F.No. 22012/80/2018-SSO(S)
Government of India
Ministry of Home Affairs
(Secretariat Security Organisation)
.....

NDCC-II, Jai Singh Road,
New Delhi, the 28th Dec., 2018

DRAFT TENDER NOTICE

Sub: Draft Tender Notice for Installation of Access Control System in the buildings under Ministry of Home Affairs – reg.

Ministry of Home Affairs wants to install Access Control System in the buildings under Ministry of Home Affairs, New Delhi. Draft tender notice is attached.

2. The interested Central Public Sector Undertakings (CPSU) may submit the comments/views to the undersigned within 15 days.

(S.Samanta)
Under Secretary to Govt. of India
23438052

F.No.
Government of India
Ministry of Home Affairs
(Secretariat Security Organisation)
.....

NDCC-II,Jai Singh Road,
New Delhi, the 20th Dec., 2018

TENDER NOTICE

Sub: Limited Tender Notice for inviting Technical and Financial Proposal (two Bid system) for Installation of Access Control System in the buildings under Ministry of Home Affairs – reg.

Ministry of Home Affairs invites Limited Tender to install Access Control System in the buildings under Ministry of Home Affairs, North Block, New Delhi. The specification of various components of the system are as per list enclosed (Annexure-I).

2. The crucial dates for the tender are as under:

Notice issue Date	
Bid Submission Start Date & Time	
Bid Submission End Date & time	
Technical Bid Opening Date & Time	

3. The interested Central Public Sector Undertakings (CPSU) may submit the tenders online only through e-Procurement Portal http://eprocure.gov.in/eprocure/app in the prescribed proforma. Tender submitted by any other mode or incomplete tenders will not be accepted. No tender documents will be accepted after the expiry of stipulated date and time for the purpose under any time circumstances whatsoever. The bids will be submitted in two packet bids (Technical and Financial bid) as specified in tender details by _____(till 03.00 PM).

4. General Terms and conditions of the tender are given in annexure – II and details of financial bid Annexure-II Technical Bid Annexure-IV.

5. The bids will be opened in the presence of "Bid Opening Committee – members" of this Ministry on _____at 03.00 (PM). Selection of the L-I CPSU of Technically qualified bidder will be based on the recommendation of the "Technical Evaluation Committee" of this Ministry. The Financial bids will be opened only for technically qualified CPSUs, the date and time will be communicated to them, accordingly.

Enclosed : As above.

(S.Samanta)
Under Secretary to Govt. of India

ANNEXURE-I

Technical specification

TECHNICAL SPECIFICATIONS OF VARIOUS COMPONENTS OF THE ACCESS CONTROL SYSTEM TO BE INSTALLED BUILDINGS UNDER MHA SECURITY COVER

INDEX

APPENDIX-A

1(a) Smart Cards – Contactless

S.N	Parameter	Minimum Requirements
1	Card Type	Microprocessor based single chip contact less card with 64Kbytes of available EEPROM
2	Compliance to Standard	ISO 14443-1,2,3 A or B and SCOSTA – CL (latest) platform as specified and certified by NIC
3	Power	3 Volt or 5 Volt
4	Protocol	T = CL (Contact less)
5	Transmission Rate	100k Baud data transmission rate
6	Distance Range	10 cm operating distance range in case of Contact Less data transfer as per ISO 14443 standard for Read/Write.
7	Retention Period	Minimum 5 years
8	Write Cycle	3,00,000
9	Chip Temperature	-25°C to +80°C
10	Operating Temperature	-25°C to +80°C
11	Construction	Plastic construction PVC with PVC overlay
12	Surface	Glossy
13	Visual Design	To be approved by the MHA
14	General	Sample card with SAM shall be provided to the shortlisted bidder only for application development

1(b) Smart Card Biometric Reader cum Controller as one single Terminal

a. The Wall Mounted Smart Card Terminal is a computing device which can host the software and data. It executes the software to perform following,
   i. Automatically senses and reads a contactless smart card (ISO 14443 1/2/3/4 A and B compliant) when brought in its vicinity (within 10 cm).
   ii. Performs external card authentication (Active Authentication) using the SAM card securely placed within.
   iii. Performs Hotlist Validation from the synchronized list on the terminal
   iv. Performs at single factor as well as two factor based authentication: card and biometric or card and pin depending upon the areas of access.

v. Reads custom format data and fingerprint templates stored in card chip.
vi. Graphically prompts in the color display of the terminal for one randomly selected finger out of ten to be placed over the fingerprint scanner mounted on the terminal.
vii. Reads the fingerprint, and performs 1:1 matching.
viii. Reads and verifies the Zone, Gate, Timing and validity permissions from the user card.
ix. Reads and performs local and global anti pass back on the user card.
x. If all above verifications are performed successfully, sends signal to the EM Lock/Turnstile/Flap Gate etc. to open for one entry only.
xi. Writes back entry login the user card.
xii. Writes entry log into the reader cum controller memory.
xiii. Transmits the log to the local server periodically in batches
xiv. Synchronizes Hotlist periodically from the local server
xv. No storage of fingerprint template is envisaged
xvi. Photograph of the card holder is stored on local server not on the card.

b. Security Specifications
i. Self-Destruction of Programs and SAM on physical opening of box.
ii. No open port for application loading once energized.
iii. Must support Crypto Algorithms like RSA,3DES etc.

#	**Parameters**	**Minimum Requirements**
Smart Reader cum Controller		
1	Type	Capable of reading contactless smart card (ISO 14443 1/2/3/4 A and B). 64 Kbytes storage on smart card
2	Read Range	Up to 10 Cm (Maximum)
3	Memory Sufficient for application software to store one day data	Hot List and Blacklist data ● Minimum 10000 and expandable up to 25000 ● Entry / Exit data ● Minimum 25,000 and expandable up to 50,000 Chip Serial No. (CSN) shall be used for hotlisting & blacklisting. Entry/Exit data indicate Date & Time of Entry/Exit (Time stamp) corresponding to the card holder accessing the gate. Communication between Reader & Server shall be through SSL.
4	RTC	Built in most accurate RTC (Real Time Clock) with Lithium Cell Backup
5	PC Communication	Ethernet (TCP/IP)
6	Outputs	Relay output
7	Cryptography levels	3DES/AES (with 128 bit encryption)/RSA

8	SAM slots (ISO 7816)	1
9	Application Support	Multiple Application Platforms should be supported by the Controller so as to avoid 'Proprietary Scenarios' . Application should support standard OS platforms such as Windows or UNIX or Linux etc.
10	Certification	CE/ FCC/ RoHS or equivalent
11	Self-Destructive on Physical opening	If someone tries to open the device physically it should destruct the following and make it unusable 1. All Software from device (OS, Application, Device, Drivers etc.) 2. All keys from device (Hard burnt and in SAM) 3. All data from device memory (RAM, ROM, EEPROM, FLASH or any other memory device might using); Application loading/reloading only after external authentication with the derived key on SAM; No Application loading possible on field (Only in secure environment).
Biometric Reader		
11	Scanner Type	Optical
12	Sensing Area	As per ISO 19794-2
13	Resolution	Sensing Area as per ISO 19794-2
14	Setting Level	30 as defined in www.egovstandards.gov.in for fingerprints
15	Image Standards, Extractor & Minutia Template Standards	ISO 19794-2 for fingerprint minutiae template and ISO 19794-4 for fingerprint Image Template. The algorithm used for Minutiae extraction must be Minax compliant/ Listed
16	Response Time	Less than 2 seconds for single transaction
17	Preferred Operating Temperature	0 to 45 degree Centigrade
18	Preferred Storage Temperature	0 to 50 degree Centigrade
19	Preferred Humidity	10 to 90%
20	Reaction time	< 1.5 sec in 1:1 mode

21	Success/failure Indication	Indicating lights to display success /failure for access card or fingerprint authentication
22	Operating system Environment	Vendor needs to declare the compatible operating system
Keypad Reader		
24	Type	Alphanumeric keys or touch screen
Display		
25	Screen Size	4x3 Inches
26	Type	LCD or equivalent
Support		
27	Weather Protection	IP 54
28	Will the proposed product/service reach End-of-support during the currency of contract?	NO

1(c) AEC Encoder: Smart card reader contact

#	**Parameter**	**Minimum Requirements**
1	Type	USB (Universal Serial Bus) interface with PC
2	Interface	ISO 7816 compliance Interface
3	Support	PC/SE Driver and CT-API Driver Support
		Support for Windows XP/2000/2003/Vista with upgradeability with future versions

1(d) Network Controller

It must have the following features:

- One controller can control a maximum of 4 card readers or and should Control 4 door locks.
- Access decisions shall be made at each door controller, without reference to any other control or monitoring equipment.

- The system shall contain comprehensive networking capabilities, supporting multi-drop / daisy chain data communications links for other remote devices however Controllers should support direct TCP/IP Communication.
- The system shall use Industry Standard CAT -6 twisted-pair data communications wiring throughout to connect nearest LAN points each site.
- The system shall be capable of transmitting data between sites using Vendor Design data transmission protocols. The system shall only transmit encrypted data between
    - Card readers
    - Alarm monitoring equipment
    - Alarm response equipment
    - Central management system
- The Access Controller shall "concentrate" activity data and send it on to the central management system. The Access Controller shall also transmit control information, received from the central management system, out to door readers, when required.
- The Access Controller electronics shall be housed in a locked tamper protected metal cabinet.
- The Access Controller shall continue to operate in the event of mains failure for not less than 4 hours.
- Data shall incorporate parity checking and message acknowledgment checking, to ensure both integrity and consistency of all data transmitted.
- The Access Controller shall provide communications ports to enable the connection of a local operator terminal.
- Facility to accepting fire alarm inputs as a binary input is required.
- Facility to open all the doors in case of fire is required.
- Minimum No. of card handling capacity of each control panel shall be greater than 1 million expandable up to 10 million
- Minimum No. of transaction records at each controller shall be greater than 1 million expandable up to 5 million
- Communications
    - ❏ The Access Controller shall communicate with remote devices (card readers or real time monitoring software) using a fully encrypted data communications protocol. Unencrypted ASCII text or similar data transmissions are not acceptable.
    - ❏ All Access Controller to remote device communications shall be via a "poll and reply" and push data communications protocol. The communications links shall be "on-line" at all times.

