SECTION-B: TECHNICAL SPECIFICATION & SCOPE OF WORK

1. EACMS SYSTEM GENERAL FEATURES

1.1	The new Enterprise Access control and Management system proposed for LPSC comprises of multilane motorized turnstiles integrated with Multifactor authentication with contactless Smart card cum face recognition and Finger print for IN & OUT of Main gate entrances integrated with Tripod automatic Turnstile at LPSC, Valiamala and Bangalore for employees, non-employees and visitors. The biometric reader with inbuilt controller should have option to read Smart Card, Finger Print and Face and control the turnstile. There shall be provision to enable one/two factor authentication (Face, Finger, Card + Face, Card + Finger) as defined by the Department. The readers (both fixed and hand held) will communicate with server in near real time with Ethernet/Wifi connectivity and should have suitable enclosure to work in the outdoor environment.
1.2	Contactless smart card based ACS with Face / Finger print based biometric for IN & OUT at doors of second level access control (using EM Lock) for employees and non-employees. IN reader at a door/area to be installed with integrated controller and Daughter readers for OUT/Exit and shall be connected to the controller in the 'IN' reader. Hence the daughter reader need not have controller unit embedded. Exit/Emergency switch to open the doors/turnstiles from inside in case of emergency situations and reader failure is to be provided.
1.3	There shall be primary and standby servers configured at LPSC, Valiamala and LPSC, Bangalore for EACMS application, services and database. The primary server shall host the URL for the web-based integrated software and services. The standby server has to be active only when the main server fails. The database at primary server should be replicated in near real time to the standby server.
1.4	All entry / exit lanes shall have provision to display the Photo of the personnel entering through that particular lane.
1.5	For officials with vehicle permission inside campus, handheld readers with rechargeable batteries shall be supplied with minimum 4 hours' battery back-up. These readers shall be connected to ACS system via Wi-Fi and the data transfer should happen in near- real time. The hand held readers will be of two types a. Smartcard+ Face b. Smartcard+ Finger

2. SYSTEM REQUIREMENTS

2.1	Half height motorized Tripod Turnstile integrated with contactless Smartcard and Face or finger print reader for access control at main gate entrances with photo display system for Employees, Non-Employees and visitors. LPSC, Valiamala has four gates located at different geographical locations and LPSC, Bangalore has one gate. Each gate has multiple numbers of entry / exit lanes. The details of the number of entry/ exit lanes to be installed and no. of handheld readers to be provided at each gate will be detailed in the bill of material (BOM) The implementation is envisaged as half height motorized tripod turnstile integrated with photo display system for Employees, Non Employees and visitors. The following will be the types of ACS readers a. Face + Finger + smart card based ACS fixed on turnstile at main entrances b. Face + smart card based ACS fixed on turnstile at main entrances c. Mobile/Handheld Face + smart card based ACS at main entrances d. Mobile/Handheld Finger + smart card ACS based at main entrances e. Face + smart card/ Smart Card based ACS at second level (critical laboratories)
2.2	The type of users envisaged in EACMS are below a) LPSC permanent employees (LPSC, Valiamala & LPSC, B'lore) b) Employees from Other ISRO centres c) Trainees (LPSC, Valiamala & LPSC, B'lore) d) Contract workforce (LPSC, Valiamala & LPSC, B'lore) e) Visitors (LPSC, Valiamala & LPSC, B'lore) Authentication and Verification: a. Smart card and face verification in 1:1 mode at entry/exit of gates for all employees, non-employees (Trainees and contract workforce) of LPSC b. Smart card and finger print in 1:1 mode at entry/exit of gates for all employees of other ISRO centres c. The system shall also have capability to verify and authenticate face/ finger print in 1:1 or 1:N mode for visitors, labourers, etc. as per requirements of the department d. Smart card + face verification in 1:1 mode for second level at critical laboratories/buildings in the campus for authorized personnel.

2.3	Face shall be enrolled for all employees and non-employees. Two templates of left & right hand (preferably the index fingers) are to be enrolled for each person and to be stored in Smart card (4K MIFARE/DesFire) for verification in ISO 19794 formats as per the sector details provided by LPSC, ISRO during implementation. The template de-duplication feature shall be provided for biometrics. The selection of finger with best finger print should be taken into consideration for cases wherever the index finger print quality is average or below.
2.4	1. There is Centralized Server maintained by ISRO that stores the details of blacklisted cards across various Centers/Units of DOS/ISRO which will be pushed to local server (not in scope of this tender) and EACMS should handle and record the denial of entries of black listed cards of local and other ISRO centres as well . The database table details will be shared with successful Vendor 2. Data of other ISRO centre employees (employee data, biometrics) fetched from central server will be available in LPSC's intermediary database table (table schema will be provided by LPSC). These details should be synced to readers for access control operations. 3. EACMS should maintain a separate table/view for LPSC's blacklisted cards.
2.5	EACMS hardware and software shall be scalable for the future expansion requirements in terms of additions of locations, gates, readers, Tripod Turnstiles, access levels etc. No limit shall be set by the Vendor on the number of additional devices that can be included in this system
2.6	LPSC should have direct access to the transaction data stored. This system shall support API calls for interfacing with various in-house developed software.
2.7	a. All fixed readers shall be of IP-65 rated. b. All hand held readers shall be of IP-65 rated and IK 06 or equivalent Indian Standard IS 17050:2018. It should be rugged and should not be easily tampered. c. All Electrical Equipment shall be CE/UL/Equivalent Indian Standard Compliant.
2.8	LPSC has an Access Control System in place with fingerprint based readers and turnstiles. The Installation and Commissioning process shall be of seamless migration from existing system to new system.
2.9	EACMS shall provide a standard browser based Graphical User Interface (GUI) for access control management. EACMS shall support a variety of access control

	functionalities, including but not limited to: a. Controller (Unit) management, turnstile, door management, and area management. b. Cardholder and cardholder group management, credential management, and access rule management. c. Personalization of smart card with biometric and signature d. ID card printing and template creation with a provision for Hindi language. The software should be customizable and source code of ID card printing and template creation should be available at LPSC. e. Card Validation and Authentication module as per ISRO standard and source code should be handed over to LPSC
2.10	The Platform shall be an enterprise class TCP/IP based solution. System architecture shall make use of the industry standard Ethernet IEEE802.3, TCP/IP protocols, etc. to interconnect all nodes / subsystem. EACMS shall be IPv4 and IPv6 compliant. All components of EACMS shall be in sync with NTP (Network Time Protocol) servers. Synchronization of hardware units shall be automated and transparent to users and shall occur in the background. It shall also be possible to manually synchronize units or to synchronize units on a schedule. The readers (both fixed and hand held) should sync data to the server in near real time over ethernet/Wifi network
2.11	The System shall be designed in such a way that failure of any sub system shall not affect the overall functionality of EACMS. In the event of a network failure, the readers should store data locally and push data to server when network becomes available
2.12	a. The system should be able to enroll and store minimum two finger templates of left & right hand index for each person and to be stored in 4K contactless smart card (MiFARE Classic, MiFARE Plus, DESFire EV1/EV2) with 7 byte CSN for verification in two formats – native and ISO 19794 -2 formats as per the sector details to be provided by LPSC/ISRO during implementation b. The system should be able to enroll and store face templates for each person and to be stored in 4K contactless smart card (MiFARE Classic, MiFARE Plus, DESFire EV1/EV2) with 7 byte CSN i. Face Enrollment shall be considered to be mainly done with Enrollment Station (with action from local UI)

	ii. Face Enrollment shall also be possible with uploading a Face Picture in the standard ISO/IEC 19794-5 c. The biometric data capture and interchange should be strictly according to ISO/IEC 19794-2 and 19794-4 respectively. d. Server and reader communication should be using a secure protocol like TLS
2.13	An emergency switch shall be installed for each lane door/barrier, and in case of emergency, the lane door/barrier can be disabled by pressing the emergency switch. The switches can be in a centralized location preferably independent switches for each lane/door or a group of lanes that is accessible to only authorized personnels. The turnstiles normally should be in closed condition, ie in the event of power failure; by default, the gates should be closed.
2.14	The Access control system for controlling critical laboratories (Readers and the EM lock) should have a mechanism to draw power from two separate power sources to ensure redundancy
2.15	EACMS should have the flexibility of being deployed and controlled in decentralized mode at various geographical locations. However, a centralized view for the management should be available. The detailed architecture is described in Section A, Sl.No 1.3
2.16	The Vendor should supply perpetual licenses for the solution, one for Valiamala and one for Bangalore. All components i.e., hardware, software and firmware should be operational from day one

3. DETAILED SPECIFICATIONS

3.1 Face + Finger + Smart card reader cum controller - Fixed

This device should be a single integrated unit with face sensor, finger sensor and Smart card reader. This device will be fixed appropriately at multiple lanes at the main gates for controlling the turnstiles based on the card validation outcome

