REQUEST FOR PROPOSAL (RFP)

FOR

MOBILE DEVICE MANAGEMENT (MDM) SOLUTIONS

FOR

UBI Services Limited
504-506, 5th Floor, Centrum, S. G. Barve Road, Wagle Estate,
MIDC, Thane (W), Pin code – 400604.

BID FOR SUPPLY OF MDM SOLUTIONS

Sr No.	Particulars	Page No.
1	Background	3
2	Requirements	3
3	Scope of Work	3
4	Eligibility Criteria (Technical & Commercial)	4 – 5
5	Bid Details in Brief	5 – 6
6	Empanelment Period and Terms	7
7	Bid Evaluation Criteria	8
8	MDM Solution (Annexure A)	9-11

1. BACKGROUND: -

UBI Services Limited (“UBISL” or “The Company”) is a wholly owned subsidiary of Union Bank of India (UBI) engaged in various activities that range from distribution of Retail Loan products & manpower solutions to the Parent Bank. The Company is a Corporate Selling Agent of Parent Bank and into distribution of various retail and other loan products mainly of Home Loan, Car Loan, Education Loan, and MSME Loan etc. The Company is also providing manpower solutions to various department / process of parent Banks like Centralized Vendor Payment Cell (CVPC), Core Banking Solutions (CBS) Helpdesk, Credit Compliance & Monitoring Cell (CMCC), etc.

2. REQUIREMENTS:

UBI Services Limited (“UBISL” or “The Company”) invites quotations from suppliers (“Suppliers or Bidder”) from open market from Mumbai, Navi Mumbai and Thane Locations. Interested suppliers who deal in MDM Solutions (Items as per **Annexure A**) related materials or work and meeting the eligibility criteria shall respond to these bid documents. Suppliers shall be selected based on technical scrutiny followed by Financial Bid.

3. SCOPE OF WORK:

The selected Bidder shall supply MDM Solutions Approximate 2400 licenses based on Requirement as mentioned in Annexure - A.

4 ELIGIBILITY CRITERIA:

Only those Bidders who fulfill the following criteria are eligible to respond to the RFP document. Offers received from the bidders who do not fulfill following criteria are considered as ineligible bidder.

(a) TECHNICAL BID:

S No.	Eligibility Criteria	Documents Required
1	Bidder must be legally registered entity i.e. Registered Firm / Limited Liability Partnership / Registered Domestic Company	Registration certificate issued by Registrar of Firms / Ministry of Corporate Affairs etc. Also Shop & Establishment License issued by local authority.
2	Valid / Active Shop & Establishment, PAN and GST registration numbers	Self-certified S&E Certificate, PAN and GST copies
3	Annual Turnover of Rs. 1.5 Cr. for the last three financial years i.e. FY 2021-22, 2022-23 & 2023-24.	Audited Financial Statements for the last three years (if not audited then Financial Statement certified by Chartered Accountant along with Income Tax Return filed for respective year)
4	Work Experience: - The bidder / supplier should have a minimum of Two year of experience in supply of MDM Solutions to any organization like Banks, Govt. Organizations, PSU, Pvt. Ltd. Organization etc.	Copies of purchase orders from the organizations shall be submitted.

5	The bidder / suppliers should not have been blacklisted by any company in the past or services terminated due to poor performance	An undertaking stating that the Company / Firm have not been blacklisted should be submitted.

(b) COMMERCIAL BID: -

- The Bidder should submit the bid which will contain a Scope of work (as referred in Annexure A).
- The Bidder should give MRP and Quoted / Offered Price.

