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

* 1. 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.
1. **Scope of Work, Design Requirements, and Performance**
	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: -
2. Supply and installation of the complete SACS for doors along with all associated equipment and accessories.
3. Supply and installation of the complete SACS for security gates (turnstiles) along with all associated equipment and accessories.
4. 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.
	1. 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. The Contractor shall submit provide as-fitted drawings, comprehensive testing and commissioning documents, and O&M manuals.
	3. Training of Employer’s staff shall be provided.
	4. Supply of Spares, tools, and accessories for the electrical and extra low voltage installations as specified.
	5. 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.
	6. 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,
	7. 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.

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

# System Description

* 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.
	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. 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.
	4. The SACS shall be in one software platform which includes: -
1. Access Control System
2. One software and One database design.
3. The SACS server program can be installed on the cloud or on-premises.
4. The SACS can be running on the non-VPN network.
5. Software admin can create users who have different access rights for the cardholder and the controllers.
6. Allow remote maintenance of access controllers, access control readers, and time zones setting
7. Supports multi-technology (Bluetooth, Scramble QR Code, Palm Vein, Facial Recognition, RFID Card, NFC, Keypad, and Octopus) access control reader
8. Email notification for critical events
9. Integrated with NVR, swipe card playback, and recording to the external device
10. Integrated with building visitor management system
11. Integrated with facility room booking system
12. Integrated with lift destination control system
13. Integrated with video management system application
14. Integrated with turnstile body temperature and Mask check
15. Integrated with mailbox/locker system
16. Integrated with 3rd party building management system
17. Lift Control System
18. Low-level integration with lift server panel
19. Access time zone control for the lift floor
20. User has access rights for individual floors and the access time zone
21. Supports multi-technology access control reader
22. Integrated with building visitor management system
23. Visitor Management System
24. The visitor management system (VMS) can be applied to entire building tenants.
25. The VMS server can be cloud-based or on-premises.
26. Tenants can through the web browser or mobile apps maintain the VMS.
27. The VMS server keeps all the visitor pre-registered records and the visitor access records.
28. The VMS booking and access records can be auto-deleted in a certain period
29. 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.
30. The web-based application shall have an SSL certificate.
31. The VMS server program
	* 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.
32. The web-based visitor management application
	* 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 Subcontractor 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.
33. The Client application is for concierge operation
	* 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.
34. The iPad-based visitor application (optional)
	* 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.
35. Facility Booking System
36. Available to make room or facility booking on a computer via a web portal and smart device via APP
37. Integrated with Access Control System
38. Check room status and review all bookings online and outside the meeting room
39. Works with interactive touch display
40. Able to generate and export workplace analytics report
41. Customization available
42. Shuttle Bus System
43. User-friendly platform for managing shuttle bus driver and passenger
44. Driver clock in via APP
45. Real-time checking of passenger’s authority of taking a shuttle
46. Track record
47. Smart Locker / Mailbox System
48. Architecture
* This is a client-server software application that 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.
1. 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.
1. 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.
1. Database requirement
* MS SQL 2019 or above
1. 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
1. Reporting
* All kinds of reports can be viewed on-screen and sent to the printer
* Report can export to TEXT, EXCEL & PDF files.
1. Cardholder management
* Provide Import and Export data tool for 3rd party data integration
1. Door access activated by the specified card holder
* The mailbox/locker is allowed for use before the specified card authorization
1. Electronics Map Monitoring
2. Real-time display of door and sensor status
3. Real-time video monitoring
4. Control E-lock open & close
5. Group/ individual acknowledgment
6. Integrated with video management system application
7. Turnstile System
8. The turnstile system shall integrate into the lift destination control system and building visitor management system
9. 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 install on top of the turnstile top surface area. The device measure body temperature and wear mask conditions, the response time shall be less than 1.5 second
10. The body thermal and wear mask detection device shall cater to people’s height from 1.2m to 1.9m and also cater the people in a wheelchair.
