

TECHNICAL SPECIFICATIONS OF THE COMPUTERISED ATTENDANCE RECORDING SYSTEM

Specifications	
Biometric Smart Card Reader	
1.1	The Bio-metric smart card reader shall have the Mifare® technology suitable to read Bio-metric smart card at a distance from 0.1 to 5 cm and read finger print with fault rejection ratio <1% and fault acceptance ratio <0.0001%
1.2	The Bio-metric smart card readers verification speed which includes reading of smart card, finger print and verification to give the output should be <= 1.5 second in 1:1 mode and identification speed shall be <= 1.5 second in 1:N mode. The supplier should mention the response time, when validation is done centrally from the central database located at the Informatics Centre. The number of punching per minute shall be indicated in the offer. Note:1:1 means comparing the finger print with the finger print image stored in the biometric smart card 1:N means comparing the finger print image with the finger print image with the finger print image stored in the readers memory.
1.3	40 nos of Bio-metric smart card readers needs to be installed for computerized attendance recording system. The actual number of readers may vary based on requirement. Additional card readers if needed, vendor shall supply at the finalized lease rental rate.
1.4	The Bio-metric smart card reader will have LCD wide –angle display to facilitate enhanced readability even in dim lighting conditions with Alphanumeric character, Backlit display and key pad(for recording various types of movements of employees).Under normal circumstances date, time, IN/OUT mode and status of memory consumed shall be displayed . While showing the card, staff no., punched time, date validation of each punch and status of memory consumed shall be displayed. Provision shall be provided on the Bio-metric smart card readers for audio and visual display (5 mm LEDs) with a relay output. The LED Indication for Power / battery mode, IN /OUT, Accept/reject and network Status to be provided. Required length of Power cable for the reader is under vendor’s scope.
1.5	The recording speed of Biometric smart card readers shall be ≤1 second and the readers will have relay output for external audio visual tower light to indicate the card acceptance .LED indication for Power /battery mode ,Accept/ reject and network Status to be provided .The supply and installation of audio visual tower light is vendor scope. The reader units shall support local verification/ verification of each punch.
1.6	The readers shall have minimum 128KB of SRAM for storing of transaction in case when the network is off line. It shall also have minimum 256KB flash memory for programs and other applications. In case when the network is off line, it should be capable of storing more than 8000 punch records(with date, time , card no. and recorder Sr No.) for minimum period of 48 Hours., and the biometric smart card readers should have the memory capacity to store minimum 1000 employees master details with 3 finger prints in local data base.
1.7	Reader shall be operated in 230V ,AC ±10% ,with Integrated surge protection system and ambient temperature of 10 to 48°C.In case of power failure, the reader shall be suitable to punch in /out by means of battery backup for a minimum period of 6Hours. The exact hours shall be indicated in the offer. Minimum 3Years In built battery backup for real time clock and stored data.
1.8	Data residing at local Bio-metric Smart Card readers will be updated in the Central Database Server in online mode as and when punching is recorded.
1.9	Provision shall be provided to assign a particular Reader unit or a group of designated units to a particular group of employees.
1.10	Provision shall be made in Reader unit to avoid any duplicate punch within a short span of time (adjustable) and the same shall be indicated as already punched the display.

