Annexure-D: Technical Specifications

Technical Bid Form: Supply, Installation, Maintenance of Cash Dispenser and providing Managed & Cash Replenishment services

TECHNICAL REQUIREMENTS

Brand of Cash Dispenser: <<Mention the Brand Name here >>

Manufacturer: <<Mention Manufacturer Name here >>

Model : <<Mention Model number here>>

The Technical Specifications mentioned below are the **minimum required** however, the **Bidders should offer their best/higher specifications and latest model Cash Dispenser,** which will meet BANK's requirement, satisfy or perform desired functions and comply with RBI guidelines also. The offer may not be evaluated and/or will be liable for rejection in case of non-submission of make and model of the items offered. All the features noted below are MANDATORY.

Cash Dispenser / ATM	
The Cash Dispensers proposed for deployment under this RFP shall comply with RBI, IBA, EMV, NPCI/NFS, UIDAI guidelines. If any new guidelines are issued by these organisations, the bidder shall arrange for its compliance / upgradation and bear the cost for the same during the warranty period i.e. 3 years (Three years) after 3 years i.e. during AMC it will be done on mutually agreed terms. This clause is also applicable for hardware and OS of Cash Dispenser / ATM, TSS, etc offered under this RFP.	
1. Processor and Hardware	
1.1	Intel core i3 Processor with 3.3 Ghz, 4MB cache and 6th generation or above.
1.2	8 GB DDR3 RAM or higher
1.3	2x 500 GB IDE/SATA HDD (Minimum)
1.4	USB ports in front for front access Cash Dispensers (Minimum 5 USB with At least 2 USB port on the front side)
1.5	101Keys Keyboard (optional)
1.6	Bidder should provide latest OS (In case of Windows, the same should be Windows 10 or higher Operating System and In case of Linux OS, the same should be latest version with latest service) . Bidder is responsible to upgrade the OS of Cash Dispensers or higher version before expiry of extended support at no additional cost during both warranty and AMC period. Further, Bidder should ensure that on upgradation, there should be no disruptions of service and no performance related issues faced.
1.7	OS hardening (with firewall). Cash Dispenser should be adequately hardened and only essential services should be activated. No malware including viruses, worms, Trojans should enter the Cash Dispenser and affect the system.
1.8	Cash Dispenser should be accessible to physically Challenged, Wheel Chair Access and Visually Challenged as per ADA/AFA & RBI guidelines
1.9	Cash Dispenser should support reversal message of transaction.

1.10	Multilingual Software for Customer Display apart from Hindi and English which will be provided by the Bank
1.11	Trace Features (Provide log file for all Messages received and sent by cash dispenser. Especially in networked conditions, log should provide information from where the message is received and to which the message sent on their IP addresses)
1.12	Remote login facility for such utilities like Remote load of screens, to shutdown, start cash dispenser clear fitness etc.

2. Currency Chest	
2.1	UL 291 Level1 certified secured chest / CEN1 Certified Secure Chest
2.2	S&G / MAS Hamilton (KABAMAS-CENCON) (Or an equivalent make, of high international repute) dual electronic combination lock of 6+6 digits with capability having One time combination (OTC) option and audit trail without any hardware change
2.3	Alarm sensors for temperature status, vibration status and chest open status while sending signal/messages to Switch/Management Centre
3. Hybrid Dip Card Reader	
3.1	Dip Smart Card Reader / Magnetic stripe Reader with capability to read track 1 & 2
3.2	EMV Level 1 Version 4.0 or later, as certified
3.3	Cash Dispenser should be ready for using EMV chip cards
3.4	Software, firmware, license for using smart card on Cash Dispenser
3.5	EMV software on Chip Card access for cash withdrawal in Cash Dispenser
3.6	Conformance to Rupay, Mastercard, VISA standards etc.
3.7	Contactless Card integration capability
3.8	Dip card reader should have anti skimming device with the capability to prevent further transaction/shutdown/offline the machine with generation of alerts to central monitoring system after the detection of skimming.
4. Screen Specifications	
4.1	15”LCD with Touch screen and 8 function keys (Optional)
4.2	Touch Screen Specifications: Industry Standard Protective Touch Screen
4.3	Vandal Screen with Privacy Filter
4.4	Rugged spill proof Triple DES enabled keyboard with polycarbonate tactile / stainless steel EPP pin pad keys, EPP pin pad to be PCI Compliant with sealed metal keypad
4.5	Touch screen with support for visually handicapped through Function Defined Keys 4 + 4 AND EPP
4.6	Braille stickers on all devices as per requirements to support the visually challenged
4.7	Voice guidance support with internal speakers & headphone jack
4.8	Multi-lingual screens (minimum 3 languages) as per Bank’s requirements to be supported.
5. Cash Dispenser	
5.1	Dispense minimum 40 currency notes per transaction.