11. 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, QR code reader which can handle mobile scramble QR code and paper fixed QR code.
12. User can select their registered access credentials to access the turnstile.
13. 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
14. The Facial Recognition algorithm shall be provided by SenseTime or Face++.
15. The Palm Vein Recognition technology shall be provided by Fujitsu PalmSeure-F Pro sensor
16. Time Attendance System
17. Design for scheduling the staff and taking attendance
18. User’s roster can be set by company/ department/ division/ personal level
19. Unlimited shift table for people duty time period
20. Unlimited roster table assigns by different grouping levels as by company level, by department level, or by the individual.
21. Fast report generation
22. Individually attendance and Master attendance report
23. The attendance report can be automatically generated by schedule and sent to the authorized recipients through email.
24. Surveillance System Integration
25. Manage all surveillance video sources in one system
26. Configure cameras (IP address) to the system
27. CCTV playback in the access record inquiry
	1. 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.
	2. 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. 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.
	4. The SACS shall utilize the Fast Ethernet network for communication.
	5. The SACS shall enable setting as per access right privilege level such that:
28. Access rights can be granted to different groups of people at different access points.
29. 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.
	1. The SACS shall allow access control readers to be configured in the workstation to operate in any of the following modes: -
30. Free Access Mode:

The door is unlocked and no card is required for entry.

1. Secure Access Mode:

A successful card attempt is required for valid entry.

1. Secure Biometric Mode:

A successful palm vein or facial attempt is required for valid entry.

* 1. A local workstation shall be provided. The status of the system shall be monitored and repeated to the central workstation via fiber optic cables.
	2. 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. 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.
	4. 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.
	5. The SACS shall be able to work under offline mode.

* 1. 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.
	2. 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. 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.
	4. 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.

1. The Platform shall provide a Web portal for data entry.
2. The Platform shall have a user ID and password login control.
3. The Platform shall use 2 sets of 64 bits customer keys as the data exchange key on mobile and reader communication.
4. 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.
5. The Platform shall prohibit the same virtual card number to register on more than one mobile device.
6. Operator can disable the virtual card number on the registered mobile.
7. The virtual card number can be reused.
8. The Platform shall include a Mobile Virtual Card APP which is available at the Android and iOS stores. The Mobile Virtual Card APP shall have Bluetooth & Scramble QR code feature for short-range and mid-range access control applications.
9. 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.
10. 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.
11. Mobile Bluetooth communicates to access control reader shall have scramble encryption to ensure the data cannot be played back by other devices.
12. Scramble QR code virtual card by mobile APP shall be scrambled in every second, the copied QR code will be disabled after a specified time period. The specified time period shall be less than 5 seconds and different time periods can be set for each virtual card.
13. The Mobile Virtual Card APP can be running in off-line mode (no internet connection)
	1. The access control for all project areas shall be completed with an online access control system to notify an access request and the local and central database shall keep a record of the request.
	2. Firmware of SACS shall be able to be updated remotely via a network connection.
14. **Materials and Equipment**
15. Access Control System Server and Workstation
16. Server hardware and software requirement
17. Completed with 1920 x 1080 LCD monitor, mouse, keyboard, and software.
18. WIN 10 Professional 64 bits edition, English / Chinese operating system
19. SQL express 2016 or above
20. INTEL i7 Processor (3.4GHz, 8M cache) or equivalent
21. 500GB SSD, 8GB DDR4 RAM
22. 1 x LAN Port, 4 x USB3.0
23. UPS to give non-stop power supply for minimum of 30 minutes after failure of the main power
24. Workstation
25. It shall be completed with 1920 x 1080 LCD monitor, mouse, keyboard, software.
26. WIN 10 Professional 64 bits edition, English / Chinese operating system
27. INTEL i7 Processor (3.4GHz, 8M cache) or equal
28. 128GB SSD, 8GB DDR4 RAM
29. 1 x LAN Port, 4 x USB3.0
30. UPS to give non-stop power supply for minimum of 30 minutes after the failure of the main power
31. Integrated Access Control System Software
32. Architecture
33. Windows-based application which can run on WIN 10/ Windows Server 2020 or higher version.
34. Server Program is a service in the PC/Server, once the PC/Server is restarted, the server program will run automatically.
