Particular Specification for Security and Access Control System

1. General
2. Scope of Works
3. System Description
4. Materials and Equipment
5. Commissioning and Testing
6. Warranty, Maintenance and Emergency Support Requirements

Particular Specification for Security and Access Control System

1. General

1.1 This Specification shall be read in conjunction with the Drawings, as well as other relevant sections of the General and Particular Specifications.

1.2 This Section specifies the design, manufacture, supply, installation, testing, and commissioning of the Internet Protocol (IP) and network-based Security and Access Control System, hereinafter called "SACS", and the performance requirements of the system. The Works shall also include labour and material as prescribed or as necessary except where expressly specified to be provided by others. It shall not only include the major items of plant and equipment shown or specified but also include all the incidental sundry components necessary together with the labour for installing such components for the complete execution of the Works and for the proper operation of SACS installation, whether or not these sundry components are stated in detail in this part of the Specification. It shall also include interface and co-operation with other Specialist Sub-contractors involved on the Site in the coordination, programming, scheduling and the sequence of installation of the Works under all circumstances where this is stipulated in this Specification or proves necessary in practice.

2. Scope of Work, Design Requirements, and Performance

2.1 The Works to be carried out under this Specification comprise the furnishing of all labour, materials, equipment and services for the supply, installation, project and construction management, supervision, testing, commissioning, handing-over, provide warranty and operation and maintenance requirements during defects liability period of the following systems and works as stated below and shown on the Drawings: -

a. Supply and installation of the complete SACS for doors along with all associated equipment and accessories.
b. Supply and installation of the complete SACS for security gates (turnstiles) along with all associated equipment and accessories.
c. Supply and installation of Uninterruptible Power Supply (UPS) to maintain 30 minutes duration for the operation of central equipment of SACS in the respective office.

2.2 The Contractor is required to appoint competent and experienced testing and commissioning engineering team, responsible for the overall planning, organizing,

coordinating, supervising, and monitoring of the testing and commissioning works and also certifying all results and reports from the testing and commissioning works.

2.3 The Contractor shall submit provide as-fitted drawings, comprehensive testing and commissioning documents, and O&M manuals.

2.4 Training of Employer's staff shall be provided.

2.5 Supply of Spares, tools, and accessories for the electrical and extra low voltage installations as specified.

2.6 Provide one year of comprehensive maintenance during the Maintenance Period including free supply of parts for replacement and consumables items after successful handover to the Employer or his appointed representative and supply essential maintenance spare parts and tools at no charge to the Employer or his appointed representative at handover. The essential spare part and tools shall not be less than those specified in the tender document.

2.7 The Works shall also include the submissions of the relevant manufacturers' catalogues and supplies for the proper appraisal and approval of the selected hardware items. Samples of all equipment shall be submitted to the Employer's representative for endorsement before ordering,

2.8 Prior to the equipment ordering and implementation, the Contractor shall submit the technical specifications and shop drawings of the Security System for comment and approval. The Security System shall fulfil the performance standard and the equipment sizes as stipulated in this Specification.

2.9 The Contractor shall furnish all labor and materials, equipment and services necessary for and reasonably incidental to the furnishing and complete installation of the Specialist Works as shown on the drawings and/or as specified herein.

2.10 The finished works shall be operational, clean, and free from damage and defects.

3. System Description

3.1 The system described in this specification specifies the minimum requirements and

general design intent. The Contractor shall be responsible for the system design to meet the performance requirement as specified and shall include any necessary accessories for a complete system.

3.2 The following sections will describe the installation requirements of SACS installation work. The description in this section may not necessarily describe the Works in full detail. Reference shall be made to other sections of this specification and tender drawings. Due allowance shall be made to include necessary fittings, auxiliaries and sundry items compatible with good trade practices to provide a complete and efficient system to meet the specified performance requirements.

3.3 All system designs, materials and equipment shall comply with the latest applicable patent and certificate of “Card Identification System with Scramble Coding Ability”, “Scramble Encryption in Data Communication”, and “Non-Transferred Identification System Using Scrambling Two Dimension Code” from Hong Kong Patents Registry Intellectual Property Department, and any relevant Authorities or Regulatory Bodies. Plagiarism is not allowed.

3.4 The SACS shall be in one software platform which includes: -

a. Access Control System
   i. One software and One database design.
   ii. The SACS server program can be installed on the cloud or on-premises.
   iii. The SACS can be running on the non-VPN network.
   iv. Software admin can create users who have different access rights for the cardholder and the controllers.
   v. Allow remote maintenance of access controllers, access control readers and time zones setting
   vi. Supports multi-technology (Bluetooth, Scramble QR Code, Palm Vein, Facial Recognition, RFID Card, NFC, Keypad, and Octopus) access control reader
   vii. Email notification for critical events
   viii. Integrated with NVR, swipe card playback and recording to the external device
   ix. Integrated with building visitor management system
   x. Integrated with facility room booking system
   xi. Integrated with lift destination control system
   xii. Integrated with video management system application
   xiii. Integrated with turnstile body temperature and Mask check

xiv. Integrated with mailbox/locker system
xv. Integrated with 3rd party building management system

b. Lift Control System
   i. Low-level integration with lift server panel
   ii. Access time zone control for the lift floor
   iii. User has access right for individual floor and the access time zone
   iv. Supports multi-technology access control reader
   v. Integrated with building visitor management system

