सरदार वल्लभभाई पटेल राष्ट्रीय पुलिस अकादमी
SARDAR VALLABHBHAI PATEL NATIONAL POLICE ACADEMY
(भारत सरकार : गृह मंत्रालय)
(Government of India : Ministry of Home Affairs)
हैदराबाद - 500 052
Hyderabad – 500 052

No. 26011/68/2015-16/HS-OM Dated the 20 January, 2016

NOTICE INVITING TENDER

Sub : **Extension of Last Date for Submission of Quotation in Connection for Implementation of Gate Management System for S.V.P. National Police Academy, Hyderabad-Reg.**

Dear Sir,

Kindly refer to our earlier tender notice of even No. dated 23rd December 2015, toward the implementation of Gate Management System for S.V.P National Police Academy, Hyderabad.

2. Due to administrative reasons, the last date of submission of quotations against the notice under reference is hereby extended upto 2nd February 2016.

3. Your offer along with the prescribed EMD and other enclosures shall be sent in a sealed cover duly super scribed as '**QUOTATION FOR IMPLEMENTATION OF GATE MANAGEMENT SYSTEM TO S.V.P. NATIONAL POLICE ACADEMY- NOT TO BE OPENED BEFORE 03-02-2016** and sent to the Academy so as to reach on or before 02-02-2016 (17:00Hrs).

4. The other terms and conditions of our earlier notice even No. dated 23rd December 2015 remain unchanged.

Yours faithfully,

(K Shankar)
Admn. Officer (Admn.)

Copy to: Copy to Programmer with a request to please get the above requirement posted in NPA Website and provide a link with NIC web-site.

सरदार वल्लभभाई पटेल राष्ट्रीय पुलिस अकादमी
SARDAR VALLABHBHAI PATEL NATIONAL POLICE ACADEMY
(भारत सरकार : गृह मंत्रालय)
(Government of India : Ministry of Home Affairs)
हैदराबाद - 500 052
Hyderabad – 500 052

No. 26011/68/2015-16/HS-OM — Dated the 23rd December, 2015

ADVERTISED (OPEN) TENDER ENQUIRY

Sub: Implementation of Gate Management System for Library S.V.P National Police Academy, Hyderabad-Reg.

Dear Sir,

The S.V.P. National Police Academy, Hyderabad, intends to implement **Gate Management System with 3 Years onsite warranty** for the Academy.

2. Technical specifications & other terms and conditions of the above are enclosed herewith.

3. As such, if you are interested in supplying the above Gate Management system of desired features, you may submit your quotation duly indicating the cost of the equipment including all taxes and installation charges and other conditions such as warranty etc.

4. **Terms and Conditions** :

(a) **Technical bids and Commercial bids shall be in separate**, sealed envelopes, addressed to **The Director, S.V.P National Police Academy, Shivrampally, Hyderabad- 500 052**. The envelopes containing the respective bids should be super-scribed **"Technical bid: to be opened by addressee only"** and **"Commercial bid: to be opened by addressee only" at the top**. Both the envelopes should then be placed in one single, sealed envelop super scribed **"Gate management System to S.V.P National Police Academy, Hyderabad"**. On the left side near the lower corner of the envelope, the address of the tenderer(s) should be written.

(b) Technical bid should include information related to all specifications sought. It should also contain company brochures of all equipments and should be accompanied by relevant technical documents issued by the manufacturer in support of specifications asked for.

(c) Firms should be submitting only required documents in technical bid. Checklist of all the important Numbering of all the pages of technical bid is necessary. Checklist of all the important documents should also be enclosed in the technical bid.

(Contd..2)

(d) Tender should be accompanied by a Demand Draft to the value of **Rs.1,30,000/- (Rupees One lakh thirty thousand only)** towards Earnest Money deposit in the favour of 'THE DIRECTOR, SVP NATIONAL POLICE ACADEMY, Hyderabad, except those who are registered with Central Purchase Organisation, National Small Industries Corporation (NSIC) or the concerned Ministry/ Department. **Tender not accompanied by earnest money will not be considered and will be summarily rejected.**

(e) Delivery/Installation is to be completed within 90 days from the date of Purchase Order failing which, penalty @ 0.5% of the Purchase Order value will be recovered for every week period delay from the final payment. Further in case of inordinate delay of 90 days from the date of Purchase Order, this purchase order stands cancelled without any further notice and you will also be liable to be blacklisted.

(f) After the expiry of the stipulated delivery period, which includes extension period if any, no item shall be accepted by SVP NPA. If the tenderer applies for the extension of the delivery period, the extension can be granted on valid grounds only once and up to a maximum of 30 days.

(g) Payments would be made only after the receipt of all the items ordered in the supply order. In cases, where part supply has been made and the supply order for the remaining items has been cancelled, payment would be made for the supplied items after deducting the penalty, if any.

(h) No interest will be allowed on the earnest money or security deposits so remitted and no claim shall be entertained in respect of the same. It may specifically be noted that ordinarily payment will be made only after full supplies are completed as per orders and that no advance payment can be arranged.

(i) If the tenderer fails to supply goods within stipulated delivery period then the supply order will stand cancelled and the security deposit shall be forfeited. In addition, the tenderer may be blacklisted for a definite period to be decided by SVP NPA, during which no supply order would be given to the blacklisted tenderer. In this case, order for the same product(s) will be awarded to the L2 tenderer based on the same documentation & processes.

(j) During the implementation a few items may be increased / decreased by 10% -15% as per actual requirement. Vendor should be able to supply these items at the unit rate quoted for these items.

5. **Price Bid**.

(a) Prices mentioned in purchase order are till the execution of the order by the firm. Increase in price, if any, subsequently shall not be entertained.

(b) The quantity of order may vary and the Academy has the right to increase or reduce the required quantity.

6. **Taxes**. Prices quoted should be Inclusive of all taxes.

(Contd..3)

7. **Pre-Tender Qualifications**:

(a) Firm Registration Certificate.
(b) Sales Tax clearance / VAT Registration.
(c) The vendor must have minimum 2 live site in India, where proposed Gate Management System integration with RFID Based vehicle / visitor management is in operation at least for last 2 years. Provide satisfactory certificate from client.
(d) Banker details.
(e) Bidder should have minimum of 10 Cr Annual Turnover
(f) ISO Certification for the vendors firm is desirable
(g) All quoted products should be of reputed brand with necessary certifications.

8. Further on accepting your offer and on placing purchase order, you will submit Security Deposit of the amount about 5% of the purchase order value, in the form of a Bank Guarantee/ FDR drawn in favour of **'The Director, S.V.P National Police Academy, Hyderabad'** within 15 days of receiving the purchase order.

9. The Academy reserves the right to accept or reject the tenders without assigning any reason thereof.

10. Your quotation along with the requisite EMD, technical brochures/information leaflets shall be sent in a sealed cover addressed to the undersigned and duly superscribed as **'QUOTATION FOR IMPLEMENTATION OF GATE MANAGEMENT SYSTEM TO S.V.P. NATIONAL POLICE ACADEMY – NOT TO BE OPENED BEFORE 16-01-2016.**

11. The last date for receipt of quotations is 15-01-2016 **(Friday) by 17.00 Hrs**.

Yours faithfully,

(K Shankar)
Admn. Officer (Admn.)