	Item	Required Parameter
General	Facility with application	Biometric (Face and Finger) cum Smart card Access Control with built in controller. **(This device should be a single integrated unit with face sensor, finger sensor and Smart card reader)**
	Biometric Credential	Finger and Face
	RF Range	13.56 MHz MiFARE Classic,MiFARE Plus, DESFire EV1/EV2
Facial Recognition	General	Multi-modal Biometrics Face Recognition with Live-Fingerprint Optical Sensor, Fingerprint Biometric and Facial reader with built in Access control.
	Data privacy	Should comply to Digital Personal Data protection laws of GOI
	Sensing Distance	0.5m to 1.3 m (configurable)
	Face Cameras	Live face detection using 2MP IR camera and 2MP Visual camera Minimum with Mask detection and low zero lux illumination for 3D face sensing
	Face Illumination	Device must include built-in LED flash lighting in order to be able to authenticate face in all environment

		(from dark to light)
	Face Algorithm	1. Built-in algorithm for Live face detection and anti-spoofing. 2. Built-in AI processor for fine tuning of face data over the period of use.
	Face algorithm False Accept/Reject Rates	1:20,000 Genuine Verification of a Face in 30 days (testing method and acceptance criteria, success and failure should be logged and transferred to server in .csv for evaluation). System offered shall have minimum false acceptance. It shall not grant the access to the unauthorized entity under any circumstances
	Face Capture and verification speed	Face capture <1 sec 1:20,000 Genuine Verification of a Face < 2 sec or better
	Capacity	Face- 20,000 users (should store enough templates to identify the face without error within the time mentioned above) Log - 10,00,000 logs should be stored in the device.
	Face verification mode	20,000 Users in 1:1 mode, 5,000 users in 1:N (N= 5000) - visitors
	Face Recognition with Mask	Facial Recognition shall work with face masks, spectacle, cap etc
	Image	total image size and pixels (range)

	Dimension/Resolution/Size	Optimized for the storage capacity of the device. Compression is desirable
	Face template size	Optimized for the storage capacity of the device. Compression is desirable
		The enrolled images should be in ISO/IEC 19794-5 formats
	Face Enrolment	1)Face Enrolment shall be considered to be mainly done with Enrolment Station (with action from local UI) 2)Face Enrolment shall also be possible with uploading a Face Picture/photo • Supported image file size is up to 10MB Minimum – 250 x 250 pixels Maximum – 1000 x 1000 pixels • Supported image file formats are JPG, JPEG and PNG
Fingerprint Recognition	General	Fingerprint sensor shall be non-scratchable using human nail, effective for Dry & Wet finger Shall be able to distinguish between human finger and other fake fingerprints of paper, OHP film, Glue, Rubber, Clay and Silicon
	Sensing	Superior Optical sensor with min. 500 dpi, app. thumb size of an adult sensor area
	Sensor Make	Sensor Make : Sensor compliant with ISO 19794-2 minutiae based fingerprint generation

	Finger rotation & deviation	The Biometric reader should ensure automatic finger rotation detection and correction of maximum possible degree through which finger can rotate on sensor pad with Allowable Finger Displacement +/- 5 mm. **Note**: Specifically for enrolment and identification, the Vendor needs to ensure minimal rotation (not necessarily "0" angle) with the help of rotation detection and correction algorithm
	Image Dimension/Resolution	In accordance with ISO 19794-2 standard.
	Finger enrolment size	300 bytes for ISO 19794-2 for each finger template or better
	Fingerprint Template	AS per ISO 19794-2.
	Fingerprint Algorithm	Built - in algorithm for live finger detection
	Fingerprint algorithm False Accept/Reject Rates	FAR<0.001%, FRR<0.01% System offered shall have minimum false acceptance of access. It shall not grant the access to the unauthorized entity under any circumstances
	Fingerprint capture and verification	Card read <0.5 sec or better Fingerprint capture < 1 sec or better 1:20,000 Genuine Verification of a finger < 1 sec or better
	Fingerprint Capacity (1:N)	**Minimum 100,000 fingerprints**
Smart Card	General	Contactless smart card with 7 Byte CSN
	Card Types	MiFARE Classic,MiFARE Plus, DESFire EV1/EV2

	Standards	Contactless smart cards operating at 13.56 MHz with sector reading (32 bit format in accordance with ISO/IEC 14443 Type A series with dual key authentication
	Read range	Smart card reading range : 0 to 5cm or better and has to accommodate +/- 30 deg elevation error during presentation by the user.
Hardware/Firmware	Capacity	Capacity Maximum no. of faces: 20,000 or more Maximum no. of finger print : 1,00,000 or higher Maximum no. of transaction log as text : 10,00,000 or better Maximum no. of image log : 20,000 or better
	CPU	At least Quad Core Processor , In-built memory of 2GB RAM and 16 GB flash memory or more
	Authentication Mode	Primary: Card + Face Secondary: Card + Finger Option for Card only, Face only, Finger only shall be available
	Interface with tripod Barrier	Potential free contact
	Interfaces	Ethernet (IPV4 and IPV6 compliant) , RS- 485 with OSDP, USB
	display	At least 3.5" IPS LCD touchscreen with Gorilla glass 3 or better To show day, date & time by default. To display the details of valid /

		invalid entry with Name, photograph and Employee's ID at the time (24 Hrs. Format) of card flashing. To show power on, valid entry, invalid entry or any error defined by ISRO Card validation scheme in distinguishable colors Tamper indication
	Audible alarm	For valid entry, invalid entry and any error, audible alarm shall be provided with different sound to distinguish the event
	Real Time Clock	RTC with battery backup. Device shall support synchronization of RTC using NTP protocol. Provision for adding NTP server through device settings is required.
	Date and Time Retention	In case of power failure, the data retention to be provided and the Real Time Clock of the unit should be retained with current date and time
	Local and remote admin	The reader shall support local and remote administration and maintenance through network.
	Anti -Pass back	The reader shall have option for global and local Anti-pass back.
	Event/ Alarm logger	Event logging in the onboard memory for the alarm observed at each location along with time shall be archived and retrieved.
	Certifications	Compliance to BIS/ISI standard or Equivalent certification as mandated by Govt. of India. (relevant proof)

		Or equivalent international standard /certifications
	Ingress Protection	IP65 or IS 17050:2018 (relevant proof)
	Environmental	Humidity : 10% to 90% RH non condensing, Operating temperature: 0 deg to 50 deg
	Power requirement	As per Indian standard
	PoE	IEEE 802.3 or better as required
	Network traffic	Readers and Administration software should not generate broadcast traffic in the network. The device should be capable of working in an Enterprise Network environment
Security	Data security	The sensitive information residing in the readers should be encrypted. Encryption supported: 256-bit AES or better

3.2 Face + Smart card reader cum controller - Fixed

This device will be fixed appropriately at multiple lanes at the main gates for controlling the turnstiles based on the card validation outcome

	Item	**Required Parameter**
General	Facility with application	Biometric Face cum Smart card Access Control with built in controller
	Biometric Credential	Face
	RF Range	13.56 MHz MiFARE Classic,MiFARE Plus, DESFire EV1/EV2
Facial Recognition	General	Face reader integrated with smart card with built in Access control.

	Data privacy	Should comply to Digital Personal Data protection laws of GOI
	Sensing Distance	0.5m to 1.3 m (configurable)
	Face Cameras	Live face detection using 2MP IR camera and 2MP Visual camera Minimum with Mask detection and low zero lux illumination for 3D face sensing
	Face Illumination	Device must include built-in LED flash lighting in order to be able to authenticate face in all environment (from dark to light)
	Face Algorithm	1. Built-in algorithm for Live face detection and anti-spoofing. 2. Built-in AI processor for fine tuning of face data over the period of use.
	Face algorithm False Accept/Reject Rates	1:20,000 Genuine Verification of a Face in 30 days (testing method and acceptance criteria, success and failure should be logged and transferred to server in .csv for evaluation) System offered shall have minimum false acceptance . It shall not grant the access to the unauthorized entity under any circumstances
	Face Capture and verification speed	Face capture <1 sec 1:20,000 Genuine Verification of a Face < 2 sec or better
	Capacity	Face- 20,000 users (should store enough templates to identify the face without error within the time

		mentioned above) Log - 10,00,000 logs should be stored in the device.
	Face verification mode	20,000 Users in 1:1 mode, 5,000 users in 1:N (N= 5000)
	Face Recognition with Mask	Facial Recognition shall work with face masks, spectacle, cap etc
	Image Dimension/Resolution/Size	Optimized for the storage capacity of the device. Compression is desirable
	Face template size	Optimized for the storage capacity of the device. Compression is desirable
		The enrolled images should be in ISO/IEC 19794-5 formats
	Face Enrolment	1)Face Enrolment shall be considered to be mainly done with Enrolment Station (with action from local UI) 2)Face Enrolment shall also be possible with uploading a Face Picture/photo • Supported image file size is up to 10MB Minimum – 250 x 250 pixels Maximum – 1000 x 1000 pixels • Supported image file formats are JPG, JPEG and PNG
Smart Card	General	Contactless smart card with 7 Byte CSN
	Card Types	MiFARE Classic,MiFARE Plus, DESFire EV1/EV2
	Standards	Contactless smart cards operating at 13.56 MHz with sector reading (32 bit format in accordance with ISO/IEC