c. Visitor Management System
   i. The visitor management system (VMS) can be applied to entire building tenants.
   ii. The VMS server can be cloud-based or on-premises.
   iii. Tenants can through the web browser or mobile apps to maintain the VMS.
   iv. The VMS server keeps all the visitor pre-registered records and the visitor access records.
   v. The VMS booking and access records can be auto-deleted in a certain period
   vi. The visitor management system is compromised by four applications, the VMS Server program (back-end), Web-based visitor management application (for tenants), PC-based client application (for concierge operator), and the optional iPad-based visitor application (for visitors). All program language displays shall have English, Traditional and Simplified Chinese.
   vii. The web-based application shall have an SSL certificate.
   viii. <u>The VMS server program</u>
      - The server program shall be integrated into the building access control and lift destination control system.
      - The VMS shall have API for 3rd party software integration.
   ix. <u>The web-based visitor management application</u>
      - The VMS has a super admin to create the tenant's admin
      - The tenant's admin can create their user account.
      - User can input visitor booking information through a web browser or mobile apps, e.g., Visit date and time period, number of entry access, etc. Once the booking is made, the user and visitor will receive an email individually, the visitor will receive a scramble QR code (web-link) as a temporary pass.
      - Tenant can import/export the visitor booking records.
      - Tenant can export the visitor check-in and check-out records.
      - The visitor temporary pass can be controlled by the access date/time range and the

number of accesses.

- The visitor's temporary pass can be represented by a scramble QR code.
- The visitor temporary pass can be delivered by email or SMS.
- The scramble QR code shall be activated during the valid access period
- Once the scramble code is activated, the scramble code cannot be activated on other mobile devices. The Sub-contractor shall be responsible for any Certificate or Patent document if required.
- The sub-contractor shall be responsible to comply with the latest applicable patent and certificate if required. E.g., "Card Identification System with Scramble Coding Ability", "Scramble Encryption in Data Communication", and "Non-Transferred Identification System Using Scrambling Two Dimension Code" from Hong Kong Patents Registry Intellectual Property Department, and any relevant Authorities or Regulatory Bodies. Plagiarism is not allowed.

x. <u>The Client application is for concierge operation</u>

- This is a windows-based application that allows the operator to check the pre-registered visitor record.
- A connected QR code scanner can read the visitor's pre-registered record
- The program can record down the walk-in visitor record
- The program can assign the building access rights to the visitor. E.g., Male / Female toilet access.
- Real-time time monitor of the visitor count in the building
- Email notification to the user if the visitor arrives.
- Provide emergency notification by email / SMS to the visitors who are in the building area.
- Connect to a QR code printer for printing the QR code label if necessary.

xi. <u>The iPad-based visitor application (optional)</u>

- The program can allow the pre-registered user to scan their QR code for the confirmation
- The program for the walk-in visitor to input the visitor and host information.
- Operator can assign the building access rights to the visitor (e.g., Toilet rooms etc.)
- The program shall be integrated with the building's turnstile, access control and the lift destination control system.

d. Facility Booking System
    i. Available to make room or facility booking on a computer via a web portal and smart device via APP
    ii. Integrated with Access Control System
    iii. Check room status and review all bookings online and outside the meeting room
    iv. Works with interactive touch display
    v. Able to generate and export workplace analytics report
    vi. Customization available
e. Shuttle Bus System
    i. User friendly platform for managing shuttle bus driver and passenger
    ii. Driver clock in via APP
    iii. Real-time checking of passenger's authority of taking a shuttle
    iv. Track record
f. Smart Locker / Mailbox System
    a) Architecture
        - This is a client-server software application which can run on WIN 10 or the latest windows version.
        - Server Program is a service in the PC server, once the PC server restart, the server program will run automatically.
        - Client Software has multi-language features which include English, Tradition Chinese, and Simplify Chinese.
        - Users can online change the software text content.
        - Unlimited client application installed, but the maximum number of concurrent user logins will be under control
        - Same database for storing Facial template, Palm Vein template, and card number.
        - Same software interface for managing Facial, Palm Vein, Virtual Card registration, and access control distribution.
    b) Communication
        - Server program uses multi-threading programming technique, which direct communication to access the control panel on Ethernet cable, real-time response.
        - TCP/IP communication.
    c) Data Security
        - User-defined 128 bits master key in Server and Panel for data encryption.
        - A unique 192 bits random key is generated per data transmission.

- Data encryption method, master key encrypts random key, random key encrypts the exchanged data during communication.
- AES128 and 3DES Algorithm mixed.

d) Database requirement
- MS SQL 2019 or above

e) Application user authority
- Password protection
- Application's access can be filtered by View / Add / Edit / Delete
- User data access can be filtered
- Access panel access can be filtered
- Event status can be filtered
- Event acknowledge can be filtered

f) Reporting
- All kinds of reports can be viewed on-screen and sent to the printer
- Report can export to TEXT, EXCEL & PDF file.

g) Cardholder management
- Provide Import and Export data tool for 3rd party data integration

h) Door access activated by the specified card holder
- The mailbox/locker is allowed for use before the specified card authorization

g. Electronics Map Monitoring
   i. Real-time display of door and sensor status
   ii. Real-time video monitoring
   iii. Control E-lock open & close
   iv. Group/ individual acknowledgment
   v. Integrated with video management system application

h. Turnstile System
   i. The turnstile system shall integrate to the lift destination control system and building visitor management system
   ii. The turnstile shall install body thermal and wear mask detection device. The device size shall be limited to 120mm (L) x 80mm (W) x 75 (H). The device can enable or disable the facial recognition feature. The device can enable or disable temperature and wear mask check features. The device shall install on top of the turnstile top surface area. The device measure body temperature and wear mask conditions, the response time shall less than 1.5 second
   iii. The body thermal and wear mask detection device shall cater people height from 1.2m to 1.9m and also cater the people in wheelchair.