5.2	Dispense used notes.
5.3	Capable to retract notes but this functionality should be in disabled mode.
5.4	Indication (visible & audible) of proper insertion of all cassettes.
5.5	2 x Double Pick Module, and 4 cassettes with lock & key/Latch/Secure Tag.
5.6	Reject BIN or Divert cassette bin with lock and key/Latch/Secure Tag with capacity to hold atleast 500 notes.
5.7	Each Cassette should hold minimum of 2500 currency notes.
5.8	Capable of Multi currency dispensing.
5.9	Capable of dispensing all denominations Rs.50, Rs.100, Rs. 200/-,Rs. 500/-, Rs.2000, as well as new denominations, if any, issued subsequently without any extra cost to the Bank. All cassettes should be adjustable to hold and dispense the currency notes if dimensions of currency notes are changed without any additional component requirement.
5.10	Dispense at least 8-10 notes per second.
5.11	Machines should not dispense soiled, mutilated notes.
5.12	Encrypted communication and trust relation should be established between PC core and dispenser.
5.13	Should not have any hardware module sensors which could be accessible by any end consumer either during idle state or during transaction processing.
5.14	Multi-media dispenser (ticket/coupon/stamp/ receipt) with bunch presenter.
5.15	Friction / Vacuum pick technology
5.16	Vendor to provide all CDs of same make, model and specifications i.e. single make and model. Any vandalised machine will also be replaced with the same make & model.
5.17	Should support pin based authorization of transactions
5.18	Dispense minimum 40 currency notes per transaction.
5.19	Dispense used notes.
6. DES chip / Security	
6.1	Capable of supporting Remote key Management – DES/RSA
6.2	Triple DES chip with encryption / verification / validation software. Should support AES without any additional hardware.
7. Integrated Cash Dispenser Surveillance Solution	
7.1	Solution must be able to capture image of the customer approaching and performing transactions at the Cash Dispenser. This solution should be an Integrated with the machine and capture images based on motion.
7.2	Solution should be able to store the images/video in a digital format for minimum 3 months at an average of 500 transactions per day.
7.3	Solution must provide an interface to browse, search and archive the stored video / images on hard disk or external media.
7.4	Solution must be able to capture & stamp the transaction information on the images.
7.5	Superimpose date, time and transaction data on to the recorded images.

