SECTION 28 10 00
ACCESS CONTROL

ACCESS CONTROL SYSTEM SPECIFICATION

PART 1 GENERAL

1.01 Summary

A The Access Control System shall be an electronic, cloud-based system that includes:

1. Control panels
2. Expansion boards
3. Readers
4. User credentials
5. Online administrative portal

1.02 Related Requirements

A 27 00 00 Communications

1. 27 15 00 Communications Horizontal cabling

B 27 20 00 Data Communications

C 28 01 00 Operation and Maintenance of Electronic Safety and Security

1. 28 01 10 Operation and Maintenance of Access Control

D 28 05 00 Common Work Results for Electronic Safety and Security

1. 28 05 07.11 Power Sources for Access Control
2. 28 05 07.23 Uninterruptible Power Supply
3. 28 05 11 Cyber Security Requirements for Electronic Safety and Security
4. 28 05 31 Communications Equipment for Electronic Safety and Security
5. 28 05 45 Systems Integration and Unified Systems

E 28 06 00 Schedules for Electronic Safety and Security

1. 28 06 10 Schedules for Access Control

F 28 08 00 Commissioning of Electronic Safety and Security

G 28 23 00 Video Management System

H 28 30 00 Security Detection, Alarm, and Monitoring

1. 28 33 15 Security Monitoring and Control Software

I 28 40 00 Life Safety

1. 28 46 00 Fire Detection and Alarm

J 28 47 00 Mass Notification

K 28 51 00 Information Management & Presentation

1.03 References

A Abbreviations

1. ACS: Access Control System
2. ACU: Access Control Unit
3. AES: Advanced Encryption Standard
4. LAN: Local Area Network
5. LED: Light-Emitting Diode
6. REST API: Representational State Transfer Application Programming Interface
7. REX: Request to Exit
8. SSO: Single Sign-On
9. TLS: Transport Layer Security
10. VPN: Virtual Private Network
11. 1FA: Single Factor Authentication
12. 2FA: Two Factor Authentication

B Definitions

1. Anti-Passback: A feature that lets you define a sequence in which Entries must be accessed in order to gain entry.
2. Smart Hub ACU: A cloud-based control panel that manages access to a secured area.
3. Cloud Key Credential: A credential that lets users generate links to provide temporary access through a mobile app or online portal.
4. Control Center: An online portal that lets administrators manage users, set up entries and permissions, and troubleshoot hardware.
5. Credential: A key presented to a reader to gain access to an entry to include cards, key fobs, and mobile credentials.
6. Entrance: A door, gate, turnstile, or elevator floor secured with a reader.
7. Entrance State: Determines whether an entrance is locked or unlocked and defines what kinds of credentials and trigger methods are valid.
8. Magic Link: An authenticated URL that lets a user log into the ACS mobile app.
9. Mobile Credential: An access method tied to a user’s smartphone through the use of a mobile app.
10. Mobile App: A smartphone application used for providing mobile credentials and remote unlock for users.
11. Remote Unlock: A feature that lets users unlock an entry without needing to be in range.
12. Trigger Method: A combination of credential type and 1FA/2FA

13. User: A person defined in the Control Center with credentials.

C Reference Standards

1. UL 294 Standard for Access Control System Units
2. Federal Communications Commission (FCC)
    a. FCC Part 15 - Unlicensed RF Devices EME/EMC
3. ISO/IEC 14443-3:2011 – Identification Cards
4. National Fire Protection Association
    a. NFPA 70 National Electric Code
    b. NFPA 101 – Life Safety Code
5. Institute of Electrical and Electronic Engineers
    a. IEEE 802.3 Ethernet Standards

1.04 Submittals

A Informational Submittals

1. Product Data:
    a. Data sheets
    b. Installation methods
    c. Rated capacities
    d. Operating instructions
    e. Component power requirements
2. Wiring diagrams and shop drawings
3. Network requirements and settings

B Closeout submittals

1. Warranty documentation
2. Test reports
3. Installed asset listing
4. Device settings

1.05 Quality Assurance

A All ACS hardware devices shall be tested and verified by the Manufacturer prior to installation.