iv. The turnstile shall install multi-technology reader for different access conditions. The access credential shall include 13.56MHz and/or Octopus, Palm Vein, Facial Recognition, QR code reader which can handle mobile scramble QR code and paper fixed QR code.
v. User can select their registered one of access credentials to access the turnstile.
vi. The turnstile shall install a 5.5" LCD to display the graphics for body temperature and wear mask notification, the access granted and access denied message and the destinated lift car number if the turnstile system integrates to the lift destination control system
vii. The Facial Recognition algorithm shall be provided by SenseTime or Face++.
viii. The Palm Vein Recognition technology shall be provided by Fujitsu PalmSeure-F Pro sensor

i. Time Attendance System
   i. Design for scheduling the staff and taking attendance
   ii. User's roster can be set by company/ department/ division/ personal level
   iii. Unlimited shift table for people duty time period
   iv. Unlimited roster table assigns by different grouping level as by company level, by department level, or by the individual.
   v. Fast report generation
   vi. Individually attendance and Master attendance report
   vii. The attendance report can be automatically generated by schedule and send to the authorized recipients through email.
j. Surveillance System Integration
   i. Manage all surveillance video sources in one system
   ii. Configure cameras (IP address) to the system
   iii. CCTV playback in the access record enquiry

3.5 The SACS shall be fully inter-operated under one authorization management, i.e., the system shall be operated under one database system. The identification/coding of equipment, smart card holders, etc. shall follow the same logic and format.

3.6 The SACS shall consist of a workstation complete with an LCD monitor, local database server, network switches, networked door access controllers, multi-technology access control readers, electric door locks, door release buttons, resettable call points, high-security override key switch, and key switch controller, power supply boxes, and all associated software and accessories.

3.7 Systematic dynamic encryption shall be applied between the local database server to networked door access controllers and networked door access controllers to multi-technology access control readers of the SACS. A master key shall be the built-in host and a random key shall be generated during each data transmission. The master key encrypts the random key, random key encrypts transmission data.

3.8 The SACS shall utilize the Fast Ethernet network for communication.

3.9 The SACS shall enable setting as per access right privilege level such that:

a. Access rights can be granted to different groups of people at different access points.
b. Access rights can be granted to people according to pre-defined time schedules. Doors can be locked or unlocked automatically according to pre-defined time schedules.

3.10 The SACS shall allow access control readers to be configured in the workstation to operate in any of the following modes: -

a. Free Access Mode:
   The door is unlocked and no card is required for entry.
b. Secure Access Mode:
   A successful card attempt is required for valid entry.
c. Secure Biometric Mode:
   A successful palm vein or facial attempt is required for valid entry.

3.11 A local workstation shall be provided. The status of the system shall be monitored and repeated to the central workstation via fiber optic cables.

3.12 Networked door access controllers shall keep downloaded data from the database and be capable of self-independent controlling and monitoring transactions even with the breakdown of the network and power outage. The downloaded data shall remain in the controllers so that any programmed data shall not be destroyed in case of mains power failure.

3.13 The database of staff access rights to each door shall be stored at each networked door access controller so that any communications breakdown shall not affect the operation of any individual door.

3.14 Each access control reader shall communicate with the networked door access controller by RS485 cable with scramble encryption technology, the reader to controller cable distance can be extended to 1,200 meters.

3.15 The SACS shall be able to work under offline mode.

3.16 The SACS shall be able to integrate with the Digital IP CCTV cameras to record a particular person or event for entry/exit in highly secured areas.

3.17 All access control readers installed for the Works shall support access rights granted via Bluetooth, Scramble QR Code, and RFID Card in a single reader. Access rights granted via 13.56MHz contactless smart card/Keypad/ Palm Vein/ Facial Recognition/ Octopus shall be available as additional provisions to the access control reader.

3.18 The SACS shall provide a Virtual Card Platform to generate a Bluetooth/ Scramble QR Code as Virtual Credential and deliver the identity to the user's mobile through email. Users can download the APP from the Android and iOS stores, after putting the activation code sent by the operator, a virtual card number will be generated on mobile. The SACS shall direct the plug-in to the VCP.

3.19 The Virtual Card Platform shall comply with the following requirements as a minimum: -

The Platform shall have a central database installed in Cloud (Internet/ Intranet). The database shall include the operator information, the generated virtual card number record, the user's e-mail address/ mobile identity and etc.

a. The Platform shall provide a Web portal for data entry.
b. The Platform shall have a user ID and password login control.
c. The Platform shall use 2 sets of 64 bits customer key as the data exchange key on mobile and reader communication.
d. The Platform shall generate an identity representing the encrypted virtual card number and deliver the identity to user's mobile device through e-mail or SMS.
e. The Platform shall prohibit the same virtual card number to register on more than one mobile device.
f. Operator can disable the virtual card number on the registered mobile.
g. The virtual card number can be reused.
h. The Platform shall include a Mobile Virtual Card APP which is available at Android and iOS store. The Mobile Virtual Card APP shall have Bluetooth & Scramble QR code feature

for short-range and mid-range access control application.