1.11	The Reader unit shall be suitable to work in normal ambient conditions and in the gates where the readers will be mounted in open shelter.
1.12	Finger print Image shall compliance as per ISO/IEC 19794-4:2005(E), Minutiae data format standard as per ISO 19794-2:2005(E) and Contactless smart card reader should read the biometric smart cards complied with ISO 14443A.
1.13	Finger print sensor shall be impact resistant, scratch resistant, weather durable and Corrosion free optical non contact type Polaroid finger scanner. The finger print reader should be capable to read greasy and dirty finger print. The performance of the finger print reader should be demonstrated in the above mentioned conditions during the evaluation.
1.14	Supplier has to periodically replace the finger print reader sensor for every 18months or as and when need arises to ensure fail proof operation .Replacement should be done under BHEL supervision. Newness certificate should be produced for all sensors. Supplier has to mention the period of replacement of smart card sensor.
1.15	Finger print sensor Shall allow maximum allowable finger rotation +/-35° and displacement 5mm.
1.16	Finger print sensor Shall be conforming to ISO/IEC19794-4:2005(E) and should be able to transfer the finger print patterns of the card to the card reader memory and match these patterns when the finger is put on the sensor. The reader should be able to match any of 3 finger patterns.
1.17	The Readers unit shall have provision for configuration of percentage of comparison of finger print image.
1.18	The reader shall have in built TCP /IP with 100/1000 Mbps data transfer Speed.
1.19	The Reader unit shall be provided with an external switch to select IN/OUT and a reset switch if it is required to reset the reader.
Biometric Smart card	
2.1	Biometric smart cards for approximately 700 employees .The actual number of cards may vary based on requirement .
2.2	Bio-metric smart card shall be used for identity, attendance, movement, canteen, and library purpose. Preparation of Bio-metric smart card including preparation of finger print image and template are vendor scope.
2.3	Vendor shall quote separate rate for Contactless Blank Bio-metric smartcard (read and write)
2.4	Bio-metric Smart Card: compliance with ISO 14443A.Programmable smart card technology should have security protection for Read /Write. Smart card shall be of best quality &reputed make.
2.5	The card shall contain the following entities Front side 1.Company name and logo 2.Name, Staff No, 3.Department,Dept.No. &Designation 4.Card validity 5.Card control number 6.Signature of issuing authority 7.Employee's Photo 8.Two different color bands 9.Three finger prints image 10.Different color codes for Workers, Supervisors, Executives and Senior executives.
2.6	The card shall contain the following entities Back side 1.Existing standard Instruction 2.Signature of employee. 3.Blood Group 4.Date of Birth

2.7	The card should get debarred once the card validity which will be printed on the card is over. The card should not be put for further use thereafter.
2.8	Vendor shall maintain sufficient sets of PC, Smart Card Printer, Web Camera, Signature Pad, Scanner, Finger Print Reader/Recorder, Lamination machine and all consumables at M/s BHEL/Corporate R&D premises for preparation of Smart Cards on day to day basis without any delay for issuing smart cards for Employees. After authorization from HR/ Security, the vendor shall obtain details of Employees in respect of whom the smart cards are to be prepared such as taking Finger impression of Employees, Enrolment of Smart cards/details, printing of peelable PVC stickers and affixing the same on Smart Card, delivering the prepared cards to Security, obtaining signature of employee & authorized Security personnel on the card, and finally laminating the smart Card and delivering to the concerned employee under the supervision of permanent BHEL employee nominated by the security department within 2 days. This work should be carried out by the vendor initially and till the end of the contract period
General	
2.9.a	The Bio-metric smart card shall have a unique key number to relate with the staff no. to avoid duplication /copying.
2.9.b	In case missing of Bio –metric smart card, provision should be available to disable the Bio-metric smart card and issue a new Bio-metric smart card.
2.9.c	For card preparation vendor shall indicate in the offer the list of inputs required from BHEL.
2.9.d	BHEL is having digital photos with database of all employees, the same shall be used by the vendor to prepare card. However if BHEL prefers, recent photograph of the employee shall be taken and used in the card.
2.9.e	BHEL reserves right to increase or decrease the quantity based on final requirements.
Networking/Communication	
3.1	The existing data network, consisting of the fast Ethernet LAN shall be fully made use of for setting up the Computerized Attendance recording system.
3.2	Smart card reader /group of Smart card readers, shall be directly plugged into 100/1000 Mbps Ethernet switch ports wherever they fall within 100 meters.
3.3	The vendor is advised to visit the site to assess the exact requirements of the cabling and other Hardware equipment and accordingly inform it to the networking team of Informatics Centre.
3.4	Vendor should inform any problem regarding uptime and availability of network to BHEL immediately.
Software	
4.0	The Smartcard data shall be updated online in the database located at the Informatics centre.
4.1	Application Software Requirement Specifications: All Computerized Attendance Recording system related software, database, installation, Program development, Configuration, data entry and commissioning by the vendor.