- ❏ The data communications links between the Central Database and Controllers shall be monitored such that an alarm is raised at the central management system immediately should the communications link ever fail or be disconnected for any reason.
- ❏ The data communications links between the Central Database and controller shall be monitored such that an alarm is raised at the central management system if the data being transmitted is corrupted or tampered with in any way.

- The Access Controller shall be housed in a lockable steel cabinet.
- The Controller must have ARM microprocessor system shall be purpose designed for security applications. It shall incorporate a full multitasking operating module.
- The Access Controller shall include both hardware and software watchdogs to guarantee the integrity of the system. A relay output from the watchdog circuit shall be provided to enable the controller performance to be monitored by a remote monitoring station. Should the processor fail in any way, the watchdog relay shall trip, enabling the problem to be reported back to the monitoring station.
- The Access Controller shall incorporate a switch mode power supply (SMPS) which shall power the Access Controller electronics system, and charge the backup battery sub-system.
- The DC shall be capable of dynamically allocating its memory between database information and transaction history, which shall be stored if the controller has lost communication with the ACS™ server. Such transaction history shall be automatically uploaded to the ACS™ server once communication has been restored.
- It shall also be provided with at least 12 fully configurable input points, and at least 8 fully configurable auxiliary output control relays mounted on the main circuit board.
- Controller Communications Failure: Door controllers must continue to operate without performance degradation should the communications link to the central server fail. Should any card reader fail or stop operation for any reason, access through that door only shall be affected. Systems offering multiple door control from one controller using multiple reader heads cannot meet this requirement. During periods of communications failure, the card reader shall continue making full and complete access decisions. Systems, which degrade to simply checking the facility code or some other subset of the complete access criteria, are not satisfactory.
- All access attempts, valid or otherwise, and all alarm activations that occur while the card reader is offline, shall be buffered internally.
- Access Controller shall transfer the buffered activity events to the central management system when the communications link is reestablished.
- Card Entry under Duress: Access Controller shall contain a duress entry function. The duress entry function shall be activating by means of a special duress code entered immediately

after the PIN code is entered. The duress code shall immediately signal a duress alarm at the central management system.

- Door Alarms: A separate alarm message shall be transmitted to the central controller for each of the following door alarm conditions.
    - ❏ Door forced open
    - ❏ Door open too long
    - ❏ Door not locked
    - ❏ The alarm message shall be displayed in plain English text. Each alarm shall clearly identify the time, location and type of alarm.
- Access Criteria Alarms: A separate alarm message shall be transmitted to the central server for each of the following access criteria alarm conditions. The alarm message shall be displayed in plain English text. Each alarm shall clearly identify the time, location and type of alarm.
    - ❏ Card not authorized entry to this facility
    - ❏ Card not known at this reader
    - ❏ Card not authorized entry to this zone
    - ❏ Card not authorized entry at this time
    - ❏ PIN entry incorrect
    - ❏ Duress entry
    - ❏ Pass back entry attempted
    - ❏ Attempted use of non-access system card
- Controllers - Power Failure: The card readers shall continue to operate for at least Two (2) hours in the event of a main power supply failure. The system shall be capable of automatically detecting a power failure.
- The system shall be capable of automatically contacting and reporting a power failure (via SMS, dialer or similar) to appropriate technical repair staff, if require.
- The system shall be capable of interfacing with SMS Modules should be able to SMS predefined alarm messages to GSM/ CDMA Mobile Phones, if require.
- Controllers shall be fitted with automatic restart facilities to enable them to resume processing following a power and backup failure.
- Controllers shall be equipped with "watchdog" hardware and software to enable them to restart and resume normal processing, should their electronics ever be corrupted or go "haywire".
- An alarm shall be raised at the Central controller each time a card reader stops responding.

- Emergency Door Release Button : In the case when controller is hang up resulting Locking of all the doors, Break Glass type emergency door release button should be installed which when broken results in opening of the door or doors.
- Emergency door release Devices shall be installed in accordance with any applicable building or life safety codes requiring free egress during an emergency.

Door Access Controller

Specs #	Specification	Requirement
	CPU	ARM 9 32 Bit Cortex processor with an Android OS
	Memory	2 GB
	Card Holders	Min 250,000
	Transactions Recorded	Min 100000
	Reader Support (Dual/Four)	Biometric(Fingerprint /Retina Scan/Iris Scan/Face recognition), PIN , Proximity , Smart Card Reader (Mifare, i-class, Desfire)
	Data format	Weigandupto 178 - bit
	Maximum Controllers in Network	4096 per server
	LCD	16 X 2 Charracter, Mounted
	On board Buzzer	1
	On board Menu Buttons	For controller configuration, no external keypad require
	Input Ports	
	a. Dedicated input for fire alarm system integration	1
	b. Dedicated input for emergency closing of doors	1
	c. Dedicated input for tamper	1
	d. Spare programmable replay port	1
	e. Egress switch connections	2/4
	f. Door feedback inputs	2/4

	g. Reader Ports.	2/4
	Output Ports	
	a. Relay Port	2/4
	b. Programmable Auxiliary Port	2/4
	Group & Local Anti-pass Back (APB)	Available
	Time Zone	32 Time zones-expandable upto 128
	Holidays	32 -expandable upto 128
	Reader timing controls	
	a. Reader LED ON	in seconds
	b. Reader Beep ON	in seconds
	Door Control Timing	
	Door Open Timing	in seconds
	Door Open Feedback Delay	in seconds
	Readonly mode, Remote Monitoring of Transaction events	using Telnet
	Watchdog timer	Emergency release when internal controller circuitry fails
	Configuration of controller through web	
	Complete controller details, configuration details & statistics on single page	On Home Page
	Web Report of the every transaction	a. All transaction status report b. Day wise transaction report c. Transaction report for Day range
	Card Personalization	Visual interface for every card which is personalized or which has to personalized with details like, employee name, employee code, card enabling and expiry date, access rights

	Dynamic I/O Mapping	In case any inputs or output is not working, that port can be logically mapped to any other spare input or output port
	Programming of Auxiliary Output	third party interfacing of controller is possible with 16 types of event wise actions a. Latched status b. Pulse whose width in sec can be configured
	Secure mode	Should restrict web configuration of Controller upto 5 IP locations
	Auto-Reset of Controller	Available for a. No Communication b. On Day Change
	Password Level for Controller Configuration	3 main levels are available a. Installer level b. Admin Level c. User Level
	Power (Logic).	12V
	Power (Lock).	12V
	Operating environment range	-15°C to +65°C', 10% to 90% of Humidity
	Mounting	9 Screw Mount 2 Screw Hanging
	Weight	3000 gms.
	Dimensions	450mmx370mm x95mm (without Battery)
	Enclosure	Provision to mount 12 AH battery with battery charger
	Application	For Photo Display
	Approvals	CE, ISO 9001-2000 certified

1(e) Flap Barrier/Swing Gate-Normal Lane

#	Item/Specification	Minimum Requirement
1	Safety first	In the fire or power-off, the door can be free to promote and ensure unimpeded
2	Various Interfaces	I/O, RS232/485,CAN interfaces, which it is convenient to control signal input, and provides convenient centralized fire control interface
3	Two working modes	NC and NO, which is easy to deal with peak and normal use
4	Multiple control modes	There shall be unidirectional, bidirectional, free passage and authorization passage to meet fully the users needs, which consist of nine control modes
5	Precise positioning	Precise positioning by photoelectric sensors, the work cycle of door shall be regular and precise positioning to ensure correct position after long work
6	Various status information	It shall Provide operational status of each component, the direction of the status, the prevalent status, abnormal status, etc
7	Indicator control	the indicator shall be able to show three status of front and back indicator (allow through, no through, system maintenance).Also which shall show the passage direction and passage status (A to pass, B to pass, no through), According to reasonable indicator control, which is convenient for users to management
8	Biometric Mounting	Shall be able to integrate with Biometric. Biometric sensor & display shall be mounted on the surface of Flap Barrier. External Mounting / external poles is not permissible (BIOMETRIC READER & Flap/Swing Barrier SHOULD BE OF THE SAME BRAND)
9	QR Code	Shall be able to integrate with QR Code Reader
10	Size	1200x180x900mm to 1400 x290 x1000mm
11	Unlock time	0.1s to 0.2s
12	Pass Rate	35 to 40 person/min
13	Pass width	550 to 650 mm
14	Input	100V~240V
15	Motor voltage	24v
16	Environment	-25~ +70
17	Power consumption	35w
18	Certification	BIS / Make In India/ ISO/ CE

19	Integration	Flap Barrier can be integrated with any Access Control System
20	FEATURES & BENEFITS	Can be integrated with all ID Cards, IC Cards, Bar code or magnetic cards A passage indicator continuous LED shows to the pedestrian the right access points, and allows pedestrians to correct and smooth passage A combination of 6 pairs of infrared sensors and protection of pedestrians Double anti-clipping function (photocell and mechanical) Auto re-set function on, if no passing identified card reading time, the system will reset automatically the passengers are prohibited to pass until their second identified reading The barrier can be set to delay closing in 1-60s after a valid card reading A combination of 6 pairs of infrared sensors and protection of pedestrians Double anti-clipping function (photocell and mechanical) Auto re-set function on, if no passing identified card reading time, the system will reset automatically the passengers are prohibited to pass until their second identified reading The barrier can be set to delay closing in 1-60s after a valid card reading Operating Modes: o Single passage in the set direction o Bi-directional single passage o Free passage in the set direction o Always free or locked Materials: o Housing: Made in stainless steel AISI 304 o Barrier Swings: Plastic plate, toughened glass o Lid (Optional): stainless steel or artificial stone (black/brown) Mechanism: o Heavy duty design for 24 hours continuous application o Heavy duty pull type o Indoor and Outdoor application (Canopy Solicited) o High durability with industrial parts o Smooth, Noiseless and Shock less operation Communication o Dry contact relay with 12 volt or 24 volt plus o RS 485 or TCP-IP communication with computer Motor o Three Million times or above test for motor o Overheat and overload dual protection for motor

Note:- Stainless Steel Flap Barrier is a user-friendly access barrier developed for the efficient control of pedestrian movement according to the demanding Indian conditions. The barrier can be mounted with display, passage counter, card reader, token operation, command console, alarm system, which can all be interfaced with PC through RS232, RS485, TCP-IP (optional) line. The

Flap Barrier provides a fail-safe safety solution in case of emergency or power failure, providing egress with the flaps retracting into main panel.

