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 and other relevant General and Particular Specifications sections.

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, from now on called "SACS", and the system's performance requirements. The Works shall also include labor and material as prescribed or as necessary except where expressly specified to be provided by others. It shall not only include the significant items of plant and equipment shown or specified but also include all the incidental sundry components necessary together with the labor for installing such components for the complete execution of the Works and for the proper operation of SACS installation, whether these sundry components are stated in detail in this part of the Specification. It shall also include interface and cooperation 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 labor, materials, equipment, and services for the supply, installation, project and construction management, supervision, testing, commissioning, handing-over, providing 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 install the complete SACS for doors and 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 install an Uninterruptible Power Supply (UPS) to maintain 30 minutes of operation for the central equipment of SACS in the respective office.

2.2 The Contractor must appoint a 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 certifying all results and reports from the testing and commissioning works.

2.3 The Contractor shall submit and 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 spare parts, tools, and accessories for 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 crucial spare parts and tools shall not exceed those specified in the tender document.

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

2.8 Before ordering and implementing equipment, the Contractor shall submit the security system's technical specifications and shop drawings for comment and approval. The Security System shall meet the performance standards and equipment sizes 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 represent the Works in full detail. Reference shall be made to other sections of this specification and tender drawings. Due allowance shall 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 a non-VPN network.
   iv. Software admin can create users with different access rights for the cardholder and the controllers.
   v. Allow remote maintenance of access controllers, access control readers, and time zone 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. The user has access rights for individual floors 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 all building tenants.
   ii. The VMS server can be cloud-based or on-premises.
   iii. Tenants can maintain the VMS through the web browser or mobile apps.
   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 comprised of four applications: the VMS Server program (back-end), a Web-based visitor management application (for tenants), a PC-based client application (for concierge operators), 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 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.

- A scramble QR code can represent the visitor's temporary pass.
- 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 Subcontractor shall be responsible for any Certificate or Patent document if required.
- The sub-contractor shall be responsible for complying 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 Windows-based application 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 the walk-in visitor record
- The program can assign the building access rights to the visitor. E.g., Male / Female toilet access.
- Real-time monitoring of the visitor count in the building
- Email notification to the user if the visitor arrives.
- Provide emergency notification by email / SMS to visitors in the building area.
- Connect to a QR code printer to print 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 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 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 drivers and passenger
    ii. Driver clocks in via APP
    iii. Real-time checking of passenger's authority to take a shuttle
    iv. Track record
f. Smart Locker / Mailbox System
    a) Architecture
        - This client-server software application can run on WIN 10 or the latest Windows version.
        - The Server Program is a service on the PC server; once the PC server restarts, the program runs automatically.
        - Client software has multi-language features, including English, Traditional Chinese, and Simplify Chinese.
        - Users can change the software text content online.
        - 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
        - The server program uses a multi-threading programming technique, which directs communication to access the control panel on an Ethernet cable, providing a real-time response.
        - TCP/IP communication.
    c) Data Security
        - User-defined 128-bit master key in Server and Panel for data encryption.
        - A unique 192-bit random key is generated per data transmission.

- Data encryption method: The master key encrypts the random key, and the 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 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 acknowledgment can be filtered

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

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

h) Door access activated by the specified cardholder
- 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 into the lift destination control system and building visitor management system
   ii. The turnstile shall install a 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 be installed on top of the turnstile top surface area. The device measures body temperature and wears mask conditions; the response time shall be less than 1.5 second
   iii. The body thermal and wear mask detection device shall accommodate people's heights from 1.2m to 1.9m and also accommodate people in wheelchairs.

iv. The turnstile shall install a multi-technology reader for different access conditions. The access credential shall include 13.56MHz and/or Octopus, Palm Vein, Facial Recognition, and a QR code reader that can handle mobile scramble QR code and paper-fixed QR code.
v. User can select their registered 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. SenseTime or Face++ shall provide the Facial Recognition algorithm.
viii. The Fujitsu PalmSecure-F Pro sensor shall provide the Palm Vein Recognition technology

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 period
   iv. Different grouping levels, such as company, department, or individual, assign an unlimited roster table.
   v. Fast report generation
   vi. Individually attendance and Master attendance report
   vii. The attendance report can be automatically generated by schedule and sent 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 inquiry

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, intelligent 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 system's status 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 network breakdown 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 a 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 entering the activation code sent by the operator, a virtual card number will be generated on the 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 the Cloud (Internet/ Intranet).
The database shall include the operator's information, the generated virtual card number record, the user's e-mail address/ mobile identity, and other information.