5. BID DETAILS IN BRIEF:

S No.	Description	Details
1	Bid / RFP No. & Date	UBISL/RFP/IT/2025/002 Dated July 02, 2025
2	Brief Description of the RFP	MDM Solution supply as mentioned in Annexure A
3	Address for Communication	**IT Manager** **UBI Services Limited** **Registered / Head Office: Unit No. 504-506, 5th Floor, Centrum, Wagle Estate, Opp. Raila Devi Lake, Near Satkar Hotel, Thane West, Maharashtra, Pin – 400 604.** **Phone No.: 022 – 6930 3001, 8880141068** **Email: - tenders@ubisl.co.in**

S No.	Description	Details
4	Date of Issue	**July 05, 2025**
5	Pre-Bid Meeting	**July 11, 2025**
6	Last Date of submission of Bids	**July 19, 2025, 6:00 PM**
7	Date and time of opening Technical Bids.	**July 22, 2025**
8	Date of Evaluation of Technical bids and opening financial bids.	**July 24, 2025**

The bid documents should be delivered / submitted in sealed envelopes and scribed as "**BID for MDM Solutions Supply To UBISL**" to address mentioned above before last date of submission of bids. **The Bidder should compile two separate envelopes, one for technical bid (Documents and technical information) another for Financial Bid which will contain a standard quantity(Number of licenses), MRP and Quoted / Offered Price etc.**

The bidder can send their tender documents in soft copy via email to tenders@ubisl.co.in but documents should be password protected and password can be shared to Manager IT at the time of opening of bid documents which shall be communicated separately.

- The Bid / Offer should be complete in all respects and contain all information asked for in this document
- The Company or UBISL may, at its discretion, extend this deadline for submission of bids by amending the RFP Document
- The Bid should be signed by the authorized signatory of the bidder. A Power of attorney or letter of authority to that effect shall be submitted by the bidder along with bid submission.
- All supporting documents / annexures should be duly signed and stamped by

authorized signatories.

- The submitted bids should be valid for 90 days from the last date of submission of bid.

6. EMPANELMENT PERIOD AND TERMS:

The empanelment period will be valid for a period of one years (12 months) from the date of issue of an empanelment letter or purchase order. The review of the empaneled vendor may be conducted annually to review the quality of products delivered, timelines and negotiation in products prices. Based on performance, the company may consider extending the term, subject to mutually agreed upon terms and conditions. The Company may terminate the services of empaneled vendors at its discretion based on review and shall have the right to cancel this panel of vendors at any time during the empanelment period.

The Company is in process of empanelment of vendor / supplier for procurement of MDM Solutions for a period of one year. The Company will shortlist three vendors / suppliers based on the following criteria.

- Technically qualified vendors (Top 3)
- Lowest quoted Cost / discount offered (L1, L2, & L3)
- implementation period

The company will place the order to lowest quoted vendor.

7. BID EVALUATION CRITERIA:

Bidder must qualify the technical eligibility criteria and should submit the required documentary proofs as indicated above. Bids which fail to qualify for any of the following criteria will be rejected. To evaluate the technical and commercial bid, the procurement committee constituted by the Company shall examine the documents furnished by the Bidder in the Technical Bid and Presentation to be given by the bidder. Only those bids which satisfy the Eligibility Criteria will be eligible for negotiation of quoted price.

Sr No.	Bidder Credentials	Max. Marks	Supporting Documents
1	Annual turnover more than Rs.1.50 Cr. in the last three financial years	20	Audited / Certified Financial Statement for last three years
2	Minimum Two year of experience in MDM Implementation to Corporates/ Banks/ PSU / Govt. Organizations.	20	Copies of purchase orders from the organizations shall be submitted.
3	Bidder should not be blacklisted by any corporate / bank for poor performance.	20	Undertaking by Bidder
4	Provide Draft Timelines for Implementation and previous implementation schedule and UAT Report	40	1. Tentative timeline for implementation from the date of PO. 2. On letter head or other relevant documents required at least last two company's where implemented with timelines.
	TOTAL	**100**	

Annexure A

8. Scope of Work – MDM Solution.

Solution should be able to restrict (allow/block/step up authentication) access to corporate resources based on risky sign-ins, malicious IPs, anonymous logins in real time & based on conditional access.