35. Software has multi-language features.
36. User can online change the software text content.
37. The maximum number of concurrent user logins will be under control.
38. Same database for storing Facial template, Palm Vein template, Fingerprint template, and card number.
39. Same software interface for managing Facial, Palm Vein, Virtual Card registration, fingerprint, mobile virtual card, and access control distribution.
40. Communication
41. Server program uses multi-threading programming technique, which direct communication to access the control panel on Ethernet cable, real-time response.
42. TCP/IP communication.
43. Data Security
44. User-defined 128 bits master key in Server and Panel for data encryption.
45. A unique 192 bits random key is generated during per data transmission.
46. Data encryption method, master key encrypts random key, random key encrypts the exchanged data during communication.
47. AES128 and 3DES Algorithm mixed.
48. Database requirement
49. MS SQL 2019 or above
50. Application user authority
51. Password protection
52. Application’s access can be filtered by View / Add / Edit / Delete
53. User data access can be filtered
54. Access panel access can be filtered
55. Event status can be filtered
56. Event acknowledge can be filtered
57. Reporting
58. All kinds of reports can be viewed on-screen and sent to the printer
59. Report can export to TEXT, EXCEL & PDF files.
60. Email Service
61. User can receive alarm records by email
62. User can receive their daily access record by email
63. Supervisor can view group users’ access reports and different kinds of time attendance reports by email
64. Access control system
65. Real-time upload parameters to panels
66. Client software can read controller and reader parameters instantly.
67. Controller and reader parameters can be defined by global or by individual
68. 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
69. Fire Alarm Group
	* + Allow 255 fire alarm groups for any combination of the door lock released when a fire alarm is triggered
70. Cardholder management
71. Provide Import and Export data tool for 3rd party data integration
72. Cardholder access rights can be selected by department or door group
73. Software can define 1,000+ suspected cardholder groups for instant enable or disable their access rights
74. Cardholder access rights can be defined by door group or by department
75. Staff management
76. Provide Import and Export data tool for 3rd party data integration
77. Online capture of a personal photo, palm vein, fingerprint biometric templates
78. Print staff badge
79. Time zone control
80. Each time zone has 4 intervals per day, Mon to Sun & Holiday
81. 100 Holiday dates per door access control panel
82. 10,000+ door access time zone in the database, 80 door time zones per door access control panel
83. Password time zone
84. Electric Lock release time zone
85. Twin card operation time zone
86. Release button time zone
87. Door opens too long time zone
88. Alarm time zone
89. Twin card operation
90. Twin card operation with time zone control for high-security access control application.
91. Door access activated by the specified card holder
92. The door is allowed for use before the specified card authorization
93. Power Monitoring
94. A.C. power failure monitoring
95. Backup failure monitoring (20% of full load)
96. Transaction and Events viewer
97. Global viewer for card access records and events
98. Individual / Multi viewer for card access records to display card holder details information, e.g., Photo etc.
99. Alarm viewer displays the live camera
100. Card access records filter by user, control panel, date and time, and access status.
101. Different sorting order, ascending or descending, all access record, only IN or OUT or First IN last OUT record.
102. Event records can be filtered by the control panel, date and time, and status.
103. Event records can be previewed and sent the file to the printer.
104. Export the file to EXCEL, text, and PDF
105. Event monitoring system
106. Each event can be defined by different icons
107. Software can define the device input normal status in NC or NO
108. Action taken can be assigned to each device input when the alarm triggered
109. Action items as like as Acknowledgment requested, door open by the fire alarm, enable surveillance integration, signal integration with third-party BMS, and play music etc.