1(f) Flap Barrier/ Swing Gate-Wide Lane

S.N.	Parameter	Minimum Requirements
1	Safety first	In the fire or power-off, the door can be free to promote and ensure unimpeded
2	Various Interfaces	I/O, RS232/485,CAN interfaces, which it is convenient to control signal input, and provides convenient centralized fire control interface
3	Two working modes	NC and NO, which is easy to deal with peak and normal use
4	Multiple control modes	There shall be unidirectional, bidirectional, free passage and authorization passage to meet fully the users needs, which consist of nine control modes
5	Precise positioning	Precise positioning by photoelectric sensors, the work cycle of door shall be regular and precise positioning to ensure correct position after long work
6	Various status information	It shall Provide operational status of each component, the direction of the status, the prevalent status, abnormal status, etc
7	Indicator control	the indicator shall be able to show three status of front and back indicator (allow through, no through, system maintenance).Also which shall show the passage direction and passage status (A to pass, B to pass, no through), According to reasonable indicator control, which is convenient for users to management
8	Biometric Mounting	Shall be able to integrate with Biometric. Biometric sensor & display shall be mounted on the surface of Flap Barrier. External Mounting / external poles is not permissible (BIOMETRIC READER & Flap/Swing Barrier SHOULD BE OF THE SAME BRAND)
9	QR Code	Shall be able to integrate with QR Code Reader
10	Size	1200x180x900mm to 1500 x190 x1100mm
11	Unlock time	0.2s
12	Pass Rate	35 to 45 person/min
13	Pass width	850 to 950 mm
14	Input	100V~240V
15	Motor voltage	24v
16	Environment	-25~ +70

17	Power consumption	35w
18	Certification	BIS / Make In India/ ISO/ CE
19	Integration	Flap Barrier can be integrated with any Access Control System
20	FEATURES & BENEFITS	Can be integrated with all ID Cards, IC Cards, Bar code or magnetic cards A passage indicator continuous LED shows to the pedestrian the right access points, and allows pedestrians to correct and smooth passage A combination of 6 pairs of infrared sensors and protection of pedestrians Double anti-clipping function (photocell and mechanical) Auto re-set function on, if no passing identified card reading time, the system will reset automatically the passengers are prohibited to pass until their second identified reading The barrier can be set to delay closing in 1-60s after a valid card reading A combination of 6 pairs of infrared sensors and protection of pedestrians Double anti-clipping function (photocell and mechanical) Auto re-set function on, if no passing identified card reading time, the system will reset automatically the passengers are prohibited to pass until their second identified reading The barrier can be set to delay closing in 1-60s after a valid card reading Operating Modes: o Single passage in the set direction o Bi-directional single passage o Free passage in the set direction o Always free or locked Materials: o Housing: Made in stainless steel AISI 304 o Barrier Swings: Plastic plate, toughened glass o Lid (Optional): stainless steel or artificial stone (black/brown) Mechanism: o Heavy duty design for 24 hours continuous application o Heavy duty pull type o Indoor and Outdoor application (Canopy Solicited) o High durability with industrial parts o Smooth, Noiseless and Shockless operation Communication o Dry contact relay with 12 volt or 24 volt plus o RS 485 or TCP-IP communication with computer Motor o Three Million times or above test for motor o Overheat and overload dual protection for motor

Note:- Stainless Steel Flap Barrier is a user-friendly access barrier developed for the efficient control of pedestrian movement according to the demanding Indian conditions. The barrier can be mounted with display, passage counter, card reader, token operation, command console, alarm system, which can all be interfaced with PC through RS232, RS485, TCP-IP (optional) line. The Flap Barrier provides a fail-safe safety solution in case of emergency or power failure, providing egress with the flaps retracting into main panel.

1(g) Swing Gate/P-Gate

#	**Item**	**Minimum Requirements**
1	Anti-Bumping	When the swing arms meet resistance during the operation the motor shall stop working automatically and turn back to original state after the default time
2	Anti Shock	The arms shall lock automatically if receive no authorized signals.
3	Self-resetting	If the user does not pass through at the stated time, the system will cancel his/her access permission this time automatically
4	Anti-Panic	When the power off, the clutch will be triggered and the arms will be opened, which allows people to pass through unhindered
5	QR Code	Shall be able to integrate with QR Code Reader
6	Dimension	150 Lx170Wx1080H(mm) to 300Lx200Wx1100H(mm)
7	Open & Close Time	1-3s
8	Pass Rate	35 to 45 person/min
9	Pass width	850mm to 900mm
10	Input	AC220 +-10%V/ 50+-10% Hz
11	Motor voltage	24v
12	Environment	-25~ +50
13	Power consumption	40w
14	Certification	BIS / Make In India/ ISO/ CE

15	Integration	Use IC Cards, ID Cards Bar code or Cards as automatic identification system and achieve access attendance fees or function.
17	In case of power failure	Fail-safe safety solution, provides egress in case of crisis evaluation.
18	Functioning	Double anti-clipping function, photo cell anti-clipping and mechanical anti- clipping.
19	Auto Reset Function	If no passing during identified card-reading time, the system will reset automatically the passengers are prohibited to pass until their second identified reading
20	Delay in closing	The barrier can be set to delay closing in 1-60s after a valid card reading
21	Operating Modes.	Single passage in the set direction, B-directional single passage, Free passage in the set direction, Always free or locked
22	Mechanism	Heavy Duty Design for 24hours continuous application Heavy duty pull type Indoor or outdoor application High durability with industrial parts All the running is quiet without any noise and shock.

1(h) Integrated Security Management Software

Access Control Software

Description	**Minimum Requirement**
General	The ACS software system shall have the modules that connect the node controllers on TCP/IP or RS-485, scans all the units defined for any events/alarms, and downloads any settings configured by the operator.
	The ACS shall be designed and configured in such a way so that single point failure will have no degradation in overall functionality
	It shall be the responsibility of the installer to ensure that the hardware and software solution using the PC specified meets the standards and performance criteria.

	The system software architecture shall be designed not only to provide a high speed open architecture platform for individual single server applications, but also be specifically designed to insure high speed, high integrity partitioning and redundancy for large cardholder database systems
	The ACS software shall use a Web-Server architecture based on standard operating systems, networks and protocols. The system shall enable distribution of functions such as monitoring, control and graphical user interface etc. across the network.
	The ACS server application within the ACS architecture should store its data within both a conventional relational database, such as SQL Server and a network directory
	The system must be provided with an ODBC compatible database with full SQL facilities, which will allow the interfacing of industry standard report generating facilities such as Crystal Reports, or in built Dynamic reports.
	ACS server database should offer the ability to enroll in advance both visitors and their upcoming visits. Visitor information can be either imported into the system or manually entered from any licensed desktop of ACS™ station.
	The ACS should maintain and capture different categories of the users: Employees Contract employees Other location employees (Deputation from Central and State) Visitors Cleaning Staff / Service Providers Vendors…etc
	The ACS should record and highlight the event and alarm in case a particular access is opened beyond the specified time set ACS should have archiving capabilities which can be configured as per the policy of the company ACS should record the entries on a real time basis as and when it occurs. One master for both Access Control System and Visitor Management System ACS shall have user configurable fields to add and remove field not required for the employee master ACS should be able to define VIP access so that when any VIP comes then door should be free for his/her entry
	It shall have dual access verification shall be available for escort/custodian type use ACS should be capable to count employees centrally/location wise to track employees inside premises during fire/earthquake into buildings. It should open all the barriers once fire input is received

	ACS shall have facility to connect to card printer and should have user defined card layout details It shall have temporary card module wherein temporary card should replicate the access of original card for temporary period ACS should be able to maintain complete history of the cards issued to an user
Software Support	Access Control system server software shall, as a minimum, support the following features
Cardholder records	50,000 expandable up to 2,00,00,000 if required
Card readers	4,000 to 65000 per server
Alarm input points	4,000 to 65000 per server
Relay outputs	4,096 to 65000
Security	All the data between devices & server should be encrypted using minimum SHA 256 or TLS 1.2 Encryption
Access Groups	The SMS shall be capable of assigning Access Groups with a maximum of 32 Access Levels per Access Group. Each Access Group shall be assignable to an alphanumeric name using up to 64 characters
Data movement	Data movement between workstations and the server and between the DC and the server shall use two distinct connections and web service protocols. For the Network Directory an LDAP interface shall be used. These two types together in an optimized architecture aredirected towards the following goals: High-speed cardholder data replication and redundancy in both a small and large-scale LAN/WAN/Internet environment. Open architecture, insuring the ability to quickly connect to third party software for a seamless integrated enterprise solution for the client, including database sharing, import and export. Highly secure, highly reliable Visitor Management and security monitoring in an open architecture environment, through the use of Windows 2008 and Secured Socket Layers (SSL) technology
Precision Access Levels	The SMS shall be capable of assigning Precision Access Levels in addition to the 32,000 Access Levels with the ability to assign unlimited card reader and time zone combinations. Each Precision Access Level shall be assignable to an alphanumeric name using up to 64 characters.

