any unauthorized use or disclosure of the Confidential Information.

5. No Obligation. Nothing herein shall obligate either party to proceed with any transaction between them and each party reserves the right, in its sole discretion, to terminate the discussions contemplated by this Agreement concerning the business opportunity. This Agreement does not constitute a joint venture or other such business agreement.

6. No Warranty. All Confidential Information is provided by Bank as "AS IS." Bank/Disclosing Party makes no warranties, expressed, implied or otherwise, regarding its accuracy, completeness or performance.

7. Return of Materials. All documents and other tangible objects containing or representing Confidential Information which have been disclosed by either party to the other party, and all copies thereof which are in the possession of the other party, shall be and remain the property of the disclosing party and shall be promptly returned to the disclosing party upon the disclosing party's written request.

Receiving Party shall immediately return and redeliver to Disclosing Party/ Bank all tangible material embodying the Confidential Information provided hereunder and all notes, summaries, memoranda, , records, excerpts or derivative information deriving there from and all other documents or materials (“Notes”) (and all copies of any of the foregoing, including “copies” that have been converted to computerized media in the form of image, data or word processing files either manually or by image capture) based on or including any Confidential Information, in whatever form of storage or retrieval, upon the earlier of (i) the completion or termination of the dealings between the parties contemplated hereunder; (ii) the termination of the Master Agreement; or (iii) at such time as the Disclosing Party/ Bank may so request.

The receiving party shall destroy /dispose off the confidential information provided by the disclosing party together with its copies upon written request of the disclosing party, as per the directions issued by the disclosing party and such destruction shall be confirmed in writing by receiving party.

8. No License. Nothing in this Agreement is intended to grant any rights to either party under any patent, mask work right or copyright of the other party, nor shall this Agreement grant any party any rights in or to the Confidential Information of the other party except as expressly set forth herein.

9. Term. The Obligations of each receiving party hereunder shall survive even after this agreement except as provided herein above.

10. Adherence. The content of the agreement is subject to adherence audit by J&K Bank. It shall be the responsibility of the Company/Receiving party to fully cooperate and make available the requisite resources/evidences as mandated by J&K Bank Supplier Security policy.

11. Remedies. Each party agrees that any violation or threatened violation of this Agreement may cause irreparable injury to the other party, entitling the other party to seek injunctive relief in addition to all legal remedies.

12. Arbitration, Governing Law & Jurisdiction. In the case of any dispute arising upon or in relation to or in connection with this Agreement between parties, the disputes shall at the first instance be resolved through negotiations. If the dispute cannot be settled amicably within fourteen (14) days from the date on which either Party has served written notice on the other of the dispute then any party can submit the dispute for arbitration under Arbitration and conciliation Act,1996 through sole arbitrator to be appointed mutually by the parties.

The place of Arbitration shall be Srinagar, India and the language of the arbitration proceedings and that of all the documents and communications between the parties shall be English.

The decision of the arbitrator shall be final and binding upon the parties. The expenses of the arbitrator as determined by the arbitrator shall be borne equally.

The parties shall continue to be performing their respective obligations under this Agreement, despite the continuance of the arbitration proceedings, except for the disputed part under arbitration. This agreement shall, in all respects, be governed by, and construed in accordance with the Laws of the UT of J&K read with applicable Laws of India. The Courts in Srinagar India shall have exclusive jurisdiction in relation to this agreement.

All notices or other communication under or in connection with this agreement shall be given in writing and may be sent by personal delivery, or post or courier or facsimile or email. Any such notice or other communication will be deemed to be effective if sent by personal delivery, when delivered, if sent by post, five days after being deposited in the post office and if sent by courier, three days after being deposited with the courier, if sent by facsimile, when sent (on receipt of a confirmation of having been sent to correct facsimile number) and if sent by mail (on receipt of confirmation).

_____ (Contact details of Company/Receiving party)

General Manager (S&IT)
J&K Bank -Corporate Headquarters,
MA Road Srinagar, J&K

13. Miscellaneous. This Agreement shall bind and intended for the benefit of the parties hereto and their successors and assigns. This document contains the entire Agreement between the parties with respect to the subject matter hereof, and neither party shall have any obligation, express or implied by law, with respect to trade secret or propriety information of the other party except as set forth herein. Any failure to enforce any provision of this Agreement shall not constitute a waiver thereof or of any other provision.

Any provision of this Agreement may be amended or waived if, and only if such amendment or waiver is in writing and signed, in the case of amendment by each Party, or in the case of a waiver, by the party against whom the waiver is to be effective”.

The undersigned represent that they have the authority to enter into this Agreement on behalf of the person, entity or corporation listed above their names.

COMPANY NAME

Bank

By: _____

By: _____

Name: _____

Name: _____

Title: _____

Title: _____

Address: _____

Address: _____

Company Seal

Company Seal

Annexure J: Service Level Agreement

This Service Level agreement (“Agreement”) is made at Srinagar on thisday of2026 between

- i. “Jammu and Kashmir Bank Ltd, a Banking Company under Indian Companies Act,2013 having corporate and registered office at **M.A.Road,Srinagar,J&K,India-190001** represented herein by Authorized Signatory (hereinafter referred as Bank which unless the context requires include its successors in interests and permitted assigns) of the ONE PART, through its authorized signatory Mr.....

and

- ii. M/S, registered under the Act, having its Registered Office at (Hereinafter referred to as the "Successful Bidder" which expression shall unless it be repugnant to the context or meaning thereof, include its successors and assigns) of the OTHER PART, through its authorized signatory Mr.....

The Bank and Company are hereinafter collectively referred to as ‘Parties’ and individually as a ‘Party’.

Now therefore, this Agreement is witnessed as under:

Definitions of the terms

The Bank/J&K Bank:	Reference to the “the Bank”, “Bank” and “Purchaser” shall be determined in context and may mean without limitation “Jammu & Kashmir Bank”.
Bidder/Vendor/Successful Bidder/Company/ Service Provider :	An eligible entity/firm submitting a Proposal/Bid in response to this RFP/SLTE.
Proposal/Bid:	The Bidder’s written reply or submission in response to this RFP/SLTE.
SLA:	This document in its entirety, inclusive of any addenda that may be issued by the Bank.
The Contract:	The agreement entered into between the Bank and the Company, as recorded in this Contract Form signed by the

	parties, including all attachments and appendices thereto and all documents incorporated by reference therein.
The Contract Price:	The price payable to the Company under the Contract for the full and proper performance of its contractual obligations.
The Product:	All of the software or software, all hardware, database, middleware, operating systems and/or other materials which the Company is required to supply to the Bank under the Contract.
System:	A Computer System consisting of all Hardware, Software, etc., which should work together to provide the services as mentioned in the Bid and to satisfy the Technical and Functional Specifications mentioned in the Bid.
Specified Bank Location:	Banks Data Centre located at Noida and Banks Disaster Recovery Site Located at Mumbai.
PBG:	Performance Bank Guarantee.
Material Breach:	Company failure to perform a major part of this Agreement.
Charges:	Commercials as per Purchase Order.
Confidential Information:	It includes all types of Information that will be found on BANK systems that the Company may support or have access to including, but are not limited to, Information subject to special statutory protection, legal actions, disciplinary actions, complaints, IT security, pending cases, civil and criminal investigations, etc.

Scope of Work

Vendor shall be responsible for providing services to Bank the Services defined the RFP/SLTE for **Selection of Service Provider for ATM/Debit Switch & Debit Card Management System (DCMS) on hosted model** in accordance with all the terms and conditions of the RFP/SLTE clauses and as described in the Point 4 and Point 5 of Section A-Introduction of this RFP/SLTE i.e **Brief Scope of Work and Scope of Work (To be incorporated in SLA)**.

The bidder shall comply with the terms and conditions of the RFP/SLTE including General Terms and condition under Section D of this RFP/SLTE Document.

Location of Work

The successful bidder may complete the development of the solution remotely however if required successful bidder shall have to work at locations prescribed by Bank such as Banks DC/DR and other offices as per requirement. All expenses (travelling/lodging, etc.) shall be borne by the successful bidder

1. **CHQ , Srinagar**
Jammu & Kashmir Bank Ltd.
Corporate Headquarters,
MA Road, Srinagar-190001

2. **Data Center Noida**
Jammu & Kashmir Bank Ltd.
Green Fort Data Center, Plot B7, Sector 132, Noida U.P.-201301

3. **DR Mumbai**
CtrlS Data Center,
Mahape, Navi Mumbai, Maharashtra, 400701

Contract Uptime & Penalties

During Period of contract, Service Provider will maintain the services as per SLAs.

- i. Any bugs and enhancement in services shall be rectified immediately.
- ii. Any requirements amendments/modifications required by bank will have to be carried out by the identified Service Provider during the contract without any additional cost.
- iii. The maximum response time for a support/complaint from the site shall not exceed time defined, else it will fall under penalty clause.
- iv. Service Provider shall solve the software problem immediately after reporting of the problem by the Bank to the Service Provider.
- v. Any rectification required in the Application Software due to inherent bugs in the System Software/ off-the-shelf software shall also be rectified by the Service Provider, at no additional cost with timelines as defined in the SLA.

The Service Provider shall guarantee an uptime of 99.99 % during the contract period which shall be calculated on Monthly basis. The "**Uptime**", for calculation purposes, equals to the Total number of hours of the day in a month, less Downtime in number of hours. Any part of hour is treated as full hour.

- i. The "**Downtime**" is the time shall mean the time period when the Service/Application is not available as per the service standards of this SLA resulting failure. "**Failure**" is the condition that renders the solution not available to customers. "**Restoration**" is the condition when the Company demonstrates that the solution is in working order and the Bank acknowledges the same.
- ii. The percentage uptime is calculated on monthly basis as follows:

$$\frac{(\text{Total hours in a month} - \text{downtime hours within the month})}{\text{Total hours in a month}} * 100$$

iii. (A month is taken as a calendar month and number of days are actually number of days in each month)

“Uptime”: The Company shall guarantee and ensure the following SLA’s are met during the Contract Period of the Hardware/Software/License/Services:

Service Window	24*7
Uptime Commitment	99.99%
Data Availability	100%

a) The **“Uptime”**, for calculation purposes, equals to the Total number of hours of the day in a month, less Downtime in number of hours. Any part of hour is treated as full hour.

