SPECIFICATION GUIDE FOR SECURITY CONSULTANTS
The purpose of this guide is to assist specification writers in the proper specifying of electrified door hardware products when appropriate to include them in Division 28 specifications. This is typical when these hardware products are to be an integral part of a networked security or access control system. As components in these systems, coordination of these door hardware items with other related trades is of the utmost importance. These trades include electrical (including low voltage), security, door hardware, doors and frames, life safety, and access control. It is important to note who is specifying what items so that nothing is missed, and nothing is duplicated.

Here at Allegion, we want to help ensure that every project you specify with our products runs smoothly. That’s why we employ the largest team of door and hardware consultants in North America, combined with Electronic Access Control Specialists to assist with every step of a project. From design and specifications, to products, sales, and service... we’ve got you covered.
# TABLE OF CONTENTS

FOREWARD ................................................................................................................................. 2

TABLE OF CONTENTS .................................................................................................................. 3

SPECIFICATION PARAGRAPHS:

  PART 1 PARAGRAPHS .................................................................................................................. 4

  PART 2 PARAGRAPHS:

      POWER TRANSFER DEVICES – IVES 5BB ETW & VON DUPRIN EPT-10 ...................... 5
      SCHLAGE LE SERIES MORTISE LOCKS ................................................................. 5
      SCHLAGE FE410 SERIES PROGRAMMABLE INTERCONNECTED LOCKS .................... 7
      SCHLAGE NDE SERIES CYLINDRICAL LOCKS ...................................................... 10
      SCHLAGE CO SERIES LOCKSETS & EXIT DEVICES TRIM ...................................... 14
      SCHLAGE AD SERIES LOCKSETS & EXIT DEVICES TRIM ...................................... 17

      AptiQ ACCESS CONTROL READERS:

          aptiQ MT11 ............................................................................................................. 27
          aptiQ MT15 ........................................................................................................... 30
          aptiQ MTK15 ....................................................................................................... 33
          XceedID PR10 ..................................................................................................... 36
          aptiQ SM10 ......................................................................................................... 37

      CREDENTIALS ..................................................................................................................... 39

      WIRELESS READER INTERFACE – SCHLAGE WRI400 .......................................... 40
      ELECTRIC STRIKES – VON DUPRIN 6000 SERIES ..................................................... 40
      MAGNETIC LOCKS – SCHLAGE M400 SERIES & GF3000 SERIES ........................... 41
      POWER SUPPLIES – SCHLAGE PS900 SERIES ......................................................... 42
      DOOR POSITION SWITCHES – SCHLAGE 679 SERIES ............................................ 43

  PART 3 PARAGRAPHS ............................................................................................................. 44

      COORDINATION WITH DIVISION 08 ............................................................................ 45

      OPERATIONAL DESCRIPTIONS AND ELEVATION DIAGRAMS ............................... 46

      CONTACT INFORMATION ................................................................................................. 47

3
SPECIFICATION PARAGRAPHS: PART 1 - GENERAL

For proper coordination, it is recommend the following paragraphs be included in Part 1 – General of your access control specification section (28 10 00).

1.02 Related Sections

   A. Section 08 71 00 – Door Hardware

1.05 Quality Assurance

   A. Electrified Hardware Coordination Conference: Prior to ordering access control hardware, schedule and hold meeting to coordinate access control hardware with security, electrical, doors and frames, door hardware, and other related suppliers.

      1. Attendees: electrified door hardware supplier, doors and frames supplier, electrified door hardware installer, electrical subcontractor, Owner,[Owner’s security consultant,] Architect and Contractor.

      2. After meeting, provide letter of compliance to Architect, indicating when coordination conference was held and who was in attendance.

1.07 Coordination

   A. Security: Coordinate installation of door hardware, keying, and access control with Owner's security consultant.
SPECIFICATION PARAGRAPHS: PART 2 - PRODUCTS

Where appropriate, the following paragraphs should be included in Part 2 – Products of your access control specification section (28 10 00).

2.01 ELECTRIC Hinges

A. Manufacturers:
   a. Scheduled Manufacturer: Ives 5BB Series x ETW

B. Provide hinges with electrified options as scheduled in the hardware sets (see Section 08 71 00). Provide with sufficient number and wire gage to accommodate electric function of specified hardware. Locate electric hinge at second hinge from bottom or nearest to electrified locking component.

C. Provide mortar guard for each electric hinge specified.

2.05 ELECTRIC POWER TRANSFER

A. Manufacturers:
   a. Scheduled Manufacturer: Von Duprin EPT-10

B. Provide power transfer with electrified options as scheduled in the hardware sets. Provide with number and gage of wires sufficient to accommodate electric function of specified hardware.

C. Locate electric power transfer per manufacturer’s template and UL requirements, unless interference with operation of door or other hardware items.

2.17 ELECTRONIC ACCESS CONTROL LOCKSETS – WIRELESS MORTISE-TYPE

A. Manufacturer and Products:

B. Requirements: Provide wireless electronic locksets that comply with the following requirements.

   1. Provide mortise locks conforming to ANSI/BHMA A156.13 Series 1000, Grade 1 Operational, Grade 1 Security, and manufactured from heavy gauge steel, containing components of steel with a zinc dichromate plating for corrosion resistance. Cylinders: Refer to "KEYING" article, herein.
   2. Provide heavy-duty, handed, field-reversible mortise locks.
   4. Latchbolt: 3/4-inch (19 mm) throw stainless steel latch bolt with anti-friction tongue.
5. **Deadbolt**: optional 1” throw stainless steel deadbolt to support Privacy and Apartment functions.

