REQUEST FOR PROPOSAL FOR SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF ENTERPRISE ACCESS CONTROL AND MANAGEMENT SYSTEM (EACMS) FOR LPSC

Ver-02

Liquid Propulsion Systems Centre

Indian Space Research Organization

July – 2024

CONTENTS

This document describes the proposal for an Enterprise Access Control and Management system (EACMS) for LPSC, Valiamala and LPSC, Bangalore. The detailed requirements and specifications of EACMS are as mentioned below in this document. Section A of this document broadly describes scope of work, technical and commercial aspects related to the EACMS implementation as per ISRO approved standards for both First Level (Entry Gate) and Second Level (Facilities and Labs) access. Detailed Technical Specification and Scope of work is given in Section B. The Annexures that describes the documents solicited from the Vendor are given in Section C.

SECTION-A: SCOPE OF TENDER & INFORMATION TO VENDORS

1. INTRODUCTION

LPSC invites bids from interested vendors for the turnkey work for implementing Enterprise Access Control and Management System (EACMS) with face recognition and finger print based biometric access control with contactless Smartcard. The scope includes Supply, Installation, Implementation, Integration, Commissioning, Testing, Operationalization and Comprehensive Maintenance of EACMS at Liquid Propulsion Systems Centre (LPSC) ISRO, Valiamala (Thiruvananthapuram, Kerala) and Bengaluru (Karnataka).

1.1 EXISTING ACCESS CONTROL SYSTEM

At present a Fingerprint cum Smart card (Mifare Classic 13.56 MHz contactless card) based Access Control System with manual tripod turnstile is operational at LPSC (Valiamala and Bengaluru)at the main entrances (first level) for managing entry/exit of personnel. Second level door access control is also operational with various authentication modes like card only/ card+finger/finger only for restricted access at critical buildings/laboratories. Present Access Control System consists of smart card readers (fixed & handheld), Half Height Tripod turnstiles, EM locks for laboratory/building, card personalization unit, servers, management/monitoring software with backend database and network infrastructure. The current infrastructure and software is totally independent at LPSC, Valiamala and Bangalore.

1.2 NEW PROPOSAL

The new tender is to replace the existing Access Control System at LPSC Valiamala and Bengaluru campuses and to establish an Enterprise Access Control and Management System (EACMS) with new features and new modalities of access control ensuring interoperability across all ISRO Centres/Units. The system is envisaged to have a centralized monitoring from

LPSC, Valiamala (the headquarters) with decentralized management of users and readers locally at Bengaluru unit and workcentres.

The main gates at all locations will be equipped with multilane motorized tripod turnstiles for entry/exit integrated with biometric readers having capability to capture, process and operate based on contactless smartcard, finger print and face credentials. The reader should have capability to make access control decisions based on smartcard, face and finger credentials or a combination of them. However at any point of time, the reader should enable either face or finger sensor to work along with the Smartcard depending on the employee's office location read from the smartcard. When a user swipes the card, EACMS should automatically select the biometric mode (face or finger) depending on whether the user is a local user (LPSC employee or non-employee) or a global user (Any employee from other ISRO centre or Visitor)

The following are the different modes of operation for the readers.

1. Smart Card and Face recognition based ACS at main entrances for LPSC employee, trainees and contract workforce
2. Smart Card and Fingerprint based ACS at main entrances for other ISRO centre employees visiting LPSC
3. Smart Card and Face or Smart Card only or Face only based ACS at second level (critical laboratories)
4. Smart Card and Face or Smart Card and Finger or Smart Card only for Visitors

The card architecture and validation schemes will be defined by ISRO which needs to be implemented by the successful Vendor. The software features and reporting requirements are detailed in the Technical specifications. The software should be hosted in Windows/ Linux platform.

1.3 ARCHITECHTURE

The headquarters of LPSC at Valiamala, Trivandrum, its unit LPSC, Bengaluru and work centres at HAL campus and ITPF, Tumkur (Karnataka) are distributed across different geographic location and are in same IP network. However few work centres at different geographical locations are connected to LPSC, Valiamala and Bangalore are through different IP networks. The distribution of LPSC offices and an overall architecture envisaged for EACMS implementation is as shown in fig: 1.

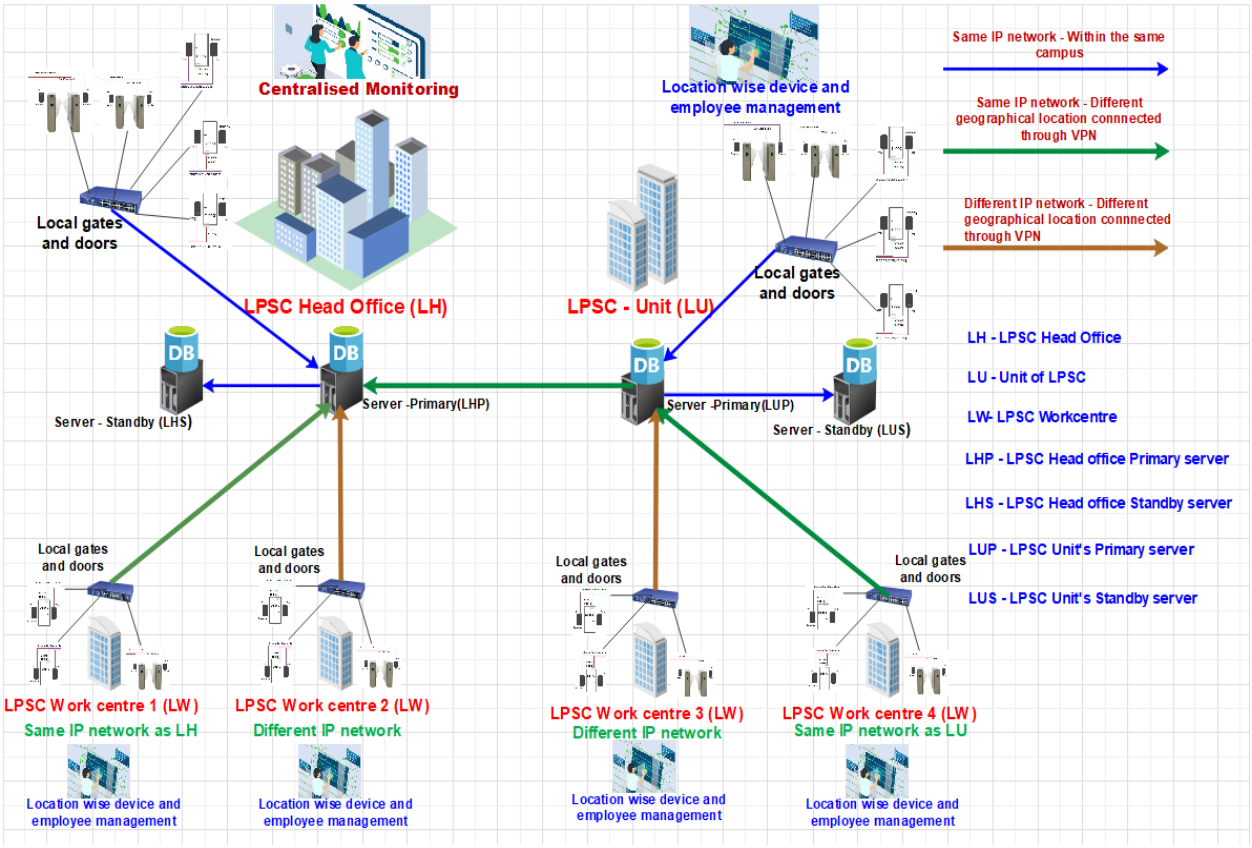

Figure – 1 – Biometric based ACS Architecture

Note: The workcentres in the above diagram is to show the scenarios and does not indicate the actual number of workcentres. The solution should be scalable to add more locations in same or different IP networks.

Abbreviations used in Architecture

1. LH – LPSC Head Office
2. LU – Unit of LH
3. LW – Work Centre of LH or LU
4. LHP, LHS– LH's Primary and secondary server respectively
5. LUP, LUS – LU's Primary and secondary server respectively

LPSC campus network consists of Intranet and Internet IP networks which are air gapped. The EACMS solution will be implemented in Intranet IP network. The readers of LH and LU at main gate and the laboratories will be in Intranet IP network. The readers at LW can be in Intranet or Internet IP network. The solution should be able to integrate the readers in Internet IP network to EACMS. Management of readers, user data movement and transaction data movement to and

from the LW readers in Internet IP network should involve an intermediary that will push or pull data to the EACMS server which is in Intranet IP network.

The following will be the mode of operation

- The offices LH, LU and LW will be having first and second level access gates and doors managed locally.
- The LH and LU locations will host the primary and standby servers with database and software.
- LWs can be in same or different IP networks and the transactions will sync to corresponding LH or LU database
- All local access transactions at LH will be synced to LHP server in near real time.
- All transactions of LWs of LH will be synced to LHP server in near real time.
- All local access transactions at LU will be synced to LUP server in near real time.
- All transactions of LWs of LU will be synced to LUP server in near real time.
- In LH and LU locations, the primary DB will be replicated in the standby server in near real time.
- The transactions from LUP server (local LU and LWs of LU) will be synced to LHP server incrementally in a scheduled time interval as desired by LPSC to facilitate centralized monitoring at LH.
- Enrolled data of different user types such as Employees, Trainees, Contract Workforce and Visitors should be auto synced only to the assigned reader groups.
- Separate instance of EACMS software should be deployed in LH and LU
- The records (transaction id) of each location should be uniquely identifiable and there should not be any collision while syncing the data to LH from LUs and LWs
- The controlling server and the readers could be deployed in different IP networks and should not affect the real time transaction data transfer

Note: The attendance monitoring of all employees of LH, LU and LWs should be possible from LH apart from local monitoring at LH, LU and LWs. However, the device and user management will be done locally. The software deployment should allow control and management of respective devices and users of LH, LU and LWs locally by authorized local administrator. So there should be a super user at LH and LU along with each instance, who can delegate powers to Local administrators to manage devices and users locally.

2. DEFINITIONS

2.1 Department: Department means Liquid Propulsion Systems Centre, ISRO, Department of Space of Government of India.

2.2 Contract/ Purchase Order: The term Contract/ Purchase Order means agreement executed between the Department and Contractor, together with the document as referred to therein including the functional requirements, specifications, drawing and instructions issued within the Contract provisions from time to time by the Contract Manager and all those documents taken shall be complementary to one another.

2.3 Contractor: Contractor shall mean the individual or firm or company, whether incorporated or not, chosen by the Department among the Bidders to this RFP, undertaking the work and shall include the legal personal representatives of such individuals or the persons composing such firm or company or the successors of such firm or company and the permitted assignee of such individual or firm(s) or company.

2.4 Contract Administrator/ Manager/ Department Representative/Key Personnel: The term shall mean the appropriate authority declared by the Department who shall co-ordinate the tasks in the execution of this contract.

2.5 Site Engineer: The term Site Engineer shall mean the authorized representative of the contractor who shall co-ordinate the execution of the contract.

2.6 Site: The term Site shall mean the actual place of the proposed work or other places on which work is to be executed under the Contract which may be allotted by Department for the purpose of carrying out the work.

2.7 Work: The term Works shall mean the places where work is performed by the Contractors.

2.8 'Specification/Proposal': shall mean collectively all the terms & conditions contained in those portions of the 'Contract' known as 'General & special terms and conditions of contract for supply, installation, testing, Commissioning', Training and support during Warranty and CAMC period.

2.9 'Date of Contract': shall mean the calendar date on which the Department and Contractor have signed the 'Contract'. 'Effective Date of Contract' shall mean the calendar date on which the Department has issued to the Vendor the 'Purchase Order' or Contract as otherwise mutually agreed to between the Department and Contractor.

2.10 'Contract Period': shall mean the period during which the 'Contract' shall be executed as agreed between 'Contractor and Department'.

2.11 'Performance Tests': shall mean such tests are prescribed in the specification to be done by the Contractor before the system is taken under warranty by the Department.