		14443 Type A series with dual key authentication
	Read range	Smart card reading range: 0 to 5cm or better and has to accommodate +/- 30 deg elevation error during presentation by the user.
Hardware/Firmware	Capacity	Capacity Maximum no. of faces: 20,000 or more Maximum no. of transaction log as text : 10,00,000 or better Maximum no. of image log : 20,000 or better
	CPU	At least Quad Core Processor , In-built memory of 2GB RAM and 16 GB flash memory or more
	Authentication Mode	Primary: Card + Face Option for Card only, Face only shall be available
	Interface with tripod Barrier	Potential free contact
	Interfaces	Ethernet (IPV4 and IPV6 compliant) , RS- 485 with OSDP, USB
	display	At least 3.5" IPS LCD touchscreen with Gorilla glass 3 or better To show day, date & time by default. To display the details of valid / invalid entry with Name, photograph and Employee's ID at the time (24 Hrs. Format) of card flashing. To show power on, valid entry, invalid entry or any error defined by ISRO Card validation scheme in

		distinguishable colors Tamper indication
	Audible alarm	For valid entry, invalid entry and any error, audible alarm shall be provided with different sound to distinguish the event
	Real Time Clock	RTC with battery backup. Device shall support synchronization of RTC using NTP protocol. Provision for adding NTP server through device settings is required.
	Date and Time Retention	In case of power failure, the data retention to be provided and the Real Time Clock of the unit should be retained with current date and time
	Local and remote admin	The reader shall support local and remote administration and maintenance through network.
	Anti -Pass back	The reader shall have option for global and local Anti-pass back.
	Event/ Alarm logger	Event logging in the onboard memory for the alarm observed at each location along with time shall be archived and retrieved.
	Certifications	Compliance to BIS/ISI standard or Equivalent certification as mandated by Govt. of India. (relevant proof) Or equivalent international standard/ certifications

	Ingress Protection	IP65 or IS 17050:2018
	Environmental	Humidity : 10% to 90% RH non condensing, Operating temperature: 0 deg to 50 deg
	Power requirement	As per Indian standard
	PoE	IEEE 802.3 or better as required
	Network traffic	Readers and Administration software should not generate broadcast traffic in the network. The device should be capable of working in an Enterprise Network environment
Security	Data security	The sensitive information residing in the readers should be encrypted. Encryption supported: 256-bit AES or better

3.3 Face + Smart card reader – Handheld

This device will be used by officials entering the campus through vehicles. The device will allow access based on the Card+ Face verification

	Item	**Required Parameter**
General	Facility with application	Wireless Face cum Smart card Access Control Reader
	Biometric Credential	Face
	RF Range	13.56 MHz MiFARE classic ,MiFARE Plus, DESFire EV1/EV2
Facial Recognition	General	Face reader integrated with smart card with built in Access control.
	Data privacy	Should comply to Digital Personal Data protection laws of GOI
	Sensing Distance	0.6m to 1.0 m (configurable)
	Face Cameras	Live face detection using 2MP IR camera

		and 2MP Visual camera Minimum with Mask detection and low zero lux illumination for 3D face sensing
	Face Illumination	Device must include built-in LED flash lighting in order to be able to authenticate face in all environment (from dark to light)
	Face Algorithm	1. Built-in algorithm for Live face detection and anti-spoofing. 2. Built-in AI processor for fine tuning of face data over the period of use.
	Face algorithm False Accept/Reject Rates	1:20,000 Genuine Verification of a Face in 30 days (testing method and acceptance criteria, success and failure should be logged and transferred to server in .csv for evaluation) System offered shall have minimum false acceptance . It shall not grant the access to the unauthorized entity under any circumstances
	Face Capture and verification speed	Face capture <1 sec 1:20,000 Genuine Verification of a Face < 2 sec or better
	Capacity	Face- 20,000 users (should store enough templates to identify the face without error within the time mentioned above) Log - 10,00,000 logs should be stored in the device.
	Face verification mode	20,000 Users in 1:1 mode, 5,000 users in 1:N (N= 5000) - visitors
	Face Recognition with Mask	Facial Recognition shall work with face masks, spectacle, cap etc

	Image Dimension/Resolution/Size	Optimized for the storage capacity of the device. Compression is desirable
	Face template size	Optimized for the storage capacity of the device. Compression is desirable
		The enrolled images should be in ISO 19794-5 formats
	Face Enrolment	Face Enrolment shall be considered to be mainly done with Enrolment Station (with action from local UI) Face Enrolment shall also be possible with uploading a Face Picture in the standard ISO/IEC 19794-5 ▪ Supported image file size is up to 10MB. ▪ Supported image file formats are JPG, JPEG and PNG
Smart Card	General	Contactless smart card with 7 Byte CSN
	Card Types	MiFARE Classic,MiFARE Plus, DESFire EV1/EV2
	Standards	Contactless smart cards operating at 13.56 MHz with sector reading (32 bit format in accordance with ISO/IEC 14443 Type A series with dual key authentication
	Read range	Smart card reading range : 0 to 5cm or better and has to accommodate +/- 30 deg elevation error during presentation by the user.
Hardware/Firmware	Capacity	Capacity Maximum no. of faces: 20,000 or more Maximum no. of transaction log as text : 10,00,000 or better Maximum no. of image log : 20,000 or better
	CPU	At least Quad Core Processor , In-built

		memory of 2GB RAM and 16 GB flash memory or more
	Authentication Mode	Primary: Card + Face Option for Card only, Face only shall be available
	Interface with Swing/tripod Barrier	Potential free contact
	Interfaces	Ethernet (IPV4 and IPV6 compliant) , Wi-Fi(WiFi 6 (IEEE 802.11ax), RS- 485 with OSDP, USB
	display	At least 3.5" IPS LCD touchscreen with Gorilla glass 3 or better To show day, date & time by default. To display the details of valid / invalid entry with Name, photograph and Employee's ID at the time (24 Hrs. Format)of card flashing. To show power on, valid entry, invalid entry or any error defined by ISRO Card validation scheme in distinguishable colors Tamper indication
	Audible alarm	For valid entry, invalid entry and any error, audible alarm shall be provided with different sound to distinguish the event
	Real Time Clock	RTC with battery backup. Device shall support synchronization of RTC using NTP protocol. Provision for adding NTP server through device settings is required.
	Date and Time Retention	In case of power failure, the data retention to be provided and the Real Time Clock of the unit should be retained with current date and time

	Local and remote admin	The reader shall support local and remote administration and maintenance through network.
	Anti -Pass back	The reader shall have option for global and local Anti-pass back.
	Event/ Alarm logger	Event logging in the onboard memory for the alarm observed at each location along with time shall be archived and retrieved.
	Certifications	Compliance to BIS/ISI standard or Equivalent certification as mandated by Govt. of India. (relevant proof) Or equivalent international standard /certifications
	Ingress Protection	IP65, IK06 or IS 17050:2018 (relevant proof)
	Environmental	Humidity : 10% to 90% RH non condensing, Operating temperature: 0 deg to 50 deg
	Power requirement	As per Indian standard
	Network traffic	Readers and Administration software should not generate broadcast traffic in the network. The device should be capable of working in an Enterprise Network environment
	Configuration	Configurable for IN/OUT selection option shall be provided
	Weight	The device shall as compact as possible and shall weigh a maximum of 1kg with battery and non-metallic enclosure
	Protective Cover	The mobile readers should be equipped with lightweight cushioned pouches with Elastic Harness/ suitable straps that is

		essential to carry the mobile readers around without accidental dropping.
	Battery backup	Rechargeable battery to withstand minimum 3.5 hrs. of operations with indication for available battery capacity. Option to go to power-saving mode when not in use. Alert shall be provided if battery is less than 20%.
	Power save mode	Provision to go to power save mode if not in operation for operation more than 30 seconds (should support customization of sleep time), which would revive on inputs in any mode (smart card / face / IN/OUT selection). Provision should be available in administration software for remote wake-up.
	Battery charger	Compatible battery charger for 230 VAC, 50 Hz Indian standard power cord
Security	Data security	The sensitive information residing in the readers should be encrypted. Encryption supported: 256-bit AES or better

3.4 Finger + Smart card reader – Handheld

This device will be used by officials from other ISRO Centres entering the campus through vehicles. The device will allow access based on the Card+ Finger verification

	Item	**Required Parameter**
General	Facility with application	Wireless Face cum Smart card Access Control Reader
	Biometric Credential	Face
	RF Range	13.56 MHz MiFARE classic ,MiFARE Plus, DESFire EV1/EV2