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 two sets of 64-bit customer keys as the data exchange key for mobile and reader communication.
d. The Platform shall generate an identity representing the encrypted virtual card number and deliver the identity to the user's mobile device through e-mail or SMS.
e. The Platform shall prohibit the same virtual card number from registering on multiple mobile devices.
f. The operator can disable the virtual card number on the registered mobile device.
g. The virtual card number can be reused.
h. The Platform shall include a mobile virtual card app available at the Android and iOS stores. The app shall have Bluetooth and a Scramble QR code feature for short-range

and mid-range access control applications.

i. Bluetooth virtual card generated by Mobile Virtual Card APP can be used for mid-range access control applications. Access control reader to mobile device read range can be configured from 0.3 meters 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 the access control reader and mobile can be configured individually.
k. Mobile Bluetooth communicates to the access control reader, which shall have scramble encryption to ensure other devices cannot play back the data.
l. Scramble QR code virtual card by mobile APP shall be scrambled every second; the copied QR code will be disabled after a specified period. The specified period shall be less than 5 seconds, and different periods can be set for each virtual card.
m. The Mobile Virtual Card APP can be running in off-line mode (no internet connection)

3.20 Access control for all project areas shall be completed with an online access control system to notify of an access request, and the local and central databases shall keep a record of the request.

3.21 SACS firmware shall be updated remotely via a 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, and software.
   ii. WIN 11 Professional 64 bits edition, English / Chinese operating system
   iii. MS SQL 2022 or above
   iv. INTEL i7 Processor (3.4GHz, 8M cache) or equivalent
   v. 1TB SSD, 8GB DDR4 RAM
   vi. 1 x LAN Port, 4 x USB3.0
   vii. UPS to give non-stop power supply for a minimum of 10 minutes after failure of the main power
b) Workstation
   i. It shall be completed with a 1920 x 1080 LCD monitor, mouse, keyboard, and software.

ii. WIN 11 Professional 64 bits edition, English / Chinese operating system
iii. INTEL i7 Processor (3.4GHz, 8M cache) or equal
iv. 512GB SSD, 8GB DDR4 RAM
v. 1 x LAN Port, 4 x USB3.0
vi. UPS to give non-stop power supply for a minimum of 10 minutes after the failure of the main power

4.2 Integrated Access Control System Software

a. Architecture
   i. Windows-based application that can run on WIN 10/ Windows Server 2020 or higher version.
   ii. The 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. Users can change the software text content online.
   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. The server program uses a multi-threading programming technique, which direct communication to access the control panel on an Ethernet cable, real-time response.
   ii. TCP/IP communication.
c. Data Security
   i. The user-defined 128-bit master key is used in the server and panel for data encryption.
   ii. A unique 192-bit random key is generated per data transmission.
   iii. In the Data encryption method, the master key encrypts the random key, and the 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 kinds of reports can be viewed on-screen and sent to the printer
ii. The report can be exported to TEXT, EXCEL & PDF files.

g. Email Service
i. The user can receive alarm records by email
ii. User can receive their daily access record by email
iii. The supervisor can view group users' access reports and different kinds of time attendance reports 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 individual
iv. Door Group
- Allow 10,000 door groups set up
- Card access per door of its time zone can be classified by different door group
- Door group can be assigned to the department

v. Fire Alarm Group
- Allow 255 fire alarm groups for any combination of the door lock released when a fire alarm is triggered

i. Cardholder management
i. Provide Import and Export data tools 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 department