Copy to: Copy to Programmer with a request to please get the above requirement posted in NPA Website and provide a link with NIC web-site.

Technical Specifications for implementation of

Gate Management System

The Academy is planning to implement Access/Gate Management System at the main entrance of the gate for recording the entry / exit of the 1000-1500 staff, visitors, contractors and labours daily. About 300-500 people & about 100 vehicles other than regular staff of NPA enter through the gate daily. In this connection, the Academy has invited tender proposal from various vendors for submitting their competitive bids duly indicating the products / solutions that meets the Academy's requirement. As part of the requirement It is proposed **to implement Visitor Management, Vehicle Management, Gate Access Management with Flap barrier, Boom barrier, Under Vehicle Scanner System with local control room, as well as remote control room.**

The bill of material is given below indicating the quantity and purpose of the item. The specified models are indicative, the vendors should supply required brands with matching specifications.

Bill Of Material(BOQ) for Gate Management System

SN	Item Description	Make / Model	Qty.	Unit	Purpose
	1.Visitor Management and Access Control System				
1	Network Controller,V1000	HID	1	No	Use to control Door Interface / Reader Controller , provide Network disconnect architecture
2	Webcam	HP / Logitech/ Targus	1	nos.	For Capturing Visitor Images
3	Signature Pad	Iball / SIGMATEK	1	nos.	Capturing Visitor Signatures
4	IO box with IO	Systimax / AMP	3	No	For connecting Pc with Patch Cord, two for above mention two pc and one for server
5	Reader Controller	HID	2	no's	Use to Control Smart Card Reader, Each Door Interface will control two Smart Card Reader
6	Smart Card Reader	HID	4	no's	Use to Control Flap Barriers and Turnstile to granting authorized access, Each gate will Carry two Smart Card Reader one for Entry and One for Exit
7	Flap Barrier double lane with all accessories	Specifications given separately	1	nos.	For Visitors IN/Out
8	junction box with accessories	Standard	1	Set	For Power cable termination at field
9	Power Cable un armoured-3 core 1.5 Sq mm	Finolex/Delton/Usha	1	Mtr	To power the equipments
10	Control Cable- 1 pair twisted ,shielded	Finolex/Delton/Usha	1	Mtr	For Data Communication

11	Control Cable-10 core .75 sqmm	Finolex/Delton/Usha	1	Mtr	For Data Communication
2. Vehicle Management System					
12	Under Vehicle Scanner with Driver Image Capture ,Automatic License Plate Reader and other accessories	Specifications given separately	1	no	For under vehicle scanning, number plate capturing and driver image capturing of vehicles
13	RF- Reader	Specifications given separately	2	no's	For to Control Boom barrier and Access to valid RF ID Card holder vehicle,one for Entry Gate and One foe Exit Gate
14	Pole For RF reader	Standard	2	no's	Two poles to fix two RF Id reader
15	Boom Barrier	Specifications given separately	2	no's	Two Boom Barriers for access control to the vehicle one at Entry Gate and Other at Exit Gate
16	Loop Cable- 1.5sq mm Multistand cable	Standard	130	mtrs	
17	Fixed HD Outdoor IP CCTV Camera	Specifications given separately	3	no's	
18	PTZ HD Outdoor IP CCTV Camera	Specifications given separately	1	no	
19	16-Channel NVR	Specifications given separately	1	no	
Local Control Room(LCS)					
20	MOP for Gadget with Push buttons	Specifications given separately	1	no	Mannual Operating Pannel to operate Gadgets mannually
21	Power Extension board	Anchor/ Havell	3	nos.	Use for Electric Supply at diiffrent Points
22	Information Outlets box	Systimax / AMP	3	nos.	For connecting Pc to the network
23	Network Rack 16U with all accessories	Standard	1	nos.	For mounting Switch,patch Pannel etc
24	PDB with MCB	Havell / Legrand	1	sets	Power Distribution
25	Accessories		1	nos.	Network Connectivity
26	Patch Panel 16 Port	Standard	1	nos.	To Terminate Network cable/cat 6
27	Network cable	Systimax	1	mtr	Network Connectivity
28	Power Cable armoured-3 core 1.5 Sq mm	Usha/delton/ Finolex	1	mtr	To power the equipments
29	Control Cable armoured-1 pair twisted ,shielded	Usha/delton/ Finolex	1	mtr	For Data Communication
Main Control Station(MCS)					

30	Rack 42 U	Standard	1	no's	For Mounting, Network switch, patch panel etc
31	Network cable	Systimax / AMP	1	mtr	1 box
32	Power Cable armoured-3 core 2.5 Sq mm	Usha / Delton / Finolex	1	mtr	Power Distribution to field equipments 100 mtrs
33	Network Accessories		1	Lot	For Networking
34	Smart Card	HID Mifare	500	no's	For Granting access to doors
35	Smart Card Programmer	HID	1	No	To program smart card
36	Smart Card Printer	HID Assure ID	1	No	To print information on smart card
37	Printer Cartridge with Ribbon	HID Assure ID	5	no's	To use in printer
38	PDB with MCB	Standard	1	Lot	Power Distribution
39	Patch Panel 24 Port	Systimax	1	No	Networking accessories
Installation					
40	Supply , Installation, Testing and Comissioning of the Integrated System.		1	Lot	
41	Training and Documentation		1	Lot	
Software					
42	VMS Software (including Pass Generation, Appointment generation & Access control Module		1	Lot	
43	Access Control System for Employee		1	Lot	
44	Vehicle Management Software Including Gadget operation, RFID system		1	Lot	

1. The detail specifications are given below for some of the products listed above mentioning the line item number. The vendors may note that **The physical specifications can vary by +/- 10%. Such deviations should be mentioned clearly.**
2. All equipment should have a lifetime of 10 years and OEM should able to supply the spare parts and give full support for the next 10 years. OEM certificate should be enclosed for each such component.

#1. Network Controller – to control door interface / reader control

S.N.	**Specifications**
1	Should Provide an open architecture family of interface devices that provides a complete and fully functional hardware/firmware infrastructure for access control software host systems.
2	The Master Controllers shall communicate with a host system by using industry standard TCP/IP protocol, over 10/100 Mbps Ethernet, Internet.
3	The Master Controller shall have two RS-232 ports, which shall allow fallback communications with the host system in the event of loss of the network (TCP/IP Ethernet) by means of dialup modem or wireless modem
4	The Master Controller should communicate with the Reader Interfaces using RS485
5	The controller should be based on minimum of 64 MB RAM, ARM 9 processor, 200 Mips Speed 100 MHz Microcontroller running the Linux 2.6 Operating System
6	Secure Shell and Transport Protocol (SSH/SCP) enabled. The Master Controller should support and communicate with 32 Reader Interfaces
7	The controller should have minimum of 256 MB On-board flash memory allows program updates to be downloaded via the network
8	TCP/IP connections shall be used for high speed connection to host and connectivity to existing and new Ethernet network cabling.
9	The Master Controller shall control and communicate with all RS-485 connected devices when offline with the host.
10	The Master Controller should interface with combinations of devices with a maximum of: • 32 Door/Reader interfaces (up to 64 doors/readers) or • 32 input monitor interfaces 9 (up to 512 monitor points) or • 32 output control interfaces (up to 384 control relays)
11	Fully featured access control hardware and firmware infrastructure for host-based access control software applications.
12	The products shall not be a proprietary product of the manufacturer of the host access control software application, and must have the ability to migrate to an alternative manufacturer's host access control software application by remote reconfiguration or firmware upgrade and without intervention from the original Master Controller manufacturer. Master Controller Should Support Multiple Applications from various manufacturers.
13	Should provide full distributed processing of all access control functions. The unit shall provide fully functional off line operation when not actively communicating with the host access control software application; performing all access decisions and event logging. Upon connection with the host access control software application, the networked door Master Controller or networked Master Controller/reader shall upload all buffered off-line transactions (minimum of 99,999) to the host software.
14	Should provide diagnostics and configuration operations through connection to a local laptop computer
16	Visual Indicators - Power LED to indicate that sufficient DC voltage is being provided to the unit. solid green to indicate successful communications to