Fingerprint Recognition	General	Fingerprint sensor shall be non-scratchable using human nail, effective for Dry & Wet finger Shall be able to distinguish between human finger and other fake fingerprints of paper, OHP film, Glue, Rubber, Clay and Silicon
	Sensing	Superior Optical sensor with min. 500 dpi, app. thumb size of an adult sensor area
	Sensor Make	Sensor Make : Sensor compliant with ISO 19794-2 minutiae based fingerprint generation
	Finger rotation & deviation	The Biometric reader should ensure automatic finger rotation detection and correction of maximum possible degree through which finger can rotate on sensor pad with Allowable Finger Displacement +/- 5 mm. **Note:** Specifically for enrolment and identification, the Vendor needs to ensure minimal rotation (not necessarily "0" angle) with the help of rotation detection and correction algorithm
	Image Dimension/Resolution	In accordance with ISO 19794-2 standard.
	Finger enrolment size	As per ISO 19794-2 for each finger template or better
	Fingerprint Template	ISO 19794-2 compatible.
	Fingerprint Algorithm	Built - in algorithm for live finger detection
	Fingerprint algorithm False Accept/Reject Rates	FAR<0.001%, FRR<0.01% System offered shall have minimum false

		acceptance of access. It shall not grant the access to the unauthorized entity under any circumstances
	Fingerprint capture and verification	Card read <0.5 sec or better Fingerprint capture < 1 sec or better 1:20,000 Genuine Verification of a finger < 1 sec or better
	Fingerprint Capacity (1:N)	Minimum 100,000 fingerprints
Smart Card	General	Contactless smart card with 7 Byte CSN
	Card Types	MiFARE Classic,MiFARE Plus, DESFire EV1/EV2
	Standards	Contactless smart cards operating at 13.56 MHz with sector reading (32 bit format in accordance with ISO/IEC 14443 Type A series with dual key authentication
	Read range	Smart card reading range : 0 to 5cm or better and has to accommodate +/- 30 deg elevation error during presentation by the user.
Hardware/Firmware	Capacity	Capacity Maximum no. of faces: 20,000 or more Maximum no. of transaction log as text : 10,00,000 or better Maximum no. of image log : 20,000 or better
	CPU	At least Quad Core Processor , In-built memory of 2GB RAM and 16 GB flash memory or more
	Authentication Mode	Primary: Card + Face Option for Card only, Face only shall be available
	Interface with	Potential free contact

	Swing/tripod Barrier	
	Interfaces	Ethernet (IPV4 and IPV6 compliant) , Wi-Fi (WiFi 6 (IEEE 802.11ax), RS- 485 with OSDP, USB,
	display	At least 3.5" IPS LCD touchscreen with Gorilla glass 3 or better To show day, date & time by default. To display the details of valid / invalid entry with Name, photograph and Employee's ID at the time (24 Hrs. Format) of card flashing. To show power on, valid entry, invalid entry or any error defined by ISRO Card validation scheme in distinguishable colors Tamper indication
	Audible alarm	For valid entry, invalid entry and any error, audible alarm shall be provided with different sound to distinguish the event
	Real Time Clock	RTC with battery backup. Device shall support synchronization of RTC using NTP protocol. Provision for adding NTP server through device settings is required.
	Date and Time Retention	In case of power failure, the data retention to be provided and the Real Time Clock of the unit should be retained with current date and time
	Local and remote admin	The reader shall support local and remote administration and maintenance through network.
	Anti -Pass back	The reader shall have option for global and

		local Anti-pass back.
	Event/ Alarm logger	Event logging in the onboard memory for the alarm observed at each location along with time shall be archived and retrieved.
	Certifications	Compliance to BIS/ISI standard or Equivalent certification as mandated by Govt. of India. (relevant proof) Or equivalent international standard/certifications
	Ingress Protection	IP65, IK06 or IS 17050:2018 (relevant proof)
	Environmental	Humidity : 10% to 90% RH non condensing, Operating temperature: 0 deg to 50 deg
	Power requirement	As per Indian standard
	Network traffic	Readers and Administration software should not generate broadcast traffic in the network. The device should be capable of working in an Enterprise Network environment
	Configuration	Configurable for IN/OUT selection option shall be provided
	Weight	The device shall as compact as possible and shall weigh a maximum of 1kg with battery and non-metallic enclosure
	Protective Cover	The mobile readers should be equipped with lightweight cushioned pouches with Elastic Harness/ suitable straps that is essential to carry the mobile readers around without accidental dropping.

	Battery backup	Rechargeable battery to withstand minimum 3.5 hrs. of operations with indication for available battery capacity. Option to go to power-saving mode when not in use. Alert shall be provided if battery is less than 20%.
	Power save mode	Provision to go to power save mode if not in operation for operation more than 30 seconds (should support customization of sleep time), which would revive on inputs in any mode (smart card / face / IN/OUT selection). Provision should be available in administration software for remote wake-up.
	Battery charger	Compatible battery charger for 230 VAC, 50 Hz Indian standard power cord
Security	Data security	The sensitive information residing in the readers should be encrypted. Encryption supported: 256-bit AES or better

3.5 Bi-directional Fully Automatic Half Height Tripod Turnstile with Drop Arm Facility

Item	**Required Parameter**
Dimension of Tripod Turnstile	LPSC, Valiamala – Gate 1 – 5 nos Gate 2 – 4 nos. Gate 3 – 2 nos. Gate 4 - 2 nos. LPSC, B'lore - Gate 1 - 5 nos Supplier has to submit drawings after site visit
Tripod	Half Height tripod with three cylindrical arms, each of 32 mm diameter or better , 500mm Long and polished stainless steel
Rotating Mechanism	Automatic 3*120 degree tripod arm movement with Way- model LED indicators

Locking mechanism	self -locking allowing only one person entry at a time with hands free operation
Prevention of reverse rotation	Prevention of reverse rotation once the head has moved 25 degree from its rest Position
Installation & Erection	By anchor bolt on plain surface
Material of case work & tripod arm	Weather proof, non - rusting high quality stainless steel ASSI 304 stainless steel with satin finish
Internal components	Corrosion, abrasion and rust free alloys
Interface with Reader	Controlled through any biometric or smart reader with opening time of 2 to 10 sec
Protection Level	IP 43 or better
Integration	Two potential Free contact (PFC) required (Entry and exit)
Security protection	Anti – pass back
Motor Type	DC Brushless motor drive, electromechanically operated locking bolts mounted on self – lubricating bearings. Silent operation
Shock Absorber	Hydraulic adjustable pressure movement shock absorber for silent smooth Operation through servo positioning drive with tooth holding brake technology
Operation	PLC controlled automatic Bi directional rotation
Tailgate detection	Positive action lock to prevent passage of two personnel at a time
Fail safe mode	In case of power failure/emergency, arm dropping function providing free and Unobstructed safe passage to users without manual intervention. On the resumption of power, the motorized drive rotates Automatically positioning the arm back to its normal & locked position (auto reset)
Data output interface	Ethernet
Audio visual Alarm	Audio visual alarm in case of error during flashing card for valid, in valid And error mode
Power requirement	230VAC Single phase @ 50HZ, power consumption not more than 50W
Temperature& relative	5^0 to 50^0 C, RH 10% to 90%
Annunciation	LED indication of Red, green
Duty Cycle	100%

3.6 Photo popup and accessories

This will be used to display the photograph of the persons entering through the turnstiles

Item	Required Parameter
Employee, Non-Employee & Visitor	On successful authentication, the photo uploaded during enrolment shall be displayed with the respective Employee ID number
Output Display	24x7 operation type, LED with monitor size 21" or better with full HD (16:9),1920x1080, Input DP/HDMI
	Shall be mounted for clear visibility to identify the photo from a distance of about 12-15 feet against each lane.
	Photo of authenticated person from each lane is to be displayed optimally.
	If photo is not found in the server, message indicating "Photo not available" shall be displayed.
	During idle condition the display shall indicate the LANE no. and a welcome message defined by department.

3.7 Electromechanical door lock for Single door with Exit switch

These locks are used with doors and allow access only to authorized persons on production of card and biometric

Item	Required Parameter
Holding Force	600 lbs. minimum (Upto 1200 lbs so as to suit all door types)
Operating voltage	Dual voltage selectable (12 VDC or 24 VDC)
Mode	Automatic release by powering off (fail safe)
Monitoring and display	Feature to monitor door sensor for door Status, RED/GREEN LED indication for EM lock status
Certification	CE / UL Certified
Mounting & Accessories	EM Lock shall be mounted on Wooden, Metal, Fireproof, Aluminium, Glass doors and shall be supplied with all required mounting brackets and accessories

Material	Anodized aluminium casing with anti-rust surface treatment & Anti-tamper jam nuts
Emergency Exit switch	Exit switch with glass enclosure with mechanism to open the doors from inside in case of emergency situations and reader failure
Input Power	Provision for dual power supply
Temperature & Relative Humidity	0^{o} to 50^{o} C, RH 10% to 90%

3.8 Electromechanical door lock for Double door with Exit switch

Item	**Required Parameter**
Holding Force	600 lbs. minimum x 2 for dual doors /1200lbs as required
Operating voltage	Dual voltage selectable (12 VDC or 24 VDC)
Mode	Automatic release by powering off (fail safe)
Monitoring and display	Feature to monitor door sensor for door Status, RED/GREEN LED indication for EM lock status
Certification	CE / UL Certified
Mounting & Accessories	EM Lock shall be mounted on Wooden, Metal, Fireproof, Aluminium, Glass doors and shall be supplied with all required mounting brackets and accessories
Material	Anodized aluminium casing with anti-rust surface treatment & Anti-tamper jam nuts
Emergency Exit switch	Exit switch with glass enclosure with mechanism to open the doors from inside in case of emergency situations and reader failure
Input Power	Provision for dual power supply
Temperature & Relative Humidity	0^{o} to 50^{o} C, RH 10% to 90%

3.9 Fixed readers for Door with controller - primary (IN reader)

This reader is used in the IN (entry) of doors to control the door open and close and allow/deny access to persons on production of card and face

- **Specification as same as Section B, Sl.no 3.2, but should operate the EM lock instead of the turnstile**

3.10Fixed readers for Door with controller -daughter (OUT reader)

This reader will be used in the OUT (exit) of doors and will be using the same controller of corresponding IN (primary reader) to control the door open and close and allow/deny access to persons on production of card and biometric

- **Specification as same as Section B, Sl.no 3.2, but without controller. This should be working as a unit along with the reader in Section B, Sl. No 3.9 and should operate the EM lock.**

3.11Finger+Face enrollment and personalization station

The same Reader device as in Sl. No 3.1 will be used at Enrollment station for capturing face and finger for enrolment.