j. Staff management
i. Provide Import and Export data tools 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 four 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 cardholder
   i. The door is allowed 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 and information, e.g., photo, etc.
   iii. Alarm viewer displays the live camera
   iv. User, control panel, date and time, and access status filter card access records.
   v. Different sorting orders, ascending or descending, all access records are only IN or OUT or First IN last OUT record.
   vi. The control panel, date and time, and status can filter event records.
   vii. Event records can be previewed, and the file can be sent to the 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 the alarm is triggered
   iv. Action items like Acknowledgment requested, door open by the 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 6 cable for the panel to PoE+ switch
b) Communication
    i. PC to Panel, TCP/IP communication
    ii. Scramble data encryption during Server-to-panel data exchanges through the network cable
    iii. Panel to the reader, OSDP V2, 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. Cardholder
        - Offline mode: 40,000 cardholders
        - Online mode: 1,000,000 cardholders
    ii. Transactions
        - Offline mode: 42,000 nos. of transactions
    iii. Events

- Offline mode: 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)

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 a 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 the panel to network switch or panel to panel (daisy chain)

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

b) 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

c) 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)

d) 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

e) Memory storage
   iv. Cardholder
   - Offline mode: 40,000 cardholders
   - Online mode: 1,000,000 cardholders
   v. Transactions
   - Offline mode: 42,000 nos. of transactions
   vi. Events
   - Offline mode: 800 nos. of events

f) Time zone control
   i. Each time zone has four intervals per day, Mon to Sun & Holiday
   ii. 100 Holiday dates per door access control panel
   iii. 10,000+ Door access time zones 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

g) 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

h) Twin card operation
   i. Twin card operation with time zone control for high-security access control applications, Such as Car park systems and treasury applications.

i) 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 the server.

j) Device Inputs
   i. Auto-detected end-of-line resistors 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
      - N.O. or N.C can define normal mode.
      - Fire alarm signal, broadcast release E-Lock command instantly though network cable
      - Non-fire signal depends on COM server command configuration

k) 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

l) 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

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

n) 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 Smart Intelligent Door Release

a. The device combines the regular and emergency door release features.
b. The device is operated by handwave for regular door release and pressing the button for door emergency release. It supports a fail-safe electric lock.
c. The device combines regular and emergency door release features. A particular tool can reset the emergency door release button, so replacing any components is unnecessary after the emergency door feature is resumed.
d. Once the “CENTER’ button is pressed, the fail-safe type E-Lock power is cut off, and the door is released. A dry contact NO / NC output to the Alarm Input Module for notification.
e. The user-defined LED color and beep sounds are for routine and emergency operations.
f. For regular operation, the LED is BLUE, and the handwave open door is GREEN. Emergency exit in RED (or blinking red) and optional has a beep sound.
g. The device has two sets of relay output: one for the regular release and another for the emergency door release notification.
h. The device shall have a voltage regulator to support E-Lock power in AC/DC, 12V/24V.
i. The device size is 86mm x 86mm x 4mm, which can be directly installed on the electric junction box.
j.

4.7 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 of electric locks installed, and 5A power supply output for TWO sets of electric locks installed.
e. The power supply shall have a battery charging function.
f. The power supply can output 0VDC or 5VDC voltage level to the controller to indicate the occurrence of the following events: -
    i. AC. power failure

ii. DC battery installed
iii. backup battery power was lower than 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.

4.8 High Security Override key switch and critical switch controller

a. The High-security override key switch works with a critical controller; no matter if the key switch has been tampered with, the electric lock keeps the original lock status
b. One LED indicator on the key switch front plate: In regular operation, the LED indicator is RED. After a crucial override, it changes to GREEN. The LED indicator goes off once the key switch has been tampered with.
c. If the key switch has been tampered with, whether it short-circuits or cuts the wires between it and the critical switch controller, the electric lock status remains unchanged.
d. Reset the button in the key switch controller to activate the critical switch function
e. The key cylinder shall have a master operation key that can open all high-security override key switches; the master key built in a small movable pellet that cannot be physically duplicated excludes the original cylinder supplier.
f. A minimum of 3 master keys shall be provided to the end customer.