110. PoE+ Networked Single Door Access Panel
111. Architecture
112. PoE+ TCP/IP based single door panel
113. The overall power consumption is 30W, max. 17W power reserves for E-Lock.
114. Wiring method: Cat 5 cable for the panel to PoE+ switch
115. Communication
116. PC to Panel, TCP/IP communication
117. Scramble data encryption during PC/Server to panel data exchanges through the network cable
118. Panel to the reader, Wiegand or scramble RS485 data encryption
119. Active upload for swipe card records and events
120. Data Security
121. Apply scramble data encryption methodology during data exchange
122. 128 bits’ user master key on PC, Panel, and Reader
123. 192 bits’ random key auto-generated per communication
124. Master key encrypts random key, random key encrypts data exchanges between PC and Panel, Panel and Reader
125. AES 128 & 3 DES mixed Algorithm
126. Reader supports
127. 1 x IN and 1 x OUT for single door panel
128. Supports scramble RS485 reader
129. 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)
130. Card number format
131. Default 26 / 32/ 34 / 35 / 37 / 56 / 64 and three custom formats
132. Each card format can have three facility code
133. Support four card formats at the same time
134. Card number length, maximum 64 bits
135. Memory storage
136. Memory for the card holder
	* + Single door controller
			- Allow storage of at least 40,000 sets of card numbers
137. Memory for transactions
	* + Single door controller: allow storage of at least 42,000 nos. of transactions
138. Events: allow storage of at least 800 nos. of events
139. Time zone control
140. Each time zone has 4 intervals per day, Mon to Sun & Holiday
141. 100 Holiday dates per door access control panel
142. 10,000+ Door access time zone in the database, 80 time zones per door access control panel
143. Password time zone
144. Electric Lock release time zone
145. Twin card operation time zone
146. Release button time zone
147. Door opens too long time zone
148. Alarm time zone
149. LCD reader message time zone
150. Fire Alarm
151. Panel AUX #1 for fire alarm input
152. 255 fire alarm groups per panel
153. Firm alarm signal broadcasts through the network card, no need through the PC server
154. Twin card operation
155. Twin card operation with time zone control for high-security access control application. E.g., Car park system, treasury application.
156. Anti-pass back
157. Single door panel (single anti-pass back)
158. Device Inputs
159. Auto detect end-of-line resistors were installed or not, if yes, enable supervised monitoring
160. Supervised monitoring needs end-of-line resistors, 1K ohm + 1K ohm
161. Door release button (Normal Open)
162. Door Sensor (Normal close)
163. Panel temper box sensor (Normal Close)
164. 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
165. Device Outputs
166. Access granted output for E-Lock operation. 12VDC, 10A Relay (N.O. / N.C.)
167. Alarm output. 12VDC, 5A Reply (N.O. / N.C.)
168. Door Ajar. 5VDC, 10mA output
169. High-Security Key Switch
170. Tamper proof for the E-Lock override
171. Tamper proof for short circuit or open circuit of the exposed key switch’s wires
172. Expand RS485 port
173. 2 x RS485 port
174. High-level data exchange with a third-party system
175. 2 x Auxiliary input
176. Auxiliary input # 1 – Fire alarm trigger then auto release E-Lock
177. Auxiliary input # 2 – Trigger alarm relay
178. Networked Door Access Panel
	* 1. Architecture
179. TCP/IP-based network control panel
180. Built-in two LAN ports
181. Wiring method: Cat 5 cable for the panel to network switch or panel to panel (daisy chain)
182. Communication
183. PC to Panel, TCP/IP communication
184. Scramble data encryption during PC to panel data exchanges through a network cable
185. Panel to the reader, Wiegand or scramble RS485 data encryption
186. Active upload for swipe card records and events
187. Data Security
188. Apply scramble data encryption methodology during data exchange
189. 128 bits’ user master key on PC, Panel, and Reader
190. 192 bits’ random key auto-generated per communication
191. Master key encrypts random key, random key encrypts data exchanges between PC and Panel, Panel and Reader
192. AES 128 & 3 DES mixed Algorithm
193. Reader supports
194. 1 x IN and 1 x OUT for single door panel
195. 2 x IN and 2 x OUT for two-door panel