The percentage uptime is calculated on Monthly basis as follows:

$$\frac{(\text{Total hours in a month} - \text{downtime hours within the month})}{\text{Total hours in a month}} * 100$$

(A month is taken as a calendar month and number of days are actually number of days in each month)

b) The **“Downtime”** is the time shall mean the time period when the Service/Application is not available as per the service standards of this SLA resulting failure. **“Failure”** is the condition that renders the solution not available to customers. **“Restoration”** is the condition when the Company demonstrates that the solution is in working order and the Bank acknowledges the same.

c) **“Percentage down time”** shall mean the aggregate of downtime of the particular system during the month expressed as a percentage of total available time in a year i.e. 90 * 24 hours. Thus, if the aggregate downtime of System works out to 2 hours during a year then the percentage downtime shall be calculated as follows:

$$\frac{2 \times 100}{90 \times 24} = 0.09\% \text{ (Considering days in a month as 90)}$$

(A month is taken as a calendar month and number of days are actually number of days in each month)

d) **“Response Time”** shall mean the interval from receipt of first information from Bank to the company, or to the local contact person of the Company by way of any means of communication informing them of the malfunction in System/Solution to the time Company Engineer attends the problem.

- e) **“Restoration Time”** shall mean the period of time from the problem occurrence to the time in which the service returns to operational status. This may include temporary problem circumvention / workaround and does not necessarily include root cause removal.
- f) **“Resolution Time”** shall mean the period of time from the problem occurrence to the time in which the root cause of the problem is removed and a permanent fix has been applied to avoid problem reoccurrence.
- g) **Down Time”** shall mean the time period when the Service/Application is not available as per the service standards of this SLA, and the service/application is not available to the users of the Bank /Customers of the Bank (and excludes the scheduled outages planned in advance IT infrastructure), due to the problem in it and downtime is the sum of response time and restoration time with the following exclusions:

Period when Bank denies access to the Company Engineer for carrying out repair activities.

During Period of contract, Service Provider will maintain the services as per SLAs. If the bidder fails to maintain guaranteed/committed uptime of 99.99% on monthly basis. Bank shall impose penalty as mentioned below on slab basis. In case the uptime falls below the levels as tabulated below, Bank shall impose a penalty for each percent of loss of uptime below the guaranteed level as per details below:

Uptime	Penalty /Month
99.99% & Above	NA
99.50% to 99.98%	3% of the Transaction Processing Fee/Month
99% to 99.49%	5% of the Transaction Processing Fee/Month
98.50% to 98.99%	8% of the Transaction Processing Fee/Month
98% to 98.49%	10% of the Transaction Processing Fee/Month
Less than 98%	Penalty at an incremental rate of 1% (in addition to a base of 10%) of the Transaction Processing Fee/Month for every 0.5% lower than the stipulated uptime

Penalties shall also be applicable if the technical declines from the service provider are not less than 1%

Technical declines	Penalty/Month
Below 1%	NA
1-2%	2% of the Transaction Processing Fee/Month
>2-3%	3% of the Transaction Processing Fee/Month
>3-5%	5% of the Transaction Processing Fee/Month
>5%	10% of the Transaction Processing Fee/Month

Bank may recover such amount of penalty from any payment being released to the bidder, irrespective of the fact whether such payment is relating to this contract or otherwise. In case there is no pending invoices to be paid by the Bank to the bidder, the bidder has to submit a pay order / cheque payable at Srinagar in favour of Jammu & Kashmir Bank for the same within 15 days from the notice period from the Bank, failure of same may result in invoking of PBG for recovery of penalty. If the downtime exceeds 10 % and instances of downtime are more than 10

in a year, Bank has the discretion to cancel the contract.

If any penalty is levied by any regulator on the Bank which is attributed to the solution or any of its components, then the entire amount of such loss shall be recovered from the bidder on actual basis.

Note: SLA will be monitored on Monthly basis.

Service Levels:

This SLA document provides for minimum level of services required as per contractual obligations based on performance indicators and measurements thereof. The Company shall ensure provisioning of all required services while monitoring the performance of the same to effectively comply with the performance levels. The services provided by the Company shall be reviewed by Bank that shall:

- Regularly check performance of the Company against this SLA.
- Discuss escalated problems, new issues and matters still outstanding for resolution.
- Review of statistics related to rectification of outstanding faults and agreed changes.
- Obtain suggestions for changes to improve the service levels.

Non-Availability: Is defined as, the service(s) is not-available as per levels below.

- a. **Severity Level 1:** Is defined as, the Service is not available or there is a major degradation in performance of the system.
- b. **Severity Level 2:** Is defined as, the service is available but the performance is degraded or there are intermittent failures and there is an urgent need to fix the problem to restore the service
- c. **Severity Level 3:** Is defined as, the moderate degradation in the application performance. Has no impact on the normal operations/day-to-day working.

The violation of any of the above SLA’s will attract a penalty as set out in the table below:

Severity Level	Response	Restoration	Resolution
Severity-1	15 mins.	30 mins.	1 day
Severity-2	15 mins.	1 hrs.	2 days
Severity-3	30 mins.	6 hrs.	3 days

Penalties for Non-Compliance to Restoration and Resolution Time:

Severity Level	Restoration Breach	Resolution Breach
----------------	--------------------	-------------------

Severity-1	0.20% of Transaction Fee/Month for every 2hrs. of delay in restoration	0.10% of Transaction Fee/Month for every 3 day of delay in resolution
Severity-2	0.10% of Transaction Fee/Month for every 3hrs. of delay in restoration	0.10% of Transaction Fee/Month for every 7 day of delay in resolution
Severity-3	0.10 % of Transaction Fee/Month for every 6 hrs. of delay in restoration	0.10% of Transaction Fee/Month for every 10 day of delay in resolution

Penalty for delayed Delivery:

Without prejudice to the rights of Bank to terminate this agreement/ the related purchase order, in case of the failure to deliver the solution/milestones within the stipulated timelines, penalty shall be levied for every 1 week delay beyond due date at the rate of 0.5% of the order value of delayed item/milestone (inclusive of all taxes, duties, levies etc), up to a maximum of 10 weeks from the original delivery date .If delay exceeds 10 weeks, bank may in its sole discretion and without being bound to do so, extend the date of delivery or can invoke PBG and cancel the entire contract. In the event of the Bank agrees to extend the date of delivery at the request of the Company, it is a condition precedent that the validity of the Performance Bank Guarantee submitted by the Company in regard to the supply and maintenance etc. of the solution shall be extended by further period as required by the Bank before the expiry of the original Bank Guarantee. Failure to do so will be treated as breach of contract. Service Provider shall be excused of delay in case the installation could not be completed due to reasons not attributable to bidder, which shall be determined by Bank. Decision of Bank in this regard shall be final and binding.

No penalty shall be levied to the Company for delay in delivery due to reasons attributable to the Bank.

Delivery & Installation:

The solution as per the required scope needs to be rolled out as per the delivery timelines mentioned. The phases of the Schedule are as follows:

PROJECT PHASES:

1. Project Plan
2. Delivery of Solution
3. User Acceptance Testing
4. Operationalization of Solution
5. Solution Review

1. PROJECT PLAN:

Successful Bidder shall submit the project plan for complete implementation of the solution as per the Scope of Work detailed in this RFP/SLTE along with Solution Architecture, DFD and other required documents. This plan should be submitted for review and bank's acceptance within two week after the issuance of PO to the successful bidder.

Bank shall issue a Project Plan signoff accepting the same. It shall be the responsibility of the successful bidder to submit and get the plan approved by the Bank authorities within the timelines mentioned above without any delay. Bank shall have the discretion to cancel the purchase order in lieu of delay in submission of the project plan.

2. PROJECT MILESTONES & DELIVERY

The solution must be implemented as per project scope within a period defined in this RFP/SLTE. Rollout of the solution has to be as per the below timelines:

S.No	Milestone	Timeline
1	Issuance of PO	Week 0
2	Signing of Agreement	4 Weeks from the Issuance of PO
3	Submission of Project Plan Documentation	6 Weeks from the Issuance of PO
4	Supply, Delivery, Integration, Installation & Implementation of Solution (UAT Delivery) as per SOW of RFP, including mock migration.	Within 22 Weeks from the acceptance of Project Plan by bank
5	Full project Go-Live, Migration of existing Data in Production and training	Within 6 Weeks from the UAT sign off by Bank

Successful bidder is expected to provide detailed project implementation status on weekly basis.

The bidder must strictly adhere to the project timeline schedule, as specified in the purchase contract executed between the Parties for performance of the obligations, arising out of the purchase contract and any delay in completion of the obligations by the bidder will enable Bank to resort to any or all of the following provided that the bidder is first given a 30 days" written cure period to remedy the breach/delay:

- a. Claiming Liquidated Damages
- b. Termination of the purchase agreement fully or partly and claim liquidated damages.
- c. Forfeiting of Earnest Money Deposit / Invoking EMD Bank Guarantee/Performance Guarantee.

However, Bank will have the absolute right to charge penalty and/or liquidated damages as per Tender /contract without giving any cure period, at its sole discretion besides taking any other appropriate action.

EXTENSION OF DELIVERY SCHEDULE:

If, at any time during performance of the Contract, the Bidder should encounter conditions impeding timely delivery, the Bidder shall promptly notify the Bank in writing of the fact of the delay, its likely duration and its cause(s). As soon as practicable after receipt of the Bidder's notice, the Bank shall evaluate the situation and may at its discretion may extend the Bidder's time for performance against suitable extension of the performance guarantee for delivery.

NON-DELIVERY:

Failure of the successful bidder to comply with the above delivery schedule, shall constitute sufficient grounds for the annulment of the award of contract and invocation of bank guarantee (delivery) besides taking appropriate action against the successful bidder including blacklisting such bidder from participating in future tenders.

3. USER ACCEPTANCE TESTING:

Successful bidder shall assist Bank in the User Acceptance Testing of the solution for the functionalities stated in this RFP/SLTE document. Bank shall issue a UAT signoff on successful completion of the UAT for all channels. If the UAT fails or there is undue delay of the completion of the UAT due to reasons attributable to the successful bidder, Bank may at its own discretion cancel the purchase order and invoke the Bank guarantee for implementation.

4. OPERATIONALIZATION OF SOLUTION:

Bank shall issue Go Live Signoff on successful operationalization of the solution. If there is delay in the operationalization of the solution, Bank reserves the right to cancel the purchase order and invoke the Bank guarantee submitted for implementation.

5. REVIEW:

The solution shall remain under review for a period of 3 months from the date of issuance of Go Live Certificate as stated above. The Successful bidder shall be readily available during the review phase for troubleshooting and other support. During the review phase, Bank may request changes to the application as per its requirement and no extra costs shall accrue to the bank for the effort involved in the same. Bank shall issue final acceptance signoff at the end of the review phase.

Contract Period

The Contract shall be effective from date of acceptance of PO and shall be valid till (___date___), i.e 5 years from go live of the solution (___date___), unless or until terminated by Bank in accordance with the terms of this SLA. Thereafter the contract may further extended if both parties wish to continue on the mutually agreed terms and conditions subject to satisfactory performance of the vendor.