2.12Glossary of terms relevant to this Tender Document

ACS	Access Control System
AMC	Annual Maintenance Contract
A&M	Administration& Maintenance
ATP	Acceptance Test Plan
BOM	Bill Of Material
CAMC	Comprehensive Annual Maintenance Contract
EACMS	Enterprise Access Control and Management System
EDC	Expected Date of completion
EM	Electro Magnetic
LPSC	Liquid Propulsion systems centre
OEM	Original Equipment Manufacturer
OS	Operating System
PCC	Police Clearance Certificate
RTC	Real Time Clock
SRS	Software Requirement Specification
VMS	Visitor Management System

2.13 Communications

All communications affecting the terms and conditions of the contract and concerning its execution shall be made or confirmed in writing.

3 BRIEF SCOPE OF WORK

a. LPSC desires to implement Enterprise Access control and Management System (EACMS) in Valiamala, Bengaluru offices and Work Centres as per the specifications, terms, conditions and scope given in detail in this RFP document, for a period of 8 years (3-year Comprehensive Warranty and 5 year Comprehensive AMC). The installations at Valiamala and Bangalore will be separate. Vendor should be ready to install and integrate biometric readers at Work Centres at different locations connected by same or different IP networks after EACMS is commissioned and operational at LPSC Valiamala and Bangalore as per LPSC's requirement during warranty or AMC period. The proposal is for an Enterprise-wide multi-factor authentication-based Access Control System to ensure that only authorized persons can enter / leave LPSC's premises including high security areas as may be designated by LPSC from time to time. **The supply, installation, testing and maintenance as per the Timeline mentioned in the RFP should be done separately at the Head Office at Valiamala and Unit at Bangalore.**

b. EACMS should provide Tiered Access control for Employees/ Trainees / Contract workforce, visitors. It should have the capability to provide controlled access to areas, doors, rooms to different category of card holders depending on the need within the campus. The software should have option to capture the type of personnel like employee, trainee, contract manpower, visitors etc.

c. Readers should be capable to capture and process smartcard, face and fingerprint credentials but the following modality should be independently configurable for each reader as below:-

- Smart card + biometric (face) – LPSC personnel
- Smart card + biometric (finger) – Other centre personnel
- Face only
- Finger only
- Card only

The card architecture will have the details of the Centre Code to identify to which centre of ISRO an employee belongs to. The software should have option to identify this and as mentioned above the appropriate access control modality should be implemented.

d. Vendor shall propose and submit suitable solution with system configurations, detailed block diagrams and necessary techno-commercial details.

e. All necessary tools, equipments, hardware, software and software user licenses required as described in this document for the complete implementation of the EACMS shall be supplied and installed under this contract.

f. All Vendors who are desirous to participate in the tender should mandatorily visit LPSC, Valiamala and should attend pre-bid meeting to decide on the EACMS requirements. Vendors who are desirous to conduct site visit at LPSC, B'lore can also do the same on a different date after pre-bid meeting before bidding

g. All equipments supplied by the successful Vendor shall be installed, configured, programmed, tested and commissioned. The Vendor shall also supply all materials and services necessary for or incidental to the installation and commissioning of the complete system.

h. The smart card will be personalized as per LPSC's requirement. Smart card personalization, installation and configuration of hardware and software will be in the scope of this project and the details will be shared with the successful Vendor

i. The card shall have the capability to store other applications data, which may be implemented by LPSC, in due course. 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. A brief description of the card format, keys and validation scheme is given in Section B, Sl. No.3.24.

j. The successful Vendor has to provide warranty and comprehensive Annual Maintenance of the total solution after the expiry of warranty period. For maintenance of system in warranty and post warranty (Comprehensive Annual Maintenance) one onsite engineer each shall be posted at two locations of LPSC, Valiamala, Trivandrum, Kerala and LPSC, Indira Nagar, Bangalore, Karnataka.

k. Migration of essential employee data from existing system to the new solution is in the scope of the Vendor.

l. Detailed Technical Specification and Scope of work is given in Section B.

m. The successful Vendor has to study the requirements and submit the proposed drawing of placement of turnstiles and readers for approval from Department. Based on the approval, Vendor has to provide one sample unit of total system (turnstile + readers for entry and exit) for one lane. This has to be successfully demonstrated at one of entry / exit lane identified by the department. Based on the demonstration, department will give approval for production of the ordered quantity. Any changes suggested shall be implemented without any additional cost.

4 ELIGIBILITY CRITERIA FOR BIDDING

a) The proposal should be for the complete solution as per the scope of the tender. Please note that the requirement in this tender is non-divisible in nature.

b) A site visit will be arranged on the pre-bid meeting day as mentioned in tender at LPSC, Valiamala, on a date after tender release and only the bids of Vendors who have attended the pre-bid meeting will be opened for tender evaluation. Vendors who are desirous to conduct site visit at LPSC, B’lore can also do the same on a different date after pre-bid meeting at LPSC, Valiamala, but before bidding.

c) Vendor shall submit authentic documentary evidence in support of the below eligibility requirements and all the technical compliances. Bids that are not accompanied by such documents shall not be considered for further processing.

#	Parameter	Pre-Qualification Criteria	Document Required
1	OEM or Authorized Dealer	The Vendor should be OEM or authorized dealer of proposed product and should confirm that they will provide after sales support	**1) If OEM**: self-certified on letter head **2) If Dealer**: Authorization certificate in original from OEM for each item of EACMS certifying that the Vendor is an authorized dealer/agent for the OEM and the OEM shall be responsible for after-sales service, if the Vendor is unable to give proper service not only during the warranty period, but also during the CAMC period (i.e., Minimum 8 Years from the data of placement of PO). This certificate should refer to this tender with specific tender number. **3)** Section C Annexure III and IV duly filled
2	Profit & Loss Statement	The company must have made profit in at least 3 years out of 7 years ending 31/03/2023 as per audited balance sheets.	1. Audited Profit & Loss Account for those three financial years Copy of IT return filed by the company for those 3 years may be submitted.
3	Solvency Certificate	The bidder should provide a valid solvency certificate	Latest Solvency Certificate for a value of Rs.95 Lakhs issued on or after 31stDecember, 2023 from a scheduled/ commercial bank.
4	Tax/sales/PF	The Bidder should be registered for GST, PAN,	Copy of PAN card

	registration	ESI, PF	Copy of GST certificate E.P.F Registration letter/Certificate E.S.I Registration letter/certificate
5	Technical IT employees	The bidder should have qualified IT technical employees/supporting team on its payroll at the time of bidding.	Certificate on Letter Head of the Vendor with details like Name,Qualification,Post Held and Experience of employees to be given
6	Local office	Considering the 24 X 7 availability of the system, the bidder should have support office in South India during the period of the contract	Supporting document for proof of address
7	Experience Govt./PSU/Private firms	1. The Vendor should have implemented similar works*of providing the integrated access control solution with Biometric Features (Face or Finger or both) in the past 7years. *Similar work means Vendor should have supplied, installed, commissioned Biometric Access Control System with Face or Finger or both biometric with necessary s/w development for complete EACMS solution and mifare card personalization. The commissioned system should have at least 30 biometric readers to any Government Departments, PSUs or Private Industry 2. The Vendor should meet one of the following criteria. 2.a One similar work /purchase order costing not less than 254 Lakhs or 2.b Two similar works of each work/purchase order costing not less than 159 Lakhs or	1) Copy of Work Orders 2) Work Completion certificate from the client OR contact details of the client. 3) Submit details as perSection C, Annexure-I, Sl.No.3

		2.c Three similar works of each work/purchase order costing not less than 127 Lakhs Work Orders or Purchase Orders other than mentioned above are NOT considered for eligibility criteria. Hence such bids will not merit for eligibility evaluation and will be rejected. Therefore, bidders are advised to read the Work Experience of Similar work and of value before submitting bids and avoid being disqualified by submitting works experience of other than required eligibility criteria Work executed as sub-contract or joint-venture will not merit for eligibility evaluation.	
8	Blacklisting	The bidder should not have been blacklisted by Central / State Government/ PSU in India at the time of submission of the Bid	Self-declaration by Vendor Affidavit on Non Judicial Stamp Paper of Rs.100/- duly countersigned by Notary that they have not been banned or debarred by any Govt./Quasi Government Department or PSUs.
9	Compliance to GFR 144 (xi)	The bidder should comply with GFR 144 (xi) ,2017 regarding restrictions on availing / procurement of goods and services manufactured/ developed in a country which shares a land border with India.	Declaration as in Annexure VIII to be submitted with relevant proof.

5 INSTRUCTION TO VENDORS

5.0 Tender Document

a) Interested prospective Vendors are advised to go through the Tender documents carefully before participating in the bid.

b) The proposal shall be completely filled in all respects and shall be submitted together with requisite information, documentary proofs and duly filled Annexures.

c) The Proposal shall be opened on the date and time specified in the Letter Inviting Bid.

d) Conditional offers and those with specifications not in conformity with the tendered specifications shall not be considered.

5.1 Preparation of bids

5.1.1 Site Visit & Pre-bid discussion - **Mandatory**

Bidder has to mandatorily visit the site and study the site conditions to familiarize the proposed Biometric based Access Control System site, to get better understanding of the requirements, environment and shall collect all other information which may be required for submitting the Bid and entering into the contract. Claims and objections due to ignorance of existing conditions or inadequacy of information will not be considered after submission of the Bid and during implementation. The quantity tolerance shall be applicable based on the pre-bid discussion. The bids of those vendors who attended the pre-bid discussion only will be considered for evaluation. Vendors who are desirous to conduct site visit at LPSC, B'lore can also do the same on a different date after pre-bid meeting and before bidding.

5.1.2 Validity of Offer

Bid shall remain valid for acceptance for a period of 6 (six) months from the due date of submission of the Bid. The Vendor shall not be entitled during the said period to revoke or cancel his Bid or to vary the Bid except and to the extent required by Department in writing. Bid shall be revalidated for extended period as required by Department in writing. In such cases, unless otherwise specified, it is understood that validity is sought and provided without varying either the quoted price or any other terms and conditions of Bid finalized till that time.

5.1.3 Cost of Bidding

All direct and indirect costs associated with the preparation and submission of the Bid (including clarification meetings and site visit, if any), shall be added to Vendor's account and the Department will in no case be responsible or liable for those costs, regardless of the conduct or outcome of the Bid process.

5.1.4 Prices

The price must be filled in the online bid with the 'Schedule of Prices'. The price bid format is given in Section C, Annexure – VI.

5.1.5 Documents Comprising the bid

a. Part- I: The Technical and Commercial Terms & Conditions. This is **UN-PRICEDBILL OF MATERIALS**. Price of any nature in Part-I bid (Techno-Commercial) shall be rejected without any notice.
b. Part- II: **THE PRICED BID**. This should contain Price details only

5.1.5.1 Part- I: Techno-Commercial

Tender document contains technical requirements and specification of Biometric Access Control System. The detailed technical specifications of tenderer's offer should be covered in this part. **This part should not contain Price Details in any form**. Technical bid shall be submitted online. The requested documents should be attached in 'documents solicited from the vendor' and the following documents shall be attached along with the technical bid. The following need to be submitted

a. The commercial terms to be covered in this part like Delivery Terms, Delivery period, Payment terms, Validity of the offer, Warranty, Guarantee, security deposits, Performance Bank Guarantee, Liquidated Damages (for delayed supply), Price masked Bill of material, etc.
b. The Vendor is required to confirm acceptance of all terms and conditions in the tender.
c. The following Documents are to be mandatorily submitted

c.i. Section C, Annexure I – Duly filled

1. Vendor's Profile
2. Declaration by Vendor
3. Details of Past experience

c.ii. Section C, Annexure II – Duly filled

1. Technical compliance statement. Deviations if any shall be brought out clearly
2. Compliance to Commercial Terms and Conditions
3. Compliance to submission of all Documentary proof requested

c.iii. Section C, Annexure III – Duly filled

1. Authorization Form from OEM

c.iv. Section C, Annexure IV – Duly filled

1. Back to back OEM support certificate during warranty and AMC
2. Unconditional Acceptance of The Terms & Conditions of The RFP
3. Escalation Matrix
4. Certification For Local Content

5. Self-Declaration of Non-Blacklisting
6. Undertaking of Information Security Compliance
7. Undertaking of Authenticity of Solution (Hardware And Software)
8. Software/Solutions Integrity Certificate
9. Declaration On Technical Service Support Personnel
10. Declaration on EOS products

c.v. Section C, Annexure V – Duly filled

1. Unpriced version of bill of materials (Prices not to be mentioned), signed and stamped. Deviations if any shall be brought out clearly.
2. Declaration of quoting AMC rates
3. Additional Items required other than that mentioned in bill of materials

c.vi. Any other relevant document, Vendor desires to submit.