Holidays	Holiday assignments using an embedded calendar. Holidays shall be assigned an alphanumeric name using up to 64 characters and shall be grouped into eight (8) types of holidays, and shall be assignable to individual time zones. Access rights, card reader modes, and alarm masking schedules must be able to be altered when the current date is designated a Holiday. Dates for Daylight Savings Time changes shall be definable and shall take effect automatically. The SMS shall support Holiday Ranges that allow a single holiday to span across multiple calendar days:
Database Segmentation	The SMS shall be required to support data segmentation whereby each segment shall have its own set of cardholders, field hardware and system parameters (time zones, access levels etc.). This segmentation shall expand the limitations of the SMS parameters (i.e. access levels and time zones) to the maximum capacity of each parameter multiplied by the number of segments 1. The following list shall be made available for segmentation:- Access Group, Access Levels, Actions, Action Groups, Alarm Inputs, Alarm Mask Groups, Alarm Outputs, Areas, Badge Types, Card Formats, Cardholders, Card Readers, Central Station Receivers, Device Groups, Digital Video Archive Servers, Fire Alarm Panels, Guard Tours, Global I/O Function Lists, Global I/O Links, Holidays, Intercom Panels, Intercom Stations, Intrusion Detection Panel, ISC, Maps, Monitor Zones, Precision Access Groups, Receiver Accounts, System Operators, Time Zones
Area Control	The SMS shall provide five (5) area control features: Global Hard Anti-passback, Global Soft Anti-passback, Timed Anti-passback, Two Person Control, and Occupancy Limit. Area control shall be a security method of preventing a person from passing their badge to another person for dual entry into a single location utilizing one card ● Global Hard Anti-passback ● Global Soft Anti-passback ● Timed Anti-passback ● Two Person Control

Data movement	Data movement between workstations and the server and between the DC and the server shall use two distinct connections and web service protocols. For the Network Directory an LDAP interface shall be used. These two connection types together in an optimized architecture are directed towards the following goals: ● High-speed cardholder data replication and redundancy in both a small and large-scale LAN/WAN/Internet environment. ● Open architecture, insuring the ability to quickly connect to third party software for a seamless integrated enterprise solution for the client, including database sharing, import and export. ● Highly secure, highly reliable Visitor Management and security monitoring in an open architecture environment, through the use of Windows 2008 and Secured Socket Layers (SSL) technology
ACS Web client login	The SMS shall provide a minimum of 255 The Access Management should be fully web browser based application hosted in Internal server and can be accessed from any network computer with user login.
	The application access and permissions are fully based on Role based user log-in, such that an administrator has configuration and customisation rights whereas an Operator has limited rights for card and access management
	The software system design shall be object-oriented.
	The system shall have a simple, easy to use graphical user interface and all functions shall be accessible by use of either mouse or keyboard. Help text shall be provided for each screen function, and shall be sufficiently interactive that a user may access page help directly and be provided with explicit information relevant to the particular screen being displayed
	The system shall be capable of registration and issue of participant cards as per the format planned by Customer and Storing of photograph taken through digital camera in the master database..The format shall be finalized during the implementation stage.
	Logs of all user login and database changes to be maintained
	The client PCs shall be dedicated to act as a card issue terminal, system monitoring and administration purpose. The client PCs should be dedicated for defining rules and processes for ACS server system.

	Apart from this, All the rules & policy configuration can be configured using any network PC and Administrator login.
	All reports can be Viewed and Extracted from any of the network PC using standard web browsers without need of any local client installation
	Admin User Login normally have rights for actual rules definition, configuration , operations, monitoring and administration of following mention features ● Configuration of Access Controllers, readers, Company master, Department masters, designation master, communication master etc. ● Manual Entries, Outdoor duty entries., Tour entries should be possible ● Login and authority rights to the software for each operator ● Time zones definition for each time zone intervals ● Cardholder fields updation, deletion & addition ● Anti-pass back/anti-tailgate feature definition ● Bulk addition of user cards ● History/audit trail. ● Automatic card activation and deactivation with date stamp ● Global and local alarm masking by operator or cardholder
	● Access activity analysis by card reader. ● SMS & email integration, if require ● Photo capturing photo ID ● Database backup ,restore, export ,import, archival ,validation ● Access group definition , assignment, activation, deactivation ● It should define different transaction status like access denied, access granted, Egress pressed, invalid enable or expiry date for card user, anti passback violation etc. ● Emergency card definition such that on occurrence of emergency condition like fire when emergency card is shown to any DCs should opened all access door allowing free entry & exit ● Acknowledgement card definition such that when this card is shown to DCs after emergency condition should restore back DCs to normal conditions ● Windows options like tile horizontal /vertical or cascade open form

	windows ● Generation of various report for HR evaluation & administration ● Export of report to text, PDF, excel ,CSV format
Communication Manager	A real time transaction monitor software window shall be available for display on any DC transaction status. This software should be installed at ACS desktop apart from regular ACS software. It should act as a intermediate software between DC & ACS database
	The basic setup consists of one or several access controllers connected to the PC through network. This software which runs on the PC, polls i.e. communicates with access controllers connected in the network, collects the data and saves in a file which can be used later on for processing or generating the reports.
	This software should be Password protected
	It should allow effective control and monitoring of network of terminals
	The real time window shall be capable of listing the following transactions as they occur anywhere in the system. ● All transactions ● Valid card transactions ● Alarm transactions i.e. Invalidates cards of employees, Anti passback violation, fire inputs etc.
	A real time transaction monitor software should download raw Data in database in online mode
	It should support Dynamically or Batch polling-Supports both, default – batch polling
On-Line System Management & Reporting	The system shall maintain, on Server hard disks, an event transaction log file, and be capable of historical data reports as well as cardholder report listings in a variety of formats
	The system shall popup Database picture of user for every valid access transaction

	System Event Transaction Log File ● The system shall maintain an event transaction log file on hard disk for the recording of all historical event log data. ● The historical data file shall maintain the most recent one million event transactions without having to resort to archived media. ● The system shall warn the user of the need to archive historical data before data is overwritten or full.
Access Reports	The system shall be capable of producing the following reports, based on logged historical events over a specified date and time period, both individually and in any combination
	Report of rejected user access attempts for a selected cardholder, group of cardholders, selected card reader, group of card readers and selected alarm activations for a selected alarm point, group of alarm points, and by selected areas or group of areas.
	Report of operator entered comments in conjunction with alarm acknowledgments
	It shall have automatically email facility for the reports to be sent out on predefined time
	Report of manual operator override commands such as performed alarm point masking/unmasking, manual card reader door locking and unlocking, and manual auxiliary relay activate/deactivate.
	Report of automatic time controlled system commands such as automatic system On/OFF, and automatic door lock/unlocks.
	Report of unauthorized attempts to access resources/sensitive information.
	Report of access statistics including the number of valid accesses, rejected access attempts, and card read errors, reported by selected card readers, or group of card readers, or by selected areas, over a selected date and time period.
	Report of access statistics including when emergency card is shown

	In addition, the system shall offer the user the option of directing the historical reports to a client workstation control panel or Dashboard for display or to the mailbox as message.
Dynamic Report Builder	should allow the administrator to pick any available field in the system and use them as report column with simple Drag & Drop option, each selected column can used to sort, filter & group the report data.
	Dynamic Report Builder should allow any combination of system fields in report and dashboard, and should also have some pre defined reports to be build or clone other reports.
Controller – Reader report :	This report should display all configuration properties of installed controller and readers
Cardholder Reports	The system shall be capable of producing lists of selected cardholder data records on a client workstation monitor. The system shall allow the user to select sorting by card number, cardholder name or any other fields on report.
Cardholder report formats	The system shall allow the user to create report header and report format names. The system shall save and store these named formats on the Server Database for later use and recall by format name.
	Report for authenticated visitors who are allowed to entered in or leaving out with valid credential
	Report for Inactive visitors whose details are stored with application database but because of some reasons are prevented for authentication Access including visitors left out of MHA
	Report for system reset for all about when , how , how many time ,where the reset occurs
	Report for on & off of DCs describing when , who , why , how many time it occurs
	Reports related to other events like fire alarm detection if integrated, RAM file flashed , changes in controller configuration, DC operation in various modes etc

Other Master Report	• Report for currently configured employee details • Report for currently configured locations details • Report for currently assigned & configure designations & designation under which department, division, location or branch office details • Report for currently configure Holiday definition and rules set for holidays • Report for currently configure Time Zones details • Report for currently configure Access groups , active & inactive access group status details, assigned & available rights
Special Privilege report	• Report for special privileges assign to active participant like holiday bypass, Time zone bypass, anti passback bypass, enable details & expiry details
Custom Reporting Facilities	The system must be provided with an ODBC compatible database with full SQL facilities, which will allow the interfacing of industry standard report generating facilities such as Crystal Reports, Oracle, or Informix.

POC: Software & Hardware POC has to be given (Must)
*** Software should be integrated with NIC server/local server**

8. Photo Display Module

- Photo Display module is an LED Screen along with Industrial PC with Photo Display Application installed and connected to Main Access Control server installed at entrance locations (normally over Flap Barrier).
- This is to assist security personnel's to compare Database photograph and details during access authentication.
- The database at Photo Display Module & Server is always in Sync, such that any cardholder information updated on server by enrollment station, all connected Photo display module are updated.
- Photo display module display card holders image instantly on card/Fingerprint/QR code reading by Access readers.
- Access Readers send Card information to Serial port of Photo Display module.