Payment Terms

The Bidder must accept the payment terms proposed by the Bank as proposed in this section.

b) The Payments shall be made on the achievement of the following project milestones:

S.No	Project Milestone	Payment (Incl. Of applicable taxes)
1	Submission of Project Plan Documentation	10% of One Time Cost
2	Supply, Delivery, Integration, Installation & Implementation of Solution (UAT Delivery) as per SOW of RFP, including mock migration.	30% of One Time Cost
3	Final Migration, Go-Live, Trainings and Production Sign-off by Bank.	40 % of one Time Cost
4	3 months after complete go-live and bug free operations	20 % of One-Time Cost
5	Monthly Card Hosting Fee per Active Debit Card	Monthly In Arrears subject to submission of transaction reports (As per actuals)
6	Transaction processing Fee-Financial and Non Financial (switching and debit card management system with 24x7 support)	Monthly In Arrears subject to submission of transaction reports (As per actuals)
7	Monthly Charges per ATM for ATM Driving with 24x7 support.	Monthly In Arrears subject to submission of reports(As per actuals)
8	Monthly Scheme connectivity (DC & DR) for Visa, MasterCard and NPCI.	Monthly In Arrears
9	Man-day cost for any additional Customization	As per actuals

Payments shall be released on acceptance of the purchase order and:

- i) Post Signing of Service Level Agreement (SLA) between Bank and Successful bidder.
- ii) Post Signing of Non-Disclosure Agreement (NDA) between Bank and Successful bidder.
- iii) No advance payment will be made on award of the contract.
- iv) All taxes, if any, applicable shall be deducted at source as per current rate while making any payment.
- v) Payments will be withheld in case of Non-compliance of the terms and condition of this RFP/SLTE.

Assignment

The Selected Bidder shall not assign, in whole or in part, the benefits or obligations of the contract to any other person. However, the Bank may assign any of its rights and obligations under the Contract to any of its affiliates without prior consent of Bidder.

Entire Agreement, Amendments, Waivers.

- i. This Master Agreement and each Service Attachment contains the sole and entire agreement of the parties with respect to the entire subject matter hereof, and supersede any and all prior oral or written agreements, discussions, negotiations, commitment, understanding, marketing brochures, and sales correspondence and relating thereto. In entering into this Master Agreement and each Service Attachment each party acknowledges and agrees that it has not relied on any express or implied representation, or other assurance (whether negligently or innocently made), out in this Master Agreement and each Service Attachment. Each party waives all rights and remedies which, but for this Section, might otherwise be available to it in respect of any such representation (whether negligently or innocently made), warranty, collateral contract or other assurance.
- ii. Neither this Master Agreement nor any Service Attachment may be modified or amended except in writing and signed by the parties.
- iii. No waiver of any provisions of this Master Agreement or any Service Attachment and no consent to any default under this Master Agreement or any Service Attachment shall be effective unless the same shall be in writing and signed by or on behalf of the party against whom such waiver or consent is claimed. No course of dealing or failure of any party to strictly enforce any term, right or condition of this Master Agreement or any Service Attachment shall be construed as a waiver of such term, right or condition. Waiver by either party of any default other party shall not be deemed a waiver of any other default.

Severability

If any or more of the provisions contained herein shall for any reason be held to be unenforceable in any respect under law, such unenforceability shall not affect any other provision of this Master Agreement, but this Master Agreement shall be construed as if such unenforceable provisions or provisions had never been contained herein, provided that the removal of such offending term or provision does not materially alter the burdens or benefits of the parties under this Master Agreement or any Service Attachment.

Remedies Cumulative

Unless otherwise provided for under this Master Agreement or any Service Attachment, all rights of termination or cancellation, or other remedies set forth in this Master Agreement, are cumulative and are not intended to be exclusive of other remedies to which the injured party may be entitled by law or equity in case of any breach or threatened breach by the other party of any provision in this Master Agreement. Use of one or more remedies shall not bar use of any other remedy for the purpose of enforcing any provision of this Master Agreement.

Partnership / Collaboration / Subcontracting

The services offered shall be undertaken to be provided by the company directly and there shall not

be any sub-contracting without prior written consent from the Bank. Bank will only discuss the solution with company's authorized representatives. The company authorized representatives shall mean their staff. In no circumstances any intermediary (which includes Liaisoning Agents, marketing agents, commission agents etc.) should be involved during the course of project. No subletting of the contract by the will be allowed under any circumstances. Neither the subject matter of the contract nor any right arising out of the contract shall be transferred, assigned or delegated to any third party by Successful Bidder without prior written consent of the Bank

Confidentiality

All the Bank's product and process details, documents, data, applications, software, systems, papers, statements and business/customer information etc. (hereinafter referred to as 'Confidential Information') which may be communicated to or come to the knowledge of the Company and /or its employees during the course of discharging their obligations shall be treated as absolutely confidential and the Company and its employees shall keep the same secret and confidential and not disclose the same, in whole or in part to any third party nor shall use or allow to be used any information other than as may be necessary for the due performance by the Company of its obligations. The Company shall indemnify and keep Bank indemnified safe and harmless at all times against all or any consequences arising out of any breach of this undertaking regarding Confidential Information by the Company and/or its employees and shall immediately reimburse and pay to the Bank on demand all damages, loss, cost, expenses or any charges that Bank may sustain suffer, incur or pay in connection therewith.

It is clarified that "Confidential Information" includes any and all information that is or has been received by the Company (Receiving Party) from the Bank (Disclosing Party) and that (a) relates to the Disclosing Party and (b) is designated by the Disclosing Party as being confidential or is disclosed in circumstances where the Receiving Party would reasonably understand that the disclosed information would be confidential (c) is prepared or performed by or on behalf of the Disclosing Party by its employees, officers, directors, agent, representatives or consultants.

In maintaining confidentiality, the Receiving Party on receiving the confidential information and material agrees and warrants that it shall take at least the same degree of care in safeguarding such confidential information and materials as it takes for its own confidential information of like importance and such degree of care shall be at least, that which is reasonably calculated to prevent any inadvertent disclosure. The Receiving Party shall also, keep the confidential information and confidential materials and any copies thereof secure and in such a way so as to prevent unauthorized access by any third Party.

The Receiving Party, who receives the confidential information and the materials, agrees that on receipt of a written demand from the Disclosing Party, they will immediately return all written confidential information and materials and all copies thereof provided to and which is in Receiving Party's possession or under its custody and control.

The Receiving Party to the extent practicable shall immediately destroy all analysis, compilation, notes studies memoranda or other documents prepared by it which contain, reflect or are derived from confidential information relating to the Disclosing Party AND shall also immediately expunge any confidential information, word processor or other device in its possession or under its

custody & control, where after it shall furnish a Certificate signed by the Authorized person confirming that to the best of his/her knowledge, information and belief, having made all proper enquiries, the requirement of confidentiality aspect has been complied with.

The restrictions mentioned hereinabove shall not apply to:-

- (a) any information that publicly available at the time of its disclosure; or any information which is independently developed by the Receiving Party or acquired from a third party to the extent it is acquired with the valid right to disclose the same; or
- (b) any disclosure required by law or by any court of competent jurisdiction, the rules and regulations of any recognized stock exchange or any enquiry or investigation by any government, statutory or regulatory body which is lawfully entitled to require any such disclosure provided that, so far as it is lawful and practical to do so prior to such disclosures, the Receiving Party shall promptly notify the Disclosing Party of such requirement with a view to providing the Disclosing Party an opportunity to obtain a protective order or to contest the disclosure or otherwise agree to the timing and content of such disclosure.

The confidential information and material and all copies thereof, in whatsoever form shall at all the times remain the property of the Disclosing Party and disclosure hereunder shall not confer on the Receiving Party any rights whatsoever beyond those contained in this document. The confidentiality obligations shall be observed by the Company during the term of this Agreement and thereafter and shall survive the expiry or termination of this Agreement between the Bank and Company.

The Company understands and agrees that any use or dissemination of information in violation of this Confidentiality Clause will cause BANK irreparable harm, may leave BANK with no adequate remedy at law and as such the Bank is entitled to proper indemnification for the loss caused by the Company. Further the BANK is entitled to seek to injunctive relief besides other remedies available to it under law and this Agreement.

Information Security:

- a. The Successful Bidder and its personnel shall not carry any written material, layout, diagrams, floppy diskettes, hard disk, flash / pen drives, storage tapes or any other media out of J&K Bank's premises without written permission from J&K Bank.
- b. The Successful Bidder's personnel shall follow J&K Bank's information security policy and instructions in this regard.
- c. The Successful Bidder acknowledges that J&K Bank's business data and other proprietary information or materials, whether developed by J&K Bank or being used by J&K Bank pursuant to a license agreement with a third party (the foregoing collectively referred to herein as "proprietary information") are confidential and proprietary to J&K Bank; and the Successful Bidder agrees to use reasonable care to safeguard the proprietary information and to prevent the unauthorized use or disclosure thereof, which care shall not be less than that used by Successful Bidder to protect its own proprietary information. Successful Bidder recognizes that the goodwill of J&K Bank depends, among other things, upon the Successful Bidder keeping such proprietary information confidential and that unauthorized disclosure of the same by Successful Bidder could damage J&K Bank. By reason of Successful Bidder's duties and obligations hereunder, Successful Bidder may come into possession of such proprietary information, even though the Successful Bidder does not take any direct part in or furnish the

Service(s) performed for the creation of said proprietary information and shall limit access thereto to employees with a need to such access to perform the Services required by the Contract/Agreement. Successful Bidder shall use such information only for the purpose of performing the Service(s) under the Contract/Agreement.

- d. Successful Bidder shall, upon termination of the Contract/Agreement for any reason, or upon demand by J&K Bank, whichever is earliest, return any and all information provided to Successful Bidder by J&K Bank, including any copies or reproductions, both hardcopy and electronic.
- e. That the Successful Bidder and each of its subsidiaries have taken all technical and organizational measures necessary to protect the information technology systems and Data used in connection with the operation of the Successful Bidder's and its subsidiaries' businesses. Without limiting the foregoing, the Successful Bidder and its subsidiaries have used reasonable efforts to establish and maintain, and have established, maintained, implemented and complied with, reasonable information technology, information security, cyber security and data protection controls, policies and procedures, including oversight, access controls, encryption, technological and physical safeguards and business continuity/disaster recovery and security plans that are designed to protect against and prevent breach, destruction, loss, unauthorized distribution, use, access, disablement, misappropriation or modification, or other compromise or misuse of or relating to any information technology system or Data used in connection with the operation of the Successful Bidder's and its subsidiaries' businesses.
- f. The Successful Bidder shall certify that to the knowledge of the Successful Bidder, there has been no security breach or other compromise of or relating to any information technology and computer systems, networks, hardware, software, data, or equipment owned by the Successful Bidder or its subsidiaries or of any data of the Successful Bidder's, the Operating Partnership's or the Subsidiaries' respective customers, employees, suppliers, vendors that they maintain or that, to their knowledge, any third party maintains on their behalf (collectively, "IT Systems and Data") that had, or would reasonably be expected to have had, individually or in the aggregate, a Material Adverse Effect, and
- g. That the Successful Bidder has not been notified of, and has no knowledge of any event or condition that would reasonably be expected to result in, any security breach or other compromise to its IT Systems and Data;
- h. That the Successful Bidder is presently in compliance with all applicable laws, statutes, rules or regulations relating to the privacy and security of IT Systems and Data and to the protection of such IT Systems and Data from unauthorized use, access, misappropriation or modification. Besides the Successful Bidder confirms the compliance with Banks Supplier Security Policy.
- i. That the Successful Bidder has implemented backup and disaster recovery technology consistent with generally accepted industry standards and practices.
- j. That the Successful Bidder and its subsidiaries IT Assets and equipment, computers, Systems, Software's, Networks, hardware, websites, applications and Databases (Collectively called IT systems) are adequate for, and operate and perform in all material respects as required in connection with the operation of business of the Successful Bidder and its subsidiaries as currently conducted, free and clear of all material bugs, errors, defects, Trojan horses, time bombs, malware and other corruptants.