	downstream devices, red flash to indicate a failed communications attempt, solid red to indicate no communications.
17	The Master Controller shall be compatible with the following: 1. Microsoft Windows 7, XP and any other Host System supporting TCP/IP networked interface 2. TCP/IP (using applicable IEEE standards) 3. Category 5 Cable, using RJ-45 connectors 4. Wiegand Standard or Long Card Formats or C&D Output Readers (up to 128-bit data) 5. ODBC Systems and any other data storage systems whose data can be translated for transport over TCP/IP interface.
18	The Master Controller should be able to report supervised inputs/alarms with minimum of 255 priorities
19	The Master Controller shall be designed to have a lifetime of minimum ten years based on normal usage levels and environmental conditions. This shall include components such as batteries, real time clocks and non-volatile memory Regulatory Compliance a. UL Standards 1. The Master Controller should provide input monitoring and reporting functions meeting applicable UL 1076 Proprietary Burglar Alarm System standards as a UL Recognized system component, including specific requirements for speed of reporting time, verifying communications with field hardware, detection of substitution of similar field hardware device, four-state alarm monitoring. 2. The Master Controller Should meet applicable UL294 Access Control standards as a UL Recognized system component, including criteria for false accepts/rejects, attack resistance and electrical safety. b. CE Mark - The Master Controller should meet European CE Mark standards for electrical safety and RF emissions.
20	The Master Controller Should have communications Indicator LEDs, which flash whenever communications occur between the interface unit and an upstream device. The communication LED flash codes are as follows: 1. Communications TO the upstream device is green flashing. 2. Communications FROM the upstream device is red flashing. 3. Absence of one color indicates that communications are occurring in one direction only. 4. Absence of flashing indicates a communications failure.
21	The Master Master Controller Should have a voltage indicator LED on the interface unit, which shall indicate that sufficient DC voltage is being provided to the unit.
22	The Master Master Controller should be capable of using beepers in the connected held/forced, PIN Retry Error, Tamper Alarm, Communications Failure, AC Power Failure, Battery Failure, etc.
23	The Master Master Controller should include a dedicated input for enclosure tamper configurable to be supervised or unsupervised.
24	The Master Master Controller should have configurable inputs for AC Failure and Low Battery/ Battery Presence, which are compatible with Supervised DC supplies which monitor the AC Input Voltage and Battery Voltage and report status using two dry contact relay outputs.
25	Mounting a. The Master Master Controller should be capable of mounting on any flat wall surface, using the appropriate fasteners. They shall be directly mountable in their standard plastic housings, or they shall be mountable in a stacked configuration on non-conductive standoffs inside a customer supplied utility box. b. The Master Master Controller should be installed indoors, inside a secure area,

	such as in a utility closet or on a wall above a suspended ceiling.
26	The Master Master Controller should work using customer-supplied 12VDC regulated Power Supply, with Battery Backup and Input Surge protection, and AC Failure and Battery Low contact outputs.
27	The Master Master Controller should be be capable of operation from 0° to 50° C (32° to 120° F), 0-95% RH, Non-condensing.
28	The Master Master Controller should be capable of installation in an indoor environment, or otherwise protected in a NEMA-4 Rated Enclosure.
29	General Functional Description 1. The Access Master Controller should control cardholder access to secured areas. 2. The Access Master Controller should monitor and report access control activity. 3. The Access Master Controller should monitor and report input status changes pertaining to intrusion alarms. 4. The Access Master Controller should monitor and report the integrity of all network devices, circuits and communications. 5. The Access Master Controller should control various electrical and annunciation devices. 6. The Access Master Controller should enable a host system to allow a human operator to acknowledge and respond to alarm conditions. 7. The Access Master Controller should enable a host system to allow a human operator to configure the network and obtain configuration and historical reports. 8. The Access Master Controller should enable a host system to allow an operator to manually unlock and lock doors, and to shunt or unshunt input points.
30	Functional Description for Access Control Access Schedules and Holidays a. The Master Controller should provide access control based on access groups, which shall consist of groups of readers and schedules which can be named and assigned to cardholders. b. The Master Controller should allow cardholder to have one or more access control schedules consisting of a valid time period for valid days of the week, for a given reader (or group of readers). c. The Master Controller should provide a time schedule for each week day (Sunday through Saturday) and the cardholder shall also have a time schedule for up to 255 Holiday Groups, allowing Holidays to be assigned different schedules than those normally used for a given day of the week. d. The Master Controller should allow a list of Holiday calendar dates and types to be entered into the networked Master Controller. e. The Master Controller should allow any card to have a start and end date in addition to access groups such that the card shall be denied access outside the start-end period. f. The Master Controller should Schedules to be assigned to other functions such as input group suppression or output group activation
31	Extended Access Time a. The Master Controller should be capable of providing configurable normal and extended access times. b. The Master Controller should be configurable such than any designated card may have extended access time at readers also configured to provide extended access times. A second relay may also be actuated to control a powered door opener.
32	Parity Checking - The Master Controller should perform parity checking on card data, and shall notify the network device on parity failure.
33	PIN Processing a. The Master Controller should allow Card/PIN readers to be configurable to

	require Card+PIN, PIN only, Card or PIN, or Card only. b. The Master Controller should provide PIN Suppression schedules, so that a PIN/Card readers can operate in Card-only mode on a scheduled basis, such as during the day when higher security is not required. c. The Master Controller should be capable of signaling the cardholder with an alternating red/green LED on an card readers when a Card is presented and PIN is also required. d. The Master Controller should invoke a configurable PIN Error lockout period of up to 99 seconds, which shall prevent the reader from being used after a configurable number of incorrect PINs have been attempted. Anti-Tailgating - The Master Controller should be capable of invoking the Relay Timer and Alarm Shunt timer to be cancelled 100 ms after the Door Monitor input senses that the door is closed.
34	Facility Code Only - The Master Controller should be configurable to provide access on the basis on facility code only when communications with the network interface are lost; alternately the reader interface shall be configurable to deny access to all when communications with the network interface are lost.
35	REX Processing a. The Master Controller should include a Request to Exit (REX) Input for each controlled door, which is used to suppress the Door Monitor alarm, and optionally, unlock the lock for an authorized entrance or exit without the use of a card. b. The Master Controller should allow the Green LED at the associated reader to be suppressed during REX activation, to avoid alerting potential intruders when the door has been unlocked from the inside
36	Anti-Pass back a. The Master Controller should allow Anti-Passback to be implemented in one of two modes: Real and Timed. b. When implemented in Real mode: 1. The Master Controller should provide that when Real Anti pass back is implemented, each cardholder's APB status can be defined as IN, OUT, UNDEFINED and EXEMPT. 2. The Master Controller should allow an area to be defined by reader-controlled entrances and exits. Readers may be designated as IN or OUT readers. 3. The Master Controller should deny access to a card which is re-used at an IN reader prior to badging at an OUT reader. Alternatively, the family of products can be configured to grant access while logging an Anti-Passback violation at an IN reader, subsequently denying access when the cardholder attempts to exit the Anti-Passback area at an OUT reader. c. When implemented in Timed Anti-Passback mode: 1. The Master Controller should provide timed antipassback, which prevents a card from being used in a reader (or group of readers) until a configurable timer expires. 2. The Master Controller should allow any cardholder to be designated exempt from Anti-passback.
37	Area Control a. The Master Controller should provide Area Control, such that readers which control cardholder access or egress to a contiguous area and/or perimeter are logically associated in software. b. The Master Controller should keep track of which cardholders have entered or left an area. c. The Master Controller should be capable of denying access based on incorrect progression of cardholders through controlled areas.
38	Card Formats a. The Master Controller should be capable of accepting multiple card formats, allowing multiple existing card populations to be merged into the same network. b. The Master Controller should be able to accept card format files downloaded from the host. C. The Master Controller should be able to accept 255 types of formats at a time.