5.HARDWARE SPECIFICATION

Attendance Server specification

S.No.	Parameter/Feature	Detailed Specifications
1.	Make & Model	
2.	Mounting	Desktop
3.	Processor	Intel Xeon Quad core 5630,2.53GHZ,5.86GT/sec QPI
4.	No.of Processors	Two (2)
5.	Chip Set	Inter 5500 family chipset
6.	CPU Cache	12MB L3 Cache
7.	RAM	16GB DDR31066 MHZ expandable to 48GB
8.	Extension slots	4 or more PCI-Express slots(with at least 2PCI –Ex8 slot for SAN connectivity)
9.	HDD	6x300 GB OR higher SFF hot Pluggable SAS 10K rpm
10	Internal HDD bays	6 or more hot plug drive bays
11	DVDROM	8x or higher DVD-CDRW Combo Drive
12	Raid Controller	2 Nos. of 3G SAS RAID Controller, each with 256 MB battery backed cache
13	Tape drive	24/48GB or higher capacity latest generation internal /external DAT drive with controller, 40numbers of data cartridges and 5 numbers of cleaning cartridges. Required backup software.
14	LAN Card	2Nos .of separate 10/100/1000 Ethernet Cards each with 2 ports (with at least 1 card on board)
15	Power Supply	Should come with Hot Pluggable & Redundant Power Supply
16	Fans	Hot pluggable redundant fans
17	Management Software	Management software having following features provided with each server: 1)OS independent remote management capabilities. 2) Provide proactive notification of actual or impending component failure alters. 3)Inventory management(H/W&S/W) 4) Remote software deployment 5) Remote patch deployment
18	Operating System	Industry standard operating system with applicable licenses
19	Database	Compatible database with applicable licenses for the Time & Attendance management system.
20	Certifications	For OEM:ISO9001(Latest version)
		ERTL/FCC-EMC Class A or Class B
		ACPI(Latest version)
		RoHS compliant
21	Warranty	OEM onsite, labour ,parts warranty for the entire R&G period

6. MASTER DETAILS & BASIC VALIDATION REQUIREMENTS

MASTER DETAILS	
6.1.1	The following masters are to be supported by the package: Employee master containing Name, Staff No., Department & Designation, category code, punch status code Employee's Photo, Three finger prints images, Blood Group , Date of Birth, etc
6.1.2	System should provide a facility to add, modify, or delete master data by authorized

	persons.
Basic Validation Requirements	
6.2.1	There should be a minimum of two punches (IN and OUT).The staff number has to be validated with the staff number, finger print image and punch status code available in clock /server employee master.
6.2.2	Single machine shall be used for both IN and OUT punch of attendance. Depending on the grace time allowed for IN punch, short absence hours are to be calculated if IN punch is beyond the grace time. Details of grace time will be furnished by BHEL .
6.2.3	In case of an early OUT punch, short absence hours are to be calculated.
6.2.4	The system has to maintain a roster of weekly holidays and shift; to be updated every day based on data provided by authorized staff.
6.2.5	The system should also provide for recording the details of compensatory holiday; and absenteeism of staff on account of other assignments i.e proceeding On Official Duty.
6.2.6	Reports : Vendor should provide reports as specified by BHEL

7. ACCEPTANCE TEST PROCEDURE FOR THE PROJECT

7.1.	Complete system supply, installation and running of system as per requirements and technical specifications must be completed for proceeding with ATP.
7.2.	Soft copy and hard copy of complete system documentation. User manual, giving details of configuration, various wiring diagrams', layout, Marking and labelling of all cables', ports, terminations, running instruction etc. to be submitted. This will serve as reference document in case of any problem/ system augmentation etc.
7.3.	Newness certificate: The Vendor has to submit the newness certificate of all the equipment suppliers for their back to back support.
7.4.	OEM support: The Vendor has to submit the certificate from the principal equipment suppliers for their back to back support.
7.5.	After the installation and commissioning of the system as per the technical specification following are to be done
7.5a.	Demonstration of minimum 25 number of transactions from each biometric Smart Card Reader (in 1:1, 1:N mode) for proving the specified verification speed of the reader.
7.5b.	Demonstration of the readers in off line and on line mode to prove the reader's performance.
7.5c.	Online report for all the above swipes.
7.5d.	Demonstration of smooth working of all software modules as per specifications from the central application servers and from Time Office PCs.
7.5e.	Demonstration of web based report viewing facility on local area network with proper authorization & authentication.
7.5f.	Demonstration of working of biometric smart card on battery, in case of power failure during day &night , emergency situation.

MAINTENANCE AND BACKUUP:

<u>Details of maintenance and other activities.</u>	
8.1.1.	Vendor shall be responsible for the continuous and smooth operation of the hardware and software for the entire period. Vendor shall deploy full time maintenance personnel in the BHEL R&D campus for ensuring proper maintenance of the system.
8.1.2.	Vendor shall have back up support with Original Equipment Manufacturer (OEM) during contract period for PCs and Servers to ensure ability of spares and services.