i. Bluetooth virtual card generated by Mobile Virtual Card APP can be used for mid-range access control application. Access control reader to mobile device read range can be configured from 0.3 meter to 10 meters depending on the environmental condition.
j. Bluetooth virtual card can be triggered by BUTTON, SWING and HANDS-FREE mode, the effective read range between access control reader and mobile can be configured individually.
k. Mobile Bluetooth communicate to access control reader shall have scramble encryption to ensure the data cannot be played back by other devices.
l. Scramble QR code virtual card by mobile APP shall be scrambled in every second, the copied QR code will be disable after a specified time period. The specified time period shall be less than 5 seconds and different time period can be set for each virtual card.
m. The Mobile Virtual Card APP can be running at off-line mode (no internet connection)

3.20 The access control for all project areas shall be completed with an on-line access control system to notify an access request and the local and central database shall keep a record of the request.

3.21 Firmware of SACS shall be able to be updated remotely via network connection.

4. Materials and Equipment

4.1 Access Control System Server and Workstation

a) Server hardware and software requirement
   i. Completed with 1920 x 1080 LCD monitor, mouse, keyboard, software.
   ii. WIN 10 Professional 64 bits edition, English / Chinese operating system
   iii. SQL express 2016 or above
   iv. INTEL i7 Processor (3.4GHz, 8M cache) or equivalent
   v. 500GB SSD, 8GB DDR4 RAM
   vi. 1 x LAN Port, 4 x USB3.0
   vii. UPS to give non-stop power supply for minimum 30 minutes after failure of the main power
b) Workstation
   i. It shall be completed with 1920 x 1080 LCD monitor, mouse, keyboard, software.
   ii. WIN 10 Professional 64 bits edition, English / Chinese operating system
   iii. INTEL i7 Processor (3.4GHz, 8M cache) or equal

iv. 128GB SSD, 8GB DDR4 RAM
v. 1 x LAN Port, 4 x USB3.0
vi. UPS to give non-stop power supply for minimum 30 minutes after failure of the main power

4.2 Integrated Access Control System Software

a. Architecture
   i. Windows-based application which can run on WIN 10/ Windows Server 2020 or higher version.
   ii. Server Program is a service in the PC/Server, once the PC/Server is restarted, the server program will run automatically.
   iii. Software has multi-language features.
   iv. User can online change the software text content.
   v. The maximum number of concurrent user logins will be under control.
   vi. Same database for storing Facial template, Palm Vein template, Fingerprint template and card number.
   vii. Same software interface for managing Facial, Palm Vein, Virtual Card registration, fingerprint, mobile virtual card and access control distribution.
b. Communication
   i. Server program uses multi-threading programming technique, which direct communication to access the control panel on Ethernet cable, real-time response.
   ii. TCP/IP communication.
c. Data Security
   i. User-defined 128 bits master key in Server and Panel for data encryption.
   ii. A unique 192 bits random key is generated during per data transmission.
   iii. Data encryption method, master key encrypts random key, random key encrypts the exchanged data during communication.
   iv. AES128 and 3DES Algorithm mixed.
d. Database requirement
   i. MS SQL 2019 or above
e. Application user authority
   i. Password protection
   ii. Application’s access can be filtered by View / Add / Edit / Delete
   iii. User data access can be filtered
   iv. Access panel access can be filtered
   v. Event status can be filtered

vi. Event acknowledge can be filtered

f. Reporting
   i. All kind of reports can be view on screen and send to printer
   ii. Report can export to TEXT, EXCEL & PDF file.

g. Email Service
   i. User can receive alarm record by email
   ii. User can receive their daily access record by email
   iii. Supervisor can view group users' access report and different kind of time attendance report by email

h. Access control system
   i. Real time upload parameters to panels
   ii. Client software can read controller and reader parameters instantly.
   iii. Controller and reader parameters can be defined by global or by individual
   iv. Door Group
      - Allow 10,000 door group set up
      - Card access per door of its time zone can be classified by different door group
      - Door group can be assigned for the department
   v. Fire Alarm Group
      - Allow 255 fire alarm groups for any combination of the door lock released when firm alarm is triggered

i. Cardholder management
   i. Provide Import and Export data tool for 3rd party data integration
   ii. Cardholder access rights can be selected by department or door group
   iii. Software can define 1,000+ suspected cardholder groups for instant enable or disable their access rights
   iv. Cardholder access rights can be defined by door group or by department

j. Staff management
   i. Provide Import and Export data tool for 3rd party data integration
   ii. Online capture of a personal photo, palm vein, fingerprint biometric templates
   iii. Print staff badge

k. Time zone control
   i. Each time zone has 4 intervals per day, Mon to Sun & Holiday
   ii. 100 Holiday dates per door access control panel
   iii. 10,000+ door access time zone in the database, 80 door time zones per door access control panel
   iv. Password time zone

v. Electric Lock release time zone
vi. Twin card operation time zone
vii. Release button time zone
viii. Door opens too long time zone
ix. Alarm time zone

l. Twin card operation
   i. Twin card operation with time zone control for high-security access control application.

m. Door access activated by the specified card holder
   i. The door is allowed for use before the specified card authorization

n. Power Monitoring
   i. A.C. power failure monitoring
   ii. Backup failure monitoring (20% of full load)

o. Transaction and Events viewer
   i. Global viewer for card access records and events
   ii. Individual / Multi viewer for card access records to display card holder details information, e.g., Photo etc.
   iii. Alarm viewer display the live camera
   iv. Card access records filter by user, control panel, date and time, access status.
   v. Different sorting order, ascending or descending, all access record, only IN or OUT or First IN last OUT record.
   vi. Event records can be filtered by control panel, date and time and status.
   vii. Event records can be preview and send file to printer.
   viii. Export the file to EXCEL, text and PDF

p. Event monitoring system
   i. Each event can be defined by different icons
   ii. Software can define the device input normal status in NC or NO
   iii. Action taken can be assigned to each device input when alarm triggered
   iv. Action item as like as Acknowledgment requested, door open by fire alarm, enable surveillance integration, signal integration with third party BMS and play music etc.