c.vii. Section C Annexure VIII – Duly Filled

1. Declaration on compliance to GFR (Xi) and relevant proof

Note:

a) Make and Model no. of each item are to be given in respective column in Unpriced BOM (Section C, Annexure V, Sl.No 1 &3) and Technical Compliance sheet (Section C, Annexure II, Sl.No 1). Technical data sheet/literature highlighting the compliance to specifications is to be submitted.

b) Technical compliance sheet with just 'Yes/Complied' without supporting datasheet/document will not be considered for tender evaluation.

c) Bids which do not include details of Comprehensive AMC (duly filled Section C - Annexure V, Sl.No.2) will not be considered for tender evaluation

5.1.5.2 Part II -Price Bid

Price bid shall be filled and submitted in the online 'price bid format'. The price quoted in Price Bid should be only in Indian rupees

a) Total cost of the 'EACMS' for finding L1 vendorwill be basedon Total Cost of all items and labour necessary for implementation of EACMS and operational cost comprising of deploying two resident technical support personnel at each location (Valiamala and Bangalore) during three years comprehensive on-site warranty period quoted by the Vendor in Section C, Annexure VI , Sl.No. 1(PRICE BID - BILL OF MATERIAL AND PRICE SCHEDULE).**Comprehensive AMC cost will not be considered for arriving at**

L1. However, bids which do not include details of Comprehensive AMC charges (duly filled Section C Annexure VI, Sl.No.2& Sl.No.**4) will not be considered for tender evaluation**.

b) The schedule of prices shall be read in conjunction with all the sections of tender document. The price bid should not contradict the Technical bid in any manner.

c) The total cost of EACMS and operational support by deploying Resident Technical support one at each location should be filled in the tender template price bid. However, split up cost of each item must be filled in the format for 'Bill of Material and Price Schedule' as per Section C, Annexure-VI, Sl.No. 1. The unit rates quoted shall be firm and fixed. The total contract price shall be arrived at, based on unit rates quoted and the quantity specified in the proposal.

d) The quantity of consumables and accessories in the unpriced Bill of materials (Section C, Annexure V, Sl.No. 1 mentioned in EACMS RFP) are only indicative.

e) Details of additional items if any, required for establishing EACMS which are not covered in Bill of Materials (Section C, Annexure V Sl.No. 1 mentioned in EACMS RFP) must be filled mandatorily as per Section C, Annexure V, Sl.No. 3. Cost of such additional items should be given in Section C, Annexure VI, Sl.No. 3 and the total cost of that should be given in the specified row in the PRICE BID - BILL OF MATERIAL AND PRICE SCHEDULE(Section C, Annexure VI, Sl.No. 1)

f) If vendor requires any other item during implementation of the solution, apart from those listed in Section C, Annexure V, Sl.No. 1 and Sl.No. 3) cost of those items should be borne by the Vendor

g) Vendor should mandatorily quote for the following:-

Post warranty Comprehensive AMC (CAMC) charges for Five years covering, the entire EACMS encompassing all software/hardware items, all parts, services, consumables and labour after acceptance by department including Resident Technical support during CMAC period. However a separate PO will be released after warranty based on the CAMC rates quoted in this bid. Device wise split up CAMC charges per year should be mandatorily given as in the template -Section C Annexure VI Sl. No.2& Sl.No.4.

5.1.6 Bid Submission

a) Bids duly filled in by the Vendor should invariably be submitted as stipulated in the Letter inviting bid.

b) Department shall open Part – I of the bid on the due date of opening. Price Bid (Part-II) of the bid of the technically qualified bid shall be opened at a later date.

5.1.7 Bid Evaluation Criteria

a) During evaluation, Department may request Vendor for any clarification on the bid, additional documents etc. Vendor shall submit all required documents/clarifications.

b) The complete scope of work is defined in the Tender document. Only those Vendors who undertake total responsibility for the **complete** scope of work including resident Technical support and CAMC as defined in the Tender document shall be considered for evaluation.

c) In case Bid does not fully comply with the requirement of Tender document and the Vendor stipulates deviations to the clauses of the tender, which are unacceptable to the Department, the Bid will be rejected.

d) Performance of Vendor on similar nature of works executed shall be taken into consideration during technical evaluation before selecting the Vendor for opening his price bid.

e) The documentary proofs and technical data sheets are mandatory and will be considered for evaluation

As part of technical evaluation, Vendor may be called for technical presentation/demonstration. During their presentation the following technical capabilities of Vendor will be evaluated.

1. All hardware components of EACMS shall be demonstrated to ensure that all technical specifications mentioned in Section-B are complied.
2. Should demonstrate the ability to Read and Write smart cards with multiple keys(encryption and decryption to be used)
3. Should demonstrate face(live and photo) and finger enrolment
4. Should demonstrate fixed reader along with turn stile for one full cycle of authentication(Smart Card+ face and Smart Card + finger) with turnstile rotation
5. Should demonstrate hand held reader, one each for face and finger separately(Smart Card + face and Smart Card + finger)
6. Functional aspects and nonfunctional performance(load, security etc) of the standard EACMS Software modules

f) During their presentation, understanding of vendor on LPSC requirements and execution plan will be evaluated.

g) The time schedule for EACMS completion is given in the Tender document (Refer Section A, Sl.No.8).Vendor is required to meet thetimeline strictly.

h) Offers which are found to be fulfilling all the eligibility and qualifying requirements of the tender document both technically and commercially will only be considered for price bid opening.

i) The Vendors shall clearly mention the Make and Model of the items quoted in their bid documents. The detailed data sheets for the products/items offered by the Vendors are required to be submitted by them along with compliance sheets to ascertain their compliance with regard to the product specifications mentioned in the tender document. The Vendors must attach Authorization Letter from OEMs to support the offered hardware and software for the EACMS.

j) The Vendors shall submit their commercial bid strictly as per the prescribed format. The Vendors are required to offer Comprehensive Annual Maintenance Contract (CAMC) rates for next Five years after the completion of initial three-year Comprehensive Warranty period.

k) Price Bids of vendors who are qualified for the Part I (Techno- Commercial) will only be opened for evaluation

l) Price bids of Vendors who quote for all items as detailed in the Section C Annexure VI Sl.No1 , Sl. No 2 , Sl.No3 (if any) and Sl.No 4 will only be considered for evaluation. Section C Annexure VI Sl.No 3 is for additional items and vendor can quote if any additional items are required.

m) The documentary proof as detailed below are mandatory for evaluation

1	**Vendor profile and declaration**	Vendor details should be provided	Duly filled and signed Section C, Annexure I
2	**Compliance**	Vendor's Compliance to all technical , commercial terms and submission of documents is mandatory	Duly filled and signed Section C, Annexure II
3	**MAF**	Certificate of undertaking from original equipment manufacturer	Duly filled and signed Section C, Annexure III
4	**OEM Support and declarations**	1. OEM Back to back support guarantee for after sales support for entire contract period. 2. Unconditional Acceptance of The Terms & Conditions of The RFP	Duly filled and signed Section C Annexure IV Sl.No 1,2,3,4,5,6, 7,8 and 9

		3. Escalation Matrix 4. Certification ForLocal Content 5. Self-Declaration Of Non-Blacklisting 6. Undertaking Of Information Security Compliance 7. Undertaking Of Authenticity Of Solution (Hardware And Software) 8. Software/Solutions Integrity Certificate 9. Declaration On Technical Service Personnel 10. Declaration regarding End-Of –Support products 11. Declaration under Rule 144(XI) in General Financial Rules (GFR), 2017	Section C Annexure VIII
5	**Local Content**	Vendor's declaration on the total local content of the solution quoted	Declaration on Vendor's letter head certifying the local content in the total solution with MII content evaluation location.Section C Annexure IV Sl.No 4
6	**Certifications and standards**	Standards and certification asked in the technical specifications of the product should be met	Proof of the certificates and standards with respect to each product
7	**Technical specifications**	Each component for which technical specifications are given in Section B of this tender to be met	Product Brochures, datasheets, manuals, etc.
8	**Additional software features**	Vendor should be ready to add additional features to the software as per LPSC's requirement during warranty or AMC period for which a separate PO will be issued.	Self-declaration by Vendor
9	**Addition of office locations (Work Centres)**	Vendor should be ready to install and integrate biometric readers at work centres at different locations connected by same or different IP networks after EACMS is commissioned and operational at LPSC Valiamala and Bangalore as per LPSC's requirement during warranty or AMC period.	Self-declaration by Vendor

10	**Unpriced Bill of Material**	All components other than cables, consumables and accessories should be quoted with make and model/ part number	Duly filled and signed Section C, Annexure V

5.1.8 Security Deposit

Vendor has to furnish a Bank Guarantee for 3% of the order value within 10 daysof receipt of Order towards the faithful execution of the order valid till the completion of the scope of work as per order plus sixty days. (This will be returned to you immediately on execution of the order satisfactorily as per order terms. In case of non-performance / poor performance, the amount will be forfeited).

5.1.9 Performance Bank Guarantee(PBG) / Fixed Deposit Receipt (FDR)

Vendor has to submit a PBG/FDR from a Nationalized / Scheduled Bank for **5%** of the order value towards the performance of the system at the time of supply valid till the completion of warranty and CAMC period plus 60 days in favour of Accounts Officer, LPSC/lein may be marked to Accounts Officer, LPSC.

6 GENERAL FINANCIAL PROVISIONS

a) All rates of Taxes /Duties /Levies applicable with details of percentages & applicable portion of the price should be spelt out clearly in the offer.

7 TERMS OF PAYMENTS

Our normal payment is 100% within 30 days after receipt, satisfactory installation and acceptance of the entire facility as per activities in the Time line mentioned in Section A, Sl.No. 8, at our site. However, advance payment may be considered to a maximum of 30% of the order value subject to the following.

a) Bank Guarantee shall be submitted to equal value of advance for delivery period with a validity period till completion of supply and acceptance.
b) Interest shall be calculated on the amount of advance for the delivery period quoted as per prime lending rate of Reserve Bank of India (RBI) for advances and added to the landed cost while arriving L1 offer.
c) Advance shall be progressively adjusted against bills cleared for payment.
d) Interest on advance shall be charged on delayed deliveries / installation.

Balance 70% of the order value shall be paid after receipt, satisfactory installation and acceptance of EACMS facility as per activities in the Time line mentioned in Section A, Sl.No. 8, at our site.

Operational support charges during warranty will be paid quarterly based on invoice submitted by the vendor after duly certified by the LPSC focal point. Quarterly charges will be derived on pro-rata basis from the operational charges quoted under Price bid Section C, Annexure – VI, Sl.No.30.

The performance bank guarantee as stipulated shall be submitted valid from the effective date of acceptance of the entire system by LPSC and valid for entire warranty period.

8 TIME LINE FOR EACMS IMPLEMENTATION

The entire EACMS system is required to be completed (all activities listed in the timeline below) by the successful Vendor in maximum of 8 **months from the date of receipt of Purchase Order.** Details of implementation of the EACMS in various stages of time line is as below:-.