- k. That the Successful Bidder shall be responsible for establishing and maintaining an information security program that is designed to:
 - o Ensure the security and confidentiality of Customer Data, Protect against any anticipated threats or hazards to the security or integrity of Customer Data, and
 - o That the Successful Bidder will notify Customer of breaches in Successful Bidder's security that materially affect Customer or Customer's customers. Either party may change its security procedures from time to time as commercially reasonable to address operations risks and concerns in compliance with the requirements of this section.
- l. The Successful Bidder shall establish, employ and at all times maintain physical, technical and administrative security safeguards and procedures sufficient to prevent any unauthorized processing of Personal Data and/or use, access, copying, exhibition, transmission or removal of Bank's Confidential Information from Companies facilities. Successful Bidder shall promptly provide Bank with written descriptions of such procedures and policies upon request. Bank shall have the right, upon reasonable prior written notice to Successful Bidder and during normal business hours, to conduct on-site security audits or otherwise inspect Companies facilities to confirm compliance with such security requirements.
- m. That Successful Bidder shall establish and maintain environmental, safety and facility procedures, data security procedures and other safeguards against the destruction, corruption, loss or alteration of the Client Data, and to prevent access, intrusion, alteration or other interference by any unauthorized third parties of the same, that are no less rigorous than those maintained by Successful Bidder for its own information or the information of its customers of a similar nature.
- n. That the Successful Bidder shall perform, at its own expense, a security audit no less frequently than annually. This audit shall test the compliance with the agreed-upon security standards and procedures. If the audit shows any matter that may adversely affect Bank, Successful Bidder shall disclose such matter to Bank and provide a detailed plan to remedy such matter. If the audit does not show any matter that may adversely affect Bank, Successful Bidder shall provide the audit or a reasonable summary thereof to Bank. Any such summary may be limited to the extent necessary to avoid a breach of Successful Bidder's security by virtue of providing such summary.
- o. That Bank may use a third party or its own internal staff for an independent audit or to monitor the Successful Bidder's audit. If Bank chooses to conduct its own security audit, such audit shall be at its own expense. Successful Bidder shall promptly correct any deficiency found in a security audit.
- p. That after providing 30 days prior notice to Successful Bidder, Bank shall have the right to conduct a security audit during normal business hours to ensure compliance with the foregoing security provisions no more frequently than once per year. Notwithstanding the foregoing, if Bank has a good faith belief that there may have been a material breach of the agreed security protections, Bank shall meet with Successful Bidder to discuss the perceived breach and attempt to resolve the matter as soon as reasonably possible. If the matter cannot be resolved within a thirty (30) day period, the parties may initiate an audit to be conducted and completed within thirty (30) days thereafter. A report of the audit findings shall be issued within such thirty (30) day period, or as soon thereafter as is practicable. Such audit shall be conducted by Successful Bidder's auditors, or the successors to their role in the event of a

corporate reorganization, at Successful Bidder's cost.

- q. Successful Bidders are liable for not meeting the security standards or desired security aspects of all the ICT resources as per Bank's IT/Information Security / Cyber Security Policy. The IT /Information Security/ Cyber Security Policy will be shared with successful Bidder. Successful Bidders should ensure Data Security and protection of facilities/application managed by them.
- r. The deputed persons should aware about Bank's IT/IS/Cyber security policy and have to maintain the utmost secrecy & confidentiality of the bank's data including process performed at the Bank premises. At any time, if it comes to the notice of the bank that data has been compromised / disclosed/ misused/misappropriated then bank would take suitable action as deemed fit and selected Successful Bidder would be required to compensate the bank to the fullest extent of loss incurred by the bank.
- s. The Bank shall evaluate, assess, approve, review, control and monitor the risks and materiality of vendor/outsourcing activities and Successful Bidder shall ensure to support baseline system security configuration standards. The Bank shall also conduct effective due diligence, oversight and management of third party vendors/Successful Bidders & partners.
- t. Successful Bidder criticality assessment shall be conducted for all partners & vendors. Appropriate management and assurance on security risks in outsources and partner arrangements shall be ensured.

Termination of Contract

If the Termination is on account of failure of the Successful Bidder to perform the obligations under this agreement, the Bank shall have the right to invoke the Performance Bank Guarantee(s) given by the selected bidder.

The Bank will be entitled to terminate this Contract, on the happening of any one or more of the following:

For Convenience: BANK by written notice sent to the Company may terminate the contract in whole or in part at any time for its convenience giving 90 days prior notice.

In the event of termination of the Agreement for the Bank's convenience, Successful Bidder shall be entitled to receive payment for the Services rendered (delivered) up to the effective date of termination.

For Insolvency: BANK may at any time terminate the contract by giving written notice to the Company, if the Company becomes bankrupt or insolvent.

For Non-performance: BANK shall have the right to terminate this agreement or/and to cancel the entire or unexecuted part of the related Purchase Order forthwith by a written notice in the event the company fails to deliver and/or install the solution within the stipulated time schedule or any extension, if any, thereof agreed by the Bank in writing in its sole discretion OR the Company fails to maintain the service levels prescribed by BANK in scope of work OR fails to discharge or commits breach of any of its obligations under this Agreement.

In the event of termination, the company shall compensate the Bank to the extent of loss suffered by the Bank on account of such termination provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to BANK. The Bank shall inter-alia have a right to invoke the Performance Bank Guarantee submitted by the Company in regard to the supply and maintenance etc. of the solution for realizing the payments due to it under this agreement including penalties, losses etc.

Indemnity

The Successful bidder shall indemnify and hold the Bank harmless from and against all claims, losses, costs, damages, expenses, action suits and other proceedings (including attorney fees), relating to or resulting from:-

- i. Intellectual Property infringement or misappropriation of any third party trade secrets or infringement of any patent, trademarks, copyrights etc. or such other statutory infringements in respect of all components provided to fulfil the scope of this project.
- ii. Claims made by the employees who are deployed by the Successful bidder.
- iii. Breach of confidentiality obligations by the Successful bidder,
- iv. Negligence (including but not limited to any acts or omissions of the Successful bidder, its officers, principals or employees) or misconduct attributable to the Successful bidder or any of the employees deployed for the purpose of any or all of the its obligations,
- v. Any loss or damage arising out of loss of data;
- vi. Bonafide use of deliverables and or services provided by the successful bidder;
- vii. Non-compliance by the Successful bidder with applicable Laws/Governmental/Regulatory Requirements.

The Successful bidder shall be responsible for any loss of data, loss of life etc. due to acts of its representatives, and not just arising out of negligence or misconduct, as such liabilities pose significant risk.

It is hereby agreed that the above said indemnity obligations shall apply notwithstanding anything to the contrary contained in this Tender document and subsequent Agreement and shall survive the termination of the agreement for any reason whatsoever. The Successful bidder will have sole control of its defense and all related settlement negotiations

Right to Audit

“Bank reserves the right to conduct an audit/ ongoing audit of the Company/Service Provider(including its sub-contractors).The Company shall be subject to annual audit by internal/ external Auditors appointed by the Bank / inspecting official from the RBI or the persons authorized by RBI or any regulatory authority, covering the risk parameters finalized by the Bank/ such auditors in the areas of products (IT hardware/ Software) and services etc. provided to the Bank and company is required to submit such certification by such Auditors to the Bank. Company shall allow the Bank and RBI or persons authorized by it to access Bank documents, records or transactions or any other information given to, stored or processed by Company within a reasonable time failing which Company will be liable to pay any charges/ penalty levied by the Bank without prejudice to the

Page 115 of 154

other rights of the Bank. Company shall allow the Bank to conduct audits or inspection of its Books and account with regard to Bank's documents by one or more officials or employees or other persons duly authorized by the Bank.”

Limitation of Liability

Neither Party shall be liable for any indirect damages (including, without limitation, loss of revenue, profits, and business) under this agreement and the aggregate liability of Successful Bidder, under this agreement shall not exceed total contract value.

Exit Clause

The Bank reserves the right to cancel the contract in the event of happening one or more of the following conditions:

1. Failure of the Successful Bidder to accept the contract and furnish the Performance Bank Guarantee within 30 days from receipt of purchase contract.
2. Delay in delivery beyond the specified period.
3. Delay in completing implementation/customization and acceptance tests/ checks beyond the specified periods;
4. Serious discrepancy in functionality to be provided or the performance levels which have an impact on the functioning of the solution.
5. In addition to the cancellation of contract, Bank reserves the right to appropriate the damages through encashment of Bid Security /Performance Guarantee given by The Successful Bidder. Bank reserves right to exit at any time after giving notice period of one month during the contract period.

Force Majeure

- i. The Selected Company shall not be liable for forfeiture of its performance security, Liquidated damages or termination for default, if any to the extent that its delay in performance or other failure to perform its obligations under the contract is the result of an event of Force Majeure.
- ii. For purposes of this Clause, "Force Majeure" means an event explicitly beyond the reasonable control of the Contractor and not involving the contractors fault or negligence and not foreseeable. Such events may be due to or as a result of or caused by act of God, wars, insurrections, riots, earth quake and fire, revolutions, civil commotion, floods, epidemics, pandemics, quarantine restrictions, trade embargos, declared general strikes in relevant industries, events not foreseeable but does not include any fault or negligence or carelessness on the part of the parties, resulting in such a situation. In the event of any such intervening Force Majeure, either party shall notify the other in writing of such circumstances or the cause thereof immediately within five calendar days.