Item	Required Parameter
Smart Card Personalization device	The smart card Reader/Writer shall be PC connected reader and shall read & write to a 13.56 MHz contact less smart card –Mifare Classic, Mifare plus/DesFIRE EV1/EV2 (ISO 14443A) cards of 4K memory.
	Personalization reader shall be connected with desktop PC through USB2.0 or higher.
	Device shall be compatible with personalization software to format and personalize the card as per DOS/ISRO compatible format. The details of same shall be provided after the award of contract.

3.12Signature pad with pen / Pen digitizer

This device is used to capture the signature

Item	Required Parameter
Signature pad with pen / Pen digitizer	LCD touch panel for making signature
	LCD Screen Dimension: 20 cm X 15 cm (approximately)
	Technology: Electromagnetic
	Resolution: 2500 LPI or better

	Pen with Pressure Levels: 512 Levels (or better) with pen holder & pen tip
	Accuracy: ±0.5 mm or better
	Interface: USB 2.0 or better
	Simultaneous view of electronics signature on LCD pad and display monitor for visual signature verification

3.13Server

SL No		Descriptions	Qty / Server
1	**Form factor**	2U rack mountable with sliding rails	
2	**Processor slots**	Processor sockets	2
3	**Configured CPU**	(3rd generation intel Xeon scalable processor or 3rd generation AMD EPYC processor) 24C, 2.8GHz or better,32MB or better	2
4	**Memory slots**	DDR4 DIMM Slots	32
5	**Configured Memory**	16GB RDIMM, 3200MHz, Dual Rank	4
6	**Raid controller**	12Gbps PCIe 3.0 with RAID 6 with 8 GB Cache or higher	1
7	**Drive bays**	2.5” SAS HDD	12
		SSD drives	2
8	**Disk Configured**	480GB, 2.5” SATA SSD read intensive	2
		2.4 TB 10K RPM, 2.5" HDD SAS or higher	6
9	**Ethernet ports**	Dual Port 1Gb On-Board LOM	1
		Dual port 10G with SFP+ with SR trans receiver	1
		Dual Port 10GbE Base-T Adapter	2
10	**I/O ports**	USB 3.0	3
		USB 2.0	1
		VGA	1
11	**Expansion slots**	PCIe 4.0	3
12	**Management port**	IPMI interface management port for secure local and remote server management	1
13	**Security**	Trusted Platform Module 2.0 V3	1
14	**OS**	Required OS License/ Subscription for the server (latest) with support	1

15	**HTML5 support**	HTML5 support for virtual console & virtual media without using Java or ActiveX plugins	
16	**Power**	Dual, Hot-plug, Redundant Power Supply (1+1), 1400W, Mixed Mode	1
		Power Chord - C13, 1.8M, 250V, 10A (India)	2
17	**Warranty**	Standard 3-year Warranty and onsite support If OEM is warranty is longer than the duration specified, the same should be given to LPSC	1

3.14Software

3.14.1 General	
1	Vendor shall supply web based software implementing all the requirements mentioned in Sl. 3.14.2 and its subsections as below. Vendor can also add any other features that are necessary for implementation of the system. EACMS software should have an interface to migrate essential employee and smartcard details from LPSC ERP system required for the operation of EACMS. Department will provide the detailed Software Requirement document (SRD) after the award of contract. Vendor shall prepare and provide Software Requirement Specifications (SRS) based on the requirements mentioned in SRD and SRS shall be mandatorily approved by Department. The vendor has to submit the Software Design Document for mandatory approval from Department before initiating the software development.
2	Integrated web based ACS software forms the critical component which integrates and manages all the software and hardware elements. It acts as a bridge between application and the devices. On the device side, it facilitates the configuration of devices and communicates with the controllers in the device (for door/ turnstile) by exchanging commands and events. On the application side it supports enrolling users, manages access rules and user punch data. The key software components shall interact with readers through Ethernet and provide seamless connectivity with server and database. This software is envisaged as multilocation enterprise access control software with centralized monitoring and decentralized management.

	The new system should be capable of reading the existing Mifare classic ID card already issued to the employees. This is to retain the existing issued cards. Smart card format will be given by LPSC. All keys for reading and writing the smart cards will be decided by LPSC.
	The licensing model of the software should accommodate addition of devices and users as the organization grows.
3.14.2 Integrated web based application software	
a)	The following are the various modules envisaged **1) Administration & Management software** ✓ Creation of User profile and user roles ✓ Creation of device groups ✓ Configuration of all hardware elements of EACMS and provision to store the configuration ✓ Realtime Management of Devices and Users ✓ Manage Access rules definition and features ✓ Location wise administrator management (Administrator of an installation should have rights to delegate powers to local (work centres) administrators for device and employee management) Refer Sl.No 1.3 Architecture , fig 1 ✓ Blocking of Users and card, Withdraw /deactivate temporarily ✓ User and Device group management ✓ Employee management - add, edit, delete employee details in addition to employee details migrated from ERP ✓ Live Device Status monitoring and device health reports in various formats like excel, pdf , text and current device data transfer status ✓ Module to communicate to all devices of EACMS **2) Software module for biometric access control operations (readers and turnstiles)** ✓ Access control using multiple credential combinations ✓ Card and biometric reading on presentation ✓ Card validation, credential authentication, identification , decision making and operation of turnstiles/door ✓ Biometric data processing and storage ✓ Handling of black-listed cards ✓ Transaction data storage and transfer to server in near real time ✓ Display of photos in photo popup device **3) Enrolment and smart card management module** ✓ Capture/ Migration of employee data, signature ✓ Card read and write key management

	✓ Biometric enrollment (USB based Face readers, finger print enrollment device) ✓ Smart card personalization and assignment of access rights ✓ Smart card inventory management and alerting ✓ ID card template creation, ID card printing , issue and return ✓ Automatic transfer of all personalization data including finger templates, face templates, photo and signature to server and all readers to eliminate separate enrollment at each Door/gate ✓ During enrolment of an employee at any location, employee basic details and biometric credentials should be synced to both local server and readers in near real time where as to the other locations' (units & work centres) servers and readers shall be scheduled to execute asynchronously. **4)Attendance Module** ✓ Entry of Official Engagement of all employees in a division/group ✓ Entry of Late arrival, Early Departure, In between permission etc. ✓ Shift data entry ✓ Official Tour entry ✓ Holiday entry ✓ Basic Attendance reports **5)Device reports** ✓ Health status reports ✓ Configuration reports ✓ Device logs ✓ Transaction logs **6)Data management** ✓ Provision for import of employee data from LPSC's ERP ✓ Provision for export of transaction and enrollment data from EACMS for use in LPSC's software ✓ Near real time database syncing to local standby server and LPSC, Valiamala server (for units) Refer Sl.No 1.3 Architecture , Fig 1 **7)Notifications and logging** ✓ Access rule violation attempt ✓ Door held open ✓ Reader removed from turnstile **8)Visitor Smart Card Issue software shall be provided by the party to meet the requirements of visitors** ✓ Visitor enrollment ✓ Card personalization
b)	**USER ROLES**

Sl.No	Role	Description
1	System Administrator (Super User)	Over all administrator of EACMS
2	Local Administrator	Administrator of a location/ installation
3	Device management user	Hardware device and database management
4	Enrollment user	Manages enrollment and ID card printing
5	Management user	User having rights to view access and attendance reports. Here some users will have permission to view reports of all locations. Some will have location wise permissions. Some will have entity/group/division wise permissions.
6	General User	User can view their own attendance reports
7	Office Secretary user	User who manages shift entry, official engagement entry, tour entry and permission entry for an entity/group/division

System Administrator (Super User) (one each for each instance of installation)

- ✓ Should have access to all modules and configuration details of EACMS.
- ✓ User creation
- ✓ Assignment of readers and users to local administrators
- ✓ Card read and write key and encryption key management
- ✓ Database management

Local Administrator/Division Heads/Focal Point of labs

- ✓ Creation of local access groups and assignment of users to local readers
- ✓ View of access reports of location/ lab

Device management user

- ✓ Configuration of all EACMS devices
- ✓ Monitoring of all devices
- ✓ Assign a reader to IP network