Sl.No	Milestone	EDC
T1	1. Purchase order release 2. Software Requirement Document -SRD	T (LPSC Scope)
T2	Submission of the Design Documents which include the following Civil changes to be made for installation if any, with drawings 1. Site requirements, power supply & environmental requirements, accessories requirements at work site 2. Proposed drawing for positioning of half height motorized tripod turnstile at each gate of LPSC Valiamala and Bangalore 3. Drawings for positioning readers on pole in the lanes at each gate 4. Software and Firmware Requirements specification document -SRS	T1+ 3 weeks (Vendor Scope)
T3	1. The finalized configuration of EACMS (Clearance of Sl.No. 2 & 3 of T2) 2. Civil drawings approval 3. Site Clearance for implementation 4. Software and Firmware Requirements specification approval	T2+2 weeks (LPSC Scope)
T4	1. Software and Firmware design document -SDD submission 2. Sample unit (turnstile and reader) supply and demonstration with software with basic existing functionality 3. One reader in Internet IP network to be integrated and tested to demonstrate data flow to and fro with the EACMS intranet server	T3 + 1 week (Vendor Scope)
T5	1. Software and Firmware design document clearance 2. Clearance for supply of ordered quantity	T4 + 1 week (LPSC Scope)
T6	1. Software development and testing	T5 + 8 week (Vendor Scope)
T6 (i)	1. Delivery of hardware at Purchaser's site 2. Installation of servers ,database, basic software	T5 + 3 weeks (Vendor Scope)

	3. Configuration and testing of all handheld readers	
T6 (ii)	1. Installation and testing of readers at secondary level laboratories	T6(i) +2 weeks (Vendor Scope)
T6 (iii)	1. Dismantling of existing EACMS system at Gate 2 at LPSC, Valiamala , Lane 4 & 5 at LPSC, Bengaluru 2. Installation of new motorized turnstiles and fixing of readers in the above location	T6(ii) +3 weeks (Vendor Scope)
T7	1. Delivery of Software at purchase's site 2. Integrated Testing with all hardware components 3. Migration of Employee and card data 4. Photo enrolment of all employees 5. Demonstration of work centre connectivity(readers on different IP network) 6. Demonstration of decentralized management and centralized monitoring	T6+ 2 weeks (Vendor Scope)
T8	1. User Acceptance Testing, Webapp Security Testing 2. Pilot run for 5 days at Gate 2 at LPSCV and Lane 4 and 5 at LPSCB	T7+ 2 weeks (LPSC Scope)
T9	1. Dismantling of existing ACS system at Gate 1 (5 turnstiles, 10 fixed readers & 5 photo popups) 2. Erection, Installation of 5 new turnstiles, 10 fixed readers and 5 photo popups , interfacing & Testing of EACMS for Gate1 3. The above need to be done for Lane 1, 2, 3 at LPSC, B	T8 + 3 weeks (Vendor Scope)
T10	1. Dismantling of existing ACS system at Gate 3 & Gate 4(4 turnstiles, 8 fixed readers & 4 photo popups) 2. Erection, Installation, interfacing & Testing of EACMS for Gate 3 & Gate 4	T9+3 weeks (Vendor Scope)
T11	3. Full Integrated testing of EACMS for 15 days before Acceptance Testing	T10 + 2 weeks (Vendor Scope)
T12	Training – 1 week	T11+ 1week (Vendor Scope)
T13	Acceptance Testing	* T12+ min 2 weeks (LPSC and Vendor Scope)

*** Acceptance of the product only will be done by LPSC after successful completion of all test cases**

Note: **The delay in executing milestone due to activities in LPSC scope will not be attributed as vendor's delay**

9 DECLARATION

a) All components delivered as part of EACMS solution to the Department should be brand new. **The software licenses shall be perpetual.** Declaration as given in Section C, Annexure IV, Sl.No 7 to be submitted

b) Vendors shall propose only those products, which would not be declared end of life until the end of warranty period. Further, those products should also not go End of Support for 8 years (3 year warranty and 5 years CAMC) from the date of acceptance by LPSC. However, in cases where the OEM decides to phase out (end of support) any particular product model installed as part of EACMS during 8 years (3 year warranty and 5 years CAMC) from the date of acceptance by LPSC, the vendor is required to replace the product with a product having equivalent or better configuration at no extra cost to LPSC and integrate it with EACMS. Vendor must inform well in advance about such changes. Declaration as given in Section C, Annexure III and Section C, Annexure IV, Sl.No. 10 to be submitted

10 AVAILABILITY OF SPARES

The spares for the products offered should be available for at least 8 yearstill the completion of contractual obligations. The supplier should keep adequate spares in LPSC premises to maintain Service Level Agreement (SLA) and the list of spares which is kept by the supplier should be given to LPSC.

11 COMPREHENSIVE WARRANTY

a) Vendor must include comprehensive on-site warranty for **THREE YEARS** from the effective date of acceptance of the entire system by Department

b) Warranty shall include preventive & unlimited break-down maintenance calls including repair/replacement of material, spares, modules, software, etc.

c) Vendor should provide operational support by deploying one Onsite resident technical support at each location during warranty and Comprehensive AMC. Operational support charges during warranty period will be paid quarterly.

d) Vendor shall be fully responsible for the manufacturer’s warranty in respect of proper design, quality and workmanship of all equipments, accessories, etc., covered by the offer. The Vendor must provide warranty all equipments, accessories, spare parts etc., against any manufacturing defects during the warranty period. During the warranty period the Vendor shall maintain the equipment and repair / replace all the defective components at the installed site at no additional charge of whatsoever nature to the Department.

e) The Vendor should ensure that the defects in the EACMS system reported on any working day are set right **as per SLA**. In case, the system or any equipment cannot be repaired within the stipulated period, the Vendor should provide a replacement till the system/equipment is returned duly repaired.

f) Software Bug fixes, functional and performance requirement deviations from SRS should be corrected at free of cost

g) Vendor should fine tune the application for performance optimization if any performance related issues arises during Comprehensive Warranty / CAMC period

h) SLA is detailed in Section A, SL No. 22 and if not met by the supplier during warranty, PBG will be withheld by LPSC.

i) Firmware and software updates necessary for fixing security vulnerabilities that may arise during the period of contract should be carried out by the Vendor within 48 hours.

j) In the event of the Vendor's failure to supply & provide allied services within a reasonable period, the Department on its own will get the defects rectified through another agency at the risk and cost to Vendor. It will be deducted from the PBG. Repairs rectified through another agency will neither affect the liabilities of the Vendor on the warranty for its remaining period nor will it affect the Vendor's liabilities on the stipulated post-warranty Annual Maintenance Contracts.

k) Vendor shall supply replacement of spare/item of same make and model against faulty component during warranty. In case the manufacturer discontinues any model, Vendor shall supply spare/item with higher model of supplied make with better specifications at no extra cost and ensure that it gets integrated within the system.

l) The vendor shall replace and upgrade the components which are announced as end of support (EOS) by the respective OEM, at no additional cost to LPSC throughout the contract period. The bidder shall carry out such replacement & up gradation of components (hardware & Software) before end of support

m) All the mechanical parts of the system like readers, turnstiles, EM locks, exit switches shall be maintained periodically by cleaning, lubricating and alignment. Worn out mechanical parts shall be replaced at periodical interval.

n) Vendor shall carry out alignment of doors at buildings and laboratories for proper functioning of EM locks as and when required. During warranty period, the Vendor will be required to carry out maintenance and repairs if any, free of cost including replacement of spares/equipment without any additional cost.

o) **Disk Retention**: The Hard Disk Drive (HDD) and flash memory installed in any of the equipment (PC/Workstation/Server/readers etc), if found defective, the same shall be retained by LPSC. Vendor shall use their tools, etc., for identification and replace the same with a new one. Under no circumstances, the HDD would be allowed to take outside the LPSC campus and the Vendor shall replace them at free of cost during the warranty period.

12 COMPREHENSIVE ANNUAL MAINTENANCE CONTRACT

The Vendor is responsible for the maintenance of the EACMS including all hardware, accessories/components and software supplied for **Five years** (4^{th} year to 8^{th} year) after the expiry of initial warranty period of three years.

a) The Vendor shall maintain the equipment and repair/replace all defective components, major or minor and may use for this purpose spares or consumables at no additional charge other than the CAMC contract charges.

b) CAMC shall include daily, preventive & unlimited break-down maintenance including repair/replacement of material, spares, modules, software, etc.

c) **Disk Retention**: The Hard Disk Drive (HDD) and flash memory installed in any of the equipment (PC/Workstation/Server/readers etc.), if found defective, the same shall be retained by LPSC. Vendor shall use their tools, etc., for identification and replace the same with a new one. However, for the hard disk failures happening during warranty and CAMC period, the hard disks should be replaced and the defective hard disks will not be returned to the Vendor

d) Comprehensive on-site annual maintenance charges, for the post warranty period, must be quoted in rupees per year in the Price bid

- Device wise split up CAMC charges per year should be mandatorily given as in the template in Section C Annexure VI Sl. No 2

e) LPSC has the discretion to release a separate Purchase Order for Comprehensive Annual Maintenance after the expiry of Warranty period. The CAMC charges will be released in four installments in each year at the end of every three months' period against submission of a service report. CAMC charges shall be paid on quarterly basis after reviewed by the Contract Manager assigned at LPSC, Valiamala and LPSC, B'lore, duly approved by concerned authority.

f) During CAMC, if the Operating System of the deployed server for EACMS has reached End of Life, Vendor should upgrade the OS and port the software at free of cost.

g) Service Level Agreement comprising the critical activities, response time and Penalty is detailed in Section A, Sl.No. 22 and if it is not met by the supplier during CAMC, the penalties as detailed in Section A, Sl.No. 22 will be deducted from the quarterly payment

13 RESIDENT TECHNICALSUPPORT

a) During Warranty and CAMC period (3 + 5 = 8 years), the Vendor shall deploy trained Resident Technical support personnel at site (One each for LPSC, Valiamala and LPSC, Bangalore) for the operation and maintenance of EACMS to fulfill the SLA terms mentioned in Section A , Sl.No. 22

b) Trained technical support personnel shall be Diploma engineer in Electronics or Electrical (three years course from AICTE/DTE or equivalent approved institutions) with minimum one year experience in the maintenance and up-keep of Biometric Access control system

c) Resident Technical support personnel shall be available on all working days (30 minutes before and after the office hours). For any maintenance activities they may have to come on holidays also.

d) Deployed resident technical support personnel shall perform the following activities

i. Day-to-day maintenance of Readers, Turnstiles and ensure migration of punching data from readers to server.
ii. Configuration of all hardware device
iii. Maintaining configuration backup of all hardware devices
iv. Preventive and break down maintenance of the system.
v. Management of the spare parts, materials and consumables to repair defective hardware
vi. Periodical database back-up and preparation of weekly, monthly and quarterly reports on system performance in prescribed format.
vii. Maintenance of event logs.
viii. Any new installation of any components of EACMS as part of augmentation
ix. Any other related work assigned from time to time
x. Carry out the necessary Software updates to ensure the smooth running of the system

p) Police Clearance Certificate (PCC) must be obtained for each deputed engineer before deputing in LPSC.

q) LPSC reserves right to disqualify any Resident Technical support personnel deputed, for reasons like technical incompetence, indiscipline, irregularity, insincerity, disobedience,

doubtful credentials/ integrity, etc. Declaration as given in Section C, Annexure IV, Sl.No 9 to be submitted

14 FORCE MAJEURE

Should a part or whole work covered under this contract be delayed due to reasons of Force Majeure which shall include legal lockouts, strikes, riots, civil commotion, fire accident, quarantines, epidemic, acts of God and Government, fright embargoes, the completion period for work, plant or equipment referred to in this contract be extended by a period not in excess of the duration of such Force Majeure. The occurrence shall be notified by either party within reasonable time.

15 DELAY IN COMPLETION/ LIQUIDATED DAMAGES

In the event of the Vendor failing to complete the work within the time specified in the contract agreement or in extension agreed thereto, the Department shall reserve the right to recover from the Vendor as liquidated damages, a sum of one half percent (0.5%) per week or part thereof of the undelivered portion of the total contract price of plant, equipment or work. The Total liquidated damages shall not exceed the ten percent (10.0%) of the total Contract price.

16 ARBITRATION

If at any time any question, disputes or differences whatsoever shall arise between the purchaser and the Vendor upon or in connection with this contract, either party may forthwith due to the other notices in writing of the existence of such question, dispute or difference and the same shall be referred to the adjudication of two arbitrator or one to be nominated by purchaser, other by Vendor. The award of the arbitrator shall be binding on the parties to the dispute. However, any party aggrieved by such award may make a further reference for setting aside or revision of the award to the Law Secretary, Department of legal affairs, Ministry of Law and Justice, Government of India. Upon such reference the dispute shall be decided by the Law Secretary or the special Secretary/Additional Secretary when so authorized by the law secretary, whose decision shall be binding on the parties finally and conclusively. The parties to the dispute will share equally the cost of arbitration as intimated by the arbitrator. In the event of either party ceases to be an undertaking of Government of India, arbitration & conciliation act 1996 shall be applicable. The venue of arbitration should be the same place where centre is located.

17 DISCLOSURE AND USE OF INFORMATION BY THE VENDOR

Vendor shall guarantee that all information and data received during execution of Contract from Department shall be classified as confidential within the meaning of the Official

Secrets Act and will not be divulged to any third party without prior written permission of Department. All drawings & documents shall be returned after execution of work.