4.3 PoE+ Networked Single Door Access panel

a) Architecture
   i. PoE+ TCP/IP based single door panel
   ii. The overall power consumption is 30W, max. 17W power reserves for E-Lock.
   iii. Wiring method: Cat 5 cable for the panel to PoE+ switch

b) Communication
    i. PC to Panel, TCP/IP communication
    ii. Scramble data encryption during PC/Server to panel data exchanges through the network cable
    iii. Panel to the reader, Wiegand or scramble RS485 data encryption
    iv. Active upload for swipe card records and events
c) Data Security
    i. Apply scramble data encryption methodology during data exchange
    ii. 128 bits' user master key on PC, Panel, and Reader
    iii. 192 bits' random key auto-generated per communication
    iv. Master key encrypts random key, random key encrypts data exchanges between PC and Panel, Panel and Reader
    v. AES 128 & 3 DES mixed Algorithm
d) Reader supports
    i. 1 x IN and 1 x OUT for single door panel
    ii. Supports scramble RS485 reader
    iii. Support multi-technology reader Card reader (e.g., Facial + QR + Bluetooth + 13.56MHz contactless smartcard, Palm Vein+ QR + Bluetooth + 13.56MHz contactless smartcard, Keypad + QR + Bluetooth + 13.56MHz contactless smartcard and QR + Bluetooth + 13.56MHz contactless smartcard)
e) Card number format
    i. Default 26 / 32/ 34 / 35 / 37 / 56 / 64 and three custom formats
    ii. Each card format can have three facility code
    iii. Support four card formats at the same time
    iv. Card number length, maximum 64 bits
f) Memory storage
    i. Memory for card holder
        - Single door controller
            - Allow storage of at least 40,000 sets of card numbers
    ii. Memory for transactions
        - Single door controller: allow storage of at least 42,000 nos. of transactions
    iii. Events: allow storage of at least 800 nos. of events
g) Time zone control
    i. Each time zone has 4 intervals per day, Mon to Sun & Holiday
    ii. 100 Holiday dates per door access control panel
    iii. 10,000+ Door access time zone in the database, 80 time zones per door access

control panel
iv. Password time zone
v. Electric Lock release time zone
vi. Twin card operation time zone
vii. Release button time zone
viii. Door opens too long time zone
ix. Alarm time zone
x. LCD reader message time zone

h) Fire Alarm
i. Panel AUX #1 for fire alarm input
ii. 255 fire alarm groups per panel
iii. Firm alarm signal broadcasts through the network card, no need through the PC server

i) Twin card operation
i. Twin card operation with time zone control for high-security access control application. E.g., Car park system, treasury application.

j) Anti-pass back
i. Single door panel (single anti-passback)

k) Device Inputs
i. Auto detect end-of-line resistors were installed or not, if yes, enable supervised monitoring
ii. Supervised monitoring needs end of line resistors, 1K ohm + 1K ohm
iii. Door release button (Normal Open)
iv. Door Sensor (Normal close)
v. Panel temper box sensor (Normal Close)
vi. 2 x AUX inputs
- Normal mode can be defined by N.O. or N.C.
- Fire alarm signal, broadcast release E-Lock command instantly though network cable
- Non-fire signal depends on COM server command configuration

l) Device Outputs
i. Access granted output for E-Lock operation. 12VDC, 10A Relay (N.O. / N.C.)
ii. Alarm output. 12VDC, 5A Reply (N.O. / N.C.)
iii. Door Ajar. 5VDC, 10mA output

m) High-Security Key Switch
i. Tamper proof for the E-Lock override

ii. Tamper proof for short circuit or open circuit of the exposed key switch's wires

n) Expand RS485 port
   i. 2 x RS485 port
   ii. High-level data exchange with third-party system

o) 2 x Auxiliary input
   i. Auxiliary input # 1 – Fire alarm trigger then auto release E-Lock
   ii. Auxiliary input # 2 – Trigger alarm relay

4.4 Networked Door Access Panel

a) Architecture
   i. TCP/IP based network control panel
   ii. Built-in two LAN ports
   iii. Wiring method: Cat 5 cable for panel to network switch or panel to panel (daisy chain)

b) Communication
   i. PC to Panel, TCP/IP communication
   ii. Scramble data encryption during PC to panel data exchanges through network cable
   iii. Panel to reader, Wiegand or scramble RS485 data encryption
   iv. Active upload for swipe card record and events

c) Data Security
   i. Apply scramble data encryption methodology during data exchange
   ii. 128 bits' user master key on PC, Panel and Reader
   iii. 192 bits' random key auto generated per communication
   iv. Master key encrypts random key, random key encrypts data exchanges between PC and Panel, Panel and Reader
   v. AES 128 & 3 DES mixed Algorithm