	Enrollment user ✓ User data, signature and biometric capture ✓ Personalization ✓ Creation, printing and issue of cards **Management user** ✓ Access reports of all location ✓ Attendance monitoring of all locations **General User** ✓ Attendance reports **Office Secretary user** ✓ Entry of Official Engagement of all employees in a division/group ✓ Entry of Late arrival, Early Departure, In between permission etc. ✓ Shift management **Note:** The detailed activities pertaining to each role will be provided in the SRS and will be shared with the successful vendor.
c)	Canteen Management, Visitor management system etc that uses the data from EACMS will be inhouse developed software and are not in the scope of the Vendor. However, the Vendor has to provide APIs/interfaces necessary to transfer/extract information from EACMS database and smartcards needed for the in-house software development. APIs/interface envisaged • To read/write data from smartcard ✓ Employee basic data, ✓ card CSN, ✓ Biometric Info • To read daily access transaction data (formats will be specified in SRD)
d)	A software requirement document will be provided after the award of contract which will detail the software interfaces needed for the in-house software. The role-based access requirements will also be specified in that document.
e)	EACMS database schema should be made available to LPSC for future software development that uses EACMS data
f)	The smart card authentication algorithm shall be implemented based on ISRO Card Validation Scheme which will be provided after the award of contract.
g)	ID card printing software shall be developed by the Vendor based on ISRO ID card template document that will be provided after the award of contract. The source code of this software shall be handed over to the department.
h)	All Transactions that occur at Main entrances and second level access control

	shall be logged in flash memory of respective readers. Transaction data which include card UID/NUID/CSN, date, time, ID of employee/non-employee/visitor, reader ID, direction of movement (IN/OUT), transaction ID and error code/status (as per list of error codes that will be furnished with card validation logic) shall be transferred to server in near real time through network. The data from units/work centres when transferred to the LPSC, Valiamala server, the source location of the transaction data should be distinguishable with suitable mechanism like unique identifier for each location or additional column for source location identifier. Responsiveness of the software should not degrade even during heavy data traffic between readers and the server
i)	In case of failure in network, Transaction data shall remain stored in reader and shall be updated to server as and when network is restored.
j)	The system shall use a standard RDBMS package like MYSQL, MSSQL, PostgreSQL, ORACLE or SYBASE. Vendor should supply licensed enterprise versions of the database software for both primary & backup servers
k)	The software shall be scalable to add more users and devices as per LPSC requirements
l)	The application should have the capability to be hosted in a virtual environment.
m)	The system should facilitate online data updating to reader without affecting the normal functionality of the unit. The readers shall cater to access control with any combination of Smart card /biometric (finger, face) based access control as per the options configured in the reader
n)	Provision for periodic database backup / restore shall be made available e.g. daily, weekly, monthly, etc. through automatic schedules.
o)	All the generated reports shall have options to view on screen, print and exporting to text, excel and PDF file.
p)	The software shall have provision to configure the reader to any mode of authentication eg. smart card only mode / face only mode / finger prints only or any combination of these. Software should have provision to configure authentication modes at reader level and at user level. The change of mode of authentication in the device shall be logged with time stamp
q)	Vendor should support modifying EACMS software at any later point of time as

	per LPSC's requirements that are additional to those specified in SRD during warranty/ AMC period. A separate PO will be issued for the same.
r)	Web based software shall support browser based management and avoiding need to install client software. Web based software shall support all latest version browsers with backward compatibility of minimum last two version.
s)	The application shall be designed and configured in such a way so that single point failure will not have impact/degradation in overall functionality.
3.14.2.1	**Administration & Management software**
1	This module manages the users and devices of EACMS. Software shall provide tools for: 1. Role based login creations and assigning privileges 2. Configuration and management of all devices of EACMS 3. Option to authorize and block the access of personnel at entrances and second level access doors for super user and local administrator 4. Location wise administrator management 5. To set location wise reader administration privileges for local management 6. Administration of second level Access control by individual area administrators. 7. Syncing and verifying that readers are updated with the latest information from the server 8. Verify that all transaction logs from the reader has been transferred to the server 9. Create groups of users and readers. Assign entry rights for defined groups of users to specific groups of readers 10. Super user should have option to access all readers across location and delegate rights to local administrators for device and user management 11. Super user should be able to create reader groups across Valiamala and Bangalore and should be able to map syncing of user meta data to reader groups based on the user type 12. Administrator should be able to create readers groups across Valiamala and B'lore and should be able to map user meta data to reader groups based on the user type

	13. Administrator should also be able to assign reader groups to specific user 14. Enrolled data of different user types such as Employees, Trainees, Contract Workforce and Visitors should be auto synced only to the assigned reader groups. 15. Interface to migrate data from LPSC's inhouse ERP 16. Asynchronous backup of data to standby server and LPSC, Valiamala server
2	Option for displaying the number of pending transactions (yet to be transferred to server) in each reader, group wise
3	Software shall provide health monitoring of different hardware components like readers & network components on daily or for a period basis and generate status reports
4	Event logs on data upload/download server to reader, backups, scheduled scripts or any other event in the system shall be made available. Any loss of communication should be logged as event providing details of reader ID, date & time and nature of failure Door open time at second level access control shall be logged and alerted when door is left opened for long duration (5 mins)
5	Provision for viewing all relevant data (transaction, configuration and biometric/smartcard data etc) from any of the selected reader should be provided to administrators via Web GUI
6	Extensive remote diagnostics features shall be implemented and the health status of each reader shall be displayed on a separate page. Whenever the readers go unhealthy, alert shall be sent as mail to administrator and the event shall be logged with time stamp.
7	The software should have provision to update EACMS database from LPSC ERP database at schedule time interval. Appropriate connectivity and ERP database details will be provided by LPSC.
8	The system shall cater to various reports for trouble shooting and performance monitoring. The performance logs shall be generated catering to diagnostics of the system (EACMS Hardware).
9	LPSC should have rights to create additional database objects in EACMS database. Additional database objects for the following will be created by LPSC in EACMS database

	• Data of other ISRO centre employees (Basic employee data, biometrics) fetched from central server • Black listed card details of other ISRO centres The above details should be synced to readers for access control operations. EACMS should maintain a separate table/view for LPSC's blacklisted cards.
10	Should have provision to schedule access according to time and day
11	Audit trail of all activities of users in various roles has to be provided
3.14.2.2	**Software module for biometric access control operations (readers and turnstiles)**
1	This module of the software shall have the following options 1. Manage access control using multiple credential combinations 2. Card and biometric data capture on presentation 3. Card validation, credential authentication, identification, decision making and operation of turnstiles 4. Handling of black-listed cards 5. Transaction data storage and transfer to server in near real-time 6. Display of photos in photo-popup device
2	The software should record the transaction as successful only after authentication of credentials, validation of rules and turning of the turnstile fully.
3	If the employee shows the card multiple times (due to any reason) only the transaction where the full rotation of turnstile is completed should be recorded as IN/OUT punch
4	The software for the readers should handle multiple credential combinations to control the access of users in the main gate and secondary doors
5	The firmware of the biometric reader should be customized to suit the access control validation scheme of ISRO
6	The logic for card/credential validation diversified key creation logic and encryption mechanisms for the biometric data storage and transfer will be discussed with successful vendor and the same has to be implemented. Software shall collect data like Chip Serial Number (CSN) and other details mentioned in ISRO card validation document and generate unique access code for each

	individual during personalization and card authentication**. Source code of ISRO card validation and authentication module should be provided to LPSC**
7	Validation of smart card of employees and non-employees from respective Centre/Unit shall be carried out on the basis of biometric template stored in smart card/reader/server in ISO 19794 Part 2,4 and 5 format depending on the type of biometric. Whereas, validation of smart card of employees from other Centre/Unit of DOS/ISRO shall be carried out on the basis of card only mode or biometric template stored in smart card in ISO format. ISRO Card Validation Scheme will be shared with the Vendor after the award of contract. The logic for smartcard validation should be configurable based on the user types mentioned in Section B Sl.No 2.2. This is to accommodate any change in the type of biometric credential used for validation of different user types. For eg for other centre employees, department may decide to use face template instead of finger template at later point of time. The successful Vendor has to sign a Non-Disclosure Agreement before getting access to the details of the authentication logic.
8	Validation logic shall ensure denial of entry to the black listed smart cards (local and other centre cards)
9	Access failure reports: The software shall provide detailed access failure reports by generating error/status code for each transaction. The report shall display the user details, date & time, location and nature of error/status for the following cases: a) Biometric verification failure b) Unauthorized attempt by swiping of card at any location (if card source is unknown , system shall log the card details in addition to logging error) c) Biometric and / or card not authorized to enter a particular location d) Biometric and / or card not authorized to enter at a particular time e) Unknown Finger print and / or Card swipe details f) Anti Pass back entry attempted (center specific validation) g) Details of personnel not entered after valid authentication (by detecting turnstile rotation)

3.14.2.3	**Enrolment and personalization**
1	The EACMS software should have provision to capture fingerprint, signature, Face capture for enrolment, personalization, Card template creation and ID card printing.
2	This software shall include following major functions. 1. Capturing and storage of photo as per the requirement of Face Recognition System according to ISO-19794:4 and in native format. Option to upload photograph from a local folder. 2. Capturing and storage of finger-print according to ISO-19794:2 3. Capturing and storage of signature and other information needed for card printing 4. Personalization of card The above captured photo and signature will be used by Card management module for ID card printing
3	The biometric capture and smart card writer device shall be connected to PC through USB 2.0 or higher interface. The card writer should read & write to a 13.56 MHz contact less smart card – MiFARE classic, MiFARE Plus, DESFire EV1/EV2 (ISO 14443A) cards of 4K memory.
4	The software should personalize the card as per DOS/ISRO compatible format. The details of same shall be provided after the award of contract.
6	Software shall capture the photograph of an individual and store it in the server associated with employee data in the database. This photograph shall be displayed during the photo-flashing at gates. There shall be also option to upload photo already captured and stored in a specified location
7	It should have option to select any two fingers for enrollment and duplicate search facility in order to avoid multiple enrollments of same individual. Biometric template in native format and ISO 19794 format shall be saved in server database.
8	Software shall enroll the face of employees and number of face templates to be enrolled should be decided as per the Vendor's requirement to fulfil the accuracy and latency specifications of the face reader in the tender and the same to be saved in native and ISO 19794 format in server