18 INDEMNITY

a. The prices indicated in the Purchase Order/Contract shall be deemed to include all amounts payable for the use of patents, copyrights, registration charges, trademarks or other industrial property rights

b. The contractor/supplier shall, at all times, indemnify the Centre/Unit against all claims including claims by any third party relating to stores for infringement of any rights protected by patent registration of design or trademarks

c. Till the supplies reach their destination, the contractor/supplier shall be responsible for any damage to the supplies arising from whatever cause other than Force Majeure factors.

d. The contractor/supplier shall also take the entire responsibility for adequacy of supplies/services for fulfillment of the Purchase Order/Contract.

19 LEGAL

The CONTRACTOR shall abide by the law of the land including all labour related laws/ Acts or any new regulations/legislations enacted in this regard and its compliance as applicable during the tenure of the CONTRACT. CONTRACTOR shall ensure minimum wage to their human resources coming under category of Resident Technicalsupport as per minimum wage act 1948 and as per the orders issued time to time by Chief Labour Commissioner, Ministry of Labour and Employment, Government of India. Department shall in no way be responsible for any default of the CONTRACTOR regarding statutory obligation.

20 NON-DISCLOSURE AGREEMENT (NDA)

Personnel deputed by Vendor during implementation of the system, warranty period and CAMC shall maintain absolute secrecy and security of the processes and data stored on various computing systems at LPSC. The data / information provided by LPSC from time to time, are for the execution of this work only; and should not be used / copied / reproduced / published in any form or disclosed to third party, by Vendor or their personnel. Thus, Vendor is required to sign a Non-Disclosure Agreement (NDA) with LPSC. Vendor will also be responsible for any violation or infringement of NDA by their personnel.

21 TERMINATION OF CONTRACT

Under normal circumstances, termination of the contract is not foreseen. However, in case of continued non-performance of the Contract resulting in inordinate delays in the delivery dates and rectification of issuesin spite of repeated written requests for meeting the delivery schedule and SLA as provided in the Contract, DEPARTMENT reserves the right to terminate wholly or partly, the Contract, by giving a notice of not less than one month.

22 SERVICE LEVEL AGREEMENT (SLA)

a. SLA defines the successful Vendor's responsibility in ensuring the performance of the solution based on the agreed performance indicators as detailed in the technical specification - Section B of tender.

b. The table below summarizes the severity/criticality indicators for the services to be offered by the Vendor

1. Category of Issues

Sl.No	Severity	Issues
1	Critical	1. Hardware failure or misbehavior – Any hardware component of EACMS 2. Data breach 3. Firmware and software updates necessary for fixing security vulnerabilities 4. Missing transactions (in/out punch not getting recorded) 5. FAR and FRR of biometric readers are not as per the specifications during operations 6. Repeated data syncing issues between reader and server 7. Software fails to perform any critical software function # listed out in the RFP due to a software bug 8. Uptime *- If less than 99% 9. Resident Technical support- Vendor does not deploy the required specified quantity & quality of personnel as per RFP or a person deployed is not reporting to the duty
2	High	1. Enrolment issues 2. Data syncing issues between databases 3. Hardware or software performance degradation
3	Normal	1. Reports related issues 2. Replacement of End of Support components before due date at no extra cost to LPSC

*Calculation of Uptime percentage of any component

- **Total Available Time** – 24 hrs per day for seven days a week

Critical S/w Function

a. Proper working of User authentication and entry/exit validation logic based on user types
b. Assignment of users to reader groups
c. Enrollment of user with proper biometrics
d. Centralized monitoring of data of all locations at LH (LPSC, Valiamala)
e. Addition/updation and configuration of devices in the EACMS
f. Personalization of smart cards and printing smart card based on user type
g. Syncing personalization details to server and from server to other readers across locations
h. Syncing of data from LU and LWs to LH
i. Syncing of punching details from reader to server within 5 minutes
j. In case of network issue, storing the punching details in reader and pushing to server once the network issue is resolved
k. Workflow for denial of blocked cards
l. Replication of data from online server to standby server in near real time
m. Proper generation of MIS Reports mentioned in the Integrated Software(Section B, SL.No.3.14.2)

2. Response Time

Sl.No	Severity level	Target /Response Time	Resolution/Work around
1	Critical	4 Business Hours	8 Business Hours
2	High	4 Business Hours	12 Business Hours
3	Normal	8 Business Hours	24 Business Hours
4	Resident Technical support	Availability as per Tender	If deputed Resident technical support is not available as per tender , he/she has to be substituted within 24 Business Hours

3. Penalty

Penalties will be recovered from CAMC charges during quarterly payment if successful bidder is not able to achieve required Service Levels as mentioned in Section A, Sl.No. 22 Amount equivalent to 0.5% of the quarterly CAMC charges per week will be deducted if the SLA is not met, as penalty charges.

4. Exclusions

The Supplier will be exempted from any delays or slippages on SLA parameters arising out of following reasons: -

1. Delay in execution due to delay (in approval, review etc.) from Purchaser's side. Any such delays will be notified.
2. Delay due to Network issues that can affect the data transfer and other software operations

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. Thedatabase at primary server should be replicated in near realtime 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. 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 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, two for Valiamala (Primary and Redundant servers) and two for Bangalore (primary and redundant servers). All components i.e., hardware, software and firmware should be operational from day one onwards

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 the following key principles of Digital Personal Data Protection Act ,2023 of GOI **1.Lawfulness**: Personal data must be processed lawfully, fairly, and transparently. **2.Purpose Limitation**: Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

		3.Data Minimization: Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. **4.Accuracy**: Personal data must be accurate and, where necessary, kept up to date. **5.Storage Limitation**: Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. **6.Integrity and Confidentiality**: Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.
	Sensing Distance	0.5m to 1.3m (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. Both cameras are mandatory.
	Face Illumination	Device must include built-in IR or Flash LED 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 algorithm 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 (Image of the presented face along with employee details should be logged irrespective of whether authentication is valid/ invalid. These image logs should be pushed to the server for verification of FAR and FRR.). 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	Facial Recognition shall work with

	Mask	face masks, spectacle, cap etc
	Image Dimension/Resolution/Size	All enrolled face image to be stored in the ISO format in the server and Image size and pixels range will be as per ISO format requirements. However, vendor can use their own proprietary image format for internal operations of the device.
	Face template size	Face enrollment process should generate and store face template in ISO/IEC 19794-5 formats.However, vendor can have a device specific face template format for internal operations
	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 to10MB 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	Slight deviation in finger position (horizontally) possible in the limited space of the finger sensor pad should be accommodated by the enrollment software. 180 deg vertical rotation is not envisaged as fingerprint capture is done under supervision
	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
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
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 compliant) , RS- 485 with OSDP, USB

	display	At least 3.5" IPS LCD touch screen 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 (relevant proof)
	Environmental	Humidity : 10% to 80% RH non condensing, Operating temperature: 0 deg to 50 deg
	Power requirement	As per Indian standard
	PoE	Power supply with external adaptor is mandatorily required. PoE is optional
	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 the following key principles of Digital Personal Data Protection Act ,2023 of GOI **1.Lawfulness**: Personal data must be processed lawfully, fairly, and transparently. **2.Purpose Limitation**: Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. **3.Data Minimization**: Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. **4.Accuracy**: Personal data must be accurate and, where necessary, kept up to date. **5.Storage Limitation**: Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. **6.Integrity and Confidentiality**: Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.

	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. Both cameras are mandatory.
	Face Illumination	Device must include built-in IR or Flash LED 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 algorithm 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 (Image of the presented face along with employee details should be logged irrespective of whether authentication is valid/ invalid. These image logs should be pushed to the server for verification of FAR and FRR.). 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	All enrolled face image to be stored in the ISO format in the server and Image size and pixels range will be as per ISO format requirements. However, vendor can use their own proprietary image format for internal operations of the device.
	Face template size	Face enrollment process should generate and store face template in ISO/IEC 19794-5 formats.However, vendor can have a device specific face template format for internal operations
	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 to10MB 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
Hardware/Firmware	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 compliant) , RS- 485 with OSDP, USB

	display	At least 3.5" IPS LCD touch screen 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
	Environmental	**Humidity : 10% to 80% RH non** condensing, Operating temperature: 0 deg to 50 deg
	Power requirement	As per Indian standard
	PoE	Power supply with external adaptor is mandatorily required. PoE is optional
	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 the following key principles of Digital Personal Data Protection Act ,2023 of GOI **1.Lawfulness**: Personal data must be processed lawfully, fairly, and transparently. **2.Purpose Limitation**: Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. **3.Data Minimization**: Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. **4.Accuracy**: Personal data must be accurate and, where necessary, kept up todate. **5.Storage Limitation**: Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. **6.Integrity and Confidentiality**: Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or

		damage, using appropriate technical or organizational measures.
	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. Both cameras are mandatory
	Face Illumination	Device must include built-in IR or Flash LED 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 algorithm 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 (Image of the presented face along with employee details should be logged irrespective of whether authentication is valid/ invalid. These image logs should be pushed to the server for verification of FAR and FRR.). 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	All enrolled face image to be stored in the ISO format in the server and Image size and pixels range will be as per ISO format requirements. However, vendor can use their own proprietary image format for internal operations of the device.
	Face template size	Face enrollment process should generate and store face template in ISO/IEC 19794-5 formats.However, vendor can have a device specific face template format for internal operations
	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 to10MB. ▪ 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
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 compliant) , Wi-Fi(WiFi 5 (IEEE 802.11ac), RS- 485 with OSDP, USB
	display	At least 3.5" IPS LCD touch screen 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
	Environmental	Humidity : 10% to 80% 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 Finger cum Smart card Access Control Reader
	Biometric Credential	Finger
	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	Slight deviation in finger position (horizontally) possible in the limited space of the finger sensor pad should be accommodated by the enrollment software.
	Image	In accordance with ISO 19794-2 standard.

	Dimension/Resolution	
	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
Smart Card	General	Contactless smart card with 7 Byte CSN
	Card Types	MiFARE Classic,MiFARE Plus, DESFire EV1/EV2
	Standards	Contactless smart cardsoperating 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
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	Processor 1.2 GHz or more and 4 GB Flash + 64 Mb RAM or more
	Authentication Mode	Primary: Card + Finger Option for Card only, Finger only shall be available
	Interface with Swing/tripod Barrier	Potential free contact
	Interfaces	Ethernet (IPV4 compliant) , **Wi-Fi (**WiFi 5 (IEEE 802.11ac), RS- 485 with OSDP, USB,
	display	At least 3.5" IPS LCD touch screen 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
	Environmental	Humidity : 10% to 80% 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 80%

Humidity	
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 80%

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 80%

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	LCD touch panel for making signature

pen / Pen digitizer	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	Server Certification	The offered server shall be certified for Latest version of RHEL, Windows Server (latest), Ubuntu and SUSE Linux platform. The URL for OS certifications by respective OS OEM for the supported hardware- list shall be provided for each platform along with the offer.	1
16	**HTML5 support**	HTML5 support for virtual console & virtual media without using Java or ActiveX plugins	
17	**Power**	Dual, Hot-plug, Redundant Power Supply (1+1), 1400W, Mixed Mode	1
		Power Chord - C13, 1.8M, 250V, 10A (India)	2
18	**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

3.14.1General	
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 multi location 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 (workcentres) 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 realtime ✓ 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

<table>
<tr><td></td><td>
✓ 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
</td></tr>
<tr><td>b)</td><td>
USER ROLES
<table>
<tr><th>Sl.No</th><th>Role</th><th>Description</th></tr>
<tr><td>1</td><td>System Administrator (Super User)</td><td>Over all administrator of EACMS</td></tr>
<tr><td>2</td><td>Local Administrator</td><td>Administrator of a location/ installation</td></tr>
<tr><td>3</td><td>Device management user</td><td>Hardware device and database management</td></tr>
<tr><td>4</td><td>Enrollment user</td><td>Manages enrollment and ID card printing</td></tr>
<tr><td>5</td><td>Management user</td><td>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.</td></tr>
<tr><td>6</td><td>General User</td><td>User can view their own attendance reports</td></tr>
<tr><td>7</td><td>Office Secretary user</td><td>User who manages shift entry, official engagement entry, tour entry and permission entry for an entity/group/division</td></tr>
</table>
System Administrator (Super User) (one each for each instance of installation)
✓ Should have access to all modules and configuration details of EACMS.
✓ User creation
</td></tr>
</table>

	✓ 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/workcentres 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. Provision to scale up 25% users and 50% devices (The users in EACMS RFP is 20,000 and devices are as mentioned in Bill of materials)
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 LPSCERP 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.
5	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
6	It should have option to select any two fingers for enrollmentand duplicate search facility in order to avoidmultiple enrollments of same individual. Biometric template in native format and ISO 19794 format shall be saved in server database.
7	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
8	This software shall be used at multiple locations for enrolment & card personalization of employees, non-employees and visitors.
9	Software shall have option to categorize the enrolled staff into Employees, Contractors, Trainees, and Visitors.
10	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.
11	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.
12	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
13	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
14	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).
15	Enrolled users should appear in dashboard of Local Administrator and Super user for assigning access permission to reader/reader groups
16	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.
17	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 lateentry/ 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%~80%
12.	IPV4 & 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 workshall be specified with details as per Section C, Annexure V, Sl.No 3– Unpriced and Annexure VI Sl.No 3 for price bid.