196. Supports scramble RS485 reader
197. 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)
198. Card number format
199. Default 26 / 32/ 34 / 35 / 37 / 56 / 64 and three custom formats
200. Each card format can have three facility code
201. Support four card formats at the same time
202. Card number length, maximum 64 bits
203. Memory storage
204. Memory for the card holder
	* + Single door controller
			- Allow storage of at least 40,000 sets of card numbers only
		+ Two-door controller
			- Allow storage of at least 20,000 sets of card numbers only
205. 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
206. Events: allow storage of at least 800 nos. of events
207. Time zone control
208. Each time zone has 4 intervals per day, Mon to Sun & Holiday
209. 100 Holiday dates per door access control panel
210. 10,000+ Door access time zone in the database, 80 time zones per door access control panel
211. Password time zone
212. Electric Lock release time zone
213. Twin card operation time zone
214. Release button time zone
215. Door opens too long time zone
216. Alarm time zone
217. LCD reader message time zone
218. Fire Alarm
219. Panel AUX #1 for fire alarm input
220. 255 fire alarm groups per panel
221. Firm alarm signal broadcasts through the network card, no need through the PC server
222. Twin card operation
223. Twin card operation with time zone control for high-security access control application. E.g., Car park system, treasury application.
224. Anti-pass back
225. Single door panel (single anti-pass back)
226. Two-door panel (single or global anti-pass back)
227. Global anti-pass back, through the server.
228. Device Inputs
229. Auto detect end-of-line resistors were installed or not, if yes, enable supervised monitoring
230. Supervised monitoring needs end-of-line resistors, 1K ohm + 1K ohm
231. Door release button (Normal Open)
232. Door Sensor (Normal close)
233. Panel temper box sensor (Normal Close)
234. 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
235. Device Outputs
236. Access granted output for E-Lock operation. 12VDC, 10A Relay (N.O. / N.C.)
237. Alarm output. 12VDC, 5A Reply (N.O. / N.C.)
238. Door Ajar. 5VDC, 10mA output
239. High-Security Key Switch
240. Tamper proof for the E-Lock override
241. Tamper proof for short circuit or open circuit of the exposed key switch’s wires
242. Expand RS485 port
243. 2 x RS485 port
244. High-level data exchange with third-party system
245. 2 x Auxiliary input
246. Auxiliary input # 1 – Fire alarm trigger then auto release E-Lock
247. Auxiliary input # 2 – Trigger alarm relay
248. Electric Lock
249. Electromagnetic Lock with built-in door sensor
250. Fail-Safe: unlocks when the power supply fails
251. Easy installation: suitable for both new and retrofit usage
252. High holding force (280KG or above)
253. Self-alignment: armature plate pivots to accommodate door drop
254. Silent operation: no humming or buzzing
255. Dual voltage: site selectable 12 or 24 VDC
256. Instantaneous release: smart electronics on the A Series Electromagnets eliminate residual magnetism
257. Two secured metal wires for the Lock body mounted on the door frame
258. One secured metal wire for the armature plate mounted on the door
259. Door Release Button
260. Infra-red sensor door release button shall be provided.
261. 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.
262. Door emergency exit device (Resettable Call Point)
263. The resettable call point comes with a hinged front cover to prevent the unit from activating randomly.
264. Once the “PRESS HERE” button was pressed, the E-Lock power is cut, and the door is released.
265. The call point can be reset by inserting a plastic key horizontally into the front panel of the resettable call point.
266. The call point unit shall have an LED light to identify the operation mode. RED, GREEN, BLUE, and mixed colors shall be assigned for normal mode and emergency exit mode.
267. 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.
268. For emergency exit mode, the call point shall have a beep sound notification.
269. The LED and buzzer setting shall be operated by a DIP switch.
270. The call point shall have two set dry contact switches, one set for E-Lock power, and another set for signal output. The current rate of the switch is 5ADC under a 12VDC power supply.
