

**Smart Mailbox / Locker Specification**  
**Manufacturer - Matrix Research Limited**  
**Product Brand - ACX**

**1. Mailbox/Locker 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 smart lock system installation work. The description in this section may not necessarily describe the Works in full detail. Reference shall be made to other sections of this specification and tender drawings. Due allowance shall be made to include necessary fittings, auxiliaries, and sundry items compatible with good trade practices to provide a complete and efficient system to meet the specified performance requirements.
- 3.3 By using mobile scramble / dynamic QR code technology, 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 smart lock system shall be in one software platform which includes: -
- a. Smart Locker System
    - i. Design for lock rental services
    - ii. Supports multi-technology (Bluetooth, Scramble QR Code, Palm Vein, Facial Recognition, RFID Card, Keypad, and Octopus) access control reader
  - b. Smart Mailbox System
    - i. Allow checking mailbox status via email, APP and SMS
    - ii. Real-time notification upon receiving a letter through email, SMS or mobile apps.
    - iii. Mailbox / Locker application server has API for 3<sup>rd</sup> party software integration
    - iv. Enable unlocking mailbox lock by smartphone via Bluetooth or Scramble QR Code
    - v. Supports multi-technology (Bluetooth, Scramble QR Code, Palm Vein, Facial Recognition, RFID Card, Keypad, and Octopus) access control reader
- 3.5 The smart lock system shall be fully interoperated under one authorization management, i.e. the system shall be operated under one database system. The identification/coding of equipment, smart card holders, etc. shall follow the same logic and format.

- 
- 3.6 The smart lock system shall consist of a workstation complete with an LCD monitor, local database server, network switches, networked mailbox master controller/ mailbox expansion controller, multi-technology smart lock readers, and mailbox/ locker locks, and all associated software and accessories.
- 3.7 The smart lock system shall utilize the Fast Ethernet network for communication.
- 3.8 A local workstation shall be provided. The status of the system shall be monitored and repeated to the central workstation via fiber optic or CAT6 cables.
- 3.9 Networked mailbox master controller/ mailbox expansion controller 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 main power failure.
- 3.10 The database of access rights to each mailbox/ locker shall be stored at each networked mailbox master controller/ mailbox expansion controller so that any communications breakdown shall not affect the operation of any individual door.
- 3.11 Each smart lock reader shall communicate with networked mailbox master controller/ mailbox expansion controller by RS485 cable with scramble encryption technology, the reader to controller cable distance can be extended to 1,200 meters.
- 3.12 The smart lock system shall be able to work under offline mode.
- 3.13 All smart lock 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 NFC/ Keypad/ Palm Vein/ Facial Recognition/ Octopus shall be available as additional provisions to the smart lock reader.
- 3.14 The smart lock system 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 inputting the activation code sent by the operator, a virtual card number will be generated on mobile. The mobile virtual card can be running on no internet connection.
- 3.15 The access control for mailboxes/ lockers 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.
- 3.16 Firmware of the smart lock system shall be able to be updated remotely via a network

connection.

- 3.17 The mail arrival and the mailbox door status shall be real-time updated to the mailbox server.
- 3.18 The mail server shall have API for 3<sup>rd</sup> party application development.

## 2. Materials and Equipment

### 4.1 Smart Lock System Server and Workstation

#### a) Server hardware and software requirement

- i. Completed with 1920 x 1080 LCD monitor, mouse, keyboard, and software.
- ii. WIN 10 Professional 64 bits edition, English / Chinese operating system
- iii. MS SQL Express 2020 or above
- iv. INTEL i7 Processor (3.4GHz, 8M cache) or equivalent
- v. 1TGB SSD, 16GB 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 the 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 10 Professional 64 bits edition, English / Chinese operating system
- iii. INTEL i5 Processor (2.4GHz, 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 Smart Lock System Software

#### a) Architecture

- i. This client-server software application can run on WIN 11 or the latest Windows version.
- ii. The Server Program is a service on the PC server. Once the PC server restarts, the server program runs automatically.
- iii. Client Software has multi-language features, which include English, Traditional Chinese, and Simplify Chinese.
- iv. Users can change the software text content online.
- v. Unlimited client application installed, but the maximum number of concurrent user logins will be under control
- vi. Same database for storing the Facial template, Palm Vein template, and card number.

- vii. Same software interface for managing Facial, Palm Vein, Virtual Card registration, and access control distribution.
- b) Communication
  - i. The server program uses a multi-threading programming technique, which directs 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) Cardholder management
  - i. Provide Import and Export data tools for 3rd party data integration
- h) Door access activated by the specified cardholder
  - i. The mailbox/locker is allowed for use before the specified card authorization

#### 4.3 Network Mailbox Master Controller/ Mailbox Expansion Controller

- a) Designed in IP-based, high-speed data communication
- b) The mailbox master controller can control 12 sets of locksets, and the mailbox expansion controller can control 16.
- c) The mailbox master controller is IP-based and connects to the mailbox system server
- d) The mailbox master controller has an RS485 port, connecting to 31 sets of mailbox expansion controllers.
- e) One available IP address can handle 508 sets of mailboxes
- f) Real-time message of the letter's arrival
- g) Mailbox's door and E-Lock status are available through SMS / POP Message / Email / API.
- h) The master locker/mailbox controller can connect two pcs smart lock readers. The multi-

technology smart lock reader refers to item 4.5 / 4.6 / 4.7 / 4.8.