3.18 System 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.

3.19 Acceptance 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)

3.20 Training

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

3.23Special 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 isRead & 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.

SECTION-C

DOCUMENTS FROM VENDOR

Annexure - I

1. VENDOR'S PROFILE

1.	Name of the Organization and Address :
2.	Year of Establishment :
3.	Status of the firm (Whether Pvt. Ltd. company / Pubic Ltd. company/ Partnership Firm) :
4.	Name of the Chairman/Managing Director/CEO (as the case may be) :
5.	Whether registered with the Registrar of Companies/Registrar of Firms in India? If so, mention number and date and enclose Registration Certificate copy :
6.	Name and address of Bankers: a) b)
8.	Whether registered for sales tax purposes? If so, mention number and date. Also furnish copies of sales tax clearance certificate:
9	Is the Company / Firm a manufacturer of the components of the Access control System? If yes, a) Name of the place where manufacturing unit is located: b) Address and phone number of the company's office: c) Date of opening of company's office:
10	Since when and how long Company/firm has been manufacturing **ACS** Systems:
11	Whether company has been pre-qualified by other Central Government organization for ACS? (Furnish organizations names, category and date of registration):

<table>
<tr><td>12</td><td>Furnish the names of renowned organizations, where company has installed ACS Systems in India in the last seven years
<table>
<tr><th>Name of Organization with Address</th><th>Year of Installation</th><th>Value of orders</th></tr>
<tr><td>1.</td><td></td><td></td></tr>
<tr><td>2.</td><td></td><td></td></tr>
<tr><td>3.</td><td></td><td></td></tr>
</table>
Self attested copies of Performance Certificate (please do not enclose any work order) issued by organization in their letter head after completion of work must be enclosed failing which it will be treated that company has no past experience in the field of ACS.</td></tr>
<tr><td>13</td><td>Whether company is an authorized dealer/agent for the original equipment manufacturer? (Furnish a certificate in original from the original equipment manufacturer with respect to this tender):</td></tr>
<tr><td>14</td><td>Whether company is an ISO certified company? If yes, attach the relevant ISO certificate.</td></tr>
</table>

Place: SIGNATURE

Date: NAME & DESIGNATION

SEAL OF ORGANISATION

2. DECLARATION

a) I / We have read and understood the Tender document and I / We understand that if any false information is detected at a later date, any future contract made between ourselves and LPSC, on the basis of the information given by me / us can be treated as invalid by LPSC, and I / We will be solely responsible for the consequences.

b) I / We agree that the decision of LPSC in selection of Vendors will be final and binding to me / us.

c) All the information furnished by me hereunder is correct to the best of my knowledge and belief.

d) I / We agree that I / we have no objection if enquiries are made about the work listed by me / us in the accompanying sheets.

e) I / We agree that I / We have not applied in the name of sister concern for the subject empanelment process.

f) I / We hereby certify that none of my relative(s) is/are employed in DOS/ISRO. In case at any stage it is found that the information given by me/us is false/incorrect, DOS/ISRO shall have the absolute right to take any action as deemed fit without any prior intimation to me/us.

g) I / We have understood the terms and conditions of the tender document and fully agree with same.

h) I also agree to abide by all the statutory requirements as prevailing from time to time.

i) I/We hereby Undertake that our Company/Firm do not have any legal suit/criminal case either pending against me/us/proprietor or any of our Directors or being contemplated and have not been earlier convicted on the grounds of moral turpitude or for violation of laws in force.

Place: SIGNATURE

Date: NAME & DESIGNATION

SEAL OF ORGANISATION

3. EXPERIENCE

Details of implementation of similar works as detailed in Section A, Sl.No 4. d (Eligibility for Bidding)placed and completed for Govt./ PSU/ Private firms for implementing and maintaining face and finger based Biometric access control systems during last 7 years indicating the name of client, contact person, contract value, nature of work, work completion certificate, month & year of commencement & completion etc

Sl. No	name of client	contact person	contract value	Type of Biometric	No of employees of the client	month & year of commence ment	month & year of completion	If multilocation solution, office locations
1								
2								
3								

Place: SIGNATURE

Date: NAME & DESIGNATION

SEAL OF ORGANISATION

Annexure – II

1. TECHNICAL COMPLIANCE STATEMENT

Note: Vendors should state 'Yes' if their offer conforms to the Requirements and Technical specifications as stated in Section-B of the Tender document, or else they should state 'No' with reasons.

Sl No	Requirements	Make & Model wherever applicable	Compliance (Yes/No)	Reasons for non-compliance	Reference to Datasheet(mandatory for items other than spares and consumables)
1	Proposed system with all accessories complying to all features listed in Section A and Section B of this document and cyber security requirements as laid by ISRO/DOS.				
2	Proposed solution should have all the software features as listed in Section B Sl.no 3.14				
	Hardware components				
3	Biometric(Face and finger) and smart card readers – all integrated as a single unit with built-in controller that will be fixed on the tripod turnstiles Section B - Sl.No : 3.1				
4	Biometric(Face) and smart card readers with built-in controller that will be fixed on the tripod turnstiles Section B - Sl.No : 3.2				
5	Biometric(Face) and smart card				

	readers with built-in controller that are mobile/handheld Section B - Sl.No : 3.3				
6	Biometric(Finger) and smart card readers with built-in controller that are mobile/handheld Section B - Sl.No : 3.4				
7	Half height tripod turnstiles Section B - Sl.No : 3.5				
8	Photo popup ad accessories Section B - Sl.No : 3.6				
9	Electromechanical door lock for Single door with Exit switch Section B - Sl.No : 3.7				
10	Electromechanical door lock for Double door with Exit switch Section B - Sl.No : 3.8				
11	Biometric(Face) and smart card readers with built-in controller that will be fixed on doors that work as IN reader with EM locks Section B - Sl.No : 3.9				
12	Biometric(Face) and smart card readers without controller that will be fixed as ‘out’ readers on doors Section B - Sl.No : 3.10				
13	Biometric(Face and Finger) enrollment and personalization station Section B - Sl.No : 3.11				
14	Signature pad with pen Section B - Sl.No : 3.12				
15	Server Section B - Sl.No : 3.13				

16	Mifare classic 4k , 7byte smartcards Section B - Sl.No : 3.15				
17	Wireless access points Section B - Sl.No : 3.16				
18	Accessories, Cables and conduits Section B - Sl.No : 3.17				
19	List of Additional items required, if any, for realization of contract. (Specify with details as per Section C **Annexure-V – Sl.No 3**)				
20	System integration requirements Section B - Sl.No : 3.18				
21	Acceptance testing Section B - Sl.No : 3.19				
22	Training (Section B - Sl.No : 3.20				
23	Documentation Section B - Sl.No : 3.21				
24	Deliverables SectionB – Sl. No : 3.22				
25	Special conditions: Section B - Sl.No : 3.23				

Place: SIGNATURE

Date: NAME & DESIGNATION

SEAL OF ORGANISATION

2. COMMERCIAL COMPLIANCE STATEMENT

Sl No	Requirements	Compliance		Reasons/Statement for Non-Compliance
		Yes	No	
1	Scope of work (As per Sl.no 3 of Section-A)			
2	Eligibility Criteria All the document proof should be submitted and the document compliance sheet to be filled (As per Sl.no 4 of Section-A)			
3	Instruction to vendors including Site visit, Prebid meeting and details on part I and II of bid and the criteria for bid evaluation (As per Sl.no 5 of Section-A)			
4	General Financial provisions (As per Sl.no. 6 of Section-A)			
5	Terms Of Payments (As per Sl.no. 7 of Section-A)			
6	Time frame for completion (As per Sl.no 8 of Section-A)			
7	Declaration (As per Sl.no 9 of Section-A)			
8	Availability of Spares (As per Sl.no 10 of Section-A)			
9	Comprehensive Warranty (As per Sl.no 11.0 of Section-A)			
10	Comprehensive Annual Maintenance Contract for next five years after three years warranty period. (As per Sl.no 12.0 of Section -A)			

11	ResidentTechnical supportterms and scope (As per Sl.no 13 of Section -A)			
12	Force Majeure (As per Sl.no 14.0 of Section -A)			
13	Liquidated Damages (As per Sl.no 15.0 of Section -A)			
14	Arbitration (As per Sl.no 16.0 of Section -A)			
15	Disclosure and use of information by the Vendor (As per Sl.no 17.0 of Section -A)			
16	Indemnity clause (As per Sl.no 18.0 of Section -A)			
17	Legal clause (As per Sl.no 19.0 of Section -A)			
18	Non-Disclosure Agreement (As per Sl.no 20 of Section -A)			
19	Termination of contract (As per Sl.no 21 of Section -A)			
20	Service Level Agreement (As per Sl.no 22 of Section -A)			

Place: SIGNATURE

Date: NAME & DESIGNATION

SEAL OF ORGANISATION

3. COMPLIANCE STATEMENT FOR DOCUMENTS SUBMITTED

Sl. No.	Particulars	Uploaded (Yes/No)	Document Name
1.	Copy of Registration certificate		
2.	Copy PAN card.		
3	Solvency Certificate from a scheduled/ commercial bank		
4.	GST Certificate.		
5.	E.P.F Registration letter/Certificate		
6.	E.S.I Registration letter/certificate.		
7.	Audited Financial Statements for last three financial years out of 7 years ending 31/03/2023 showing annual turnover		
	a. Profit & loss Account		
	b. Balance Sheet		
	c. Copy of IT return filed by the company		
8.	Documentary proof of Work experience		
	Experience proof as detailed in Section A , Sl.No 4,c(8). The Annexure I, Sl.No 3 in Section C indicating the name of client, contact person, contract value, nature of work, work completion certificate, month & year of		

	commencement & completion etc should be duly filled and submitted		
	a. completion certificate		
	b. Performance certificate		
	c. Annual maintenance contract details, contact details of the client.		
9	ISO Certificate (If ISO certified company)		
10	Section C Annexure 1 (Sl.No 1&2))		
	a. Duly filled and signed Vendors Profile		
	b. Duly filled and signed Declaration		
11	Annexure II		
	Technical Compliance Statement		
	Commercial Compliance statement		
	Documents compliance statement		
12	Annexure III- A certificate from Original Equipment Manufacturers (OEM) certifying that the Vendor is an authorized dealer/agent		
13	Annexure IV- All the following documents are to be submitted 1. OEM Back-To-Back Support Guarantee 2. Unconditional Acceptance Of The Terms & Conditions Of The RFP 3. Escalation Matrix 4. Certification For Local Content		

	5. Self-Declaration Of Non-Blacklisting 6. Undertaking Of Information Security Compliance 7. Undertaking Of Authenticity Of Solution (Hardware And Software) 8. Software/Solutions Integrity Certificate 9. Declaration On Technical Service Personnel 10. Declaration regarding End-Of-Support products 11. Declaration under rule 144(XI) in general financial rules (GFR), 2017		
14	Annexure V – Unpriced version of BOM with Make and model/part numbers		
15	Proof of all certifications of supplied products		
16	Proof of adherence to standards mentioned against supplied products		
17	Documentation (Product Brochures, datasheets, manuals, etc.)		