4.9 3-in-1 Multi-technology Smart Card Reader (Bluetooth + Scramble QR Code + RFID Card)

a) Supports 13.56MHz NXP Mifare Class, Mifare Plus, Mifare DESFire, and LEGIC card technology.
b) 13.56MHz card read range: 5cm+; Bluetooth read range: 0.5m to 10m; QR Code read range: 4cm to 22cm
c) Programmable reader buzzer beep sound interval and times for access granted and access denied
d) Programmable reader LED color (7 colors) interval and times for access granted and access denied
e) Reader configuration can be updated through the network by ACX proprietary software
f) Reader firmware can be upgraded through the network by ACX proprietary software
g) Reader outputs ACX proprietary scramble encryption RS485 format
h) Reader Tamper: Optical sensor
i) Reader size shall be no larger than 80mm(W) x 130mm(H) x 20mm(D)
j) Waterproof, IP65 rated

4.10 4-in-1 Multi-technology Smart Card Keypad Reader (Keypad + Bluetooth + Scramble QR Code + RFID Card)

a. Supports 13.56MHz NXP Mifare Class, Mifare Plus, Mifare DESFire, and LEGIC card

technology.

b. 12 capacitance touch keypads, 0~9,*,#. The keypad has a backlight in 7 different colors.
c. Supports 13.56MHz NXP Mifare Class, Mifare Plus, Mifare DESFire, and LEGIC card technology.
d. 13.56MHz card read range: 5cm+; Bluetooth read range: 0.5m to 10m; QR Code read range: 4cm to 22cm
e. Programmable reader buzzer beep sound interval and times for access granted and access denied
f. Programmable reader LED color (7 colors) interval and times for access granted and access denied
g. Reader configuration can be updated through the network by ACX proprietary software
h. Reader firmware can be upgraded through the network by ACX proprietary software
i. Reader outputs ACX proprietary scramble encryption RS485 format
j. Reader Tamper: Optical sensor
k. Reader size shall be no larger than 80mm(W) x 130mm(H) x 20mm(D)
l. Waterproof IP65 rated

4.11 4-in-1 Multi-technology Palm Vein Smart Card Reader (Palm Vein + Bluetooth + Scramble QR Code + RFID Card)

a) The Fujitsu PalmSecure-F Pro sensor should provide Palm Vein recognition technology
b) Palm Vein Sensor supports binocular infrared live detection
c) Palm Vein recognition can be completed for 2,000 palm vein users in one second. Each user can register two palm vein templates
d) FRR is 0.00001%, Palm Vein detective range of the Palm Vein Sensor from 30mm to 70mm
e) Supports 5,000 local personnel
f) Supports 13.56MHz NXP Mifare Class, Mifare Plus, Mifare DESFire, and LEGIC card technology.
g) 13.56MHz card read range: 5cm+; Bluetooth read range: 0.5m to 10m; QR Code read range: 4cm to 22cm
h) Programmable reader buzzer beep sound interval and times for access granted and access denied
i) Programmable reader LED color (7 colors) interval and times for access granted and access denied
j) Reader configuration can be updated through the network by ACX proprietary software
k) Reader firmware can be upgraded through the network by ACX proprietary software
l) Reader outputs ACX proprietary scramble encryption RS485 format
m) Reader Tamper: Optical sensor
n) Reader size shall be no larger than 80mm(W) x 130mm(H) x 20mm(D)
o) Waterproof IP55 rated

4.12 4-in-1 Multi-technology Facial Recognition Smart Card Reader (Facial Recognition +

Bluetooth + Scramble QR Code + RFID Card)

a) Facial Recognition Algorithm by Face++ / SenseTime technology
b) Facial detection supports binocular infrared live detection
c) Face recognition can be completed in 300 milliseconds
d) The recognition accuracy rate is higher than 99%, and 0.5m-1.5m recognition distance is supported
e) Supports 20,000 local personnel
f) Real-time detection and tracking of human faces; accurate detection can be carried out in situations such as side faces, half occlusion, and blur
g) Minimum 0.5 lux recognition
h) Effective defense against non-living attacks such as 3D printing, electronic screens, video, pictures, masks, hoods, etc.
i) Supports 13.56MHz NXP Mifare Class, Mifare Plus, Mifare DESFire, and LEGIC card technology.
j) 13.56MHz card read range: 5cm+; Bluetooth read range: 0.5m to 10m; QR Code read range: 4cm to 22cm
k) Programmable reader buzzer beep sound interval and times for access granted and access denied
l) Programmable reader LED color (7 colors) interval and times for access granted and access denied
m) Reader configuration can be updated through the network by ACX proprietary software
n) Reader firmware can be upgraded through the network by ACX proprietary software
o) Reader outputs ACX proprietary scramble encryption RS485 format
p) Reader Tamper: Optical sensor
q) Reader size shall be no larger than 80mm(W) x 130mm(H) x 20mm(D)
r) Waterproof IP55 rated