7.6	The solution must not degrade the performance of Cash Dispenser, e.g. speed of normal transaction
7.7	The hardware should be integrated within the Cash Dispenser
7.8	Solution must be capable to take necessary backup of stored image and retrieval the same at any point of time.
7.9	Machine should support third camera if required which would be deployed by the Bank in Cash Dispenser lobby.
7.10	External dome camera along with required cabling. The angle of dome camera should be so as to cover the full view of person operating Cash Dispenser.
7.11	The solution must be capable of monitoring from a central location. The solution must be able to pull the required images from the central location and share the same over e-mail with bank as and when required.
7.12	The solution must have a search facility to locate an image/event by date and time, card no, transaction reference no. and Cash Dispenser ID.
8. Software Agent	
8.1	The Cash Dispenser should be capable of supporting a third party software agent such as SDMS/Infobase/Radia, etc. Bidder should provide software agent for EJ pulling and Remote Monitoring Software support for the Cash Dispenser to monitor its functions from a Central site. Bidder should install EJ software on all Cash Dispensers and pull the EJs on daily basis to its Managed service Centre.
8.2	Should be capable of interface using ISO message standard with Bank's ATM switch.
8.3	Software for reading EMV Chip cards, smart card/ chip card EMV Version 4.0, Level 2 approved terminal resident application
9. Connectivity	
9.1	Should have Network Interface Card 10/100 Ethernet Card
9.2	Should be capable of interfacing Bank's Switch IST using existing device handlers (NDC/D912) at no additional cost to the Bank
9.3	Cash Dispenser must support TCP/IP
9.4	Cash Dispenser should be Ipv6 Complaint
10. Others	
10.1	Minimum 40 Column 80 mm Graphic Thermal Receipt Printer
10.2	DMP/Graphic Thermal Journal Printer to print audit trail
10.3	Low media warning for all items viz. bills, journal roll, consumer printer roll etc.
10.4	Machine should be print customers slip in HINDI, ENGLISH and Regional Language.
10.5	EJ to be also written on Cash Dispenser hard disk and replicated on the second hard disk. The solution should include EJ viewer and support centralised EJ pulling
10.6	EJ should be non-editable with encryption or with checksum or any other solution to prove the authenticity of EJ before a third party such as the regulator (RBI) a Banking Ombudsman, Police Authorities
10.7	In-built SMPS to work on 230V 50 Hz power supply.
10.8	Support input voltage of 230V AC /50 Hz with +/- 5%variation.

10.9	Should provide hardware and software for the day-to-day operations required by the custodian.
10.10	Cash Dispenser should have pin pad shield covering all three sides.
11. Transactions to be made available at the Cash Dispenser with Interface / connectivity to Bank's ATM Switch and Core Banking Software	
11.1	Card less transactions to be made available.
11.2	Card based transactions to be made available.
11.3	Payment of taxes, Bills and any other value added services bank may have
11.4	Biometric Finger printer reader with Software (UIDAI Approved Standard). The bidder should upgrade the Biometric Finger printer reader with Software during the contract period as per UIDAI/any statutory authorities guidelines/directions without any additional cost to the Bank. Bank may ask to implement as and when required.
12. Interface for Banking Software & ATM Switch Connectivity	
12.1	Bidder shall provide software required for connecting the Cash Dispenser to Bank's own Network.
12.2	Bidder to provide utility for converting the Cash Dispenser files, Containing transaction details, into ASCII format.
12.3	Cash Dispenser should be preloaded with CEN XFS 3.0 compliant or equivalent layer and should be capable of running multi-vendor software
12.4	The model must support downloading of screens & state tables.
12.5	(Bank will only introduce Cash Dispenser bidder to CBS software vendor/Switch vendor and assist in obtaining clarifications, software etc., as may be needed from the latter. Bidder shall bear expenses, if any, for procuring such assistance/software etc.)
12.6	Required supporting Software to support visually challenged persons using the software (Bidder/OEM should mention the name of software).
12.7	EMV compliant software for CHIP Card reader along with license.
13. Others	
13.1	Bidder to integrate – where feasible -- the alarm sensors of the Cash Dispenser to the branch siren/hooter without any additional cost to Bank.
13.2	Cash Dispenser should have rear mirrors covering majority area of ATM site which allow users to see what is happening behind him when he enters the PIN to avoid shoulder surfing.
13.3	Cash Dispenser should have PIN pad shield covering all three sides to avoid shoulder surfing and capture by the external cameras.
13.4	Two Colour Branding as per Bank's requirement.
13.5	Bank stickers consisting of instruction set to the customers for operating Cash Dispenser's have to be affixed at Bidder's is cost on the fascia at the time of installation.
13.6	The Cash Dispensers need to be energy efficient. The Cash Dispenser s to be supplied have to be fully functional in extreme weather conditions (temperature, humidity, dust, etc) as per industry standard within the country
13.7	All operating system upgrades / proprietary software upgrades / patches/ licenses will be provided free of cost and also installed in all the Cash Dispenser s at no cost to the Bank for the entire period of support committed. OS Hardening has to be done for the