271. The resettable call point shall have a voltage regulator to support E-Lock power in AC/DC, 12V/24V.
272. Power Supply Box
273. The power supply box shall have a metal casing.
274. The power supply box shall have earth wiring.
275. The size of the power supply box shall be not more than 340mm(H) x 290mm(W) x 80mm(D).
276. 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 of electric lock installed.
277. The power supply shall have a battery charging function.
278. The power supply can output 0VDC or 5VDC voltage level to the controller to indicate the occurrence of the following events: -
279. AC. power failure
280. DC battery installed
281. backup battery power was lower than 20%
282. A 7AH DC battery shall be included. In case of AC power supply failure, the door access system can be operated for 4 hours.
283. High Security Override key switch and key switch controller
284. The High-security override key switch works with a key controller, no matter if the key switch has been tampered, the electric lock keeps the original lock status
285. 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 has been tampered with, the LED indicator goes off.
286. If the key switch has been tampered with, no matter short-circuits or cuts the wires between the key switch and key switch controller, the electric lock status remains unchanged.
287. Reset the button in the key switch controller which to activate the key switch function
288. 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.
289. Minimum 3 sets of master keys shall be provided to the end customer.
290. 3-in-1 Multi-technology Smart Card Reader (Bluetooth + Scramble QR Code + RFID Card)
291. Supports 13.56MHz NXP Mifare Class, Mifare Plus, Mifare DESFire, and LEGIC card technology.
292. Supports 13.56MHz NXP Mifare Class, Mifare Plus, Mifare DESFire, and LEGIC card technology.
293. 13.56MHz card read range: 5cm+; Bluetooth read range: 0.5m to 10m; QR Code read range: 4cm to 22cm
294. Programmable reader buzzer beep sound interval and times for access granted and access denied
295. Programmable reader LED color (7 colors) interval and times for access granted and access denied
296. Reader configuration can be updated through the network by ACX proprietary software
297. Reader firmware can be upgraded through the network by ACX proprietary software
298. Reader outputs ACX proprietary scramble encryption RS485 format
299. Reader Tamper: Optical sensor
300. Reader size shall be not larger than 80mm(W) x 130mm(H) x 20mm(D)
301. Waterproof, IP65 rated
302. 4-in-1 Multi-technology Smart Card Keypad Reader (Keypad + Bluetooth + Scramble QR Code + RFID Card)
303. Supports 13.56MHz NXP Mifare Class, Mifare Plus, Mifare DESFire, and LEGIC card technology.
304. 12 capacitance touch keypads, 0~9,\*,#. Keypad has blacklight in 7 different colors.
305. Supports 13.56MHz NXP Mifare Class, Mifare Plus, Mifare DESFire, and LEGIC card technology.
306. 13.56MHz card read range: 5cm+; Bluetooth read range: 0.5m to 10m; QR Code read range: 4cm to 22cm
307. Programmable reader buzzer beep sound interval and times for access granted and access denied
308. Programmable reader LED color (7 colors) interval and times for access granted and access denied
309. Reader configuration can be updated through the network by ACX proprietary software
310. Reader firmware can be upgraded through the network by ACX proprietary software
311. Reader outputs ACX proprietary scramble encryption RS485 format
312. Reader Tamper: Optical sensor
313. Reader size shall be not larger than 80mm(W) x 130mm(H) x 20mm(D)
314. Waterproof IP65 rated
315. 4-in-1 Multi-technology Palm Vein Smart Card Reader (Palm Vein + Bluetooth + Scramble QR Code + RFID Card)
316. Palm Vein recognition technology should be provided by Fujitsu PalmSecure-F Pro sensor
317. Palm Vein Sensor supports binocular infrared live detection
318. Palm Vein recognition can be completed in one second for 2,000 palm vein users. Each user can register 2 palm vein templates