- iii. Unless otherwise directed by the Bank in writing, the selected bidder shall continue to perform its obligations under the Contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.
- iv. In such a case the time for performance shall be extended by a period(s) not less than duration of such delay. If the duration of delay continues beyond a period of three months, the Bank and The Successful Bidder shall hold consultations in an endeavor to find a solution to the problem.
- v. Notwithstanding above, the decision of the Bank shall be final and binding on the successful Company regarding termination of contract or otherwise

Intellectual Property Rights

- 1.1 For any technology / software / product used by Company for performing Services for the Bank as part of this Agreement, Company shall have right to use as well as right to license such technology/ software / product. The Bank shall not be liable for any license or IPR violation on the part of Company.
- 1.2 Without the Bank's prior written approval, Company will not, in performing the Services, use or incorporate link to or call or depend in any way upon, any software or other intellectual property that is subject to an Open Source or Copy left license or any other agreement that may give rise to any third-party claims or to limit the Bank's rights under this Agreement.
- 1.3 Company shall, at its own expenses without any limitation, indemnify and keep fully and effectively indemnified the Bank against all costs, claims, damages, demands, expenses and liabilities whatsoever nature arising out of or in connection with all claims of infringement of Intellectual Property Right, including patent, trademark, copyright, trade secret or industrial design rights of any third party arising from the Services or use of the technology / software / products or any part thereof in India or abroad.
- 1.4 The Bank will give (a) notice to Company of any such claim without delay/provide reasonable assistance to Company in disposing of the claim; (b) sole authority to defend and settle such claim and; (c) will at no time admit to any liability for or express any intent to settle the claim provided that (i) Company shall not partially settle any such claim without the written consent of the Bank, unless such settlement releases the Bank fully from such claim, (ii) Company shall promptly provide the Bank with copies of all pleadings or similar documents relating to any such claim, (iii) Company shall consult with the Bank with respect to the defence and settlement of any such claim, and (iv) in any litigation to which the Bank is also a party, the Bank shall be entitled to be separately represented at its own expenses Of successful bidder
- 1.5 Company shall have no obligations with respect to any infringement claims to the extent that the infringement claim arises or results from: (i) Company's compliance with the Bank's specific technical designs or instructions (except where Company knew or should have known that such compliance was likely to result in an Infringement Claim and Company did not inform the Bank of

the same); or (ii) any unauthorized modification or alteration of the deliverable (if any) by the Bank.

Corrupt and Fraudulent practice.

- i. It is required that Company observe the highest standard of ethics during the procurement and execution of such contracts and not to indulge in any corrupt and fraudulent practice.
- ii. “Corrupt Practice” means the offering, giving, receiving or soliciting of anything of value to influence the action of an official in the procurement process or in contract execution.
- iii. “Fraudulent Practice” means a misrepresentation of facts in order to influence a procurement process or the execution of contract to the detriment of the Bank and includes collusive practice among bidders (prior to or after bid submission) designed to establish bid prices at artificial non-competitive levels and to deprive the Bank of the benefits of free and open competition.
- iv. The Bank reserves the right to reject a proposal for award if it determines that the Company recommended for award has engaged in corrupt or fraudulent practices in competing for the contract in question.
- v. The Bank reserves the right to declare a bidder ineligible, either indefinitely or for a stated period of time, to be awarded a contract if at any time it becomes known that the firm has engaged in corrupt or fraudulent practices in competing for or in executing the contract.

Governing Laws and Dispute Resolution

This agreement shall be governed in accordance with the Laws of UT of J&K read with laws of India so far as they are applicable to the UT of J&K for the time being and will be subject to the exclusive jurisdiction of Courts at Srinagar with exclusion of all other Courts. The Bank and the Successful Bidder shall make every effort to resolve any disagreement or dispute amicably, arising in connection with the Contract, by direct and informal negotiation between the designated Officer of the Bank **ATM/Debit Switch & Debit Card Management System (DCMS) on hosted model** and designated representative of the Successful Bidder. If designated Officer of the Bank and representative of the Successful Bidder are unable to resolve the dispute within reasonable period, which in any case shall not exceed 30 days they shall immediately escalate the dispute to the senior authorized personnel designated by the Bank and the Successful Bidder respectively. If even after elapse of reasonable period, which in any case shall not exceed 60 days, the senior authorized personnel designated by the Bank and the Successful Bidder are unable to resolve the dispute amicably OR any party fails to designate its officer/representative/ senior authorized personnel within days from the date of request in writing for the same by the other party for amicable settlement of dispute, the dispute shall be referred to a sole arbitrator to be appointed by Bank. The Arbitration and Conciliation Act, 1996 will be applicable to the arbitration proceeding and the venue of the arbitration shall be at Srinagar. The language of the arbitration proceedings shall be in English. The award of the arbitrator shall be final and binding. The courts at Srinagar shall have exclusive jurisdiction at Srinagar.

Notices

Unless otherwise provided herein, all notices or other communications under or in connection with this Agreement shall be given in writing and may be sent by personal delivery or by post or courier or facsimile or e-mail to the address below, and shall be deemed to be effective if sent by personal delivery, when delivered, if sent by post, three days after being deposited in the post and if sent by courier, two days after being deposited with the courier, and if sent by facsimile, when sent (on receipt of a confirmation to the correct facsimile number) and if sent by e-mail (on receipt of a confirmation to the correct email)

Following shall be address of BANK for notice purpose:

**General Manager (S&IT), J&K Bank Ltd,
Technology & Development Division,
Corporate Headquarters, M.A. Road, Srinagar, 190001 Jammu & Kashmir (India)**

Following shall be address of Company for notice purpose:

Other Terms and Conditions

- i. If any provision of this agreement or any document, if any, delivered in connection with this agreement is partially or completely invalid or unenforceable in any jurisdiction, then that provision shall be ineffective in that jurisdiction to the extent of its invalidity or unenforceability. However, the invalidity or unenforceability of such provision shall not affect the validity or enforceability of any other provision of this agreement, all of which shall be construed and enforced as if such invalid or unenforceable provision was/were omitted, nor shall the invalidity or unenforceability of that provision in one jurisdiction affect its validity or enforceability in any other jurisdiction. The invalid or unenforceable provision will be replaced in writing by a mutually acceptable provision, which being valid and enforceable comes closest to the intention of the Parties underlying the invalid or unenforceable provision.
- ii. Bank reserves the right to conduct an audit/ ongoing audit of the services provided by Company. The Company agrees and undertakes to allow the Bank or persons authorized by it to access Bank documents, records or transactions or any other information given to, stored or processed by the Company within a reasonable time failing which Bidder will be liable to pay any charges/ penalty levied by the Bank without prejudice to the other rights of the Bank. The Company shall allow the Bank to conduct audits or inspection of its Books and account with regard to Bank's documents by one or more officials or employees or other persons duly authorized by the Bank.
- iii. The company, either by itself or through its group companies or Associates, shall not use the name and/or trademark/logo of Bank, in any sales or marketing publication or advertisement, or in any other manner.

- iv. Any addition, alteration, amendment, of this Agreement shall be in writing, signed by both the parties.
- v. The invalidity or unenforceability for any reason of any covenant of this Agreement shall not prejudice or affect the validity or enforceability of its other covenants. The invalid or unenforceable provision will be replaced by a mutually acceptable provision, which being valid and enforceable comes closest to the intention and economic positions of the Parties underlying the invalid or unenforceable provision.
- vi. Each party warrants that it has full power and authority to enter into and perform this Agreement, the respective executants are duly empowered and/or authorized to execute this Agreement, and performance of this Agreement will not result in breach of any provision of the Memorandum and Articles of Association or equivalent constitutional documents of the either party or any breach of any order, judgment or agreement by which the party is bound.
- vii. The terms and conditions laid down in the RFP/SLTE shall be read and construed forming part of this service level agreement. In an event of contradiction on any term or condition between RFP/SLTE and service level agreement, the terms and conditions of service level agreement shall prevail.

In witness whereof the parties have set their hands on this agreement in duplicate through their authorized signatories on the day, month and year first herein above mentioned.

Agreed and signed on behalf of
Company's Authorized Signatory

Name.....
Designation.....

Signature.....

Witness (1):

Name.....
Designation.....

Signature.....

Witness (2):

Name.....

Agreed and signed on behalf of
J&K Bank Limited

Name.....
Designation.....

Signature

Witness (1):

Name.....
Designation.....

Signature

Witness (2):

Name.....

Designation.....

Signature.....

Designation.....

Signature

Annexure K: Undertaking

Bidder has to submit Undertaking on company letter head as per format given below

**The General Manager
Strategy & IT
Corporate Headquarters
Jammu & Kashmir Bank M.A Road, Srinagar**

Dear Sir,

Sub: RFP/SLTE no: _____ for Selection of Service Provider for ATM/Debit Switch & Debit Card Management System (DCMS) on hosted model

Having examined the tender documents including all annexures the receipt of which is hereby duly acknowledged, we, the undersigned, offer **ATM/Debit Switch & Debit Card Management System (DCMS) on hosted model** to Bank as mentioned in RFP/SLTE document in conformity with the said tender documents in accordance with the Commercial bid and made part of this tender.

We understand that the RFP/SLTE provides generic specifications about all the items and it has not been prepared by keeping in view any specific bidder.

We understand that the RFP/SLTE floated by the Bank is a confidential document and we shall not disclose, reproduce, transmit or made available it to any other person.

We hereby undertake that supporting software/license supplied, if required will be licensed, legally obtained and with latest version.

We understand that the Bank is not bound to accept the offer either in part or in full and that the Bank has right to reject the RFP/SLTE in full or in part without assigning any reasons whatsoever.

We have read, understood and accepted the terms/ conditions/ rules mentioned in the RFP/SLTE, proposed to be followed by the Bank.

Until a formal contract is prepared and executed, this tender offer, together with the Bank's written acceptance thereof and the Bank's notification of award, shall constitute a binding contract between us.

We undertake that in competing for and if the award is made to us, in executing the subject Contract, we will strictly observe the laws against fraud and corruption in force in India and the UT of J&K including Prevention of Corruption Act 1988.

We have never been barred/black-listed by any regulatory / statutory authority in India.

We understand that the Bank is not bound to accept the lowest or any offer the Bank may receive.

We hereby undertake that all the components/parts/assembly/software used in the Networking Hardware shall be original new components / parts / assembly / software only, from respective OEMs of the products and that no refurbished / duplicate / second hand components / Parts / Assembly / Software are being used or shall be used.

This Bid, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract between us.

We enclose cost of RFP/SLTE Rs. 10,000/- (Ten Thousand Only) and EMD of Rs. 1,50,00,000/- (Rupees One Crore Fifty Lacs Only) in Bank Transfer/Demand Draft/Bank Guarantee favoring J&K Bank Ltd, towards cost of RFP/SLTE/bid security, details of the same is as under

No. :

Date:

Name of Issuing Bank:

Dated at _____ this _____ day of _____ 2026

We certify that we have provided all the information requested by the Bank in the format requested for. We also understand that the Bank has the exclusive right to reject this offer in case the Bank is of the opinion that the required information is not provided or is provided in a different format. It is also confirmed that the information submitted is true to our knowledge and the Bank reserves the right to reject the offer if anything is found incorrect.