	Cash Dispensers. Bidder is responsible for ensuring that system does not get affected by virus/malware.
13.8	Modification of the software pertaining to Cash Dispenser for the purpose of enhancing the functionality will be done by Bidder at no additional cost to the Bank
14	**Control Measures**
14.1	**The Cash Dispenser / ATM should contain Anti-skimming device integrated with Switch with to prevent the skimming attacks without additional cost to the Bank.**
14.1 a	The device should be capable of providing comprehensive skimming protection solution which achieves the following objectives 1. Senses unauthorised attachment of any device on the card reader module **2.** Sends the signal to switch and further to the remote Management Centre to put the machine out of service as well as block the card reader from accepting any more card insertions.
14.2	**The Cash Dispenser / ATM deployed should be ready to carry out the EMV and PIN transactions from the day one without additional cost to the Bank for certification, licensing and testing etc**
14.3	**The Cash Dispenser / ATMs deployed should be integrated with TSS (Terminal Security Solution) covering various control measures as per the RBI/IBA/NPCI/VISA/MASTER/ any other statutory authorities' guidelines including Hard Disk encryption, whitelisting, disabling USB ports, disabling autorun facility applying the latest patches of OS, other software, time based admin access, BIOS passwords etc without additional cost to the Bank. The bidder is required to maintain the required set up at their Managed Service Centre or DC. This facility is to be provided without additional cost to the Bank.**

TSS Solution Specification Compliance:-	
S.No	**Minimum Functionality required for Terminal Security Solution**
1	**Terminal Security Client**
1.1	The TSS client software should be compatible with ATMs running on any version of latest OS (In case of Windows, the same should be Windows 10 or higher Operating System and In case of Linux OS, the same should be latest version with latest service) installed in the terminals.
1.2	The TSS client software should be able to manage policies on terminals in OS domain as well as in workgroup.
1.3	The TSS client software should protect the terminal from any attempt to change the terminal security settings, registry level changes or policies.
1.4	The TSS client software should be able to detect and prevent any malware and spyware attacks and intrusion programs.
1.5	The TSS client software should be password protected to prevent its un-installation, stopping, disabling or change of settings.
1.6	In the cases of TSS client software unable to communicate with the central TSS server, Security Solution Agent policies should work / be intact with the last uploaded policies.