9	This software shall be used at multiple locations for enrolment & card personalization of employees, non-employees and visitors.
10	Software shall have option to categorize the enrolled staff into Employees, Contractors, Trainees, and Visitors.
11	Software shall format and personalize the card as per DOS/ISRO card format with dual key authentication. Software shall have provision to read contents of already personalized card with edit/modify/disable options.
12	Keys for reading the cards should be stored in the database and transferred to individual readers during configuration. Keys for writing the cards, format, contents and methods of ensuring card data security will be as per DOS/ISRO guidelines and will be shared with the successful vendor.
13	Enrollment user of an instance will have access to only employees in the respective instance. When an employee is enrolled his/her data will be pushed to the default reader group of the location. During enrollment or at later point of time, there should be an option to assign/reassign a user to any reader/ reader group. During enrollment or at later point of time, there should be an option to assign/reassign a user to a reader/ reader group
14	The system shall facilitate GUIs to alter the reader configurations to any mode like smart card only mode. The provision to set access mode (Face+card, Finger+card, Face/Finger/Card only) should be configurable at reader level and at user level
15	The Face and Fingerprint data after enrolment shall be stored in the Smart Card Memory as DOS/ISRO Card Architecture requirements. The enrolled data shall be pushed to the server and reader in near real time as specified in the architecture(Section A Sl.No. 1.3).
16	Enrolled users should appear in dashboard of Local Administrator and Super user for assigning access permission to reader/reader groups
17	The biometric readers mentioned in section 3.1 can be used for biometric data enrollment. The Vendor has to make necessary arrangements to mount the readers at the enrollment stations at the necessary height.
18	There shall be 3 enrollment station in LPSC, Valiamala and 2 in LPSC, Bangalore

3.14.2.4	**Smart card management software**
1	Software should ensure that a user is assigned to only a single card at a time. Old card should be automatically disabled when a new card is issued to the user. The details of inventory for smart card is given below : a. New cards when received from stores will be checked-in to the card database using the UID/NUID/CSN. b. When such card is taken up for personalization, the software shall tag the CSN to the employee/non-employee code. c. When the card is lost, it should be updated accordingly as lost and the card should be blocked. If lost card is found, the same will not be used again. d. When a new card is issued to a user, the software should mandatorily block the old card on completion of issue of new card. At any point of time, an employee should have only one active card. e. Expired cards, old cards, when returned, shall be formatted and the keys A & B shall be reset and card shall be disposed securely and provision to update the card status should be available f. The software shall maintain inventory of Smart Card usage and maintain history for its life cycle. (From card creation till it is disposed). g. There should be provision to view the lifecycle of any card.
2	Software shall have provision for smart card layout design with bi-lingual (Hindi & English) text capability & Barcode printing on any side of the card.
3	The Vendor should develop the software for printing the ID cards for various category of workforce like Employees, Contract workforce, trainees, visitors etc
4	The layout and format for printing the software is defined by ISRO. The documentation regarding the same shall be provided after the award of contract.
5	The source code of ID card template creation and printing software shall be handed over to LPSC and Vendor has to do any modification suggested by department during warranty time and later during CAMC time.
6	The software should have a customizable template to generate ID cards for various categories (employee, contract, trainee, visitor etc) and the ID card

	generated will be approved and printed on smart card.
7	ID card issue, re-issue and return process should be handled
8	Card printing software shall support uploading of photograph and signature
3.14.2.5	**Attendance Module**
1	Entry of Official Engagement: If an employee goes out of office for official duty, the same should be captured and added to the total working hours.
2	Entry of Permission for Entry of Late arrival, Early Departure, In between going: If an employee goes out of office with permission, the same should be captured and should be shown in the report accordingly.
3	Shift data entry : Provision for entering the shift details and the employee to shift mapping
4	Official Tour entry : Provision for entering the tour details of employee Holiday entry : Provision for entering the holiday details of a calendar year
5	Basic Attendance reports: a) Daily/ Monthly Attendance reports show time of entry, time of exit, total working hours, indication of late entry/ early departure if any. Incase multiple entry/exit is there a link to the details to be provided. Attendance report shall include leave, official tour, Official Engagement and shift details of every individual. All the attendance reports should list only the successful transactions b) Late comers, early goers list c) Overtime report : Report showing number of hours of stay in office before/after office hours d) Chronic late comers & early goers (more than 10 days a month) e) Average entry/ exit time of a user for a specific period f) Details of employees coming before/after a specific time (provision to enter time) g) Details of employees leaving before/after a specific time (provision to enter time)
6	Holiday, Saturday, Sunday attendance report
7	Second level access control report with list of employees allowed or restricted
8	Shift details report

9	Tour details report
10	Other Centre/Unit employee & Non-employee access control report that can be exported in excel, '.csv' format
11	Failed transaction reports should specify the failure condition
12	Current count strength (Count provided for employees, non-employees, other centre employees and visitors)
3.14.2.8	**Visitor Management System (VMS) Software**
1	Visitor Management System shall allow access based on a. Smart card cum face b. Smart card cum fingerprint c. Smart card only based on configuration during enrollment. Each visitor shall be provided with unique ID (specific to Centre/Unit) as per the structure defined by Department.
2	VMS should be capable of maintaining the visitor details including face data, fingerprint template, visitor id, name, designation, nationality, visitor type, address, phone nos., email id, photograph, passport details and provision to scan and store documents/images.
3	Visitor pass generation shall include registration of individual visitor by capturing the photograph and/or signature, scanning the visitor's photo id or business card, enrolment of face and finger print template, personalization of smart card, generation of 'Smart Card Gate Pass', restrictions for access area (buildings/laboratories) and validity date & time.
4	Each visitor shall be provided with personalized card which can be re-programmed.
5	Visitor enrolment and biometric details for each visitor shall be uploaded to all concerned readers and servers in near real time
6	Software should provide the reports with respect to visitor, company, visitor type, visiting frequency for various combinations of time Zones / date / durations.
7	Live display of list of visitors in the campus with approved exit time in the dashboard
8	The system shall generate following reports on daily/weekly/monthly / between

	dates. No. of visitors Visitors who have over stayed No. of foreign nationals visited Visitor access / movement reports for Main gate entrances and second level. Visitor for selected area/group/division, Regular visitor, VIP visitor Visitor in the denied list
9	The software should cater provision for generation of denied list which will be controlled by administrator for the visitor module. Whenever there is a re-visit of visitor in the denied list there should be an alarm at the registration level
10	The readers identified for visitor entry should read the smart card, face, finger print of an arriving visitor and check whether the visitor is registered/ allowed. The readers should make sure the visitor is not on a denied list. Photo flashing of the visitor shall be provided at the identified gates
3.14.3 Software Security	
1	The solution should follow the industry best practices for IT security for similar systems. Code should be developed as per secure coding practices and peer reviewed (or through tool) to ensure the same. Source code access should be authenticated and logged for authorized users only which will ensure integrity and confidentiality of code. Declaration as given in Section C,Annexure IV,Sl.No 8 to be submitted
2	The Vendor shall develop, implement, maintain and use best in class industry proven safeguards that prevent the misuse of information systems and appropriately protect the confidentiality, integrity, and availability of information systems. Follow industry standards like OWASP etc. during design and development phase as Information Security is paramount for LPSC. Declaration as given in Section C,Annexure IV,Sl.No 6 to be submitted
3	The Proposed system will undergo static Vulnerability Assessment, Penetration Testing and other Security and risk assessment by the Vendor before software delivery. Dynamic security tests on the executable will be done by LPSC IT security team before Go-Live. If there are any major issues in the assessment, it

	is the responsibility of the Vendor to fix those issues before 'Go-Live'.
4	The solution shall not be considered accepted until the independent review by LPSC is completed and all security issues have been resolved and closed by Vendor.
5	The Vendor shall disclose the origin of all software components used in the product including any open source or 3rd party licensed components
6	Vendor shall not copy any data obtained while performing services under this RFP to any media, including hard drives, flash drives, or other electronic device, other than those approved by LPSC.
7	The solution should have secure transmission of data and information throughout the application and system
8	The application should be compliant to all provisions of the Information Technology Act, 2000 (along with amendments as per Information Technology (Amendment) Act, 2008) and other applicable laws with latest amendments at the time of delivery.
9	The solution should ensure data retention as per prevailing statutory requirements as well as the LPSC's policies

3.15Mifare /Mifare Plus/DESFire EV1/EV2 Smart Cards with (4K)