Place: SIGNATURE

Date: NAME & DESIGNATION

SEAL OF ORGANISATION

Annexure III

UNDERTAKING BY ORIGINAL EQUIPMENT MANUFACTURER (OEM)

(To be submitted in Original on Letterhead)

(This certificate should be submitted along with the technical bid, signed &sealed by respective Original Equipment Manufacturer/s. The individual signing the OEM undertaking shall have the power of attorney to sign the undertaking and has to be signed with direct contact details)

We, M/s ....., the manufacturer of .....…… (Item Name, Make, Model No.), here by authorize M/s …….. (Vendor Name) to participate in the tender ……..

(Tender No.) for …… (Tender Name). We guarantee that the equipments supplied are manufactured by us and are brand new and these items have not been used anywhere else before.

We hereby confirm the following points.

1. All components supplied by us as part of this tender are compatible with the offered solution.
2. All components supplied by us as part of this tender will be available for minimum of EIGHTyears from date of acceptance by LPSC.
3. Components supplied will not be declared as End-Of- Support for 8 years (3 year warranty and 5 years CAMC) from the date of acceptance by LPSC.
4. Components supplied will not be declared as End-Of-Life until next 3 years (warranty period) fromthe date of acceptance by LPSC.

Authorized Signatory (OEM)

Name

Designation

Seal/Stamp of the OEM

Place:

Date:

Annexure IV

1. BACK-TO-BACK SUPPORT GUARANTEE BY OEM

(To be submitted in Original on Letterhead)

Agreement with product vendors on Back to Back support

This is to certify that we M/s....., the manufacturer of .....……. (Item Name, Make, Model No.) has agreed to provide back to back support to M/s …… (Vendor Name & Address) for implementation, operations and maintenance phases of the items supplied for the tender …… (Tender No.) for …… (Tender Name).

Also, we hereby authorize M/s …….. (name of Vendor) to provide support and service for the supplied equipment during warranty period and operation & maintenance contract period after warranty as per the terms and conditions specified in the tender document,…… (Tender No.). In case M/s …….. (name of Vendor) is not able to perform their duties including service support for our supplied equipment during installation, warranty, operation and maintenance period, we are ready to extend our support to LPSC for our supplied equipment, either directly or through our mutually agreed authorized service partner, under the same terms and conditions of this tender document, without any additional expenditure to LPSC. We further guarantee the availability of spares and upgrades to LPSC for a minimum period of 8 years from the date of commissioning of the system in conformance to the tender terms and conditions.

We undertake, that adequate specialized expertise are available to ensure that the support services are responsive and we assume total responsibility for the fault free operation of the solution proposed and maintenance during the support period.

We undertake that during support period we will maintain an Uptime of 99.9 % on monthly basis for the entire/core solution proposed.

Yours faithfully,

Authorized Signatory
Name
Designation
Seal/Stamp of the Vendor

Place:

Date:

2. UNCONDITIONAL ACCEPTANCE OF THE TERMS & CONDITIONS OF THE RFP

(To be submitted on the Vendor Company**'**s Letter Head**)**

Ref:

Sir/Madam,

This is to confirm that we unconditionally accept all the terms and conditions as mentioned in the said RFP including all addendum/amendment/ corrigendum floated for LPSC pertaining to this RFP Ref.

Authorized Signatory

Name

Designation

Seal/Stamp of the Vendor

Place:

Date:

3. ESCALATION MATRIX

(To be kept in the Part I – Techno commercial Bid)

Ref:

The escalation matrix up to top level of company is tabulated below in hierarchy-

Sr. No.	Particulars	Level-1 Escalation	Level-2 Escalation	Level-3 Escalation
1		Name: Phone No: Cell No: Email :	Name: Phone No: Cell No: Email :	Name: Phone No: Cell No: Email :

Note- Kindly mention escalation matrix of all verticals (support, sales and delivery) of the company. There should be a single point of contact of senior level for verticals.

Yours faithfully,

Authorized Signatory
Name
Designation

Place:
Date:

4. CERTIFICATION FOR LOCAL CONTENT

Ref:

Vendor Name:

This is to certify that proposed <products and services as per scope of work> is having the local content of ---------% as defined in the above mentioned RFP and amendment thereto.

This certificate is submitted in reference to the Government issued Public Procurement (Preference to Make in India) [PPP-MII] Order 2017 vide the Department for Promotion of Industry and Internal Trade (DPIIT) Order No.P-45021/2/2017-B.E.-II dated 15.06.2017 and subsequent revisions vide Order No. 45021/2/2017-PP(BE-II) dated 28.05.2018, 29.05.2019, 04.06.2020 and 16.09.2020

Signature of Statutory Auditor/Cost Auditor

Registration Number:

Seal

Countersigned by the Vendor: Vendor-

Authorized Signatory

Name

Designation

Seal/Stamp of the Vendor

Place:

Date:

5. SELF-DECLARATION OF NON-BLACKLISTING

(This letter should be on the letterhead of Vendor duly signed by an authorized signatory).

Ref:

We (Company Name) hereby confirm that our company (Firm/ Company/LLP) or its group company / subsidiary company / holding company /affiliate /associate company / partner was never been black listed and/ or banned and /or barred and / or disqualified and or prohibited by Govt/Public sector organizations /or NCLT and/ or NCLAT and / or any court of law and / or quasi-judicial authority / and or any other statutory and/ or regulatory authority, in undertaking any work directly or indirectly which is required to perform as stated in this RFP and/ or issuance of any certificate of audit directly or indirectly with respect to the work sated herein the RFP.

Yours faithfully,

Authorized Signatory
Name
Designation
Seal/Stamp of the Vendor

Place:
Date:

6. UNDERTAKING OF INFORMATION SECURITY COMPLIANCE

(This letter should be on the letterhead of both Vendor and OEM duly signed by an authorized signatory)

Ref:

We hereby undertake that the proposed solution / software to be supplied will be free of malware, free of any obvious bugs and free of any covert channels in the code (of the version of the application being delivered as well as any subsequent versions/modifications done) during entire contract period. If any case reported, the same to be resolved/fixed by the Vendor without any additional cost to LPSC on immediate basis.

Yours faithfully,

Authorized Signatory
Name
Designation
Seal/Stamp of the Vendor

Place:
Date:

7. UNDERTAKING OF AUTHENTICITY OF SOLUTION (HARDWARE AND SOFTWARE)

(This letter should be on the letterhead of both Vendor & OEM duly signed by an authorized signatory).

Ref:

With reference to the subject matter, we hereby undertake that all the components/parts/assembly/software used in the Solution, Hardware, Software for Proposed Solutions shall be original and new components / products only, from respective OEMs of the products and that no refurbished / duplicate / second hand components / Parts / Assembly / Software are being used or shall be used.

We also undertake that in respect of licensed operating system/other required software, if any, the same shall be supplied along with the authorized license certificate (e.g. Product Keys, if any on Certification of Authenticity) and also that it shall be sourced from the authorized source (e.g. Authorized Microsoft Channel in case of Microsoft Operating System).

We hereby undertake to produce the certificate from our OEM supplier in support of above undertaking at the time of delivery / installation. It will be our responsibility to produce such letters from our OEM Supplier's at the time of delivery or within a reasonable time.

In case of default and we are unable to comply with above at the time of delivery or during installation, we agree to take back entire setup (i.e. Servers, Software and hardware) for the proposed solution without demur, if already supplied and return the money if any paid to us by you in this regard.

We (system OEM name) also take full responsibility of both Parts & Service SLA as per the content even if there is any defect by our authorized Service Centre / Reseller / SI etc.

Authorized Signatory
Name
Designation
Seal/Stamp of the Vendor

Place:
Date:

8. SOFTWARE/SOLUTIONS INTEGRITY CERTIFICATE

(To be issued by OEM on OEM Company's Letter Head)

Ref:

INTEGRITY STATEMENT

This is to certify that our product ……, Version: …… developed by and a copyright of …….. follows

Standard secure coding practices and has been tested and certified for the following checks:

1. That the application has undergone the required level of unit, system, stress and volume tests and is free of any obvious bugs.
2. That the software is tested with anti-virus/anti-malware software and is free of any known virus/malwares at the time of sale.
3. That the application is free of any covert channels in the code being provided and subsequent modifications to be done on them.

We have evaluated the cryptographic implementation and have ensured that only cryptographic modules based on authoritative standards and reputable protocols are used.

We confirm that Source code testing is carried out on application source code (to identify and detect security threats and weaknesses in its systems) and there are no OPEN vulnerabilities.

We confirm that Application Security testing is carried out for application (to identify and detect security threats and weaknesses in its systems) and there are no OPEN vulnerabilities.

We confirm that we are conducting secure coding training programs for our software developers/testers on periodical basis.

We also confirm that the above practices will be met by us for all the changes that we make in the application/ module on a regular basis.

Authorized Signatory
Name
Designation
Seal/Stamp of the Vendor

Place:

Date:

9. DECLARATION ON TECHNICAL SERVICE PERSONNEL

(This letter should be on the letterhead of Vendor duly signed by an authorized signatory).

To:

Ref :

Sir,

We _____(name of the company) hereby confirm that all the manpower (both on-site and offsite) deployed/to be deployed on LPSC's project for ……. (Name of the RFP) have undergone our internal Employee background verification process and requisite checks have been performed prior to employment of said employees as per our policy.

We undertake and agree to save defend and keep harmless and indemnified LPSC against all loss, cost, damages, claim penalties expenses, legal liability because of non-compliance of KYE (Know your employee) and of misconduct of the employee deployed by us to LPSC.

We further agree to submit the required supporting documents (Process of screening, Background verification report, police verification report (issued in last six months), character certificate regarding fit and satisfactory conduct, ID card copy, Educational document, etc) to LPSC before deploying officials in LPSC premises for …….. (Name of the RFP).

Yours faithfully,

Authorized Signatory

Name

Designation

Seal/Stamp of the Vendor

Place:

Date

10.DECLARATION REGARDING END-OF-SUPPORT PRODUCTS

(This letter should be on the letterhead of Vendor duly signed by an authorized signatory).

Ref:

We hereby confirm the following points.

1. All components supplied by us as part of this tender are compatible with the offered solution.
2. In any case, if the OEM declares products supplied by us as End-Of-Support during 8 years (warranty and CAMC period), then it will be our responsibility to replace it with a product having equivalent or better configuration at no extra cost to LPSC and integrate it with EACMS.

Authorized Signatory
Name
Designation
Seal/Stamp of the Vendor

Place:
Date:

Annexure-V

UNPRICED VERSION OF BILL OF MATERIALS

1. SUPPLY AND INSTALLATION OF ALL HARDWARE AND SOFTWARE COMPONENTS OF EACMS

Note: Prices are not to be furnished in this Annexure

Sl. No.	Description	Make and model/Part Number	GST/Applicable tax (%)	Service Tax(%)	Quantity	Remarks
1.	Smart Card +Finger+Face reader cum controller to use with Turnstile for Entry/Exit Gates in LPSC				50	
2.	Installation charges of Sl.No 1				50	
3.	Face and Mifare-Smart Card based controller to use with Turnstile for Entry/Exit Gates in LPSC				25	
4.	Installation charges of Sl.No 3				25	
5.	Face and Mifare-Smart Card based Door Controller cum reader for in various Labs in LPSC				52	
6.	Installation charges of Sl.No.5				52	
7.	Face and Mifare-Smart Card based daughter reader for in various Labs in LPSC				52	
8.	Installation charges of Sl.No 7				52	
9	Half height motorized Tripod turnstiles				21	
10	Installation charges of Sl.No 9				21	
11	Handheld Readers – Face with smart card				20	
12	Installation charges of Sl.No 11				20	

13	Handheld Readers – Finger with smart card				5	
14	Installation charges of Sl.No 13				5	
15	Photo flashing - LED Panel Display and other accessories				21	
16	Installation charges of Sl.No 15				21	
17	EM locks for single/double door with Exit Switch				52	
18	Installation charges of Sl.No 17				52	
19	Exit switches				52	
20	Installation charges of Sl.No 19				52	
21	Integrated web based Software and license				4 Licenses	4 Licenses(two each at each location for primary and backup server)
22	Installation charges of Sl.No 21				4	
23	Personalization Station – Biometric enrolment (Face and finger) and smart card personalization				8	
24	Signature pad with pen				8	
25	Mifare classic 4k , 7byte smart cards				6500	
26	MIFARE DESFire EV2				100	
27	Servers				4	
28	Installation charges of Sl.No 27				4	
29	Wireless access point				19	
30	Operational Charges which includes cost for deploying two resident technical support (one at each location –Valiamala and Bangalore) during Warranty for three years				1 lot	