We agree to all terms & conditions of the RFP/SLTE.

Place:

Seal and signature of The Bidder

Annexure L: Know Your Employee (KYE) Clause

Bidder has to submit Undertaking on company letter head as per format given below.

1. We on the behalf of _____ (name of the company) hereby confirm that all the resources (both on-site and off-site) working on the Bank's project ie. **Selection of Service Provider for ATM/Debit Switch & Debit Card Management System (DCMS) on hosted model** have undergone KYE (Know Your Employee) process and all the required checks have been performed prior to employment of said employees as per our policy.
2. We confirm to defend and keep the bank indemnified against all loss, cost, damages, claim penalties expenses, legal liability because of non-compliance of KYE and of misconduct of the employee deployed by us to the Bank.
3. We further agree to submit the required supporting documents (Process of screening, Background verification report, police verification report, character certificate, ID card copy, Educational document, etc.) to Bank before deploying officials in Bank premises for **ATM/Debit Switch & Debit Card Management System (DCMS) on hosted model**

Sign and seal of Competent Authority
Name of Competent Authority
Dated

Annexure M: Compliance Requirements

1. The solution should be in accordance with the security norms of RBI/NPCI/TRAI from time to time. The Regulatory mandates by any regulator pertaining to the application or solution provided by the bidder has to be complied during the validity of contract period without any extra cost to the Bank.
2. The solution proposed has to be in strict compliance with extant Laws and Regulations like but not limited to IT Act 2000 read with IT Amendment Act 2008, Draft Master Directions of RBI Directions on Outsourcing, RBI Digital Payment Security Directions 2021, TRAI, RBI Cyber Security Framework Circular Dated 2nd June 2016, NPCI Circulars and Directions.
3. As the Bank is opting for Managed Services Model, the bidder must ensure strict compliance with the Technology & Security Standards Viz, ISO 27001 ISMS or Equivalent Standard, ITIL Framework, DevSecOps, ISO 27018 Code of Practice for Personally Identifiable Information and other Software Development Standards.
4. The bidder shall ensure that a strong Project Governance Framework is put in place for adequately addressing associated risks and measuring the success of the project at any given point of time. The same needs to be communicated as part of the RFP/SLTE response along with the escalation matrix.
5. In case the bidder opts for providing the services via a Multi-tenancy environment, it must be protected against data integrity and confidentiality risks and against co-mingling of data. The architecture should enable smooth recovery and any failure of any one or combination of components across the managed services architecture should not result in data/ information security compromise.
6. The Bidder shall share the appropriate update and release cycles affecting the service features (Such as: Security, Continuity, legal and governance...etc.). The bidder must be flexible to align the same with the Banks Patch, Vulnerability and Change Management Processes.
7. The Bidder, as part of bid submission shall share the detailed information on how the Service Provider ensures and applies agile and rapid yet comprehensive risk management. This must include the Risk Control checking Methodology.
8. In case the Service Provider is proposing the solution on Virtualized mode, the Service Provider has to ensure that the controls are in place to guarantee that only authorized snapshots are taken, and that these snapshots level of classification and storage location and encryption is compatible in strength with the production virtualization environment. Besides, the Service Provider has to ensure that the complete logs of Virtualized environment that are provided to Bank are accessible to Bank.
9. The bidder shall provide the Bank with its Service Providers user list that will have access to the Bank's data; at any point throughout the duration of the agreement. Service Providers should also update the Bank with any change in the employee list.

10. The bidder shall ensure to submit the high-level/low level design document as part of the solution offering mentioning integration of the application with Banks Privileged Identity and Access Management Solution. The Bank shall be open to provide Identity Federated integration using SAML / OpenID / Open Auth, RADIUS etc.
11. The Admin & User Management Framework provided by the Service Provider must be in alignment with RBI's Authentication Framework for Customers, Privileged Accesses and other Internal Users.
12. The Service Provider must provide the Bank secure control for managing its identities (Including Identity Creation and Deletion / Modification & Termination).
13. The Service Provider shall ensure Authentication, Authorization, Accounting, Access control and logging (Format, retention and Access) meet the Bank's regulatory and legal requirements.
14. The Service Provider shall ensure that the logging is enabled for all activities including OS and, Application level for a period not less than 180 days online and then Backed up for the period of project. The Live logs as stipulated above shall as well be integrated with Bank's SIEM Solution.
15. The Service Provider shall have the information readily available on Location and time of access of the Service Provider Team.
16. The Service Provider shall ensure Micro-segmentation of Banks services. The Service Provider shall further shall ensure to put in place, in addition to the Infrastructure Security, the Application Layer Firewalls, conduct source code reviews prior to provisioning any application release, Adopt Secure web development best practices like OWASP secure development guidelines, Adopt OS and Applications security hardening best practices. Service Provider shall submit the source code audits reports mentioning closure of all identified vulnerabilities at yearly frequency to the Bank.
17. Service Provider shall ensure to conduct Periodic Vulnerability Assessment & Penetration testing of its Infrastructure and applications. The MPS shall ensure that these activities are done as part of Vulnerability Management and remediation program is defined, and it includes fixing the vulnerabilities based on priority. All vulnerabilities should be prioritized and must be fixed and patched within SLAs agreed upon by the Bank and the CSP in line with Banks Patch & Vulnerability Management procedure.
18. Service Provider shall ensure to follow a proper software development life cycle (SDLC) and that security is an integrated part in at least the following phases:
 - a. Planning and requirements gathering
 - b. Architecture and functional Design Phase Coding
 - c. Testing
 - d. Maintenance

19. The bidder shall ensure to adopt and is in compliance with Change Management and Incident Response Procedures as specified in (ITIL).
20. The Service Provider shall share its DR plan with Bank so as to ensure it matches the Bank's BCP requirements.
21. The Service Provider has the ability to retrieve and restore data following data loss incidents.
22. Service Provider to provide the Bank at least bi-annually with the DR testing reports. The reports should be comprehensive, covering from the exercise scope till the final outcome and recommendations.
23. Service Provider to ensure the DR solution is capable of maintaining the same levels of security measures and controls utilized in the normal operation mode.
24. Ensure that the DR solution is also owned and managed entirely by the Contracted Service Provider. Conducting DR Drills & DR compliances shall be the responsibility of Contracted Service Provider.
25. The Bidder shall ensure to meet the Maximum Time to Recover (MTTR) also known as RTO (Recovery Time Objective) of 3 Hours and Recovery Point Objective of Zero (0).
26. The Service Provider shall submit the data-segmentation and separation controls at each of the four main layers at the Service Provider: (1) Network, (2) physical, (3) system and (4) Application. The same must be kept updated and produced to the Bank as and when there are any changes or as sought by the Bank.
27. The bidder must be open for evaluation of each of the Data segmentation controls at each layer, as well as the number and type of controls at each layer every 6 months and after major system changes and upgrades.
28. The Service Provider shall ensure that data is encrypted at storage and in transit and in full compliance (at any given point in time) with Bank's Cryptographic Procedure, ISO 27001 and PCI-DSS Standard. The Databases must support the function of Encryption, Redaction/Masking and Comprehensive Audit Logging.
29. The Service Provider shall ensure that it is using a unique set of encryption key(s) for Bank. The unique encryption keys shall help protect data from being accessible in the event that it is inadvertently leaked from one Service Provider customer to another.
30. The Service Provider shall ensure to provide the "Exclusive" right to data ownership to the Bank throughout the duration of the agreement. The ownership includes all copies of data available with the Service Provider including backup media copies if any. The Service Provider is not permitted to use Bank's data for advertising or any other non-authorized secondary purpose.

31. The Service Provider shall contractually ensure that they inform the Bank “immediately” on any confirmed breach without any undue delay. The Service Provider shall ensure that Bank is notified within 4 hours of any “Suspected” breach from the time of breach discovery.
32. An “Exit Management Plan” must be put in place to define the rules of disengagement. Service Provider should provide the detailed description of the exit clause including agreed process, TAT for exit, data completeness and portability, secure purge of Bank’s information, smooth transition of services, complete plan of how data shall be moved out from the hosted infrastructure with minimal impact on continuity of the Bank’s operations.
33. It shall be responsibility of the service provider to ensure smooth transition of all the data of the Banks data including audit trails, logs, to Bank specified location/storage on the conclusion of services. It would be obligatory for the Service Provider not to delete any data without the written permission from the Bank.
34. Service Provider shall ensure to comply with the data and media destruction and sanitization controls as stipulated in Media Disposal and Sanitization Policies of Bank. The Service Provider shall further preserve documents as required by law and take suitable steps to ensure that Banks interests are protected, even post termination of the services. This would include ensuring full integrity data transition from service provider to alternate service provider or on premise setups.
35. The bidder shall ensure that the services are duly audited and certified by Cert-In Empaneled Audit Companies. The bidders are required to comply with requisite audit requirements as is specified under the security standards followed under the Information Technology Act and as stipulated by the Regulators from time to time.
36. Bank shall ensure that the Service Provider shall neither impede/ interfere with the ability of the Bank to effectively oversee and manage its activities nor impede the supervising authority in carrying out the supervisory functions and objectives.
37. The Service Provider shall ensure that the arrangement shall comply with all the policies of the Bank including, but not limit to, Information Security Policy, BCP, IT Outsourcing Policy, Incident Management Policy, etc. The service provider has to comply with all the laws/ regulations issued by RBI from time to time.
38. The Service Provider shall grant unrestricted and effective access to data related to the outsourced activities.
39. The relevant business premises of the Service Provider; subject to appropriate security protocols, for the purpose of effective oversight use by the Bank, their auditors, regulators and other relevant Competent Authorities, as authorized under law.
40. In case the technology/software platform/ hardware / infrastructure offered under the solution on hosted model reaches end of life / support during the contract period, the

bidder has to ensure that the systems are either replaced or upgraded at their/bidders own cost without any disruption in the ongoing business transactions of the Bank.