39	Visitor Control - The Master Controller should allow cardholders to be designated as visitor cards, which shall be assigned to an escort card such that badging by visitors shall also require an escort badging to obtain access
40	Elevator Control a. The Master Controller should provide Elevator Control by using a Card/PIN reader to control relays, which in turn can enable or disable elevator floor call buttons. This should be accomplished by assigning output control relays to be to specific floors, and by allowing cardholders to be configured for access to specified floors and schedules. b. The Master Controller should defined elevator control components as 1. A designated reader located in the Elevator Cab. 2. A reader interface device. 3. One or more Output Control Devices, with relay outputs connected to logic inputs of the elevator control equipment. 4. Designated cardholder with an associated predefined group of output relays. c. The Master Controller should allow card badging to invoke timed relay closures which enable the floor call buttons in the elevator, allowing the user to press the desired floor call button(s). d. The Master Controller should have the reader located in the elevator cab, and the Output Control Devices located in the Elevator Machine Room. e. The Master Controller should allow Elevator Control to be implemented on a schedule, such that certain floors shall be configured for public access during normal business hours, and a card shall not be required to use them. Some or all floor call buttons may be restricted at night and/or on weekends, so that a card is required to use them. Certain floors shall always require a card for access. f. The Master Controller should allow Elevator Control access privileges to be assigned to cardholders for specific Floors.
41	Elevator Control - The Master Controller should allow biometric readers to be used, where the biometric template is recorded on a smart card, and the biometric reader compares the stored template with a live biometric read. If the live read compares with the stored template, the reader sends access control data from the card to the reader interface
42	Card Control - The Master Controller should allow keypad commands to lock or unlock the door –through command entry
43	Functional Description for Input Point Monitoring a. The Master Controller should provide Input Points to monitor switch contact status changes. All inputs shall be capable of being supervised, with a specified resistor value wired both in series and parallel with the switch and a voltage applied to the circuit, allowing an input to be reported in any of three states: Normal, Off-Normal and Alarm. b. The Master Controller should also provide two-state inputs that report either OPEN or SHORT as the active state. 2. Input Point Groups a. The Master Controller should provide input points that can be logically grouped in software to allow simultaneous control. b. The Master Controller should enable input reporting of any point or group of input points to be suppressed on a Scheduled basis. For example, this can be used to disarm intrusion or door-open detectors during the day. 3. Input Point Status a. The Master Controller should provide input points that shall be configurable such that the normal or off normal state of any given input can be set for NO or NC devices. b. The Master Controller should provide input points that shall be configurable to match the EOL resistance used with any input. c. The Master Controller should allow the host system to query the digital representation of the DC voltage present at any input. d. The Master Controller should allow status changes to be reported to the Host in

	0.5 Seconds or less. (This may be subject to Network conditions.)
44	Network Communications a. The networked Master Controller should have TCP/IP connectivity. b. The Master Controller models should send a periodic "I'm Alive" message to the host at configurable intervals. d. The Master Controller should have a firewall which can be used to restrict access thru the TCP/IP port. e. The Master Controller should be capable of deploying AES 256 with symmetrical key encryption for all communications between the Master Controller and host(s) system(s).
45	Reader Supervision - The Master Controller should be capable of monitoring a periodic Reader Supervision message from a reader with this capability, and shall send a reader offline message to the Host, if the message is not received in the event of reader failure or tampering.
46	Clock Synchronization - The Master Controller should allow all networked Master Controllers to be synchronized with the Host. Time Sync shall be sent automatically at regular intervals.
47	Host Control Commands Support by the Access Master Controller a. The Master Controller should be able to execute operator or system commands received via the Network from the Host, including: 1. Open Door – specify door name – unlocks door, shunts associated alarm, for locally programmed unlock times -- door relocks automatically when timers expire -- overrides any restrictions 2. Open a Group or list of doors – same as open door – specify door group or list 3. Open all Doors – same as above 4. Unlock Door (or group/list, or All doors)– specify door(s) – unlocks doors indefinitely -- usually used in an emergency situation -- overrides any restrictions 5. Lock Door (or group/list, or All Doors) – resets Unlock Door --overrides any current/pending "door unlock by time schedule" controlled at the interface level 6. Set Output Relay – latch a relay, or group/list of relays indefinitely 7. Reset Output Relay (or group/list) 8. Suppress Input Point (or group/list) – disable reporting/logging from a specified input points 9. Un-suppress Input Point (or group/list) 10. Reset Various Local Alarm conditions (as annunciated by aux relay or reader beeper) including: a. PIN Code error count b. Door Held c. Door Forced
48	a. The Master Controller should allow the Host System to query any local database for status or configuration information. b. The Master Controller should contain persistent application and data storage, allowing them to be reprogrammed from the Host if necessary. c. The Master Controller should be capable of receiving a command from the Host system operator which shall manually override any locally-invoked relay condition, in either latched or timed mode. d. The Master Controller should be capable of receiving a command from the Host system operator which shall manually override the condition of any Aux relay. It shall also be capable of enabling, disabling or resetting any individual alarm. e. The Master Controller should be capable of receiving a command from the Host system operator which shall manually activate or release the Hold line on any connected reader having the Hold feature. f. The Master Controller should allow the Host system to query any reader, output or input interface as to the application file revision, EEPROM file revision, ID number, and type.