#### 4.4 Mailbox / Locker Lock

- a) The mailbox/locker lock includes a DC motorized lock, one set door sensor, one set internal infra-red sensor, and two sets of external sensors for object detection.
- a) Electric lock: fail-secured mode.
- b) Total 4 sensors for mailbox/locker door tamper monitoring and mail arrival notification.
- c) Support emergency opening design. If the locker/mailbox's electric lock is not functioning properly, the user can remove the temper label on the locker/mailbox door and open the electric lock manually with special tools.
- d) 100mA for regular operation, 1.5A for opening the electric lock.
- e) Locker lock size shall be not larger than 104mm(W) x 80mm(H) x 17mm(D)
- f) The wiring of the locker/mailbox lock cannot be exposed inside the locker/mailbox area.

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

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

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

- a. Supports 13.56MHz NXP Mifare Class, Mifare Plus, Mifare DESFire, and LEGIC card technology.
- b. 12 capacitance touch keypad
- c. Supports Mobile Virtual Card, Bluetooth 4.0+ and Scramble QR Code
- d. 13.56MHz card read range: 5cm+; Bluetooth read range: 0.5m to 10m; QR Code read range: 4cm to 22cm
- e. NFC technology compatibility (13.56 MHz NFC)
- f. Programmable buzzer beep sound interval for access granted and access denied
- g. Red / Green / Blue or mixed LED for visual notification

- h. Programmable LED flash interval for access granted and access denied
- i. Reader can be configured online
- j. Reader outputs ACX proprietary scramble encryption RS485 format
- k. Reader Tamper: Optical sensor
- l. Reader size shall be not larger than 80mm(W) x 130mm(H) x 20mm(D)
- m. IP55 rated

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

- a) Supports 13.56MHz NXP Mifare Classic, Mifare Plus, Mifare DESFire, and LEGIC card technology.
- b) Supports Mobile Virtual Card, Bluetooth 4.0+ and Scramble QR Code
- c) 13.56MHz card read range: 5cm+; Bluetooth read range: 0.5m to 10m; QR Code read range: 4cm to 22cm
- d) Palm Vein recognition technology should be provided by Fujitsu PalmSecure-F Pro sensor
- e) Palm Vein Sensor supports binocular infrared live detection
- f) Palm Vein recognition can be completed in one second for 2,000 palm vein users. Each user can register 2 palm vein templates
- g) The recognition accuracy rate is higher than 99% and 0.5m-1.5m recognition distance is supported
- h) Supports 20,000 local personnel
- i) Programmable buzzer beep sound interval for access granted and access denied
- j) Red / Green / Blue or mixed LED for visual notification
- k) Programmable LED flash interval for access granted and access denied
- l) Reader can be configured online
- m) Reader outputs ACX proprietary scramble encryption RS485 format
- n) Reader Tamper: Optical sensor
- o) Reader size shall be not larger than 80mm(W) x 130mm(H) x 20mm(D)
- p) IP55 rated

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

- a) Supports 13.56MHz NXP Mifare Classic, Mifare Plus, Mifare DESFire, and LEGIC card technology.
- b) Supports Mobile Virtual Card, Bluetooth 4.0+ and Scramble QR Code
- c) 13.56MHz card read range: 5cm+; Bluetooth read range: 0.5m to 10m; QR Code read range: 4cm to 22cm
- d) Facial detection supports binocular infrared live detection
- e) Face recognition can be completed in 300 milliseconds
- f) The recognition accuracy rate is higher than 99% and 0.5m-1.5m recognition distance is supported

- g) Supports 20,000 local personnel
- h) Real-time detection and tracking of human faces; accurate detection can be carried out in situations such as side faces, half occlusion, and blur
- i) Minimum 0.5 lux recognition
- j) Effective defense against non-living attacks such as 3D printing, electronic screens, video, pictures, masks, hoods, etc.
- k) Programmable buzzer beep sound interval for access granted and access denied
- l) Red / Green / Blue or mixed LED for visual notification
- m) Programmable LED flash interval for access granted and access denied
- n) Reader can be configured online
- o) Reader outputs ACX proprietary scramble encryption RS485 format
- p) Reader Tamper: Optical sensor
- q) Reader size shall be not larger than 80mm(W) x 130mm(H) x 20mm(D)
- r) IP55 rated

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

- a) Supports Octopus, Mobile Virtual Card by Bluetooth 4.0+, and Scramble QR Code
- b) Bluetooth read range: 0.5m to 10m; QR Code read range: 4cm to 22cm
- c) Received the Octopus Holding Limited Type Approval Certificate
- d) Programmable buzzer beep sound interval for access granted and access denied
- e) Red / Green / Blue or mixed LED for visual notification
- f) Programmable LED flash interval for access granted and access denied
- g) Reader outputs ACX proprietary scramble encryption RS485 format
- h) Reader Tamper: Optical sensor
- i) Reader size shall be not larger than 94mm(W) x 196mm(H) x 55mm(D)
- j) Flush mount design with only 6mm extruded from the wall

**3. 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 the test and having the work retested. Such costs shall also include the provision of all instruments necessary for the test.

5.2 A specialist Sub-contractor (SSC) shall carry out the commissioning. The SSC shall commission the installed service systems according to the Drawings and Specifications. The SSC shall provide network, software, and commissioning engineers for the commissioning works.

**4. 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 perform maintenance and repair services throughout the 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-