41. Bidder shall not propose any solution/components which is near to end of life or end of support during the tenure of the contract.
42. The company shall comply to the Master Directions of RBI on IT outsourcing and bank's policy on IT Outsourcing with specifically on following points:
 - i. *The service provide shall ensure that the Bank has an effective access to all data, books, records, information, logs, alerts and business premises relevant to the outsourced activity of the Bank, available with the service provider;*
 - ii. *The service provider shall facilitate regular monitoring and assessment of the service provider by the Bank for continuous management of the risks holistically, so that any necessary corrective measure can be taken immediately;*
 - iii. *The service provider shall inform the Bank about the material adverse events (e.g., data breaches, denial of service, service unavailability, etc.) and the incidents required to be reported to Bank to enable Bank to take prompt risk mitigation measures and ensure compliance with statutory and regulatory guidelines;*
 - iv. *The service provider shall ensure that the services being offered are in compliance with the provisions of Information Technology Act, 2000, other applicable legal requirements and standards to protect the customer data;*
 - v. *The service provider shall ensure that storage of data (as applicable) is only in India as per extant regulatory requirements;*
 - vi. *The service provider shall provide bank with details of data (related to Bank and its customers) captured, processed and stored;*
 - vii. *The service provider shall not share any types of data/ information that the service provider (vendor) is not permitted to share with Bank's customer and / or any other party;*
 - viii. *The Service provider shall have in place effective contingency plan(s) to ensure business continuity and testing requirements, in line with the Banks BCP;*
 - ix. *Bank shall have right to seek information from the service provider about the third parties (in the supply chain) engaged by the former;*
 - x. *The service provider shall be contractually liable for the performance and risk management practices of its sub-contractors;*
 - xi. *It shall be obligation of the service provider to comply with directions issued by the RBI in relation to the activities outsourced to the service provider, through specific contractual terms and conditions specified by the Bank;*
 - xii. *It shall be obligation of the service provider to co-operate with the relevant authorities in case of insolvency/ resolution of the Bank;*
 - xiii. *There shall be a provision to consider skilled resources of service provider who provide core services as "essential personnel" so that a limited number of staff*

- with back-up arrangements necessary to operate critical functions can work on-site during exigencies (including pandemic situations);*
- xiv. *The service provider should have a suitable back-to-back arrangements with the concerned OEM, if applicable*

Annexure N: Hosting Assessment Checklist

	Control Domain	CID	SP Assessment Questions	Requirement	Answer (Yes/No) 1 Marks for each Point	Reference
		CO.01	*Do you allow customers to view your third party audit reports?	Mandatory		
		CO.02	*Do you conduct network penetration tests of your service infrastructure regularly? If yes please elaborate on your test and remediation process	Mandatory		
		CO.03	*Do you conduct regular application penetration tests of your infrastructure according to the industry best practices? If yes please elaborate on your test and remediation process.	Mandatory		
		CO.04	*Do you conduct internal audits regularly according to the industry best practices? If yes please elaborate on your test and remediation process.	Mandatory		
		CO.05	*Do you conduct external audits regularly according to the industry best practices? If yes please elaborate on your test and remediation process.	Mandatory		
		CO.06	Are the results of the network penetration tests available to customers at their request?			
		CO.07	*Are the results of internal and external audits available to customers at their request?	Mandatory		
	Third Party Audits	CO.08	Do you permit customers to perform independent vulnerability assessments?			

	Contact / Authority Maintenance	CO.9	Do you maintain updated liaisons and points of contact with local authorities? If yes then how frequently you validate the contacts?			
	Information System Regulatory Mapping	CO.10	*Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single customer only, without inadvertently accessing another customer's data?	Mandatory		
		CO.11	*Do you have capability to logically segment, isolate and recover data for a specific customer in the case of a failure or data loss?	Mandatory		
	Intellectual Property	CO.12	*Do you have policies and procedures in place describing what controls you have in place to protect customer's data marked as intellectual property?	Mandatory		
		CO.13	If utilization of customers services housed is mined for provider benefit, are the customers' defined IP rights preserved?			
		CO.14	If utilization of customers services housed is mined for provider benefit, do you provide customers the ability to opt- out?			
INFORMATION GOVERNANCE	Ownership	IG.01	*Do you follow or support a structured data-labelling standard (ex. ISO 15489, Oasis XML Catalogue Specification, CSA data type guidance)? If yes please specify	Mandatory		

	Classification	IG.02	Do you provide a capability to identify virtual machines via policy tags/metadata?			
		IG.03	Do you provide a capability to identify hardware via policy tags/metadata/hardware tags?			
		IG.04	Do you have a capability to use system geographic location as an authentication factor?			
		IG.05	*Can you provide the physical location/geography of storage of a customer's data upon request?	Mandatory		
		IG.06	*Do you allow customers to define acceptable geographical locations for data routing or resource instantiation?	Mandatory		
	Handling / Labelling / Security Policy	IG.07	Do you consider all customer data to be "highly sensitive "and provide the same protection and controls across the board or you apply the controls according to the data specific classification or label?			
		IG.08	*Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?	Mandatory		
INFORMATION GOVERNANCE	Retention Policy	IG.09	*Do you have technical control capabilities to enforce customer data retention policies?	Mandatory		
		IG.10	*Do you have a documented procedure for responding to requests for customer data from governments or third parties?	Mandatory		
	Secure Disposal	IG.11	*Do you support secure deletion (ex. degaussing / cryptographic wiping) of	Mandatory		

			archived data as determined by the customer?			
		IG.12	*Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of customer data once a customer has exited your environment or has vacated a resource?	Mandatory		
	Nonproduction Data	IG.13	*Do you have procedures in place to ensure production data shall not be replicated or used in your test environments?	Mandatory		
	Information Leakage	IG.14	*Do you have controls in place to prevent data leakage or intentional/accidental compromise between customers in a multi-customer environment?	Mandatory		
		IG.15	Do you have a Data Loss Prevention (DLP) or extrusion prevention solution in place for all systems which interface with your service offering?			
PHYSICAL ACCESS	Policy	PA.01	*Can you provide evidence that policies and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas?	Mandatory		
	User Access	PA.02	*Pursuant to local laws, regulations, ethics and contractual constraints are all employment candidates, contractors and third parties subject to background checks?	Mandatory		

	Controlled Access Points	PA.03	*Are physical security perimeters (fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) implemented?	Mandatory		
	Secure Area Authorization	PA.04	*Do you allow customers to specify which of your geographic locations their data is allowed to traverse into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)?	Mandatory		
	Unauthorized Persons Entry	PA.05	*Are ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises monitored, controlled and isolated from data storage and process?	Mandatory		
	Offsite Authorization	PA.06	Do you provide customers with documentation that describes scenarios where data may be moved from one physical location to another? (ex. Offsite backups, business continuity failovers, replication)			
	Offsite equipment	PA.07	Do you provide customers with documentation describing your policies and procedures governing asset management and repurposing of equipment?			
	Asset Management	PA.08	*Do you maintain a complete inventory of all of your critical assets?	Mandatory		
HR	Employment	HR.01	*Do you specifically train your employees regarding their role vs. the customer's role in	Mandatory		

	Agreements		providing information security controls?			
		HR.02	Do you document employee acknowledgment of training they have completed?			
	Employment Termination	HR.03	*Are Roles and responsibilities for following performing employment termination or change in employment procedures assigned, documented and communicated?	Mandatory		
INFORMATION SECURITY	Management Program	IS.01	*Do you provide customers with documentation describing your Information Security Management System (ISMS)?	Mandatory		
	Management Support / Involvement	IS.02	*Are policies in place to ensure executive and line management take formal action to support information security through clear documented direction, commitment, explicit assignment and verification of assignment execution?	Mandatory		
	Policy	IS.03	Do your information security and privacy policies align with particular standards (ISO-27001, NIA, CoBIT, etc.)?			
		IS.04	Do you have agreements which ensure your providers adhere to your information security and privacy policies?			
		IS.05	*Can you provide evidence of due diligence mapping of your controls, architecture and processes to regulations and/or standards?	Mandatory		

	Baseline Requirements	IS.06	*Do you have documented information security baselines for every component of your infrastructure (ex. Hypervisors, operating systems, routers, DNS servers, etc.)?	Mandatory		
		IS.07	Do you have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?			
		IS.08	*Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?	Mandatory		
	Policy Reviews	IS.09	Do you notify your customers when you make material changes to your information security and/or privacy policies?			
INFORMATION SECURITY		IS.10	*Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	Mandatory		
		IS.11	*Are employees made aware of what action might be taken in the event of a violation and stated as such in the policies and procedures?	Mandatory		
	User Access Policy	IS.12	*Do you have controls in place ensuring timely removal of access rights and permissions which is no longer required?	Mandatory		
		IS.13	*Do you provide metrics which track the speed with which you are able to remove access rights following a request from us?	Mandatory		

	User Access Restriction / Authorization	IS.14	*Do you document how you grant and approve access to customer data?	Mandatory		
		IS.15	Do you have a method of aligning provider and customer data classification methodologies for access control purposes?			
	User Access Revocation	IS.16	*Is timely de-provisioning, revocation or modification of user access to the organizations systems, information assets and data implemented upon any change in status of employees, contractors, customers, business partners or third parties?	Mandatory		
	User Access Reviews	IS.17	*Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your customers)?	Mandatory		
		IS.18	*If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?	Mandatory		
		IS.19	Will you share user entitlement remediation and certification reports with your customers, if inappropriate access may have been allowed to customer data?			
	Training / Awareness	IS.20	*Do you provide or make available a formal security awareness training program access and data management	Mandatory		

			issues (i.e., multi-tenancy, nationality, delivery model segregation of duties implications, and conflicts of interest) for all persons with access to customer data?			
		IS.21	*Are administrators properly educated on their legal responsibilities with regard to security and data integrity?	Mandatory		
	Industry Knowledge / Benchmarking	IS.22	Do you participate in industry groups and professional associations related to information security?			
		IS.23	*Do you benchmark your security controls against industry standards?	Mandatory		
	Roles / Responsibilities	IS.24	Do you provide customers with a role definition document clarifying your administrative responsibilities vs. those of the customer?			
	Management Oversight	IS.25	Are Managers responsible for maintaining awareness of and complying with security policies, procedures and standards that are relevant to their area of responsibility?			
INFORMATION SECURITY	Segregation of Duties	IS.26	Do you provide customers with documentation on how you maintain segregation of duties within your service offering?			
	User Responsibility	IS.27	*Is your staff made aware of their responsibilities for maintaining awareness and compliance with our published security policies, procedures,	Mandatory		

			standards and applicable regulatory requirements?			
		IS.28	Are users made aware of their responsibilities for maintaining a safe and secure working environment?			
		IS.29	Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?			
Workspac e		IS.30	*Do your data management policies and procedures address customer and service level security requirements?	Mandatory		
		IS.31	Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to customer data?			
		IS.32	*Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?	Mandatory		
Encryptio n		IS.33	*Do you have a capability to allow creation of unique encryption keys per customer?	Mandatory		
		IS.34	Do you support customer generated encryption keys or permit customers to encrypt data to an identity without access to a public key certificate. (e.g. Identity based encryption)?			