TSS Solution Specification Compliance:-	
S.No	**Minimum Functionality required for Terminal Security Solution**
1.7	The TSS client software shall not have performance impact of the terminals and the peripheral devices e.g. Switch, CD, Bunch Note Acceptor.
2	**TERMINAL OS HARDENING & WHITELISTING**
2.1	The solution should harden the terminal operating system as per industry best practices and recommendations.
2.2	The solution should be able to remotely change the hardening policy of the terminal OS
2.3	The solution should be able to block USB Storage devices on the terminal through centralized Control.
2.4	The Operating System Hardening should be managed and administered centrally by the Facility Management Team.
2.5	The solution should have a user Interface to be able to customize and manage the hardening policies by the Facility Management Team.
2.6	During policy distribution to the ATMs, the hardening policies should be protected against manipulation
2.7	The hardening solution should also be incorporated to browsers and other software components running on self-service terminals e.g. personal firewalls, ip-address/ port management.
2.8	The solutions should protect against malware being injected on to the machine and any other unauthorised Software installations. Via local means e.g. USB drive, CDROM etc.
2.9	The solution should protect against the manipulation of executables e.g .. exe, .dll, .class etc. and scripts e.g .js, .bat etc.
2.10	The solution should protect against the unauthorized updating/ changing of configuration -property files
2.11	The solution should have firewall functionality
2.12	The solution should be capable of detecting and reporting any deviation/anomalies from the policies defined for the terminal.
2.13	The solution should issue alert/ warning/ prevent once a threat has been identified
2.14	The solution shall be able to disable Auto-run facility of exe file from a network or a USB port.
2.15	The solution should block the unauthorized installation and running of software and services.
2.16	Only permitted applications to be run in the terminals using Sandboxing concept, thus effectively nullifying the need of any anti-virus solution.
2.17	The solution should have capability to allocate only required ATM resources to the Whitelisted applications. During the running of the Whitelisted applications, TSS should monitor if only those resources are being accessed. In case of any deviation, alert should be raised and resources should be blocked.
2.18	Solution should be able to prevent terminal booting from any source / media other than Hard disk.
2.19	The patch management of the solution should be managed centrally by the Facility Management Team.
3	**TERMINAL ACCESS MANAGEMENT including One TIME Admin Access**
3.1	Solution should support user access to the terminals based on One Time expiring passwords as well as tokens.

TSS Solution Specification Compliance:-	
S.No	**Minimum Functionality required for Terminal Security Solution**
3.2	Solution should provide role based user access to the terminal files and settings.
3.3	Solution should support time bound password management.
3.4	The solution should allow for the remote user management.
3.5	The solution should support online and offline password management.
3.6	The solution shall be managed from a central point of management and should work with any standard terminal agent monitoring solution.
3.7	The solution shall allow remote management of user credentials according to strong password and industry requirements.
3.8	The solution shall allow an administrator to define different roles for various users & groups and assign each of them specific user rights.
4	**HARD DISK ENCRYPTION**
4.1	The solution should support Full hard disk encryption (FHDE)
4.2	The solution should enable for an exact status of disk encryption to be retrieved and display centrally on a monitoring system
4.3	The solution should be capable of changing the configuration of the hard disk encryption and the parameters used to encrypt the disk.
4.4	The solutions should have the capability to decrypt an ATM hard drive outside of the ATM for recovery purpose only using the relevant encryption key.
4.5	The ATMs should still cater to customers while the hard disk is being encrypted (during installation)
4.6	The solution shall support Encryption of all data (user files as well as system files) from an ATM's hard disk.
4.7	The solution shall protect data confidentiality when a system is out of operation.
5	**Requirements of Central Application Software**
5.1	The central solution (Hardware & Software) should be capable of supporting a minimum of 4000 terminals throughout the contract period.
5.2	The proposed solution should conform to all regulatory, statutory, legal acts and rules more particularly from Cyber Security and IT examination Cell (CSITE), RBI.
5.3	The Solution should support various dashboard views with filtering, sorting and report generation capabilities for instant access to security status of terminals/devices.
5.4	The software should have option to group the terminals based on various parameters (such as Make & Model, Zone, State, Test / Production etc.) for applying the policies and patches.
5.5	The solution should support Deploying and updating of Security Policies and configurations.
5.6	The solution should provide SMS and E-mail alerts for significant /critical events/changes.
5.7	The Central TSS server should be able to install patches and software in the terminals remotely.
5.8	The Solution shall have a Web Based interface for the Bank to monitor the performance and activities of the solution.
6	**Requirements for Central Server Hardware**