Sl.no	Item	Required Parameter
1	Mifare 4K/Mifare Plus/DESFire EV1/EV2 Smart Cards	7 byte CSN contactless smart card compliant with ISO 14443A
		Read range:0 to 3 cm
		Glossy White finish with CR 80 Standard
		Memory 4 KB

3.16Wireless access point

No	Specifications	Value
1.	Type of Router	Wireless
2.	Standards Supported	**Wi-Fi 5** IEEE 802.11 ac/n/a 5 GHz IEEE 802.11 n/b/g 2.4 GHz
3.	Working Modes	Access Point Mode

		Router Mode
4.	Ethernet Ports	1 * Gigabit WAN Port 4 * Gigabit LAN Ports
5.	Routing Protocols	Static/Dynamic IP PPPoE PPTP L2TP
6.	Network Management	Through Web-based GUI
7.	Network Management Protocols	SNMP
8.	Security Protocol	Wi-Fi Encryption – WPA, WPA2, WPA3
9.	Network Security	SPI Firewall Access Control IP & MAC Binding Application Layer Gateway URL Filtering Time Controls
10.	Operating Temperature Range(Degree C)	0~40
11.	Operating Humidity (RH)	10%~90%
12.	IPv6 Support	Yes
13.	Accessories	Power Adapter, RJ45 Ethernet Cable, Installation Guide
14.	Certifications	BIS
15.	Warranty	3 Years

3.17Accessories

3.17.1	**Accessories, Cables and Conduits as required for the ECAMS implementation**
1	a) All electrical cables UTP cables – will be provided by LPSC b) PVC Conduits, connectors and cables – size as compatible with cables should be supplied by the Vendor c) Any other components required for the EACMS implementation

	discovered during implementation phase shall be provided free of cost to LPSC
2	All the cables should be weatherproof. ISI /BIS Certification shall be submitted.
3	Stainless Steel (SS) pole of suitable height for installing readers. SS pole shall be with suitable environmental protection (IP54 or better) including weather shade. Vendor shall discuss with LPSC for proper positioning
3.17.2	**Any additional item required**
1	Additional items if any required for realization of this TURN-KEY work, shall be specified with details as per Section C, Annexure V, Sl.No 3– Unpriced and Annexure VI Sl.No 3 for price bid.

3.18System integration requirements

1	Contractor shall provide the block-diagram depicting the integration of various hardware and software components like readers, turnstiles, readers on pole, EM locks, server, enrollment & personalization units, servers with database. Vendor shall clearly mention the installation requirements.
2	Throughput for minimum 15 persons per minute per lane at gate entrances. This value should be attainable within 15 days of Installation & Commissioning
3	Integration of turnstile and EM lock should provide emergency exit with adequate instruction of safety warning. Location of exit switch should be placed appropriately for access during emergency.
4	The server database and application software should be backed-up automatically using scheduler.
5	Design of the system shall ensure reliability and minimum down time of the system. Single point failure like server, database or network should not bring down the basic operation of ACS system.
6	Server and readers shall support various protocols including NTP protocol to update its date and time with reference to source. The server shall in turn, ensure synchronization of RTC of all readers and components connected to it across all locations of LPSC.
7	All the software installations and documents protected by password should be made available to ACS in-charge as hard copy and soft copy in DVD media. The installation document shall provide details of web links, application path, help

	information on usage of the same and frequent queries
8	Vendor shall remove all the components of existing access control equipment at Main gate entrances & second level and install & integrate all the items of new ACS in a phased manner as described in the Timeline (section A, Sl. No 8)
9	Vendor shall carry out initial one time process for enrolment, personalization and card printing for approximately 100 personnel (employees and non-employees) during installation and commissioning before ATP.
10	Vendor shall carry out initial one time process for face enrolment using existing employee photos for employees and non-employees after ATP.
11	Any issues arising during system integration should be fully addressed by the vendor.

3.19Acceptance Testing

1	The acceptance test plan (ATP) will contain comprehensive tests that will verify all the hardware technical specifications and software functionalities of the product quoted by the Vendor. Acceptance of the supplied hardware and software by LPSC will be decided based on the successful clearance of all test cases in ATP.
2	Acceptance Test will be conducted only after successful installation and uninterrupted operation of the entire system at site for minimum period of 15 days.
3	Detailed ATP will be shared by LPSC to the successful Vendor as per tender specifications & Vendor shall demonstrate EACMS specifications (hardware and software) as per tender document.
4	Vendor should clear all the test cases as mentioned in ATP as per timeline (Section A Sl.No 8)

3.20Training

1	Vendor shall upon completion of the installation, provide complete onsite training with documentations on the configuration, operation and maintenance of the systems to at least TWO EACH from LPSC, Valiamala and LPSC, Bengaluru Department's personnel. Training on database schema and performance tuning also is under the scope
2	Training should include documentation required for understanding the system, its

	working concepts and basic trouble shooting guidelines.
3	Training shall be arranged to security personnel (CISF) on basic operation of turnstiles at gates and administration staff for enrollment & personalization. It should cover aspects related to emergency exit, exigency operation, etc.
4	All above training shall conducted after 15 days of uninterrupted operation of the system and before acceptance testing

3.21Documentation

1	Vendor shall submit documents for operation and maintenance of the entire system.
2	Systems block diagram along with wiring layout of all the items of ACS Systems shall be submitted.
3	ACS software with media for all the application.
4	Software Requirements Specification Document and Software Design Document
5	EACMS User Manual
6	Brochure/datasheets of all hardware components
7	Software procedure manual which shall include customization as per requirements, flow charts, operating procedures for all applications.
8	Operating System for Servers shall be supplied with license along with paper license and original media with key no. in the name of LPSC.
9	All the documents shall be provided in CD media in two copies.

3.22Deliverables by the Successful Vendor

a. All the hardware components as per the Bill Of Material
b. Brochure/datasheet of the hardware components
c. OS license for the servers, Microsoft office license and EACMS software license
d. Database license
e. Licensed EACMS software product as per the Tender specifications
f. Software Requirement Specification, Software Design Document and Software procedure manual
g. Documentation of APIs provided
h. Source code & documentation for the software developed by the vendor for LPSC (Smartcard template creation and printing module, Smartcard validation and authentication module)

i. Installation and User manual

3.23 Special Conditions

1	The extent of the contract works shall include necessary cabling to interconnect the various EACMS components, central equipment, hardware and devices and like, for it to provide the performance as specified in this tender document.
2	All cable enclosures including conduits, cable trays, ducts, wall boxes, termination panels and the like that are required to as part of this contract.
3	Vendor shall supply material such as pipe, cables, PVC casing/capping etc. to carry out turnstiles & poles fixation works, fitting of EM locks, readers, adapters, exit switch, etc. for erection and commissioning of the system. Vendor should visit the site and assess the requirement during pre-bid meeting and should accordingly propose the items required
4	Electrical and wiring as per standards
5	The software solution should seamlessly work with LPSC ‘s antivirus solution
6	The Vendor shall ensure that EACMS must be expandable. LPSC should be able to add additional hardware units without any major modification to the existing hardware, software and network configuration.
7	Vendor shall provide site requirements, power supply & environmental requirements, accessories requirements at work site after acceptance of Purchase Order and prior to supply of items
8	Vendor shall carry out customization of all the components of hardware, firmware and software as per requirements.
9	IN/OUT lane no, reader ID, readers on pole, exit switch, etc. shall be marked with suitable color radium stickers at all installed locations of gate entrances and second level ACS.
10	Vendor shall ensure the inter-operability & compatibility for all types of readers, turnstiles, software for all requirements, servers, EM locks, enrollment & personalization stations and interfacing with network.

3.24Smart card architecture, keys and validation logic

This is given for providing a basic idea on the card architecture and validation scheme. This is provided to understand the basic logic for the software to be developed for the same and is not complete. The actual requirement will be shared with the successful vendor.

Architecture

The smart card memory will be divided into different sectors for storing general employee details, card validity and biometric data (face and finger print template according to ISO 19794). Apart from the above, various other data related to Anti pass back, centre code, location code, employee type, privilege bits are to be stored in the card in specific sector. Diversified key (unique key for each card) used for reading the cards will be stored in the sector trailer.

Keys Used

Three keys will be used for managing the card read and write operations say key 1, 2, and 3.

Key 1 – This is Read & Write Key. This is Centre specific and local centre uses this key for writing on the card during personalization and reading centre specific sectors.

Key 2 – This is Read & Write Key common to all ISRO Centres. This is used to read specific sectors in the card and to set some flags in the card memory during card swipe

Key 3 – This is Read Key common to all ISRO Centres. This is used for reading specific sector.

The implementation of Keys is based on key diversification logic and keys will be stored in encrypted form.

Validation

A smart card is flashed in front of the biometric reader for validation. The biometric reader creates the diversified key and reads the card.

1) Anti Pass back validation if enabled

   Reader creates the diversified key of Key 2, matches with sector trailer and checks the anti-pass back status in a particular sector and authenticates

2) Biometric Sector validation

   After successfully completing Anti Pass back status check, Reader creates the diversified key of Key 3, match with sector trailer. If it succeeds, reads the data stored in the biometric sector and do the further steps of biometric matching and data validations

3) ISRO Specific Sector validation

   If all the above process fails, ISRO Specific Sector validation happens. Separate key is used for ISRO Sector validation.