S.N.	Specification	Requirement
1	LED Screen : 24”inch, 3 HDMI supported, 1920 X 1080 Resolution	Required
2	PDM : Photo Display Module Client Application	Required
3	Wall Mounting Stand for LED Screen	Required

2 . IT Infrastructure

2 (a) Server :- Access Control Server(Redundant, Witness & Failover)

#	Item	Requirement Description
1	Processor	Xeon Quad Core Processor
2	Memory	Minimum 16 GB memory
3	Network Interface Ports	Minimum 2 * 10 Gbps Ethernet Ports Per Server
4	Internal RAID	Internal RAID Controller with minimum 512MB battery Backed Write Cache
5	Internal HDD	Minimum 4 * 300GB Internal SAS SFF Hot Plug HDD Per Server
6	DVD	Internal / External DVD-RW or through virtual media
7	OS	Windows 2016 Enterprise Server operating system
8	SQL	Microsoft SQL server 2016 Enterprise Core Database with Replication License
9	Pre-Failure Warranty	Critical Components like CPU, Memory, HDD and PCI Slots should be covered under Pre-Failure Warranty

2(b) Desktop: - Client Access Desktop

#	Item	Requirement Description
1	Processor	i7 processor & above.
2	Motherboard & Chipset	OEM Motherboard
3	RAM	8 GB Minimum
4	Network	Integrated 10/100/1000 Gigabit Ethernet controller
5	Ports	1 HDMI port (Preferable), 2x USB 2.0 and 2 x USB 3.0 (Preferable) , 1xKeyboard port, 1xMouse port , Built in microphone ,Stereo jack
6	Storage	500GB data II HDD 7200 RPM

7	Optical Drive	8X DVD writer or higher
8	Monitor	18.5" TFT or more (4:3 aspect ratio) LCD Monitor 1280 x 1024 resolution
9	Keyboard	104 or more Keys Keyboard
10	Mouse	USB Optical Scroll Mouse with anti-static mouse pad resolution
11	OS Support	Windows 7/8 or latest
12	Preloaded Software	Windows 8 professional 64 Bit with MS office 2013 Professional
13	Power input	100 -240V AC

APPENDIX-C

3. ACTIVE NETWORK COMPONENTS

3 (a) 24-port 10/100/1000 Base-T Layer-3 Stackable Managed Switch.

Parameters	**Technical Specifications**
Physical Interfaces	24 # 10/100/1000 Base-T RJ45 Ports
	02 # 100/1000/10GBASE-T RJ45 Ports
	02 # 1000/10GBASE-X SFP+ ports

	Ethernet: Out-of-band 1G port (Front)
	Console: RJ45 RS232 (Front)
	Console: Mini-USB (Front)
	Storage: USB (Front)
	Full-width 1-unit 1U rack mount
CPU/ Memory	CPU: 800 MHz
	RAM: 1 GB
	Packet buffer memory: 16 MB
	Flash: 256 MB
Performance	Stack height: 8 switches
	Switching fabric: 128 Gbps Line-Rate (non blocking fabric)
	Throughput: 95.2 Mpps
	Forwarding mode: Store-and-forward
	Address database size: 16,000 MAC addresses (48-bit MAC address)
	Number of VLANs: 4,093 (IEEE 802.1Q) simultaneously
	Number of multicast groups= 2K IPv4
	Number of multicast groups= 2K IPv6
	ARP/NDP= 2K
	Number of LAGs (802.3ad): 128 LAGs with up to 8 ports per group
	Number of hardware queues for QoS: 8 (Standalone)

	Number of routes: 512 IPv4 Unicast routes
	Number of routes: 256 IPv6 Unicast routes
	Jumbo frame support: up to 9K packet size
	Mean time between failures (MTBF): 1,328,968 hours (~151.7 years)
	sFlow=416 samplers, 416 pollers, 8 receivers
L2 Services	Protocol based VLAN
	IP Subnet
	IPX
	ARP
	Subnet based VLAN
	MAC based VLAN
	Voice VLAN
	Private Edge VLAN
	Private VLAN
	Guest VLAN
	Double VLAN Tagging (QoQ)
	GARP with GVRP/GMRP
	MVR (Multicast VLAN Registration)
	Multiple Registration Protocol (MRP)
	Multicast VLAN Registration Protocol (MVRP)

	LAG Hashing
	LAG Member Port Flaps Tracking
	UDLD support
	Distributed Link Aggregation
	Storm Control
	Link Dependency
	Spanning Tree Protocol
	Per VLAN STP (PVSTP) with FastUplink and FastBackbone
	Per VLAN Rapid STP (PVRSTP)
	STP Loop Guard
	STP Root Guard
	BPDU Guard
	STP BPDU Filtering
	STP BPDU Flooding
	IGMP v2/v3 Snooping support
	MLD v1/v2 Snooping support
	Expedited Leave Function
	Static L2 Multicast Filtering
	MLDv1/2 Snooping Support
	IGMPv2/3 Snooping Support

L3 Services	IGMP Proxy
	MLD Proxy
	Any Source Multicast (ASM)
	Source Specific Multicast (SSM)
	Multicast streams routing between subnets, VLANs
	Multicast Static Routes (IPv4, IPv6)
	DVMRP
	Neighbor discovery (IPv4, IPv6)
	PIM-DM (IPv4, IPv6)
	PIM-SM (IPv4, IPv6)
	PIM multi-hop RP support
	IPMC replication (hardware support)
	DHCP Client (IPv4, IPv6)
	DHCP Server (IPv4, IPv6)
	DHCP Snooping (IPv4, IPv6)
	DHCP/ BootP Relay (IPv4, IPv6)
	DHCP options 66, 67, 150, and 55, 125
	Static Routing (IPv4, IPv6)
	Port based Routing
	ECMP Static Routing

	Port Based Routing
	VLAN Routing
	RIP v1 and v2
	OSPF v2 and v3
	OSPF Flood Blocking
	Route Redistribution
	VRRP
	VRRP Route/Interface Tracking
	Loopback Interfaces
	Tunnel interfaces
	Router Discovery
	IP Helper
	IP Source Guard
	IP Event Dampening
	ECMP
	Proxy ARP
	Multinetting
	ICMP v4 and v6
	IPv4/IPv6
	DNS v4 and v6

	IPv6 Routing
	Configured v6-over-v4 tunnels
	Automatic (6to4) tunnels
QoS	IEEE 802.1p CoS
	DiffServ QoS
	WRED (Weighted Deficit Round Robin)
	Single Rate Policing
	Strict Priority queue technology
	Auto-VoIP
	iSCSI Flow Acceleration
	IP DSCP
	IP Precedence
	IP TOS
	L3 IPv6 Flow Label
	Interface Traffic Shaping
	PHB Support
	Minimum Bandwidth per-interface
Security	Broadcast, Multicast and Unicast Network Storm Protection
	CPU Protection
	DoS attack protection

	ICMP throttling
	Management ACL
	Radius accounting
	TACACS+
	L2/L3/L4 Access Control List (ACL)
	MAC, IPv4, IPv6, TCP, UDP ACL
	Protocol based ACL
	ACL over VLAN
	Dynamic ACL
	IEEE 802.1x Radius Port Access Authentication
	802.1x MAC Address Authentication Bypass (MAB)
	Port Security
	Dynamic ARP Inspection
	MAC Filtering
	Port MAC Locking
IEEE Network Protocols	IEEE 802.3 10Base-T
	IEEE 802.3 Ethernet
	IEEE 802.3i 10BASE-T
	IEEE 802.3u 100BASE-T
	IEEE 802.3ab 1000BASE-T

	IEEE 802.3z Gigabit Ethernet 1000BASE-SX/LX
	IEEE 802.3ae 10-Gigabit Ethernet
	IEEE 802.3ad Trunking (LACP)
	IEEE 802.1AB LLDP with ANSI/TIA-1057 (LLDP-MED)
	IEEE 802.1D Spanning Tree (STP)
	IEEE 802.1s Multiple Spanning Tree (MSTP)
	IEEE 802.1w Rapid Spanning Tree (RSTP)
	IEEE 802.1p Quality of Service
	IEEE 802.1Q VLAN tagging
	IEEE 802.1v protocol-based VLAN
	IEEE 802.1X Radius Network Access Control
	IEEE 802.3x flow control
	GMRP — Dynamic L2 multicast registration
	GVRP — Dynamic VLAN registration
	GARP -Generic Attribute Registration Protocol
Management	ISDP (Industry Standard Discovery Protocol)
	Out of band Management
	802.1ab LLDP and LLDP-MED
	SNMP v1, v2 and v3
	RMON 1, 2, 3, 9

	sFlow
	Command Line Interface (CLI)
	Web-based graphical user interface (GUI)
	Admin access control via Radius and TACACS+
	Telnet
	IPv6 Management
	Dual Software (Firmware) images
	Dual Configuartion file (Text-based)
	Radius accounting
	Malicious Code Detection
	SNTP
	XMODEM
	Port Mirroring
	Cable Test Utility
	SSH v1/v2
	SSL/HTTPS and TLS v1.0 for web-based access
	File Transfer (uploads, downloads) through TFTP/HTTP
	SCP/ SFTP/ HTTPS
	Syslog
	Non disruptive Config Management

	Remote Port Mirroring (RSPAN)
	OpenFlow 1.3
	Persistent log supported
Network Traffic	Access Control Lists (ACLs) L2 / L3 / L4
	Time-based ACLs
	ACL over VLANs
	IPv6 RA Guard Stateless Mode
	Network Authentication Successive Tiering
	802.1x MAC Address Authentication Bypass (MAB)
LEDs	Per port: Speed, link, activity
	Power, Fan, Stack Master, Stack ID
Environmental	Operating Temperature: 32° to 122°F (0° to 50°C)
	Operating Humidity: 90% maximum relative humidity, non-condensing
	Storage Temperature: – 4° to 158°F (–20° to 70°C)
	Storage Humidity: 95% maximum relative humidity, non-condensing
Certifications	CE mark, commercial
	FCC Part 15 Class A, VCCI Class A
	Class A EN 55022 (CISPR 22) Class A
	Class A C-Tick
	EN 50082-1