TSS Solution Specification Compliance:-	
S.No	**Minimum Functionality required for Terminal Security Solution**
6.1	Successful bidder shall design, size, supply, install and maintain the required hardware for Application software, middleware (if any), and Database etc for the total Terminal Security Solution.
6.2	The Hardware shall be sized to ensure that RAM & CPU Utilization shall not exceed more than 60% at any given point of time during the contract period. In case of violation, the hardware shall be upgraded by the bidder to reduce the utilization below 60% without any additional cost to the Bank.
6.3	The hardware technology proposed for the Terminal Security Solution should be the enterprise class, best of the breed, latest, tested and stable release of OEM and based on the latest platform enabling technology supporting the complete Terminal Security Solution.
6.4	The production hardware must be enterprise class with adequate vertical and horizontal scalability. There must be adequate CPUs and memory available to accommodate the sizing and growth aspirations of the Bank during the contract period.
6.5	Bidders are responsible to arrive at the sizing independently. The Bank is not responsible for any assumption made by the Bidder for not meeting the performance/service levels as desired in the document, the Bidder will at their cost carry out the necessary upgrades /replacements. The Bank will not pay any additional amount during the period of the contract.
6.6	The recommended hardware should have high reliability, fault tolerance, redundancy and high availability having no single point of failure in the hardware (NSPOF).
6.7	Bidder is required to provide the detailed configuration of the proposed Hardware.
6.8	The system should be configured in Active- Passive mode
6.9	Replication of data and configurations between Primary and DR Servers should be done on a daily basis. Bidder shall submit the details of synchronization methods.
6.10	Bidders shall size the DR site which must be capable of handling 100% of the storage load of DC production. The Servers-CPU, memory and other components shall be sized at 100% of the DC. The DR will be used during periodic
6.11	DR Drills to be conducted once in 3 months and DR to be made up whenever primary is not available. Penalty will be levied for Non-Performance of DR Drill once in 6 months.
6.12	All servers are required to have a minimum of dual 1000 Mbps Ethernet network interface cards (NIC) or a better equivalent installed on the board itself or on different slots. Each NIC will be cabled from a different module on the switch using gigabit speed cabling.
6.13	The offered servers must be current/ recent in the OEM"s product line and must be fully supported by the OEM for the duration of the project and for the warranty and post warranty.
6.14	The Operating System available in the servers should not be out of support by the OEM. In case of Windows Server OS, the OS version should be Windows 2016 and in case of RHEL server, the OS version should be 8.2.

The Bank reserves the right to consider only those bidders who can demonstrate a fair degree of accuracy in their Cash Dispensers. The Bank will test the machines at no cost to the bank, before placing the orders.

Additional terms

1. Deviations from technical specifications may be clearly indicated. Though the Bank has laid down the minimum configuration of both hardware and software of Cash Dispenser to meet present requirements, the Cash Dispenser should be upgradable to support any statutory /regulatory compliance requirements at mutually agreed cost.
2. Modification of the software pertaining to Cash Dispenser for the purpose of enhancing the functionality will be done by the bidder at no additional cost to the Bank.
3. All operating system upgrades / proprietary software upgrades / patches/ licenses will be provided free of cost and also installed in all the Cash Dispensers at no cost to the Bank for the entire period of support committed. OS Hardening has to be done for the Cash Dispensers. The bidder is responsible for ensuring that system does not get affected by virus/malware.
4. The Cash Dispensers need to be energy efficient. The Cash Dispensers to be supplied have to be fully functional in extreme weather conditions (temperature, humidity, dust, etc.) as per industry standard within the country.
5. Declaration:-

- We enclose the technical brochures for the model quoted.
- We agree for the delivery period of systems and installation as **mentioned under point 7.3.**
- We offer a comprehensive warranty period of 36 months from the date of installation/satisfactory commissioning of the equipment without any visit charges/part replacement charges and comprehensive AMC of 48 months after warranty period without any visit charges/part replacement charges.
- We agree for insuring the systems covering transit risk and storage cum erection risk for a period of one month from the date of delivery at the destination.
- We submit that we shall abide by your Standard terms and conditions governing the quotations and Warranty mentioned.
- We submit that we abide by the details given above.

SIGNATURE: -

Name & Designation:- Seal of the firm:-