4.13 4-in-1 Multi-technology Facial Recognition Smart Card LCD Reader (Facial Recognition + Bluetooth + Scramble QR Code + RFID Card)

a) Facial Recognition Algorithm by Face ++ / SenseTime technology
b) Reader cover material by Aluminum alloy
c) Reader LCD 5.5”
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) Supports 13.56MHz NXP Mifare Class, Mifare Plus, Mifare DESFire, and LEGIC card technology.
l) 13.56MHz card read range: 5cm+; Bluetooth read range: 0.5m to 10m; QR Code read range: 4cm to 22cm
m) Programmable reader buzzer beep sound interval and times for access granted and access denied
n) Programmable reader LED color (7 colors) interval and times for access granted and access denied
o) Reader configuration can be updated through the network by ACX proprietary software
p) Reader firmware can be upgraded through the network by ACX proprietary software
q) Reader outputs ACX proprietary scramble encryption RS485 format
r) Reader Tamper: Optical sensor
s) Reader size shall be not larger than 96mm(W) x 240mm(H) x 22mm(D)

4.14 4-in-1 Multi-technology Octopus smart lock reader (Octopus + Bluetooth + Scramble QR Code)

a) Support HK Octopus Card, Octopus mobile apps, Octopus watch
b) Supports Octopus, Mobile Virtual Card by Bluetooth 4.0+, and Scramble QR Code
c) Bluetooth read range: 0.5m to 10m; QR Code read range: 4cm to 22cm
d) The reader shall have the Octopus Holding Limited Type Approval Certificate
e) Octopus ISO card read range: 7cm+; Bluetooth read range: 0.5m to 10m; QR Code read range: 4cm to 22cm
f) Programmable reader buzzer beep sound interval and times for access granted and access denied
g) Programmable reader LED color (7 colors) interval and times for access granted and access denied
h) Reader configuration can be updated through the network by ACX proprietary software
i) Reader firmware can be upgraded through the network by ACX proprietary software
j) Reader outputs ACX proprietary scramble encryption RS485 format Reader size shall be no larger than 94mm(W) x 196mm(H) x 55mm(D)
k) 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 wear masks and have average 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 turnstile of 1.6m to 1.9m in length.
g. The turnstile height range is 1000mm to 1050mm
h. The thermal camera scan range covers people taller than 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 third-party integration of lift destination control, visitor management, and lift destination control systems.
b. It supports palm vein, facial recognition, mobile scramble QR code, contactless smart card 13.56MHz RF, and NFC technology. Once the reader detects the user's identity, the LCD screen will display the 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 a 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
j. Power input 12VDC, 1A

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
e. Power input, 12VDC, 1A

4.19 Network Alarm Panel

a. 2 x LAN Port, allow daisy chain connection
b. Suitable for huge sensor 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
i. Power input, 12V, 500mA

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 correcting any defects arising out of such a test and having the work retested. Such costs shall also include the provision of all instruments necessary for the test.

5.2 A specialist Subcontractor (SSC) shall carry out the commissioning. The SSC shall commission the respective installed service 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 a full warranty period of 1 year, including all systems, deployed equipment and version upgrades, fix and patch updates, and labor 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 materials, parts, tools, equipment, and qualified labor to carry out the maintenance and repair services throughout the full warranty period.

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

6.4 System and software problem diagnosis shall be provided on-site or remotely by the Contractor's engineer(s) or specialist(s). They should follow through with the whole diagnostic activity, including but not limited to gathering logs, discussing with the back end, setting up and applying the fixes in the environment for verification, preparing and providing information to ease the diagnostic, etc.

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

-End-