d) Reader supports
   i. 1 x IN and 1 x OUT for single door panel
   ii. 2 x IN and 2 x OUT for two door panel
   iii. Supports scramble RS485 reader
   iv. Support multi-technology reader Card reader (e.g., Facial + QR + Bluetooth + 13.56MHz contactless smartcard, Palm Vein+ QR + Bluetooth + 13.56MHz contactless smartcard, Keypad + QR + Bluetooth + 13.56MHz contactless smartcard and QR + Bluetooth + 13.56MHz contactless smartcard)

e) Card number format
   i. Default 26 / 32/ 34 / 35 / 37 / 56 / 64 and three custom formats
   ii. Each card format can have three facility code

iii. Support four card formats at the same time
iv. Card number length, maximum 64 bits

f) Memory storage
   i. Memory for card holder
      - Single door controller
        - Allow storage of at least 40,000 sets of card number only
      - Two door controller
        - Allow storage of at least 20,000 sets of card number only
   ii. Memory for transactions
      - Single door controller: allow storage of at least 42,000 nos. of transactions
      - Two door controller: allow storage of at least 21,000 nos. of transactions
   iii. Events: allow storage of at least 800 nos. of events

g) Time zone control
   i. Each time zone has 4 intervals per day, Mon to Sun & Holiday
   ii. 100 Holiday dates per door access control panel
   iii. 10,000+ Door access time zone in the database, 80 time zones per door access control panel
   iv. Password time zone
   v. Electric Lock release time zone
   vi. Twin card operation time zone
   vii. Release button time zone
   viii. Door opens too long time zone
   ix. Alarm time zone
   x. LCD reader message time zone

h) Fire Alarm
   i. Panel AUX #1 for fire alarm input
   ii. 255 fire alarm groups per panel
   iii. Firm alarm signal broadcasts through the network card, no need through the PC server

i) Twin card operation
   i. Twin card operation with time zone control for high-security access control application. E.g., Car park system, treasury application.

j) Anti-pass back
   i. Single door panel (single anti pass back)
   ii. Two door panel (single or global anti pass back)
   iii. Global anti-pass back, through server.

k) Device Inputs
   i. Auto detect end-of-line resistors were installed or not, if yes, enable supervised

monitoring

ii. Supervised monitoring needs end of line resistors, 1K ohm + 1K ohm
iii. Door release button (Normal Open)
iv. Door Sensor (Normal close)
v. Panel temper box sensor (Normal Close)
vi. 2 x AUX inputs
- Normal mode can be defined by N.O. or N.C.
- Fire alarm signal, broadcast release E-Lock command instantly though network cable
- Non-fire signal depends on COM server command configuration

l) Device Outputs
i. Access granted output for E-Lock operation. 12VDC, 10A Relay (N.O. / N.C.)
ii. Alarm output. 12VDC, 5A Reply (N.O. / N.C.)
iii. Door Ajar. 5VDC, 10mA output

m) High-Security Key Switch
i. Tamper proof for the E-Lock override
ii. Tamper proof for short circuit or open circuit of the exposed key switch's wires

n) Expand RS485 port
i. 2 x RS485 port
ii. High-level data exchange with third-party system

o) 2 x Auxiliary input
i. Auxiliary input # 1 – Fire alarm trigger then auto release E-Lock
ii. Auxiliary input # 2 – Trigger alarm relay

4.5 Electric Lock

a) Electromagnetic Lock with built-in door sensor
b) Fail-Safe: unlocks when the power supply fails
c) Easy installation: suitable for both new and retrofit usage
d) High holding force (280KG or above)
e) Self-alignment: armature plate pivots to accommodate door drop
f) Silent operation: no humming or buzzing
g) Dual voltage: site selectable 12 or 24 VDC
h) Instantaneous release: smart electronics on the A Series Electromagnets eliminate residual magnetism
i) Two secured metal wires for the Lock body mounted on the door frame
j) One secured metal wire for the armature plate mounted on the door

4.6 Door Release Button

a. Infra-red sensor door release button shall be provided.
b. Unlike traditional door release buttons, an Infrared release button does not require any form of physical pressure to operate. Simply placing a hand in front of the unit will activate the sensor, and change the internal relay state to operate the electronic lock.

4.7 Door emergency exit device (Resettable Call Point)

a. The resettable call point comes with a hinged front cover to prevent the unit from activating randomly.
b. Once the “PRESS HERE” button was pressed, the E-Lock power is cut, the door is released.
c. The call point can be reset by inserting a plastic key horizontally to the front panel of the resettable call point.
d. The call point unit shall have LED light to identify the operation mode. RED, GREEN, BLUE and mixed color shall be assigned for normal mode and emergency exit mode.
e. The LED light of the call point is provided by the E-Lock power input, if the LED light is ON, the E-Lock power supply is normal and vice versa.
f. For emergency exit mode, the call point shall have beep sound notification.
g. The LED and buzzer setting shall be operated by DIP switch.
h. The call point shall have two set dry contact switches, one set for E-Lock power, another set for signal output. The current rate of the switch is 5ADC under 12VDC power supply.
i. The resettable call point shall have voltage regulator to support E-Lock power in AC/DC, 12V/24V.