319. FRR is 0.00001%, Palm Vein detective range of the Palm Vein Sensor from 30mm to 70mm
320. Supports 5,000 local personnel
321. Supports 13.56MHz NXP Mifare Class, Mifare Plus, Mifare DESFire, and LEGIC card technology.
322. 13.56MHz card read range: 5cm+; Bluetooth read range: 0.5m to 10m; QR Code read range: 4cm to 22cm
323. Programmable reader buzzer beep sound interval and times for access granted and access denied
324. Programmable reader LED color (7 colors) interval and times for access granted and access denied
325. Reader configuration can be updated through the network by ACX proprietary software
326. Reader firmware can be upgraded through the network by ACX proprietary software
327. Reader outputs ACX proprietary scramble encryption RS485 format
328. Reader Tamper: Optical sensor
329. Reader size shall be not larger than 80mm(W) x 130mm(H) x 20mm(D)
330. Waterproof IP55 rated
331. 4-in-1 Multi-technology Facial Recognition Smart Card Reader (Facial Recognition + Bluetooth + Scramble QR Code + RFID Card)
332. Facial Recognition Algorithm by SenseTime technology
333. Facial detection supports binocular infrared live detection
334. Face recognition can be completed in 300 milliseconds
335. The recognition accuracy rate is higher than 99% and 0.5m-1.5m recognition distance is supported
336. Supports 20,000 local personnel
337. Real-time detection and tracking of human faces, accurate detection can be carried out in situations such as side faces, half occlusion, and blur
338. Minimum 0.5 lux recognition
339. Effective defense against non-living attacks such as 3D printing, electronic screens, video, pictures, masks, hoods, etc.
340. Supports 13.56MHz NXP Mifare Class, Mifare Plus, Mifare DESFire, and LEGIC card technology.
341. 13.56MHz card read range: 5cm+; Bluetooth read range: 0.5m to 10m; QR Code read range: 4cm to 22cm
342. Programmable reader buzzer beep sound interval and times for access granted and access denied
343. Programmable reader LED color (7 colors) interval and times for access granted and access denied
344. Reader configuration can be updated through the network by ACX proprietary software
345. Reader firmware can be upgraded through the network by ACX proprietary software
346. Reader outputs ACX proprietary scramble encryption RS485 format
347. Reader Tamper: Optical sensor
348. Reader size shall be not larger than 80mm(W) x 130mm(H) x 20mm(D)
349. Waterproof IP55 rated
350. 4-in-1 Multi-technology Facial Recognition Smart Card LCD Reader (Facial Recognition + Bluetooth + Scramble QR Code + RFID Card)
351. Facial Recognition Algorithm by SenseTime technology
352. Reader cover material by Aluminum alloy
353. Reader LCD 5.5”
354. Facial detection supports binocular infrared live detection
355. Face recognition can be completed in 300 milliseconds
356. The recognition accuracy rate is higher than 99% and 0.5m-1.5m recognition distance is supported
357. Supports 20,000 local personnel
358. Real-time detection and tracking of human faces, accurate detection can be carried out in situations such as side faces, half occlusion, and blur
359. Minimum 0.5 lux recognition
360. Effective defense against non-living attacks such as 3D printing, electronic screens, video, pictures, masks, hoods, etc.