	EN 55024
	CSA certified (CSA 22.2 #950)
	UL listed (UL 1950)/cUL IEC 950/EN 60950
Warranty	Lifetime Hardware Warranty

3 (b) Smart Managed Non-POE Switch

Parameters	**Specification**
Interfaces	8 RJ-45 connectors for 10BASE-T, 100BASE-TX and 1000BASE-T (Auto Uplink on all ports)
Network Protocol and Standards Compatibility	IEEE 802.3 10BASE-T Ethernet
	IEEE 802.3u 100BASE-TX Fast Ethernet
	IEEE 802.3ab 1000BASE-T Gigabit Ethernet
	IEEE 802.3x full-duplex flow control
	IEEE 802.1W Rapid Spanning Tree Protocol
Administrative Switch Management	IEEE 802.1S Multiple Spanning Tree Protocol
	Auto-voice VLAN
	SNMP v1, v2c, v3
	RFC 1213 MIB II
	RFC 1643 Ethernet Interface MIB
	RFC1493 Bridge MIB
	Jumbo Frame Support

	IEEE 802.1Q Tag VLAN
	64 Static VLANs
	IEEE 802.1p (Class of Service)
	DSCP - L3 QoS
	IEEE 802.3ad static or dynamic link aggregation (LACP)
	DHCP client function
	Broadcast storm control
	Port mirroring (many-to-one)
	Green features: Power saving by cable length (<10m). Power saving by auto power when link down
	IGMP snooping v1/v2
	IEEE 802.1x (RAIDUS)
	Access control list (ACL) - MAC, IP
	SNTP
	IEEE 802.1ab LLDP
	Protected ports (To be available via free firmware upgrade)
	HTTP and HTTPS
	Auto denial-of-service (DoS) prevention
	Syslog
	Ping & traceroute
	Web-based configuration, anywhere on the network

	Smartwizard Discovery Utility program auto discovers devices (up to 254 agents/switches); set system configuration to each agent
	Configuration backup/restore (easy to configure more than one switch)
	Password access control
	Firmware upgradeable
	Full-duplex IEEE 802.3x pause frame flow control
Active Flow Control	Forwarding modes: Store-and-forward
	Bandwidth: 16 Gbps
Performance Specifications	Network latency: : Less than 15µs for 1000 Mbps with 64 bytes
	Buffer memory: 512 KB embedded memory per unit
	Address database size: 4K media access control (MAC) addresses per system
	Mean time between failures (MTBF): : 275,533 hours
	Acoustic Noise: 0 dBA
	Unit: Power
	Per port: Link, activity, speed, duplex
LEDs	Maximum Power Consumption: 16.5W
	100-240V AC/50-60 Hz universal input
Physical Specifications	Operating temperature: e: 0° to 104°F(0° to 40°C)
	Storage temperature: -4° to 158°F (-20° to 70° C)
Environmental Specifications	Operating humidity: 90% maximum relative humidity, non-condensing

	Storage humidity: 95% maximum relative humidity, non-condensing
	Operating altitude: 10,000 ft (3,000 m) maximum
	Storage altitude: 10,000 ft (3,000 m) maximum
	CE mark, commercial
	FCC Part 15 Class A
Electromagnetic Compliance	VCCI Class B
	C-Tick
	UL listed (UL 1950)/cUL
	IEC 950/EN 60950
Safety Agency Approvals	CE mark, commercial
	CUL 60950 (Listed)/EN 60950 (Low Voltage Directive)
	CB
Warranty	Life-Time Warranty

3(c) Firewall & Security

- Recommend User Limit: 75
- Form Factor: Desktop
- Firewall throughput: 8 Gbps
- VPN throughput: 1180 Mbps
- NGFW Throughput: 1200 Mbps
- Ethernet interfaces: 8 x GE copper,1 x SFP

3(d) NAS-Storage Appliance

S.N	**Parameter**	**Specification**
i.	Form Factor/Mounting	3U/19” Rack Mounted

ii.	No. of Controllers	02 nos. in redundant mode.
iii.	Host interface Type	FC or iSCSI or FCoE or Ethernet
iv.	No of Host interface	8
v	Drive Type	NL-SAS HDD, 7000 RPM or higher
vi.	Cache	16 GB per Controller
vii.	Storage Capacity along with expansion using JBODs	100 TB Usable
viii.	Power Supply	Three redundant 250W (Up to Four) 90-264V, Hot swappable N+1 Design; per appliance
ix.	Fan	Hot swappable redundant design with battery backup module; per appliance
x.	RAID configuration	RAID 5/6
xi.	Virtual Drives	Maximum 256 virtual drives
xii.	Hot Spare Disk	It shall provide at least one hot spare disk; per appliance
xiii.	The storage system shall come with advanced RAID features that deliver robust data protection capability including Predictive Data Migration, Intelligent Bad Sector Remapping, SMART Error Handling, NVRAM Error Logging, Disk Slot Power Control, Read/Write Check Table, and Write-hole Table Protection.	Non-stop operation and data protection
xiv.	The storage system shall come standard with Advanced Battery Flash Backup design that uses power from BBU module to save write cache data held in DDR3 to non-volatile NAND flash memory.	Non-stop operation and data protection

xv.	Warranty/Replacement	Three years warranty/replacement from OEM for appliance including NL-SAS HDDs
xvi.	Certifications / Regulatory compliance	CE, FCC, UL, ROHS, BIS
		OEM should have ISO 9001 and 14001 for manufacturing

APPENDIX-D

4. Passive Network Components

4(a) SM Fiber Cable - 6 Core

1. The fiber type is a Matched Cladding Single Mode
2. Fiber dual coated with acrylate coating.
3. The fiber is optimized for operation at 1310 nm and at 1550 nm.
4. Should fulfill the requirements of: IEC 793-2: 1992, EN 188101 and ITU-T Recommendation G.652

5. Testing methods are in accordance with the following standards: ITU-T G.652.D, IEC 793-1 and Telecordia : GR-20 Core,ISO : 11801
6. Maximum induced permanent loss after 1000 h at 1 bar H2 at 70 °C and out gassing for 72 h at 70°C (valid both at 1310 nm and at 1550 nm): 0.2 dB/km

4(b) CAT 6A Cable

Features	Requirements
Features	Category 6 Unshielded Twisted Pair 4 pair 100W cable shall be compliant with ANSI/TIA/EIA-568-C.2 Additional Transmission Performance Specifications for 4-pair 100W Category 6 Cabling.
	Category 6 UTP cables shall extend between the work area location and its associated telecommunications closet and consist of 4 pair, 23 AWG, UTP.
	All Category 6 cables shall be tested upto 600 MHz (Certificate to be submitted Along)
Mechanical Characteristics	Construction: 4 twisted pairs separated by internal X shaped, 4 channel, polymer spine / full separator. Half shall not be accepted.
	Conductor Solid bare Copper
	Conductor Diameter 0.56±0.005mm (23 AWG)
	Insulation :High Density Polyethylene
	Jacket FR PVC
	Outer Diameter 6.1 mm nominal
	Temperature Range -20° to +70°C

4(c) Power Cable

3 Core Power Cable- 1.5 sqmm Unarmoured

4(d) PVC Conduit

25mm PVC Conduits ISI Marked [IS:9537(Part-III)/1983]

4(e) CAT 6 24 Port Jack Panel

Features	Be made of powder coated steel, in 24 port configurations.
	Allow for a minimum of 200 re-terminations without signal degradation below standards compliance limit.
	Have port identification numbers on the front of the panel.
	Should have self-adhesive, clear label holders (transparent plastic window type) and white designation labels with the panel, with optional color labels / icons.
	IDC: Suitable for 22-26 AWG stranded and solid wire compatible with both 110 & Krone punch down tools
	Each port / jack on the panel should be individually removable on field from the panel.
	Improved cable management with optional cable management bar
	The Cat-6 transmission performance is in compliance with the ANSI/TIA/EIA 568C.2 standard
Mechanical : Jack Connector	Plastic Housing: ABS , UL94V-0 rated
	Operating Life: Minimum 750 insertion cycles
	Contact Material: Copper Alloy
	Contact Plating: 50µ" Gold plated on plug contact area
	Contact Force: 20N max (IEC 60603-7-4)

	Plug Retention Force: 15 lb.
IDC Connector	Plastic Housing: Polycarbonate, UL94V-0 rated or equivalent
	IDC cap : ABS, UL 94V -0
	Contact Material: Copper Alloy
	IDC Contact Plating: Phosphor bronze with tin plated
	Insertion Force: 20N max (IEC 60603-7-4)
	Wire Accommodation: 22-26 AWG solid

4(e) OFC Termination Accessories

Optical Fiber Equipment Cords (minimum 3 meter)

Sr.No	Requirements
1	All optical fiber patch leads shall comprise of Single mode 9/125µm fiber with SC/LC/FC, fiber connectors terminated at each end. The optical fiber patch leads shall comply with the following specifications:
2	Optical Fiber – Corning Single Mode
3	Connector: Zirconia ceramic ferrule
4	Pre-radiuses and pre-polished ferrule
5	Simplex / Duplex
6	Color-coded Yellow for SM
7	Insertion Loss - <0.2 db
8	Cable: 9/125, SM

9	Repeatability - < 0.2 db
10	Durability – 1000 mating cycle
11	Working Temp : -40 deg C.to + 85 deg. C
12	Standard : G652D, G 657A & G 657B
13	Length : 1,2,3,5 & on request