4.8 Power Supply Box

a. The power supply box shall have a metal casing.
b. The power supply box shall have earth wiring.
c. The size of the power supply box shall be not more than 340mm(H) x 290mm(W) x 80mm(D).
d. The power supply box shall have 12VDC, 3A power supply output for ONE set electric lock installed; and 5A power supply output for TWO sets electric lock installed.
e. The power supply shall have battery charging function.
f. The power supply can output 0VDC or 5VDC voltage level to controller to indicate occurrence of the following events: -
    i. AC. power failure
    ii. DC battery installed

iii. backup battery power lower 20%

g. A 7AH DC battery shall be included. In case of AC power supply failure, the door access system can be operated for 4 hours.

4.9 High Security Override key switch and key switch controller

a. The High security override key switch works with key controller, no matter the key switch is tampered, the electric lock keeps the original lock status
b. One LED indicator on the key switch front plate: LED indicator in RED in normal operation, after key override, the LED indicator changes to GREEN. Once the key switch is tampered, the LED indicator goes off.
c. If the key switch is tampered, no matter short-circuits or cutting the wires between the key switch and key switch controller, the electric lock status remains unchanged.
d. Reset button in key switch controller which to activate the key switch function
e. The key cylinder shall have a master operation key which can open all high security override key switches, the master key built-in a small movable pellet which cannot be physical duplicated excludes the original cylinder supplier.
f. Minimum 3 sets master key shall be provided to end customer.

4.10 Multi-technology Smart Card smart lock reader (Bluetooth + Scramble QR Code + RFID Card)

a) Supports 13.56MHz NXP Mifare Class, Mifare Plus, Mifare DESFire, and LEGIC card technology.
b) Supports Mobile Virtual Card, Bluetooth 4.0+ and Scramble QR Code
c) 13.56MHz card read range: 5cm+; Bluetooth read range: 0.5m to 10m; QR Code read range: 4cm to 22cm
d) NFC technology compatibility (13.56 MHz NFC)
e) Programmable buzzer beep sound interval for access granted and access denied
f) Red / Green / Blue or mixed LED for visual notification
g) Programmable LED flash interval for access granted and access denied
h) Reader can be configured online
i) Reader outputs proprietary scramble encryption RS485 format
j) Reader Tamper: Optical sensor
k) Reader size shall be not larger than 80mm(W) x 130mm(H) x 20mm(D)
l) IP55 rated

4.11 Multi-technology Smart Card smart lock reader (Bluetooth + Scramble QR Code + Keypad RFID Card)

a. Supports 13.56MHz NXP Mifare Class, Mifare Plus, Mifare DESFire, and LEGIC card technology.
b. 12 capacitance touch keypads
c. Supports Mobile Virtual Card, Bluetooth 4.0+ and Scramble QR Code
d. 13.56MHz card read range: 5cm+; Bluetooth read range: 0.5m to 10m; QR Code read range: 4cm to 22cm
e. NFC technology compatibility (13.56 MHz NFC)
f. Programmable buzzer beep sound interval for access granted and access denied
g. Red / Green / Blue or mixed LED for visual notification
h. Programmable LED flash interval for access granted and access denied
i. Reader can be configured online
j. Reader outputs proprietary scramble encryption RS485 format
k. Reader Tamper: Optical sensor
l. Reader size shall be not larger than 80mm(W) x 130mm(H) x 20mm(D)
m. IP55 rated

4.12 Multi-technology Palm Vein smart lock reader (Bluetooth + Scramble QR Code + RFID Card + Palm Vein)

a) Supports 13.56MHz NXP Mifare Classic, Mifare Plus, Mifare DESFire, and LEGIC card technology.
b) Supports Mobile Virtual Card, Bluetooth 4.0+ and Scramble QR Code
c) 13.56MHz card read range: 5cm+; Bluetooth read range: 0.5m to 10m; QR Code read range: 4cm to 22cm
d) Palm Vein recognition technology should be provided by Fujitsu Palm Secure-F Pro sensor
e) Palm Vein Sensor supports binocular infrared live detection
f) Palm Vein recognition can be completed in one second for 2,000 palm vein users. Each user can register 2 palm vein templates
g) The recognition accuracy rate is higher than 99% and 0.5m-1.5m recognition distance is supported
h) Supports 20,000 local personnel
i) Programmable buzzer beep sound interval for access granted and access denied
j) Red / Green / Blue or mixed LED for visual notification
k) Programmable LED flash interval for access granted and access denied
l) Reader can be configured online
m) Reader outputs proprietary scramble encryption RS485 format
n) Reader Tamper: Optical sensor

o) Reader size shall be not larger than 80mm(W) x 130mm(H) x 20mm(D)
p) IP55 rated

4.13 Multi-technology Facial Recognition smart lock reader (Bluetooth + Scramble QR Code + RFID Card + Facial Recognition)

a) Supports 13.56MHz NXP Mifare Classic, Mifare Plus, Mifare DESFire, and LEGIC card technology.
b) Supports Mobile Virtual Card, Bluetooth 4.0+ and Scramble QR Code
c) 13.56MHz card read range: 5cm+; Bluetooth read range: 0.5m to 10m; QR Code read range: 4cm to 22cm
d) Facial detection supports binocular infrared live detection
e) Face recognition can be completed in 300 milliseconds
f) The recognition accuracy rate is higher than 99% and 0.5m-1.5m recognition distance is supported
g) Supports 20,000 local personnel
h) Real-time detection and tracking of human faces, accurate detection can be carried out in situations such as side faces, half occlusion, and blur
i) Minimum 0.5 lux recognition
j) Effective defense against non-living attacks such as 3D printing, electronic screens, video, pictures, masks, hoods, etc.
k) Programmable buzzer beep sound interval for access granted and access denied
l) Red / Green / Blue or mixed LED for visual notification
m) Programmable LED flash interval for access granted and access denied
n) Reader can be configured online
o) Reader outputs proprietary scramble encryption RS485 format
p) Reader Tamper: Optical sensor
q) Reader size shall be not larger than 80mm(W) x 130mm(H) x 20mm(D)
r) IP55 rated