31	CAT6A UTP cables or as recommended by OEM				2000 metres	
32	Power cables – 3 Core 1.5sqmm or as recommended by OEM				500 metres	
33	Other interconnecting cables as recommended by OEM				As required	
34	Accessories like connectors, relays etc				As required	
35	PVC Conduit for cable laying				500 metres	
36	PVC casing and caping				500 metres	
37	SS Pole for Readers				42	
38	Un-installation of existing items as given in **Section-C, Annexure VII**				Lot	
39	Training				Lot	
40	Packing and forwarding charges				lot	
41	Transportation charges				Lot	
42	Supply and installation of any other additional items required for EACMS implementation. (Split up to be given in Section C, Annexure-V , Sl. No 3)				Lot	

Authorized Signatory

Name

Designation

Seal/Stamp of the Vendor

Place:

Date

2. POST WARRANTY COMPREHENSIVE AMC FOR 5 YEARS

Sl. No.	Description CAMC charges along with two resident technical support (one at each location -Valiamala and Bangalore)	GST/Applicable tax (%)	Service Tax(%)	Quantity	Vendor's Confirmation - Quoted (Yes/No)
1	4th year			Lot , Per year	
2	5th year			Lot , Per year	
3	6th year			Lot , Per year	
4	7th year			Lot , Per year	
5	8th year			Lot , Per year	

Place: SIGNATURE

Date: NAME & DESIGNATION

SEAL OF ORGANISATION

3. ADDITIONAL ITEMS

Note: Additional items, if any required which is not mentioned in Unpriced Bill of material (Section C, Annexure V, Sl.No1) but essentialfor realization of this turn-key work shall be listed with details , The supply and installation charges to be quoted separately

Sl. No.	Item Description	Make and model/Part Number	GST/Applicable tax (%)	Service Tax(%)	Quantity	Justification/Purpose for the item
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						

Place: SIGNATURE

Date: NAME & DESIGNATION

SEAL OF ORGANISATION

Annexure-VI

PRICE BID

BILL OF MATERIAL AND PRICE SCHEDULE

1. SUPPLY AND INSTALLATION OF EACMS COMPONENTS

Sl. No.	Description	Make and model/Part Number	Price per unit (Rs)	GST/Applicable tax	Service Tax	Total Amount Per unit(Rs)	Quantity	Total Cost
1.	Smart Card +Finger+Face reader cum controller to use with Turnstile for Entry/Exit Gates in LPSC						50	
2.	Installation charges of Sl.No 1						50	
3.	Face and Mifare-Smart Card based controller to use with Turnstile for Entry/Exit Gates in LPSC						25	
4.	Installation charges of Sl.No 3						25	
5.	Face and Mifare-Smart Card based Door Controller cum reader for in various Labs in LPSC						52	

6.	Installation charges of Sl.No.5						52	
7.	Face and Mifare-Smart Card based daughter reader for in various Labs in LPSC						52	
8.	Installation charges of Sl.No 7						52	
9.	Personalization Station – Biometric enrolment (Face and finger) and smart card personalization						8	
10.	Half height motorized Tripod turnstiles						21	
11.	Installation charges of Sl.No 10						21	
12.	Handheld Readers – Face with smart card						20	
13.	Installation charges of Sl.No 12						20	
14.	Handheld Readers – Finger with smart card						5	
15.	Installation charges of Sl.No 14						5	
16.	Photo flashing - LED Panel Display and other accessories						21	

17.	Installation charges of Sl.No 16						21	
18.	EM locks for single/double door with Exit Switch						52	
19.	Installation charges of Sl.No 18						52	
20.	Exit switches						52	
21.	Installation charges of Sl.No 20						52	
22.	Integrated web based Software and licenses - 4 Licenses(two each at each location for primary and backup server)						4 Licenses	
23.	Installation charges of Sl.No 22						4	
24.	Signature pad with pen						8	
25.	Mifare classic 4k , 7byte smart cards						6500	
26.	MIFARE DESFire EV2						100	
27.	Servers						4	
28.	Installation charges of Sl.No 27						4	

29.	Wireless access point						19	
30	Operational Charges which includes cost for deploying two resident technical support (one at each location - Valiamala and Bangalore) during Warranty for three years						1 lot1 lot	
31	CAT6A UTP cables or as recommended by OEM						2000 metres	
32	Power cables – 3 Core 1.5sqmm or as recommended by OEM						As required	
33	Other interconnecting cables as recommended by OEM						As required	
34	Accessories like connectors, relays etc						As required	
35	PVC Conduit for cable laying						500 metres	
36	PVC casing and caping						2000 metres	
37	SS Pole for Readers						42	
38	Un-installation of existing items as given in Section-C, Annexure VII						Lot	
39	Training						Lot	

40	Packing and forwarding charges						lot	
41	Transportation charges						Lot	
42	Supply and installation of any other additional items required for EACMS implementation. Total cost of items under Section C, Annexure-VI, Sl. No 3 to be given (Split up to be given in Section C, Annexure-VI, Sl. No 3)						Lot	

Note: The EACMS total cost to be quoted in the tender template is the cost of all items, except Sl.No. 30(Operational Support Charges during Warranty for three years).Operational Support Charges during Warranty for three years must be quoted separately in the tender template.

Place: SIGNATURE

Date: NAME & DESIGNATION

SEAL OF ORGANISATION

2. POST WARRANTY COMPREHENSIVE AMC RATES PER ANNUM

Sl. NO.	Description	CAMC charges along with two resident technical support (one at each location - Valiamala and Bangalore)	GST/Applicable tax	Service tax	Total Comprehensive AMC charges
1.	4th year				
2.	5th year				
3.	6th year				
4.	7th year				
5.	8th year				
	Total				

Note:

1. **The prices quoted are inclusive of all taxes, duties and levies.**
2. **Device wise split up AMC charges should be mandatorily provided in the template in Annexure VI, Sl. No 4**

Place: SIGNATURE

Date: NAME & DESIGNATION

SEAL OF ORGANISATION

3. ADDITIONAL ITEMS

Note: Additional items, if any required which is not mentioned in Unpriced Bill of material (Section C, Annexure V, Sl.No1) but essential for realization of this turn-key work shall be listed with details .The supply and installation charges to be quoted separately

Sl. No.	Description	Make and model/Part Number	Price per unit (Rs)	GST/Applicable tax	Service Tax	Total Amount Per unit(Rs)	Quantity	Total Cost
1.								
2.								
3.								
4.								
5.								
6.								
7.								
8.								
9.								
10								

Place: SIGNATURE

Date: NAME & DESIGNATION

SEAL OF ORGANISATION

4. DEVICE WISE AMC RATES

Sl. No.	Description	AMC Rates per year after warranty period					Tax	Total Amount (Total of five years amount + Tax)
		I	II	III	IV	V		
1.	Smart Card +Finger+Face reader cum controller to use with Turnstile for Entry/Exit Gates in LPSC							
2.	Face and Mifare-Smart Card based controller to use with Turnstile for Entry/Exit Gates in LPSC							
3.	Face and Mifare-Smart Card based Door Controller cum reader for in various Labs in LPSC							
4.	Face and Mifare-Smart Card based daughter reader for in various Labs in LPSC							
5.	Half height motorized Tripod turnstiles							
6.	Handheld Readers – Face with smart card							
7.	Handheld Readers – Finger with smart card							
8.	Photo flashing - LED Panel Display and other accessories							
9.	EM locks for single/double door with Exit Switch							
10.	EACMS Integrated web based Software							
11.	Personalization Station with signature pads –							

	Biometric enrolment (Face and finger) and smart card personalization							
12.	Servers							
13.	Wireless Access points							
14.	Any other Additional items quoted by vendor in Section C, Annexure VI, Sl.No 3							
15.	Operational Charges which includes cost for deploying two resident technical support (one at each location - Valiamala and Bangalore)							

Place: SIGNATURE

Date: NAME & DESIGNATION

SEAL OF ORGANISATION

Annexure VII

1. LIST OF EXISTING ITEMS

The following are the details of existing BACS components available in LPSC, Valiamala and Bangalore that need to be dismantled.

LPSCV- LPSC , Valiamala , Thiruvananthapuram

LPSCB- LPSC , Bangalore

Items	Qty LPSCV +LPSCB	Year of installation
Tripod turnstiles	13 +5	2015
Photo displays at main gate	13+5	2015
Biometric readers integrated with Turnstiles	26+10	2015 and later
Biometric readers integrated with doors	10+20	2015 and later
EM locks integrated with doors	10+10	2015

Annexure VIII

1. DECLARATION UNDER RULE 144(XI) IN GENERAL FINANCIAL RULES (GFR), 2017

We, the Vendor / bidder are desirous of participating in the Tender/Enquiry process in response to your RFPs and in this connection we hereby declare, confirm and agree as under:

A. We, the Vendor / Bidder have read and understood the contents of the Office Memorandum & the order (Public Procurement No. 1) both bearing no. F. No. 6/18/2019/PPD dated 23rd July 2020 issued by Department of Expenditure, Ministry of Finance, Government of India on insertion of Rule 144(xi) in the General Financial Rules (GFRs) 2017 and the amendments & clarifications thereof, regarding restrictions on availing / procurement of goods and services , of any bidder from a country which shares a land border with India.

B. We, the vendor / Bidder understands that as per the Rule 144(xi) of General Financial Rule, 2017, any vendor / bidder from a country which shares a land border with India will be eligible to bid in any procurement whether of goods, services (including consultancy services and non-consultancy services) or works (including turnkey projects) only if the vendor / bidder is registered with the competent authority ie., Department for Promotion of Industry and Internal Trade (DPIIT). Hence, Vendors or Agents of a Vendor (Indian or others) from a country sharing boarder with India shall submit copy of valid registration made with Department for Promotion of Industry and Internal Trade (DPIIT), Government of India mandatorily, without which any offer made by such a vendor / bidder will be treated as invalid.

C. In terms of the above and after having gone through the said amendments including in particular the words defined therein (which shall have the same meaning for the purpose of this Declaration cum Undertaking), I/we the vendor / Bidder hereby declare and confirm that:

(i) ***** We, the Vendor / Bidder are not from such a country which shares a land border with India, in terms of the said amendments to GFR, 2017.

OR

(ii) ***** We, the Vendor / bidder are from such a country and has/have been registered with the competent authority i.e. the Registration Committee constituted by the Department of Promotion of Industry and Internal Trade, as stated under Annexure I to the said Office memorandum / Order and we submit proof of registration herewith.

OR

(iii) We, the Bidder are from such a country which shares a land border with India, however our country has been extended lines of credit by Government of India or/and Government of India is engaged in development projects in our Country.
(* Delete whichever is not applicable)

D. We, the Vendor / Bidder agree and undertake that if the Purchase order is awarded to us, we will not sub-contract or outsource the order, and / or any part thereof unless such subcontract / outsourcing is permitted by LPSC in writing, in which case the aforesaid OM and clarifications shall be equally applicable to such sub-contractor/vendor. Thus, subject to the aforesaid OM &clarifications thereof, we shall not sub-contract or outsource the order to a vendor from such countries, unless such vendor is registered with the Competent Authority and proof of same is obtained.

E. We the vendor/ bidder, also certify that this vendor/bidder/products/any component of the products offered by us fulfils all requirements in this regard and is eligible to be considered. We also agree and accept that if our declaration and confirmation is found to be false at any point of time including after awarding the Purchase Order, LPSC shall be within its right to forthwith terminate the Enquiry /Purchase Order without notice to us and initiate such action including legal action against us.

F. This declaration cum undertaking is executed by us through our Authorized signatory/ies after having read and understood the Office Memorandum and Order (Public Procurement No. 1) both bearing F. No. 6/18/2019/PPD of 23rd July 2020 of Ministry of Finance, Department of Expenditure, Public Procurement Division, Government of India and clarification issued in pursuance to the aforesaid OM from Government of India from time to time.

Authorized Signatory
Name
Designation
Seal/Stamp of the Vendor

Place:

Date