CAT 6 Mounting Cords

Features	Requirements
Features	Category 6 Equipment cords
	The work area equipment cords shall, at a minimum comply with proposed ANSI/TIA/EIA-568-C.2 Commercial Building Cabling Standards Transmission Performance Specifications for 4 pair 100W Category 6 Cabling.
	Equipped with modular 8-position modular plugs on both ends, wired straight through with standards compliant wiring.
	Should have 50 micro inches of gold plating over nickel contacts.
	Should be covered by ETL verification program for compliance with TIA 568.C.2
Mechanical : Cable	Conductor size: 24 AWG stranded bare copper
	Max O.D.: 5.6mm (.22”)
	Jacket: PVC UL-94V-O
	Temperature range: -10oC to +80oC

Mechanical Characteristics – Plug	Operating life: Minimum 750 insertion cycles
	Contact blade: Phosphor bronze
	Contact plating: 50µ" Gold
	Plug dimensions & tolerances compliant with FCC Part 68.500 and IEC 60603-7
	Approvals: UL 444 for copper conductor
	Operating life: Minimum 750 insertion cycles
Electrical Characteristics – Plug	Diélectrique with standing voltage :500 V AC
	Insolation résistance : 35 M Ohm (Max)
	Operating temperature: -10oC to 80oC

4(g) Rack 42U Rack

Sr.No	Requirements
1	42U Enclosure Frame-800X1000-STEEL, Caster Wheels Set of 4 (2 with Brakes & 2 without Brakes)
2	Adjustable Levellers set of 4
3	Glass Door-800-42U, Metal Door-800-42U-Vented, Side Panels-1000-42U-Vented
4	Mounting Hardware-(Pack of 20), FHU with 4 FAN 360CFM

5	Vertical Power Distribution Unit with 12 x 5/15 sockets Round Pin, 230 Volts AC, 32 Amp with Plug
6	Vertical Cable Manager-42U-Loop, Horz. Cable Manager-1U-Loop
7	Conforms to DIN 41494 OR equivalent ISO Standards
8	Adjustable 19" equipment mounting verticals provide the better mounting flexibility maximizing the usable mounting space
9	Depth adjustable mounting slots
10	Top and bottom Panel with ventilation and cable entry facility
11	Provision to mount the cooling fans on the top panel
12	Powder coated finish with pretreatment process meeting all industry standards
13	Grounding and Bonding Options can be provided
14	100% assured compatibility with all equipment conforming to DIN 41494. General industrial standard for equipment
15	Conforms to DIN 41494 or equivalent standard
16	Welded Frame, Lockable Toughened Glass Door, Metal Vented Door Steel,
17	DIN Standard 10mm Sq. Slots / Direct M6 Tap, 19" Mounting angles made of formed steel Powder Coated
18	Welded to Frame, Vented and Field Cable entry exit cut outs
19	Static Load 500 KG

Terms & Conditions

1. **CPSU will ensure that the entire work should be completed within the stipulated period of time i.e. within 180 days of award of work order.**

2. CPSU will bear the responsibility to bring the items and installation the same in the office.

3. The Bidder has to make the demonstration/ Proof of Concept (POC) of the Quoted Biometric Reader, Card Enrollment & Photo Display module along with other required equipments during evaluation of the technical bid.

4. Ministry of Home Affairs reserves the right to reject any quotation completely or partially without assigning any reason.

5. Ministry of Home Affairs also reserves the right to cancel the contract before installation, if the items of the CPSU are not found satisfactory.

6. The payment charged by the bidder for maintenance will be released quarterly on pro-rata basis in every year and any deficiency found in the service, 5% penalty on the cost of yearly maintenance charges should be imposed to the Contractor.

7. OEM should have a turnover of 25cr

8. OEM should have Purchase orders of min. 1000 Biometric Readers & 50000 cards

9. The OEM should have prior experience in implementing physical access control solution with multi-factor authentication for a user base of at least eight thousand users per organization at multiple locations in at least 3 different organisations in last 7 year. Bidder to submit satisfaction/ credential letter from the client clearly stating the scope of work including location and user base of the solution

10. Flap Barrier & Biometric/card reader should be from the same OEM

11. **Source Code provided will not part of Escrow**

12. The contractual firm will provide Comprehensive Annual Maintenance Contract for Access Control surveillance system and LAN system up to five years after the expiry of warranty period of one year. The condition for CAMC (Comprehensive Annual Maintenance Contract) and replacing of spare parts, will be as under:-

12.1 **Scope of Maintenance**

a. The contractor shall be responsible for maintenance of all equipments mentioned in Schedule with a view to provide uninterrupted service of the Access Control System including necessary preventive maintenance, attending to major and minor breakdowns post failure repairs and modifications if any, required for the Access Control system of Ministry of Home Affairs.

b. The Access Control System installed in Ministry of Home Affairs is monitored round the clock by our Control Room staff. Hence the contractor shall depute only competent and efficient staff for routine maintenance as well as to attend the breakdowns to ensure the

trouble free working of Access Control system.

c. The CAMC shall also include the trouble shooting of any network issues arising in the Access Control network.

d. The service personnel deputed by the contractor shall be well qualified and having enough knowledge in the field of Wireless networking and Access Control System. The list of service personnel along with their qualifications and experience shall be enclosed along with the tender document with proper proof.

e. Contractor shall only deploy their service engineers whose antecedents have been verified by the local police authority.

f. At the end of each major breakdown repair, contractor's Engineer should prepare a service report and submit the same to the In-Charge Control Room.

g. All the tools and testing instruments required for checking testing and attending to routine maintenance and breakdowns shall be arranged by the contractor.

h. **The preventive Maintenance shall be carried out once in a month.** The contractor shall undertake preventive maintenance of Access Control System in the last week of every month in each building. In addition to the preventive maintenance the contractor shall attend break down calls whenever emergency arises and there will be no limit for such calls.

i. The components of the equipment will be the whole responsibility of contractor for procurement and replacement as and when required during the period of AMC.

j. The contractors staff will carry the routine spares required for preventive maintenance to ensure minimum down time without any additional cost. In addition to those spares contractor will also arrange other spares if required without any additional charges.

k. Breakdown call shall be attended with a time frame after getting the message by phone or fax /email. If the repair is major contractor shall provide a standby equipment at contractor cost.

l. In case of major repairs necessitating removal of the equipment to the contractors service centre, the system or its parts shall be reinstalled at the owner premises after repairing the set in working condition. Provision of standby comes under the scope of contract.

m. Trained and supervisory control staff shall be permitted to minor urgent changes if required for which suitable log will be maintained by police control room staff.

n. A log book will be maintained in the control room in which day to day failures and problems notices shall be entered and informed to the contractor indicating date and time. The contractor's Engineer/representative has to till up the log book as per schedule maintenance check up giving the details as well as corrective measures taken by the contractors engineers with date and time.

o. All remedial maintenance of the equipments and its preventive maintenance required periodically shall be provided by the contractor. Such maintenance comes under the scope of contractor. Supply of and fitment of all parts including consumable will need replacement from time to time with understanding that replaced part immediately will

become govt. property and the part removed will become contractor's property with condition that the contractor shall use new and unused except those parts which can be reused after required servicing.

p. The contractors shall ensure that the full configuration of the equipment is in proper working condition, after repair and maintenance.

q. All minor repairs/services should be made only at Department's premises. As far as possible no equipment will be sent to the contractor's premises for any repair. If at all, it is found necessary to take the equipment to the contractor' premises, the configuration of the equipment in details must be got noted before it is sent out. The items will be taken out only with proper documentation such as materials gate passes and with proper acknowledgements. All endeavors will be made by the contractor to return such items taken out for servicing with in a reasonable period of one week Stand by equipment similar to the equipment under service to be provided before taking it out on material gate pass, till the original component is replaced AT NO EXTRA COST. The contractor is required to record all such issues, returns / replacements of equipment promptly.

r. In any case where the equipment could not be rectified / replaced by the firm with in the reasonable time, Ministry of Home Affairs reserves the right to get the equipment repaired / replaced through an other agency at the risk and cost of the contractor. The contractor will have to bear expenses incurred by the Department on this account. This action will be taken if the equipment is neither rectified/ replaced nor any stand-by is provided even after the reasonable time.

s. Taking shelter under flimsy reasons such as damage could have been caused by rat bite, power outage, rough handling on the part of the user and similar such reasons, and failing to provide maintenance / replacement support will not be acceptable.

t. Complete hardware and software support to be extended by the contractor.

u. Carrying any software changes if required with out additional charges with the consent of In-Charge Control Room, Ministry Home Affairs.

v. In case of odd hour's failures and emergencies even on holidays and Sundays normal service is to be rendered by the contractor. The Contractor shall ensure that the equipment is in good working condition and is with full configuration while handing over at the end of the contract period.

12.2 SITE OF WORK

The intending tenderer is advised to study the tender documents, concerned specifications and other instructions carefully. The tenderer shall inspect the proposed site of work and acquaint himselfl themselves with the site conditions, working hours and all relevant items connected with execution of work. The submission of tender shall be deemed to have been done after careful study and examination of the tender papers with full understanding of the implications thereof.

12.3 MAINTENANCE OF SERVICE REGISTER:

The contractor shall upkeep the service *I* maintenance record for all the units and

Peripherals with the following details.

a) Location of the Unit.
b) Name of Equipment.
c) Date of Periodical Maintenance attended.
d) Due date for next Periodical Maintenance.
e) Nature of Defecti ve Noticed.
f) Details of Defect Attended with date.
g) Name of Service Engineer.
h) Name of the In-Charge of Ministry of Home Affairs with signature and office seal.

12.4 <u>INSPECTION:</u>

The contractor shall offer the units for inspection after periodical maintenance *I* Service Repair to an authorized representative of and also get a report signed by the concerned Control Room in charge with office seal before submission of bill for quarterly payment from Ministry of Home Affairs.

13. Training

(i) The scope of work envisages that the Bidder shall undertake to train the staff nominated by department in different aspects of equipment, functioning, testing, operation & administration.