	g. The Master Controller should allow the Host to set time of day on all Network Gateways, to view add or modify card records, to control outputs, to get input or output status, to write to the EEPROM, to read local memory, to get A/D values, to upload the current messages or all messages in the Event log, to clear the event file, to reload the card database, to reload access configuration files, to get or set I/O linker inputs, to reboot any interface. h. The Master Controller should report the current state of each input and output upon query from the host.
49	The Master Controller should be capable of sending the following event messages to the host system for event log 1. Access Granted 2. Access Granted PIN only 3. Extended Access Granted 4. Deny Access Card not found 5. Deny Access Door Schedule Not Valid 6. Deny Access Unknown Reader 7. Deny Access Card Deleted from database 8. Deny Access PIN not found 9. Deny Access PIN deleted from database 10. Deny Access Wrong PIN used 11. Deny Access Timed Antipassback violation 12. Deny Access Real Antipassback violation 13. Deny Access Real Antipassback violation at Exit Reader 14. Deny Access Area Violation 15. Deny Access Area Violation at Exit Reader 16. Deny Card Access – Not in Door Group
50	The Master Controller should be capable of sending the following alarm messages to the host system: 1. Door Forced 2. Door Held 3. Tamper Failure 4. Tamper Alarm 5. Battery Failure 6. Battery Alarm 7. AC Failure 8. AC Alarm 9. REX Door Bit 10. REX Door Alarm The Master Controller should have configurable command priorities for each event type. The Master Controller should optionally be encrypted to prevent data from being intercepted or simulated by an intruder
51	The Master Controller should have non-latching relay outputs for the following: a. Two (2) door locking devices (configurable) b. Two (2) auxiliary devices (door held/forced alarm, alarm shunt, communication failure, or general purpose)
52	The Master Controller should have local processing capabilities as follows: a. Alarm Shunt and Strike relay timing and latching functions b. Access control decisions based on facility code (degraded mode) c. Simple input/output linking on the same V100

	d. LED / Beeper control during Card + PIN and other transactions
53	Communication Ports : RS-485 – two wire; TCP-IP – one port, 10 or 100 Mbps
54	Power Supply Requirements - 140 mA @ 12-18 VDC
55	Operating Environment - Indoors or customer supplied NEMA-4 rated enclosure
56	Temperature - 32° to 122° F (0° to 50° C)
57	Humidity - 5% to 95% relative, non-condensing
58	Certifications UL 294 and UL 1076 Recognized Component, FCC Class A Verification, EMC, CE Mark,

#3. Signature Pad

S.N.	**Features**	**Required Parameter**
1	Sensor Type	Electromagnetic Resonance
2	Sensor/ Pen Technology	Battery free pen on tempered glass
3	Pen Type	Wireless and tethered Pen
4	Signing Area	3.8" x 2.4"
5	Data Conversion Rate	200 Points or higher
6	Resolution	2540 LPI or higher
7	Software	Inclusive
8	Connectivity	USB 2.0
9	Text Display	1024 Pen pressure

#5. Reader Controller

S.N.	**Specifications**
1	The reader interface device should perform all of the basic input / output and access control functions for two doors (or one door with entry and exit readers).
2	The reader interface device should connect to a Master controller via an RS-485 network, and shall have a rotary address switch (Range: 0 - 15).
3	The reader interface device should have the following IO connections: a. Two (2) Readers, in one of the following configurations: 1. Two (2) Wiegand interface readers with or without PIN keypads 2. Two (2) Clock-and-Data readers 3. Two (2) Keypad readers b. Two (2) Door Monitor switch/contact inputs c. Two (2) Request-to-Exit device inputs d. AC Fail (if provided by power supply) Monitor input e. Battery Fail (if provided by power supply) Monitor input f. Enclosure Tamper Monitor input
4	The reader interface device should have non-latching relay outputs for the following: a. Two (2) door locking devices (configurable) b. Two (2) auxiliary devices (door held/forced alarm, alarm shunt, communication failure, or general purpose)
5	The reader interface device should have local processing capabilities as follows: a. Alarm Shunt and Strike relay timing and latching functions

	b. Access control decisions based on facility code (degraded mode) c. Simple input/output linking on the same Reader Interface d. LED / Beeper control during Card + PIN and other transactions
6	Enclosure Material: UL94 Polycarbonate
7	Communication Ports RS-485 – two wire
8	Power Supply Requirements - 140 mA @ 12-18 VDC or better
9	Operating Environment - Indoors or customer supplied NEMA-4 rated enclosure
10	Temperature - 32° to 122° F (0° to 50° C)
11	Humidity - 5% to 95% relative, non-condensing
12	Certifications UL 294 and UL 1076 Recognized Component, FCC Class A Verification, EMC, CE Mark,

#6. Smart Card Reader

S.N.	**Specifications**
1	The contactless smart card reader(s) shall be designed to securely read, interpret, and authenticate access control data from 13.56 MHz contactless smart card credentials
2	Customized security protection through support of the device-independent Secure Identity Object™ (SIO) portable credential methodology to provide enhanced security and performance features
3	Unique read selection that enables reading of the Secure Identity Object™ (SIO) and standard iCLASS technologies
4	Participates in an advanced, bounded and trust-based security system utilizing the Trusted Identity PlatformTM (TIP) architecture
5	Guaranteed compatibility to read all data formats and ensuring card-to-reader interoperability in multi-location installations and multi-card and reader populations when used with Genuine products
6	Backwards compatibility with legacy 13.56 MHz contactless smart card access control formats (E.g. 26-bit, 32, 35-bit, 37-bit, 56-bit). Compatibility across the product line shall be assured without the need of special programming The contactless smart card reader shall be Secure Identity Object™ (SIO) enabled. The contactless smart card reader platform shall support the standards-based, device-independent Security Identity Object™ (SIO) portable credential methodology to ensure data authenticity and privacy. The SIO shall be able to reside on any number of identity devices, including iCLASS SE, MIFARE Classic SE, and MIFARE DESFire EV1 SE credentials
7	The contactless smart card reader shall be a certified end-point (TIP Node) within a

	Trusted Identity Platform™ (TIP) infrastructure. TIP shall provide a scalable, on-demand, secure identity delivery system that validates, registers and provides lifecycle management support for certified trusted end-point contactless smart card readers
8	The contactless smart card reader shall increase security by narrowing the possibility of unwanted configuration changes and denials of service. The contactless smart card reader shall utilize TIP-enabled secure configuration of contactless smart card readers with counters and uniquely diversified configuration cards
9	The contactless smart card reader shall utilize Secure Element Technology™ to protect keys and cryptographic functions to the international standard Evaluation Assurance Level (EAL) 5+.
10	The contactless smart card reader shall be configurable to utilize Velocity Checking to provide breach resistance against electronic attacks that invoke multiple improper authentication attempts
11	The contactless smart card reader shall be configurable to provide multiple hierarchical degrees of key compatibility for accessing the smart card access control data.
12	The contactless smart card reader shall simplify troubleshooting through Anti-passback Notification that the card has already been processed and it must be removed from reader field temporarily prior to processing again
13	The contactless smart card reader shall provide enhanced user feedback options through the use of clear and bright tri-colored LEDs configurable to support any three color combinations (RGB - Red, Green, and Blue).
14	The contactless smart card reader shall enable backwards compatibility with legacy 13.56 MHz access control formats (E.g. 26-bit, 32, 35-bit, 37-bit, 56-bit).
15	The contactless smart card reader manufacturer shall provide global, off-the-shelf availability
16	Contactless smart card reader shall allow the reader firmware to be upgraded in the field without the need to remove the reader from the wall through the use of factory-provided Programming Cards
17	Contactless smart card reader shall allow for secure installation practices through mounting methods utilizing tamper resistant screws
18	Contactless smart card reader shall provide the ability to transmit an alarm signal via and integrated optical tamper switch if an attempt is made to remove the reader from the wall. The tamper switch shall be programmable to provide a selectable action to provide a selectable action compatible with various tamper communication schemes provided by access control panel manufacturers. The selectable action shall include one of the following: 1. The reader open collector line changes from a high state (5V) to a low state (Ground). 2. During a tamper state, the "I'm Alive" message is inverted.