4.14 Multi-technology Octopus smart lock reader (Bluetooth + Scramble QR Code + Octopus)

a) Supports Octopus, Mobile Virtual Card by Bluetooth 4.0+ and Scramble QR Code
b) Bluetooth read range: 0.5m to 10m; QR Code read range: 4cm to 22cm
c) Received the Octopus Holding Limited Type Approval Certificate
d) Programmable buzzer beep sound interval for access granted and access denied
e) Red / Green / Blue or mixed LED for visual notification
f) Programmable LED flash interval for access granted and access denied

g) Reader outputs proprietary scramble encryption RS485 format
h) Reader Tamper: Optical sensor
i) Reader size shall be not larger than 94mm(W) x 196mm(H) x 55mm(D)
j) Flush mount design with only 6mm extruded from the wall

4.15 Thermal Camera for turnstile installation

a. Built-in black body to increase the temperature accuracy.
b. Embedding camera to the turnstile to check body temperature & mask on, and allow facial access.
c. Automatically check whether passengers are wearing a mask and have normal body temperature without physical contact.
d. With an effective scan range of 3m.
e. Tiny and streamlined enclosure without any display.
f. The enclosure surface is 75 degrees to the ground which is suitable for a 1.6m to 1.9m length turnstile.
g. The turnstile height range is 1000mm to 1050mm
h. The thermal camera scan range cover people tall from 1.2m to 1.9m standing in front of the edge of the turnstile.
i. Superior low-light performance.
j. Latest 3.0µm pixel with ON Semiconductor DR-Pix technology with Dual Conversion Gain.
k. Full HD support at up to 1080p 60fps for superior video performance.
l. Liner or high dynamic range capture.
m. Auto black level calibration.

4.16 Turnstile Reader

a. Provides an open platform for 3rd party integration of lift destination control and visitor management system and lift destination control system.
b. Supports palm vein, facial recognition, mobile scramble QR code, contactless smart card 13.56MHz RF and NFC technology. Once the reader detects user's identity, the LCD screen will display lift ID and user access status instantly.
c. Programmable buzzer beep sound interval for access granted and access denied
d. Red / Green / Blue or mixed LED for visual notification
e. Programmable LED flash interval for access granted and access denied
f. Reader outputs Wiegand and scrambles encryption RS485 format
g. The turnstile readers and the thermal device shall work with 8980 turnstile gateways

4.17 Networked Lift Control Master Panel

a. A multi-purpose device that provides an interface between field level input, output devices and an Lift application server
b. True IP device, support DHCP
c. 2 x LAN Port, allow daisy chain connection
d. Dry contact supervised monitoring
e. User-defined NC / NO at normal mode
f. 2 x INPUTs for Manual key overwrite and Fire Alarm input
g. 28 x RELAY outputs for 28 Floors access, RELAY in 3A DC output
h. Panel installation depends on the IP address available
i. RS485 port for 8907 Lift control expand panel

4.18 Networked Lift Control Expansion Panel

a. Works with Networked Lift Control Master Panel
b. RS485 connection
c. User-defined NC / NO at normal mode
d. 38 x RELAY outputs for extra 38 Floors access, RELAY in 3A DC output

4.19 Network Alarm Panel

a. 2 x LAN Port, allow daisy chain connection
b. Suitable for huge sensors monitoring
c. Dry contact supervised monitoring
d. User-defined NC / NO at normal mode
e. 28 Input Points, 2 RELAY 10A output per panel
f. Panel installation depends on the IP address available
g. Relay status triggered by 28 Inputs AND / OR program logic
h. RS485 port for proprietary device communication

5. Commissioning and Testing

5.1 The Contractor shall include in his tender all costs associated with the above mentioned testing and commissioning procedures including the cost of making good any defects arising out of such test and having the work retested. Such costs shall also include the provision of all instruments necessary for the test.

5.2 The commissioning shall be carried out by a Specialist Sub-contractor (SSC). The SSC shall undertake the commissioning of the respective installed services systems in accordance with the Drawings and Specification. The SSC shall provide network engineers, software engineers and commissioning engineers for the commissioning works.

6. Warranty, Maintenance and Emergency Support Requirements

6.1 All products offered shall have full warranty period of 1 year, including all systems, deployed equipment and version upgrade, fix and patch update and, labour starting from the employer's acceptance of handover to the employer operation service unless otherwise approved by the employer's representative.

6.2 The Contractor should provide all necessary material, parts, tools, equipment and qualified labours to carry out the maintenance and repairing services throughout the full warranty period.

6.3 The Contractor should state clearly if the support is directly provided by the manufacturer or from other supplier, with any value-added service from the Contractor.

6.4 System and software problem diagnosis shall be provided on-site or remote by the Contractor's engineer(s) or specialist(s). They should follow through the whole diagnostic activity, such as but not limited to gathering logs, discussing with back-end, setup and apply fix in the environment for verification, prepare and provide information to ease the diagnostic, etc.

6.5 Within the warranty period, maintenance activities shall include half yearly inspection of the system, repairs or replacement of defective parts and consumables should be carried out free of charge.

-End-