(ii) The PSU shall at every stage of installation; testing and commissioning provide all facilities for adequate training to the staff nominated by Ministry in Ministry of Home Affairs, North Block who may be deputed to work on the project.

(iii) The system Administration and Maintenance Training program, at the user's location, will be structured so as to train 2 (Two) officers/officials nominated by Ministry.

(iv) The training programme should be of atleast three days and atleast 6 hours per day.

(v) Bidder will provide complete details on the training programs to be offered including :

(a) Material to be covered.
(b) Number of hours of training per operator of technician for each specific course
(c) Supporting documentation to be provided

14 Spare Parts

(i) The L-1 firm to whom the tender will be awarded have to maintain stock of spare parts of the system for atleast five years from the date of completion of the installation work. Payment to firm for replacing the spare part will be made as per the clause 11 of terms & conditions.

(ii) The Bidder will undertake that supplies of necessary maintenance equipment and spare parts will be made available for all the equipment and the complete System for a period 6 (Six) years on continuing basis .

15 Site Preparation

(i) The site for installation of the system shall be provided by the Purchaser as per the required environmental conditions before the installation of the system.

(ii) The tentative site plan for installation of Access Control System is at annexure VII which may differ as per actual requirement at the time of installation of the Access Control System.

(iii) The complete installation of the System at the Purchaser's site shall be the responsibility of the PSUs.

(iv) Earthing arrangements for all the equipment shall be the responsibility of the Supplier and to be carried out as per standard procedures.

(v) Responsibility of Completion & Software Optimization: Any fitting or items which may not be specially mentioned in the specifications but which are necessary are to be provided by the PSU without any extra charge for completeness of the work under this Tender.

16. The firm will ensure that all the work of supply, installation, erection and commissioning of Access Control System in Ministry of Home Affairs , North Block is completed in the prescribed time and in no case the contractor firm may do any activity which may disturb senior officers to work/hamper the official duties of the employees of various Departments in Ministry of Home Affairs , North Block..

17. The Ministry shall have no liability, financial or otherwise, for any harm/ damage/ injury caused to the manpower/machinery deployed by the firm in the course of performing work of this Ministry. Neither the firm nor its workers shall have any claim on this Ministry for compensation or financial assistance on this account

18. The service provider's personnel shall not divulge or disclose to any person any details of office, operation process, technical know-how, security arrangements, administrative and organizational matters as all of these are confidential in nature. It is binding for the contractor firm to not disclose the networking module of above work any other information related to this work to any individual/group/firm which may cause harm to the security of Ministry of Home Affairs, North Block.

19. The service provider shall replace immediately any of its personnel, if they are unacceptable to the User Department/Ministries because of security risk, incompetence, conflict of interests and breach of confidentiality or improper conduct upon receiving a written notice from any of the User Department in Ministry of Home Affairs , North Block..

20. The damage caused, if any, to Government property through the acts of the firm and/or by its workers shall be made good by the agency and decision of the Ministry in this regard shall be final/binding.

21. The performance security shall be valid till all contractual obligations are fulfilled by the firm and will be released after two months of the above seven year contract period. The same shall stand forfeited in case of cancellation of the contract for any breach of contract or for any deficiency in the performance noticed during the currency of the contract.

22. The tender is in two parts (TECHNICAL AND FINANCIAL). for installation of Acess Control System in Ministry of Home Affairs , North Block by Central Public Sector Undertakings (CPSUs) only who have adequate experience for installation and day to day maintenance of Acess Control

23. Manufacture Authorization Letter required to be submitted confirming that bidder is authorized to quote the products of OEM & product should comply with the requirement of this Ministry as per specifications given to the PSU.

24. The Access Control OEMs must have its own office & service and support centre in India registered under the Indian companies act and in operation for period of min 10 years as on 31/03/2018. Copies of company incorporation certificate shall be submitted.

25. Brochure of each item in respect of which rates are quoted should also be attached.

26. Compliance sheet should also be attached from bidders' end giving undertaking that the items to be provided by them comply with the specifications provided.

27. Bidder should clearly mention if there is any deviation from the specification or else no deviation certificate may be enclosed.

28. The service provider should not have been debarred/black-listed by any Central/State Government Agency.

29. Every page of the tender document should be signed and stamped by the bidder and the same has to be uploaded in technical bid.

30. Configurations for all items as mentioned in Annexure-II are minimum. Bidders are free to quote for equipments/ items having higher configuration.

31. L-1 will be decided on the basis of lowest rates received in Financial Bid (Annexure –V).

32. Items of which specifications are not mentioned in tender document should be of ISI marked or according to applicable Governments Norms. The items should be of reputed brands.

33. Offered items should be available on website of the OEM. The items should not be of dying nature.

34. Payment Procedure:

a. 70 % on delivery of material
b. 20% on Installation
c. 10% on Handover & Sign-off

ANNEXURE-III

TECHNICAL BID Performa

Sl.No.	Description	Details to be given by the Bidder
1.	CPSU's Name and Full Postal Address	
2.	Name of the representative of the PSU and his Telephone/Mobile No.	
3.	Date of CPSU's Registration with details (Copy of registration to be enclosed).	
4.	GST Number	
5.	PAN Number	
6.	Service Tax Number	
7.	Present/past experience in the field (Satisfactory performance certificate from other Ministries/Departments is to be enclosed)	

It is confirmed that we have fully understood the scope of work and all other requirements for Supply, installation, erection and commissioning of Access Control system in Ministry of Home Affairs , North Block as per the given details in the Tender. We hereby agree to the General as well as Special Terms and Conditions of the Contract as detailed in the tender document. We undertake that the documents enclosed herewith are genuine and no material/facts have been concealed or suppressed. We are not debarred / blacklisted by any Government organization in the field of supply, installation, erection and commissioning of Access Control System. We also understand that the contract is liable to be cancelled if found to be obtained through fraudulent means or by concealment of information/facts.

This offer is made to be valid for acceptance by your Department within 1 year days from the date of opening of the technical bid.

(Signature of authorised representative of the firm)

Stamp/ Seal of the firm

Annexure -IV

S.N.	Description	Make	Model	Qty	Unit	Supply		Installation	
						Unit Cost	Total Cost	Unit Cost	Total Cost
1	Scosta Card			1,50,000	Nos.				
2	Fingerprint Terminal (S1) - 2 Templates each User with inbuilt SCOSTA(SAM Module) Card Reader with 4.3 Inch LCD Display, Keypad, Inbuilt QR Code Reader			640	Nos.				
3	Smart Card Personalization Kit - Card Personalization Software with USB Smart Card writer/Reader with FP Enrollment Scanner (4-4-2)			5	Nos.				
4	Two Reader Network Access Controller with PS Cabinet, Power supply & Onboard TCP/IP (IPW V3 Series - Onboard IP & remote Telnet & Web Browser Interface)			320	Nos.				
5	Swing Barriers- Stainless Steel LEFT/RIGHT, Single Side Flap, Specify L or R while ordering Lane Opening 600 mm (Normal Lane)			115	Nos.				
6	Swing Barriers- Stainless Steel LEFT/RIGHT, Single Side Flap, Specify L or R while ordering Lane Opening 900 mm (Wide Lane)			182	Nos.				
7	Swing Gate (P Type)			23	Nos.				
8	Framework for PLATFORM (Users & Device Management) with 10 Web User Login			1	No				
9	Access Control Add On, Access Groups, Time Zones, Door Security Management			1	No				
10	Base Module PLATFORM (Users & Device Management) - Failover Server with Witness Service			1	No				

11	Photo Display Module Add On, Database Photo Display at Access / Attendance Points on external monitor (PC) - integrates with Platform			1	Nod				
12	Photo Display Module Client for Photo display on external monitor - integrates to PLATFORM			320	No				
13	Integration with NIC / Local Server			1	Lot				
14	Source Code			1	Lot				
Network & Cables									
15	3 Core Power Cable- 1.5 sqmm Unarmoured			6700	Mtrs				
16	CAT 6 Cable			6880	Mtrs				
17	OFC Cable-6 Core			32550	Mtrs				
18	SC Couplers - Duplex			532	Nos.				
19	SC-LC OFC Duplex Patch Cords SMF (3Mtr)			532	Nos.				
20	SC-SC OFC Duplex Patch Cords SMF (3Mtr)			532	Nos.				
21	OFC Pigtails SC-Type SMF (1Mtr)			3192	Nos.				
22	12 Port LIU Fully Loaded With Adapter Plates & Couplers			532	Nos.				
23	Rack : 36U			47	Nos.				
24	Patch Panel: 24 Por, Fully loaded			266	Nos.				
25	Patch Cord: 3 Mtr (Patch panel side)			266	Nos.				
26	Patch Cord: 2 Mtr (for device end)			640	Nos.				
27	I/O module			640	Nos.				
28	Surface Plate with Box			640	Nos.				

29	PVC Conduit			6880	Nos.				
30	Railing(in Feet)			1545	Nos.				
31	SFP Module-SM 1gig			438	Nos.				
32	L2-8 Port Switch Non POE			219	Nos.				
33	L3-24 Port Switch			47	Nos.				
Server, Desktop, Database & Firewall									
34	Primary Server, Witness Server with Redundant Server			3	Nos.				
35	MS SQL Enterprise Core Database with Replication License			1	Nos.				
36	Desktop PC with Monitor			5	Nos.				
37	Monitor - 24 inch with all accessories			320	Nos.				
38	NAS-Storage Appliance			1	Nos.				
39	UTM Appliance			1	Nos.				
AMC									
40	Comprehensive onsite support charges for Access Control system and LAN system			5	Per Year				

Note: Above Items mentioned are approximate quantities. Access Control System and other items mentioned may be increased or decreased up to 25%. The payment will be made as per actual basis.

(Signature of authorised representative of the firm)

Stamp/ Seal of the firm