361. Supports 13.56MHz NXP Mifare Class, Mifare Plus, Mifare DESFire, and LEGIC card technology.
362. 13.56MHz card read range: 5cm+; Bluetooth read range: 0.5m to 10m; QR Code read range: 4cm to 22cm
363. Programmable reader buzzer beep sound interval and times for access granted and access denied
364. Programmable reader LED color (7 colors) interval and times for access granted and access denied
365. Reader configuration can be updated through the network by ACX proprietary software
366. Reader firmware can be upgraded through the network by ACX proprietary software
367. Reader outputs ACX proprietary scramble encryption RS485 format
368. Reader Tamper: Optical sensor
369. Reader size shall be not larger than 96mm(W) x 240mm(H) x 22mm(D)
370. 4-in-1 Multi-technology Octopus smart lock reader (Octopus + Bluetooth + Scramble QR Code)
371. Support HK Octopus Card, Octopus mobile apps, Octopus watch
372. Supports Octopus, Mobile Virtual Card by Bluetooth 4.0+ and Scramble QR Code
373. Bluetooth read range: 0.5m to 10m; QR Code read range: 4cm to 22cm
374. The reader shall have the Octopus Holding Limited Type Approval Certificate
375. Octopus ISO card read range: 7cm+; Bluetooth read range: 0.5m to 10m; QR Code read range: 4cm to 22cm
376. Programmable reader buzzer beep sound interval and times for access granted and access denied
377. Programmable reader LED color (7 colors) interval and times for access granted and access denied
378. Reader configuration can be updated through the network by ACX proprietary software
379. Reader firmware can be upgraded through the network by ACX proprietary software
380. Reader outputs ACX proprietary scramble encryption RS485 format Reader size shall be not larger than 94mm(W) x 196mm(H) x 55mm(D)
381. Flush mount design with only 6mm extruded from the wall
382. Thermal Camera for turnstile installation
383. Built-in black body to increase the temperature accuracy.
384. Embedding camera to the turnstile to check body temperature & mask on, and allow facial access.
385. Automatically check whether passengers are wearing a mask and have normal body temperature without physical contact.
386. With an effective scan range of 3m.
387. Tiny and streamlined enclosure without any display.
388. The enclosure surface is 75 degrees to the ground which is suitable for a 1.6m to 1.9m length turnstile.
389. The turnstile height range is 1000mm to 1050mm
390. The thermal camera scan range cover people tall from 1.2m to 1.9m standing in front of the edge of the turnstile.
391. Superior low-light performance.
392. Latest 3.0µm pixel with ON Semiconductor DR-Pix technology with Dual Conversion Gain.
393. Full HD support at up to 1080p 60fps for superior video performance.
394. Liner or high dynamic range capture.
395. Auto black level calibration.
396. Turnstile Reader
397. Provides an open platform for 3rd party integration of lift destination control and visitor management system and lift destination control system.
398. 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.
399. Programmable buzzer beep sound interval for access granted and access denied
400. Red / Green / Blue or mixed LED for visual notification
401. Programmable LED flash interval for access granted and access denied
402. Reader outputs Wiegand and scrambles encryption RS485 format
403. The turnstile readers and the thermal device shall work with 8980 turnstile gateways
404. Networked Lift Control Master Panel
405. A multi-purpose device that provides an interface between field level input, output devices and an Lift application server
406. True IP device, support DHCP
407. 2 x LAN Port, allow daisy chain connection
408. Dry contact supervised monitoring
409. User-defined NC / NO at normal mode
410. 2 x INPUTs for Manual key overwrite and Fire Alarm input
411. 28 x RELAY outputs for 28 Floors access, RELAY in 3A DC output
412. Panel installation depends on the IP address available
413. RS485 port for 8907 Lift control expand panel
414. Power input 12VDC, 1A
415. Networked Lift Control Expansion Panel
416. Works with Networked Lift Control Master Panel
417. RS485 connection
418. User-defined NC / NO at normal mode
419. 38 x RELAY outputs for extra 38 Floors access, RELAY in 3A DC output
420. Power input, 12VDC, 1A
421. Network Alarm Panel
422. 2 x LAN Port, allow daisy chain connection
423. Suitable for huge sensors monitoring
424. Dry contact supervised monitoring
425. User-defined NC / NO at normal mode
426. 28 Input Points, 2 RELAY 10A output per panel
427. Panel installation depends on the IP address available
428. Relay status triggered by 28 Inputs AND / OR program logic
429. RS485 port for proprietary device communication
430. Power input, 12V, 500mA
431. **Commissioning and Testing**
432. 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.
433. 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.
434. **Warranty, Maintenance and Emergency Support Requirements**
	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.
	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.
	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.
	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.
	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-