B A Manufacturer-approved Contractor shall perform the installation of the ACS hardware.

1.06 Warranty

A Manufacturer shall correct, by repair or replacement of the defective part or parts, any defect or defects in workmanship or materials in the System which may develop under proper or

normal use during the period of one (1) year from the date of installation of the Hardware, unless necessitated by reason of negligence or misuse of the equipment.

B Warranties for hardware not provided by the Manufacturer shall be provided by the original manufacturer of that specific hardware device or component.

PART 2 PRODUCTS

2.01 Manufacturer

A Openpath

1. 600 Corporate Pointe, Suite 400, Culver City, CA 90230

   Phone +1 844 673-6728

   info@openpath.com

2. Products

   a. Online administrative portal: Control Center

   b. Access control panel: Smart Hub ACU

   c. Credential reader: Smart Reader

   d. Elevator expansion board: Elevator Board

2.02 Access Control System (ACS) Description

A The ACS shall function as an electronic, cloud-based access control system that includes an online administrative portal, access control panels, credential readers, and user credentials.

B The ACS shall conform to the UL 294 Standard for Access Control System Units.

C Administrative portal: The ACS shall provide an online admin portal that can be accessed via any web-enabled device through an Internet browser.

1. The online portal shall not reside on a LAN or VPN.
2. The online portal shall be cloud-based and not require a dedicated local server.
3. System administrators shall be able to configure online portal access to selected authorized users, either within the company or outside.
4. The online portal shall support an unlimited amount of users, entry events, zones, sites, readers, and access control panels.
5. Supported Administrator functions:

   a. Monitor via real-time dashboards user activity, entry activity, and hardware states, including:

      1) Access control panel cloud and LAN connection status, hardware version, and software version

      2) Credential reader connection status, hardware version, software version, and temperature

   b. Identify hardware by activating the lights on the specified access control panel and indicator lights and buzzer on the specified credential reader for troubleshooting

purposes

c. Unlock entries from the main dashboard

d. Create users, assign credentials, and define entry access

e. Define sites, zones, and entries

f. Define Anti-Passback areas with inbound and outbound entries

g. Define schedules and default entry states

h. Share zones with other organizations to support landlord/tenant scenarios

i. Add access control panels and credential readers

j. Monitor and troubleshoot hardware

k. Unlock entries, provided the entries are configured to support remote unlock

l. Provide access logs for all unlock attempts that can be exported to CSV file format

m. Support third-party integrations, including identity providers and other applications

n. Support SSO, allowing Administrators to authenticate via identity providers including, but not limited to, Microsoft Azure Active Directory, Google G Suite, and Okta integrations

o. Set up email alerts for payment due dates, expired Terms and Conditions, and/or when the account is frozen

p. Set up email/SMS alerts for forced entries, ajar entries, unlock failures, and/or Anti-Passback breaches

D Access Control Panels:

1. Compliance: UL 294, FCC

2. Communications

   a. Encryption: communications to the access control panel shall be encrypted via TLS

   b. Connection to credential reader: RS-485

   c. Connection to administrative portal: network via router to cloud service

3. Power: 12VDC

   Manufacturer recommends installing an optional backup battery to ensure uptime during power outages.

4. Capacity:

   a. Entrances per panel: up to 4

   b. Credential readers per panel: up to 8

5. Expansion: support elevator and I/O interface modules

6. Indicators (LED):

   a. Panel power

   b. Status

c. Relay

d. Reader power

7. The Smart Hub ACU shall continue to function and make entry decisions throughout Internet outages.

E Elevator Expansion Board:

1. Compliance: UL 294, FCC
2. Communications:
   a. Encryption: communications to the access control panel shall be encrypted via TLS
   b. Connection to access control panel: USB
   c. Connection to credential reader: RS-485
3. Power: 12-24VDC
4. Capacity:
   a. Elevator floors per board: up to 16
   b. Credential readers per board: up to 2
   c. General purpose inputs: 16, 3V-24VDC
5. Indicator: seven-segment display for identification

F Credential Readers: The ACS shall support Manufacturer's credential readers and legacy Wiegand readers.