	Encryption Key Management	IS.35	*Do you encrypt customer data at rest (on disk/storage) within your environment?	Mandatory		
		IS.36	*Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	Mandatory		
		IS.37	Do you have a capability to manage encryption keys on behalf of customers?			
		IS.38	Do you maintain key management procedures?			
	Vulnerability/Patch Management	IS.39	*Do you conduct network-layer vulnerability scans regularly?	Mandatory		
		IS.40	*Do you conduct application-layer vulnerability scans regularly?	Mandatory		
		IS.41	*Do you conduct local operating system-layer vulnerability scans regularly?	Mandatory		
		IS.42	*Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems?	Mandatory		
INFORMATION SECURITY		IS.43	Will you provide your risk-based systems patching timeframes to your customers upon request?			
	Antivirus / Malicious Software	IS.44	Do you deploy multi anti-malware engines in your infrastructure?			

	IS.45	Do you ensure that security threat detection systems which use signatures, lists, or behavioural patterns are updated across all infrastructure components within industry accepted timeframes?			
Incident Management	IS.46	*Do you have a documented security incident response plan?	Mandatory		
	IS.47	Do you integrate customized customer requirements into your security incident response plans?			
	IS.48	Do you have a CERT function (Computer Emergency Response Team)?			
	IS.49	Do you publish a roles and responsibilities document specifying what you vs. your customers are responsible for during security incidents?			
Incident Reporting	IS.50	Does your security information and event management (SIEM) system merge data sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?			
	IS.51	Does your logging and monitoring framework allow isolation of an incident to specific customers?			
Incident Response Legal Preparation	IS.52	*Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes & controls?	Mandatory		
	IS.53	*Does your incident response capability include the use of	Mandatory		

INFORMATION SECURITY			legally admissible forensic data collection and analysis techniques?			
		IS.54	*Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific customer without freezing other customer data?	Mandatory		
		IS.55	Do you enforce and attest to customer data separation when producing data in response to legal subpoenas?			
	Incident Response Metrics	IS.56	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?			
		IS.57	Will you share statistical information security incident data with your customers upon request?			
	Acceptable Use	IS.58	Do you provide documentation regarding how you may utilize or access customer data and/or metadata?			
		IS.59	Do you collect or create metadata about customer data usage through the use of inspection technologies (search engines, etc.)?			
		IS.60	Do you allow customers to opt-out of having their data/metadata accessed via inspection technologies?			
	Asset Returns	IS.61	*Are systems in place to monitor for privacy breaches and notify customers	Mandatory		

		expeditiously if a privacy event may have impacted their data?			
	IS.62	*Is your Privacy Policy aligned with industry standards and Indian Law	Mandatory		
e-Commerce Transactions	IS.63	Do you provide standard encryption methodologies (3DES, AES, etc.) to customers in order for them to protect their data if it is required to traverse public networks? (ex. the Internet)			
	IS.64	*Do you utilize standard encryption methodologies any time your infrastructure components need to communicate to each other over public networks (ex. Internet-based replication of data from one environment to another)?	Mandatory		
Audit Tools Access	IS.65	Do you restrict, log, and monitor access to your information security management systems? (Ex. Hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)			
Diagnostic / Configuration Ports Access	IS.66	*Do you ensure hardening of admin workstations and Role Based Access Control to enforce the 'least privilege' principle	Mandatory		
Network / Infrastructure Services	IS.67	Do you collect capacity and utilization data for all relevant components of your service offering?			

		IS.68	Do you provide customers with capacity planning and utilization reports?			
	Portable / Mobile Devices	IS.69	*Do you allow mobile devices in your facility for administration purposes (e.g., tablets,)?	Mandatory		
	Source Code Access Restriction	IS.70	*Are controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?	Mandatory		
		IS.71	*Are controls in place to prevent unauthorized access to customer application, program or object source code, and assure it is restricted to authorized personnel only?	Mandatory		
	ESV Programs Access	IS.72	*Are utilities that can significantly manage virtualized partitions (ex. shutdown, clone, etc.) appropriately restricted and monitored?	Mandatory		
		IS.73	Do you have a capability to detect attacks which target the virtual infrastructure directly (ex. shimming, Blue Pill, Hyper jumping, etc.)?			
		IS.74	*Are attacks which target the virtual infrastructure prevented with technical controls?	Mandatory		
LEGAL	Non-disclosure Agreements	LG.01	*Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented and reviewed at planned intervals?	Mandatory		

	Third Party Agreements	LG.02	*Can you provide a list of current 3rd party organization that will have access to the customer's (My) data?	Mandatory		
OPERATIONS MANAGEMENT	Policy	OM.01	Are policies and procedures established and made available for all personnel to adequately support services operations roles?			
	Documentation	OM.02	Are Information system documentation (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure Configuring, installing, and operating the information system?			
	Capacity / Resource Planning	OM.03	Do you provide documentation regarding what levels of system (network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?			
		OM.04	*Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	Mandatory		
	Equipment Maintenance	OM.05	If using virtual infrastructure, does your solution include hardware independent restore and recovery capabilities including offsite storage of backups?			
		OM.06	*If using virtual infrastructure, do you provide customers with a capability to restore a Virtual Machine to a previous state in time?	Mandatory		

		OM.07	*If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new provider?	Mandatory		
		OM.08	*If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?	Mandatory		
		OM.09	Do you share reports on your backup/recovery exercise results?			
		OM.10	Does your solution include software / provider independent restore and recovery capabilities?			
RISK MANAGEMENT	Program	RM.01	Is your organization insured by a 3rd party for losses?			
		RM.02	*Do your organization's service level agreements provide customer remuneration for losses they may incur due to outages or losses experienced within your infrastructure?	Mandatory		
	Assessments	RM.03	*Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	Mandatory		
		RM.04	Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g., audit			

		results, threat and vulnerability analysis, and regulatory compliance)?			
Mitigation / Acceptance	RM.05	*Are risks mitigated to acceptable levels based on company-established criteria in accordance with reasonable resolution time frames?	Mandatory		
	RM.06	*Is remediation conducted at acceptable levels based on company-established criteria in accordance with reasonable time frames?	Mandatory		
Business / Policy Change Impacts	RM.07	*Do risk assessment results include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective?	Mandatory		
Third Party Access	RM.08	Do you monitor service continuity with upstream internet providers in the event of provider failure?			
	RM.09	Do you have more than one provider for each service you depend on?			
	RM.10	Do you provide access to operational redundancy and continuity summaries which include the services on which you depend?			
	RM.11	Do you provide the customer the ability to declare a disaster?			
	RM.12	Do you provide a customer triggered failover option?			
	RM.13	*Do you share your business continuity and redundancy plans with your customers?	Mandatory		

SW DEPLOYMENT	New Development / Acquisition	SD.01	*Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities?	Mandatory		
	Production Changes	SD.02	*Do you provide customers with documentation which describes your production change management procedures and their roles/rights/responsibilities within it?	Mandatory		
	Quality Testing	SD.03	Do you provide your customers with documentation which describes your quality assurance process?			
	Outsourced Development	SD.04	*Do you have controls in place to ensure that standards of quality are being met for all software development?	Mandatory		
		SD.05	*Do you have controls in place to detect source code security defects for any outsourced software development activities?	Mandatory		
	Unauthorized Software Installations	SD.06	*Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	Mandatory		
DISASTER RECOVERY	Impact Analysis	DR.01	Do you provide customers with on-going visibility and reporting into your operational Service Level Agreement (SLA) performance?			

		DR.02	Do you provide customers with on-going visibility and reporting into your SLA performance?			
	Business Continuity Planning	DR.03	Are you BS25999 or ISO 22301 certified?			
		DR.04	Do you provide customers with geographically resilient hosting options?			
	Business Continuity Testing	DR.05	*Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	Mandatory		
	Environmental Risks		*Is physical protection against damage from natural causes and disasters as well as deliberate attacks anticipated, designed and countermeasures applied?	Mandatory		
	Equipment Power Failures	DR.07	*Are Security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	Mandatory		□
	Power / Telecommunications	DR.08	Do you provide customers with documentation showing the transport route of their data between your systems?			
		DR.09	Can customers define how their data is transported and through which legal jurisdiction?			
ARCHITECTURE	Customer Access Requirements	AR.01	Are all identified security, contractual and regulatory requirements for customer access contractually addressed			

			and remediated prior to granting customers access to data, assets and information systems?			
		AR.02	Do you use open standards to delegate authentication capabilities to your customers?			
		AR.03	*Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	Mandatory		
		AR.04	Do you have a Policy Enforcement Point capability (ex. XACML) to enforce regional legal and policy constraints on user access?			
		AR.05	Do you have an identity management system in place which enables both role-based and context-based entitlement to data (enables classification of data for a customer) if requested?			
		AR.06	*Do you provide customers with strong (multifactor) authentication options (digital certs, tokens, biometric, etc...) for user access?	Mandatory		
		AR.07	Do you allow customers to use third party identity assurance services?			
		AR.08	Do you utilize an automated source-code analysis tool to detect code security defects prior to production?			
		AR.09	*Do you verify that all of your software suppliers adhere to	Mandatory		

			industry standards for Systems/Software Development Lifecycle (SDLC) security?			
	Data Integrity	AR.10	*Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	Mandatory		
	Production / Nonproduction Environments	AR.11	*Do you provide customers with separate environments for production and test processes?	Mandatory		
		AR.12	Do you provide customers with guidance on how to create suitable production and test environments?			
	Remote User Multifactor Authentication	AR.13	*Is multi-factor authentication required for all remote user access?	Mandatory		
ARCHITECTURE	Network Security	AR.14	Do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?			
	Wireless Security	AR.15	*Are policies and procedures established and mechanisms implemented to protect network environment perimeter and configured to restrict unauthorized traffic?	Mandatory		

		AR.16	*Are policies and procedures established and mechanisms implemented to ensure proper security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings? (e.g., encryption keys, passwords, SNMP community strings, etc.)	Mandatory		
		AR.17	*Are policies and procedures established and mechanisms implemented to protect network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?	Mandatory		
	Shared Networks	AR.18	*Is access to systems with shared network infrastructure restricted to authorized personnel in accordance with security policies, procedures and standards. Networks shared with external entities shall have a documented plan detailing the compensating controls used to separate network traffic between organizations?	Mandatory		
	Clock Synchronization	AR.19	*Do you utilize a synchronized time-service protocol (ex. NTP) to ensure all systems have a common time reference?	Mandatory		
	Equipment Identification	AR.20	Is automated equipment identification used as a method of connection authentication to validate connection authentication integrity based on known equipment location?			

	Audit Logging / Intrusion Detection	AR.21	*Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents?	Mandatory		
		AR.22	*Is Physical and logical user access to audit logs restricted to authorized personnel?	Mandatory		
		AR.23	*Can you provide evidence that due diligence mapping of currently applicable regulations and standards to your controls/architecture/processes has been done?	Mandatory		
	Mobile Code	AR.24	*Is mobile code tested (in terms of security) before its installation and use and the code configuration checked to ensure that the authorized mobile code operates according to a clearly defined security policy?	Mandatory		
		AR.25	*Is all unauthorized mobile code prevented from executing?	Mandatory		