Solution should provide native integration with proposed email, collaboration and unified communication systems

Solution should be able to integrate with Digital Rights Management solutions to protect data in transit

MDM solution should add security by wrapping app to apply a layer of security and policy management, with/without a SDK or source code changes For Android, IOS and Windows.
- User authentication, re-authentication, and single sign-on
- Data Encryption (FIPS Certified Algorithms)
- Enabling Offline Access
- Enabling document sharing, copy/paste or other data loss policies
- Secure Network Communication
- Jailbreak / root detection

MDM solution should be able to restrict users to have only work mail
- secure app that brings organization/corporate email, calendar, contacts, notes, and tasks to the users.
- Email data at rest on the device must be protected with FIPS-certified encryption that is independent of the device to help secure organization/corporate data in the event the device passcode is compromised.
- Secure application days by configuring security policies such as preventing copy/paste of content or limiting the apps in which email attachments can be opened.

MDM solution should have work web - secure Web browser to provide safe access to internal Web-based applications and content.

MDM solution should provide application management that enables self-service distribution of apps to employees and other authorized users, such as contractors or partners with Work Hub.

The Solution must be SaaS based & the OEM should have the SOC 2/SOC 3 Certificate.

The solutions should have the capability to Whitelist/Blacklist application installation by software publisher, application, Software category/genre (Application Categorization), URLs, application hash etc

The solution should have the capability to rotate the passwords of the local admin accounts

The blacklist/Whitelist/Elevation should work for all user categories such as end user, local admin user, domain user etc.

The solution to be able track the geo location of the endpoints

The solution should be able to work offline for the blacklist/whitelist profiles

MDM solution should provide checklist for CIS benchmark for iOS and macOS devices.

Solution must be able to encrypt devices and must be able to deploy certificates centrally.

Solution should be able to provide insights into employee experience like Proactive Avg. resource Usage, Device Health Monitoring etc.

Solution should be able to restrict (allow/block/step up authentication) access to corporate resources available over intranet and intranet from devices only compliant to organization policy like Network location, Managed Devices, Approved applications and enforce users if they are not adhering to corporate polices.

Mobile Device Management solution should have centralized system for device management and data security for the complex and heterogeneous mobile device landscape (iOS, Windows, Android, macOS, Linux, ChromeOS).

MDM solutions should allow mobile administrators to enable policy controls from passwords and application restrictions, certificate distribution and remote actions like device lock or wipe. Solution should be able to do out-of-the-box & custom compliance check on the managed devices based on device status (jailbreak, rooted, patch level, password complexity, encryption), user status (group membership), or threat protection status (security installed, definitions up-to-date and no malware)

MDM solution should provide end-user friendly apps delivery & application lifecycle for mobile devices of web apps, organization/corporate apps, third-party apps and apps form the OEMPlay store. It should support both push delivery of organization/corporate required apps and on-demand delivery of end user selected optional apps. To safeguard apps and data, IT can apply granular application-level policies related to user authentication, data loss prevention and more on managed, un- managed devices or BYOD devices.

MDM solution should report exact details of enterprise mobile assets at all times by leveraging built-in dashboards, reports, and alerts. Provides user, device, app, and profile details through detail views and customizable reports.

Solution should allow admin to create policies to restrict enrollment of devices based on conditions like : - No of device per user.

Solution should allow admin send custom notifications, term and conditions, organizational messages to the end users

MDM,MAM,IAM solution should be natively integrated as one solution.

Real time device data reporting and dashboard views. Centralized event log to capture all device and administrative events (logins, policy changes, application updates, configuration updates, etc.).

The solution should be able to control USB access, Bluetooth file sharing, the same should be workflow enabled for approval

Remote access should be possible without the RDP being enabled on the endpoints. The streamers should be implemented on-premises

The solution should also provide a feature of unattended access i.e. for approved user one can remote access to the endpoints based on approvals

The solution should be capable of monitoring the sessions of end- point users on need to do basis.