19	Contactless smart card reader shall provide ability of an on-line “I'm Alive” message so the reader's functional health can be monitored at all times when paired with a compatible access control panel
20	The contactless smart card reader shall provide customizable reader behavior options either from the factory, or defined in the field through the use of pre-configured command cards. Reader behavior programming options shall include: 1. Audio/Visual Templates for card reads, and attack detection. 2. Velocity Check timing and thresholds 3. Optical tamper actions 4. RF scan delay 5. Hold Mode 6. Intelligent Power Management 7. Key diversifiers 8. Key rolling 9. CSN output configuration 10. Data Model prioritization 11. Default LED color 12. Hold mode .
21	Contactless smart card reader shall provide the following programmable audio/visual indication: 1. An audio beeper shall provide various tone sequences to signify: access granted, access denied, power up, and diagnostics. 2. A high-intensity red/green/blue (RGB) light bar shall provide clear visual status. The light bar shall provide uniform distribution of light eliminating individual bright spots
22	Contactless smart card readers shall provide the following enhanced performance features a. The contactless smart card reader shall enable user prioritization of High-frequency/High-frequency credential reads. Technology prioritization shall synchronize a site's credential technology read priority to the access panel configuration while reducing unintended credential reads. b. The contactless smart card reader shall have the ability to provide consistent optimal read range by implementing an auto-tune function that adjusts for manufacturing tolerances to enhance consistency of performance from reader to reader. c. The contactless smart card reader shall be field programmable to provide secure upgrades for migration and extended lifecycle. d. The contactless smart card reader shall be designed as a system to provide optimal read range and read speed for increased access control throughput.
22	Contactless smart card reader shall provide enhanced environmental and sustainability features. a. The contactless smart card reader shall reduce power consumption by as much as 75% through the use of Intelligent Power Management (IPM) technology. b. The contactless smart card reader shall be manufactured with 10% recycled material to provide the potential of LEEDS building credits in new construction projects. c. Contactless smart card reader shall be fully compliant with Restriction of Hazardous

	Substances directive (RoHS) restricting the use of specific hazardous materials found in electrical and electronic products. The substances banned under RoHS are lead (Pb), mercury (Hg), cadmium (Cd), hexavalent chromium (CrVI), polybrominated biphenyls (PBB) and polybrominated diphenyl ethers (PBDE). d. Contactless smart card reader shall be manufacturers with 10.5% (Pigtail) and 11% (Terminal Strip).
23	Contactless smart card reader shall comply with the following 13.56MHz-related standards to ensure product compatibility and predictability of performance: a. ISO 15693 , b. ISO 14443A , c. ISO 14443B
24	Contactless smart card reader shall be suitable for global deployment by meeting worldwide radio and safety regulatory compliance including: a. UL294 (US) b. cUL (Canada) c. FCC Certification (US) d. IC (Canada) e. CE (EU) f. C-tick (Australia, New Zealand) g. SRRC (China) h. MIC (Korea) i. NCC (Taiwan) j. iDA (Singapore)
25	Contactless smart card reader shall provide the following typical contactless read ranges: a. 2.8" (7.1 cm) reading SIO on iCLASS SE Card b. 1.6" (4.1 cm) reading SIO on MIFARE DESFire EV1 SE Card c. 2.6" (6.6 cm) reading SIO on MIFARE Classic SE Card d. 1.5" (3.8 cm) reading SIO on iCLASS SE Tag or Fob e. 1.2" (3.0 cm) reading SIO on MIFARE Classic SE Tag or Fob
26	Operating voltage: 5 – 16 VDC, reverse voltage protected. Linear power supply recommended
27	Current requirements and power consumption: 1. 45 mA (Standard Power Mode) 2. 25 mA (Intelligent Power Management Mode) 3. 75 mA (Peak Current Draw) 4. 0.7 W (Standard Power Mode @ 16VDC) 5. 0.4 W (Intelligent Power Management Mode @ 16VDC)
28	Material: UL94 Polycarbonate
29	Operating temperature: -31 to 150 degrees F (-35 to 65 degrees C)
30	Operating humidity: 5% to 95% relative humidity non-condensing
21	Storage Temperature: -67 to 185 degrees F (-55 to 85 degrees C)
32	Weatherized design suitable to withstand harsh environments with a certified rating of IP55

#7. Flap Barrier Double Lane with all accessories

Items	Descriptions
Operation	Bi-directional
Protection	Three surface layers in accordance with special coating (zinc plus 2 layers of plastic coating)
Application	Indoor
Lane Width	900 mm
Lane Type	Double
Flaps	Regular lane: Soft Wing with steel reinforcement
Locking	Electromagnet locking with two optical sensors.
Throughput	25 to 30 persons per minute (excluding card validation time)
Power Supply	230+/- 10%VAC, 50 Hz
MTBF – Mean Time Between Failure	2 Million Cycles
Housing Dimension	Regular lane: L1300mm x W250mm x H 1035mm with Telescopic Flap.
Protection	Three surface layers in accordance with special coating (zinc plus 2 layers of plastic coating)
Power – Off/Emergency	Fail Safe Mode - Flaps shall automatically open during power failure. Also can be configured for Flaps to remain closed during power failure.
Duty Cycle	100%
Integration	Shall function in integration with Smart cards, RF Cards reader based access control systems, Bio-metric systems etc., Capable of Integration with the overall architecture of Surveillance & Access Control System
Temperature Range	-5°C to +55°C

#12. UVSS (Under Vehicle Scanning System) accessories specifications :

Line Scan Camera Specification

Resolution (Pixels)	3 Lines X 4080
Sensor Type	Tri-linear CCD (Mono/Color & Gigabit Ethernet)
Pixel Size (μm)	10.0 x 10.0 x 10.0 pitch
Synchronization	Via external trigger or free-run
Video Output Format	Dual pixel 8 bits or 10 bits or 8 bits RGB (selectable)
Exposure Control	Edge-controlled, level controlled or programmable
Mechanical / Electrical	
Power Requirements	12 VDC (±10%), max. 8.0W
Mount Type	F-mount, M58 x 0.75
Certifications	CE and FCC complaint
Housing Temperature	Up to 50°C
Software Environment	
Operating System	Windows 32 bit or 64 bit

Auxiliary Camera Specification

Camera	
Image Device	1/3 type progressive scan Exmor CMOS sensor
Number of Pixels	640 X 480 X 704 X 480 Pixels
Resolution	480 TV Lines
Sensor Type	CCD/CMOS Color Area Sensor
Video Format	NTSC/PAL
Power Supply	12 V DC
Image :Coded Image Size (H X V)	1280 x 1024, 1280 x 960, 1280 x 800, 1280 x 720, 1024 x 768, 1024 x 576, 800 x 480, 768 x 576, 720 x 576, 720 x 480, 704 x 576, 640 x 480, 640 x 368, 384 x 288, 320 x 240, 320 x 192 (H.264, MPEG-4, JPEG)
Video Compression Rate	H.264, MPEG 4, JPEG
Maximum Frame Rate	H.264: 20fps (1280 x 1024) /30 fps (1280 x 720) MPEG 4: 25fps (1280 x 1024) / 30 fps (1280 x 720) JPEG: 30fps (1280 x 1024) / 30 fps (1280 x 720)
Network Protocols	IPv4, IPv6, TCP, UDP, ARP , ICMP , IGMP , HTTP , HTTPS, FTP (client/server) SMTP, DHCP, DNS, NTP, RTP/RTCP, RTSP, SNMP (MIB 2)
Ingress Protection	IP 66
Analog Video Output Signal System	NTSC / PAL