1. Compliance: UL 294, FCC
2. Environmental rating: IP65
3. Access control panel connection: RS-485
4. Types:
   a. Credential readers shall be available in low frequency (LF) and high frequency (HF) configurations.
   b. Credential readers shall be available in single gang and mullion mount configurations.
   c. Single gang readers
      1) Color options: white, black
      2) Mounting: surface, flush
      3) Frequency: LF, HF
   d. Mullion readers:
      1) Color: black
      2) Mounting: surface
      3) Frequency: LF, HF

5. Mobile credential communication: Bluetooth, Wi-Fi, cellular
6. LED indicators:
    a. Locked/unlocked state
    b. Identification state
    c. Offline
    d. Configuration
7. Security
    a. Credential readers shall not store sensitive data or secret material.
    b. All information sent to the administrative portal shall be encrypted via TLS.
8. Legacy: Credential readers shall support connection to standard Wiegand format readers.

G Credentials:

1. Types supported:
    a. Mobile credential with end-to-end encryption to administrative portal.
    b. Cloud key credentials to provide temporary access to users via web links.
    c. RFID cards and key fobs including:
        1) High frequency reader:
            a) MIFARE DESFire (ISO14443A)
            b) MIFARE DESFire EV1 (ISO14443A)
            c) MIFARE DESFire EV2 (ISO14443A)
            d) MIFARE Classic (ISO14443A)
            e) MIFARE Ultralight (ISO14443A)
        2) Low frequency reader:
            a) Prox 26-bit (H10301)
            b) Prox 33-bit (D10202)
            c) Prox 35-bit Corporate 1000 (H5XXXX)
            d) Prox 37-bit (H10302)
            e) Prox 37-bit with Facility Code (H10304)
            f) Prox 37-bit with Facility Code (S10401)
2. The ACS shall support the use of Wiegand-based keypad readers with PIN in conjunction with credential readers.
3. Mobile credentials shall be assigned individually or as part of an identity provider integration.

H Mobile App: The ACS shall support mobile credentials via a mobile app.

1. The mobile app shall run in the background on a device with minimal battery usage.
    a. Devices supported: mobile devices with Android and IOS operating systems, including Apple Watch
2. Functions supported:
    a. Touch entry
    b. Auto proximity unlock
    c. Remote unlock
    d. Last to Leave locking, allowing users to lock an entrance regardless of schedule
    e. 24 hour activity log
    f. Send diagnostic feedback
3. Logging into the mobile app shall not require a password but will employ magic links.

I Third Party Integration: The ACS shall include an open, documented REST API framework for the online portal to support customized automation of access control-related tasks and third-party integrations.

PART 3 EXECUTION

3.01 Pre-Installation

A A thorough site survey shall be conducted by the Contractor to determine wiring requirements, number of entries, and additional hardware components to support.

3.02 Installation

A Hardware installation and wiring shall be performed by a Manufacturer-authorized Contractor.

B The Contractor shall provide proof of training certification from the Manufacturer.

C The Contractor shall follow all documented installation procedures published by the Manufacturer.

D The Contractor shall coordinate with Manufacturer for hardware provisioning and to ensure all hardware devices are online and functioning.

3.03 Documentation

A The Contractor shall provide a summary of all devices installed, with location, configuration, and network settings.

B The Contractor shall provide a report indicating successful operation of all field devices and communication with the administrative portal.

3.04 Training

A The Manufacturer shall provide training for Administrators that shall cover system usage, maintenance, and troubleshooting.

B Training shall be offered at Customer’s convenience.

C Up to four hours of training shall be provided in two 2-hour sessions.

D The Manufacturer shall provide user documentation in the form of manuals, release notes, online portal tooltips, and online resources.

END OF SECTION