

FINGERPRINT AND ACCESS CARD READER:

- Provide contact less smart card + Fingerprint readers
- Authentication should make using Smartcard + Password Or Live Finger print and giving an audible and visual indication of a successful authentication.
- The fingerprint module shall be Optical and have the ability to continue uninterrupted operation.
- A 3x4 keypad which can provide supplemental PIN operation. The keypad shall provide the most popular industry formats including 4 bit or 8 bit bursts for every Key press.
- Data security with contactless cards shall use 64 bit authentication keys to reduce the risk of compromised data or duplicate cards.
- The contactless smart card reader and cards shall required matching keys in order to function together.
- All RF data transmission between the card and the reader shall be encrypted, using a secure Algorithm.
- Card readers shall be provided with keys that are compatible with the contactless smartcards.
- Typical contactless smart card read range shall be 2"-3" (5.0-7.6 cm))
- Contactless smart card readers shall meet the following environmental

Specifications:

- Operating temperature : (0 to 45 degrees C)
- Operating humidity : 5% to 80%
- Fingerprint Reader with inbuilt Access Card Reader
- Communication based on TCP/IP protocol
- 1:1 verification identification shall be possible
- 500 dpi optical sensor
- 1:1 verification time < 1 sec
- FAR <0.001% Adjustable FAR according to security requirements
- Manages up to minimum 20 users
- Transaction capacity minimum to 20,000

- Capable of simultaneous identification and verification
 - Buzzer and multi color LED's which 20 x 2 with back light
 - Real time Clock work without power at least 48 hours
 - Battery Backup available up to 5 hrs.
 - Operation mode: support both online and offline. In case of link failure authentication done locally and then link is up then data transfer to host PC/Server.
 - **Door lock option : No**
 - Electromagnetic locks (Wherever required by IMD) for doors: Unlocks when the valid entry/exit ID of the Users reads.
 - Exit Reader : For recording exit time stamp
 - Emergency out switch : Unlocks the door from inside
- **SOFTWARE SPECIFICATIONS**
 - Software should be based on Server-Client architecture
 - As user authenticates, status can be monitored on line
 - System connectivity status can be monitored on line for all machines connected with software
 - Upload/Download of users from one machine to another from standard software only, for all/selected users.
 - Real time monitoring of entry for all machines/users connected with software.
 - Software should display invalid punches/unsuccessful entries also
 - Software should be able to generate reports as per UGVCL requirement, as & when required.
 - Software should have feature of upgrading of higher version when ever available.

special terms & conditions

- a) The vendor to provide 1 year comprehensive on site warranty of the machine & communication software including all spare parts.

- b) The Successful vendor should provide necessary operation and maintenance training of badge readers to the concerned HR section & System employees and this training shall be a part of commissioning and handing over of Attendance Recording System for operation and no separate Training cost shall be paid by UGVCL.
- c) The Successful vendor has to commission all the machines within 30 days after commencement of one month.
- d) Successful bidder has to arrange onsite photograph of employees at various locations of UGVCL within 15 days after receipt of AT.
- e) Successful bidder has to collect the employee's data from concern office, within two weeks of the AT.
- f) Details of the service centre along with contact nos. and name of persons in the service station should be clearly mentioned and submitted at the time of bid submission.