ALPR Camera Specifications

Format	HDTV 720 P, day and night
Resolutions	1280 X 800 (1 MP) to 160 X 90
Image Sensor	Progressive scan RGB CMOS
Optical Size	1/4"~
Max Frame Rate	30 fps in all resolutions
Video Compression	H.264 (MPEG 4 Part 10/AVC) Motion JPEG
Pan / Tilt / Zoom	Digital PTZ, preset positions, guard tour
Shutter Time	1/24500 s to 1/6 s
Interface	IP
Memory	128 MB RAM, 128 MB flash
Lens Type	IR corrected, CS mount Lens
Focus, Zoom	Varifocal 3 - 8 mm: 72 28° View, F1.2, DC iris
Video Streaming	Multiple, individually configurable streams in H.264 and motion JPEG
Intelligent Video	Video motion detection, tampering alarm, audio detection
Operating Condition	Humidity: 20 - 80% Temperature: 0° - 50°C
Power	8-20 V DC or power over Ethernet (PoE) IEEE 802.3af

UVSS features :

The UVSS is able to capture very high resolution & complete composite underbody image of any vehicle passing over it, without the vehicle being required to be fully stopped, by using a high quality color Line-Scan Area Scan CCD camera, with resolution more than 4,000 pixels.
The UVSS is able to handle vehicles moving at different speeds ranging from 5-30Km/hr, while the composite image so captured by the system should be automatically and dynamically adjusted according to the speed of the vehicle using multiple loop based sensors.
There are three or more additional view cameras for capturing motion video images of the deeper hard-to-view areas of the underside, e.g. areas around suspensions, below the engine areas, side wall of fuel tanks & exhaust pipes etc.
The UVSS is capable of displaying a pre-stored image of the underside of the vehicle, for visual comparison purpose identified either by its License plate number automatically read by the system or by choosing the class/type of the vehicle by the operator. Also, the UVSS is capable of adding standard templates/images of different makes/models of vehicles, for ease of such visual comparison.
The UVSS system has a facility to take back-up of all the transactions to any usual backup/storage media and also able to print out reports.
Vehicle Detection The system is capable of automatically detecting a vehicle approaching the installed location by means of dependable and proven means.
License Plate Detection .
a)The system is capable of automatically detect license plate in the real time.
b) The system is capable of performing OCR (Optical Character Recognition) of the license plate characters (English alphanumeric characters in standard fonts).
c)The system is capable of storing JPEG image of the vehicle and license plate and enters the license plate number into Postage SQL database along with date time stamp and site location details.
d) System is able to detect and recognize the English alpha numeric License plate in all the standard fonts and formats of all four wheelers including cars, HCV, LCV.
e) The system Processing is real time i.e. the recognition of license number plates will happen instantaneously (within less than a second delay).
f) The system is able to process and read number plates of vehicles with speed even up to 40Km/hr.
g) The system is able to store Image of the vehicle approaching and leaving the location.
Vehicle Status Alarm
a) On successful recognition of the number plate, system is able to generate automatic alarm to alert the control room and also send mail and SMS to the authorized personnel for vehicles which have been marked as "Wanted", "Suspicious", "Stolen", "Expired" and also it has provision to add more categories for future need.
b) This system can be integrated with a boom barrier gate on site, if required.
Vehicle Log
a) This system is able to do easy and quick retrieval of snapshot and other data for post incident analysis and investigations.
b) This system is able to generate suitable MIS reports that will provide meaningful data and facilitate optimum utilization of resources, such as:
Total Vehicles registered
Total Vehicles not registered
Report of vehicle flow at each of the installed location for Last Day, Last Week and Last Month.
Report of the vehicle in the detected categories at each of the installed location.
c) The system has search option to tune the reports based on license plate number, date and time, site location as per the need.
d)The system has option to save customized reports for subsequent use.
e) The system provides advanced and smart searching facility of License Plates from the database. There is an option of searching number plates almost matching with the specific number entered (up to 1 and

2 character distance).
Vehicle Category Editor
a) The system has option to input certain license plates according to category like "wanted", "suspicious", "stolen", "expired", etc by authorized personnel.
b)The system has option to add new category by authorized personnel.
c)The system is able to update vehicle status in specific category by authorized personnel, i.e. on retrieval of stolen vehicle, system entry should be changed from "stolen" to "retrieved".
d)The system also has the option to specify maximum time to retain vehicle records in specific categories.
System Settings
a) System has provided an option for advanced users to tune the system parameters according to the requirement (lighting conditions, minimum Psize, etc.) along with its various other features.
b)The System has option to configure lane and data management settings.
List of Daily vehicle entering and exiting the Premises with complete MIS.
Summary Report indicating the Number of vehicle registered and not registered with date time and location.
The system has option to specify maximum time to retain vehicle records in specific categories.
Certification -CE Certified

#13. RF Reader

Operating temperatures	- 20C° to +50C°
Storage temperatures	- 40C° to +85C°
Protection level	I.P. 65
Relative humidity	90%, without condensing
Power supply	12 ~ 24 VDC - 18 W
Frequency band	2.45 GHz
Data rate (between tag &reader)	30000 kbps minimum
Number of reading channels	31 or more
Fault reading protocol	HDLC
Modulation type	BPSK
Rate of (Fault reading/Failure reading*)	1E-7/1E-4*
Radiated power	75mW - 200mW - 350mW
Nominal reading distance*	10m
Maximal reading distance	10m
Speed	up to 100Km/h
Approvals	EN 60950, EN 300489-1&3, EN 50364 ETS 300440 - CE 0536

#15. Boom Barrier

Lane width	5.0 m
Opening / closing time	2.2 s / 4.0 s
Power consumption max.	25 W / 30 W
Duty cycle	100%
Supply voltage	Wide voltage range 85 - 264 V AC
Frequency	50 - 60 Hz
Housing design	Powder-coated aluminium
Base frame	Powder-coated stainless steel
Protection class	IP 54
Compliant with	2004/108/EC, 2006/95/EC, 2006/42/EC, CE, UL 325
Temperature range	-30 to +55 °C
Standard colours	RAL 2000
Control unit	MGC

Control unit modularly extendable	Radio control and additional loop detector only
Number of digital inputs	8
Number of relay / digital outputs	6/4
Specified number of cycles	10 Moi

#34. Smart Card

S.N.	Specifications
1	The contactless smart card shall function as an access control card, used with access readers to gain entry to controlled portals and to hold identification information specific to the user.
2	The contactless smart card shall be a passive device, with an operating frequency of 13.56 MHz, and shall meet ISO 15693 and ISO 14443B2
3	The card shall contain a 64 bit unique serial number
4	Memory - 2 Kbits (256 bytes) EEPROM memory configured with 2 application areas.
5	Each application area shall contain a unique 64 bit diversified authentication key to reduce the risk of compromised data or duplicate cards. The contactless smart card and card reader shall require matching keys in order to function together. All radio frequency (RF) communication between card and reader shall be encrypted, using a secure algorithm
6	Wiegand card data, up to 84 bits in length, shall be encoded in Application Area 1 for use with access control systems
7	There should be compatibility with all available Access control formats (E.g. 26-bit, 32, 35-bit, 37-bit, 56-bit).
8	The contactless smart card will support programming and updating of custom applications after issue, using an appropriate reader/writer
9	Dimensions as per ISO 7810 specifications
10	Typical contactless smart card read ranges shall be 2.0-3.0" (5.0-7.6cm) with the proposed Reader.
11	Material and construction: PVC card materials. Card surface shall be glossy and of a material compatible with direct to card dye-sublimation or thermal transfer printing. Card construction shall meet durability requirements of ISO 7810 Operating Temperature: -40oF to 158oF (-40oC to 70oC)
12	Operating Humidity: 5% to 95% relative humidity non-condensing

#17. Outdoor IP fixed Camera

S.N.	Feature	Parameter
1.	Image Sensor	1/3" CCD/ CMOS/MOS/EXMOR Sensor
2.	Effective Pixels	1920(H) x 1080(V)
3.	S/N Ratio	>=50db
4.	Sensitivity	Color: 0.1 lux, B/W: 0.08 lux or better
5.	Shutter Speed	AES
6.	Wide Dynamic Range	ON/OFF, not <120dB
7.	Video Compression	Dual H.264high profile stream&Motion JPEG simultaneously or H.264 high profile stream.
8.	Image Resolution	Main stream: 1920x1080 @ 25/30fps

9.	Bit Rate	32Kbps-8Mbps at reduced band width CBR/VBR or better.
10.	Audio Compression	G.711/ G.726
11.	Audio Stream	Full Duplex, Bidirectional
12.	Supported Protocol	TCP/IP, UDP, RTP, RTSP, RTCP, HTTP, DNS, DDNS, DHCP, FTP, NTP, PPPOE,SMTP, UPNP,IPv4
13.	Data Storage	Video or Snapshot
14.	Standard	ONVIF protocol
15.	Alarm Trigger	Intelligent video motion detection and 3 external input
16.	Motion Detection	4 zones or Better
17.	Power Supply	12V DC
18.	Day/Night	TDN (True Day Night)
19.	PoE	IEEE 802.3af
20.	Lens Mount	C/CS Lens Mount with 5-50 mm or better IR corrected Megapixel lens
21.	Local Storage	Micro SDHC card; SD2.0 standard, maximum 32G
22.	Connector	RJ-45 10BaseT/100BaseTX; DC jack; 3Alarm Input / 1 Output;1 Audio In / 1 Audio Out
23.	Protection Class	(IP 66 Outdoor housing accessory)
24.	Operating Humidity	0 to 90% (non condensing).
25.	Operating Temperature	-10°C ~ 50°C
26.	Certification	UL& FCC and EMC-EN61000

#18 Outdoor IP PTZ Camera (30X or better optical zoom)

S.N.	Feature	Specification
1.	Image Sensor	1/2.8" or 1/3" CMOS/ CCD/MOS/EXMOR Sensor
2.	Optical Zoom	30x or better
3.	Number of Pixels (H x V)	1920 x 1080 (1080p) or better
4.	Wide Dynamic Range	On/Off, not <100dB
5.	S/N Ratio	>or = 50 dB (AGC Off)
6.	Minimum Illumination	0.05 lux (colour)/0.01 lux (B/W) or better.
7.	Focal Length	4.3to 129mm or better.
8.	White Balance	Auto/Indoor/Outdoor/ATW/Manual
9.	Iris Control	Auto/Manual
10.	Electronic Shutter	1/30~1/10k sec.

11.	AGC Control	Shall be available
12.	Back Light Compensation	On/Off
13.	Pan Travel	360° endless
14.	Tilt Travel	-15° to 185° or better.
15.	Manual Speed	0.5° to 100°/s or better.
16.	Presets	256
17.	Maximum Preset Speed	Up to 300°/s or better.
18.	Preset Tours	8 or Better
19.	Auto Pan	4 or Better
20.	Privacy Mask	16 or Better
21.	Auto Resume After Power Failure	Yes
22.	Home Function	Preset, Preset tour, Auto pan,
23.	Auto Flip	Mechanical/Digital/Off
24.	Digital Slow Shutter	On/Off
25.	Motion Detection	On/Off
26.	Day/Night: IR Cut Filter	On/Off
27.	Noise Reduction	On/Off
28.	Power Source	24 VAC ± 10%
29.	Power Consumption	50 W (with heater)
30.	Operating Temperature	-10°C to 50°C
31.	Relative Humidity	10% to 90%, non-condensing
32.	Waterproof Standard	IP66 standard (Outdoor)
33.	Video Compression	H.264 Main Profile
34.	Video Stream	Dual streamingofH.264 and MJPEG Constant or variable bit rate
35.	Video Resolution	Up to 1920 x 1080p
36.	Frame Rate	Up to 30/25 fps
37.	Audio Compression	G.711/G.726 ADPCM/AAC
38.	Audio Stream	Full-duplex, Bi-directional
39.	Interface	RJ-45, 10/100 Mbps Ethernet
40.	Supported Protocols	IPv6, TCP/IP, UDP, RTP, RTSP, HTTP, HTTPS, ICMP, FTP, SMTP, DHCP,PPPoE, UPnP, IGMP, SNMP, IEEE 802.1x, QoS, ONVIF
41.	Event Notification	HTTP, FTP, SMTP
42.	Micro SD	Support for Micro SDHC up to 32GB(card not included)
43.	Micro SD Function	Event trigger recording Continuous and scheduled recording

		Automatic recording when network fails
44.	Standards	ONVIF
45.	Certification	UL& FCC and EMC-EN61000
46.	Outdoor Protection	Vandal resistant IK10& IP66
47.	Other Features	Fog Compensation, Sand Storm Compensation
48.	Dome Clear Sight Feature	Rain Wash Coating/Super Dry Technology/Integrated Wipers
49.	Environment Protection	Inbuilt Heater& Blower or Dehumidification device

#19. **16 Channels NVR**

S.N.	Specifications
1	The NVR shall be capable of connecting to up to 16 network cameras without extra license fees and their images can be recorded simultaneously. IT shall be equipped with up to 2TB HDD
2	The NVR shall have quick intuitive search by calendar and timeline without PC
3	The NVR shall have optionally "Face matching function" with a face displayed on live images after registering the license
4	The NVR shall be viewable from any properly connected PC using Microsoft Internet Explorer version 7.0 or later
5	Supported protocols: TCP/IP, UDP/IP, HTTP, FTP, SMTP, DNS, NTP, SNMP, RTP, DDNS, RTSP over HTTP.
6	The NVR shall have the alarm history relating to the i-VMD of the camera: (1)Intruder detection, (2) Loitering detection,(3) Direction detection and (4) Scene change detection.
7	The NVR shall have dual recording function that enables to record same images and voices into two HDD.
8	The power source shall be 220 ~ 240 V AC, 50 Hz/60 Hz at approx. 45W
9	The NVR shall be certified CE , GOST : Safety/EMC Standard.