6. **Chassis**: Provide standard A115.1 preparation for mortise locks for 1-3/4-inch (44 mm) doors.

7. **Applicable Standards:**
   a. Listed, UL 294 - Standard of Safety for Access Control System Units.
   b. Compliant with ANSI Standard A156.25 and A156.13 Series 1000, Grade 1 strength and operational requirements.
   c. Compliant with ANSI/BHMA A156.25 Grade 1 Operation and Security Requirement.
   d. Certified to UL10C, FCC Part15, IC RSS-210, ADA, RoHS, ICC ANSI A117.1
   e. Compliant with FBC TAS 201, TAS 202, TAS 203 for door assemblies.
   f. Certified to FBC 3905, 12400 and 14482

8. **Lockset Functions**: Provide locks with storeroom, privacy, apartment or office function as specified in hardware groups.

9. **Emergency Override**: Provide mechanical key override; cylinders: Refer to “KEYING” article, herein.

10. **Levers:**
   a. Levers shall operate independently of each other.
   b. Provide levers to match mechanical mortise locks.
   c. Tactile Warning (Knurling): Where required by authority having jurisdiction. Provide on levers on exterior (secure side) of doors serving rooms considered to be hazardous.

11. **Power Supply:**
   a. Provide lockset powered by four AA batteries
   b. Provide locksets with the ability to communicate battery status and battery voltage level by means of an application on mobile device, at the door, and remotely by integrated software.

12. **Features**: Provide locksets with the following features.
   a. Ability to communicate unit’s communication status via LED
   b. Capable of being programmed via Mobile or Web based App to lock via BLE or via integrated SW partner system via BLE Gateway or existing building Wi-Fi
   c. Visual tri-colored LED indicator that indicate activation, operational systems status, system error conditions and low power conditions as determined by integrated software partner.
   d. Audible feedback that can be enabled or disabled.
   e. Tamper-resistant screws: Single tamper-resistant torx screw on inside escutcheon.
   f. Capable of reacting to a lockdown command in under 5 seconds when used with a software partner that has integrated this feature.

13. **Adaptability:**
   a. Open Architecture: Provide locksets manufactured with open architecture characteristics capable of handling new and existing access control software and credential reading technology. Can be supported by cloud-based web and mobile apps without the need for an integrated software partner.

14. **Switches**: Provide locksets with the following switches:
   a. Door Position Switch
   b. Interior Cover Tamper Guard
c. Request to Exit
d. Optional Deadbolt Position
e. Optional Interior Push Button

15. Credential Reader:

a. Credential Reader Configuration: Provide credential reader modules in the following configurations, as indicated in door hardware sets. Multi-tech contactless reader shall be NFC-Compatible, including NFC Peer to Peer compatible, and read access control data from both 125 kHz and 13.56 MHz contactless smart cards. The multi-tech contactless reader shall be optimally designed for use in access control applications that require reading both 125 kHz proximity and 13.56 MHz contactless smart cards.

16. 

a) Credential reader capabilities:
i. 13.56 MHz Smart credentials:
   (a) Secure section (Multi-Technology and Smartcard): aptiQ MIFARE Classic, aptiQ MIFARE DESFire EV1
   (b) 13.56 MHz Serial number only (Multi-Technology and Smart credential): DESFire CSN, HID iCLASS CSN, MIFARE CSN, MIFARE DESFire EV1 CSN
ii. 125 kHz Proximity credentials: Schlage, XceedID, HID, GE/CASI, AWID
iii. Multi-Technology readers that read both 13.56 MHz Smart and 125 kHz Prox credentials.

2.23 ELECTRONIC PROGRAMMABLE INTERCONNECTED LOCKSETS OPTION: AND DEADBOLTS

A. Manufacturers and Products:

1. Scheduled Manufacturer and Product: Schlage FE410F.


1. Provide interlocked locksets conforming to ANSI A156.12 Series 5000, Grade 2 with simultaneous retraction of deadbolt and latch for single motion egress.
2. Provide locks with 2-3/4 inches (70 mm) backset, based on door detail, with 1/2 inch (13 mm) latch throw latchbolt and 1 inch (25 mm) throw deadbolt.
3. Provide independently operating levers with two external return spring cassettes mounted under roses to prevent lever sag.
4. Provide manufacturers standard T-strike, unless extended lip strike is necessary to protect trim, and deadbolt strike.
5. OPTION: Lever Design: Schlage Addison (ADD) Trim with Lever Trim:

   a. Accent (ACC)
   b. Avilla (AVA)
   c. Birmingham (BIR)
   d. Elan (ELA)
   e. JAZZ (JAZ)
   f. Jupiter (JUP)
   g. Latitude (LAT)
   h. Neptune (NEP)
   i. Sacramento (SCA)
j. Saturn (SAT)

6. **OPTION**: Lever Design: Schlage Greenwich (GRW) Trim with Lever Trim:
   a. Accent (ACC)
   b. Broadway (BRW)
   c. Elan (ELA)
   d. JAZZ (JAZ)
   e. Jupiter (JUP)
   f. Latitude (LAT)
   g. Manhattan (MNH)
   h. Neptune (NEP)
   i. Northbrook (NOR)
   j. Saturn (SAT)

C. **OPTION**: Product: Schlage BE467F Addison (ADD) **OPTION**: Greenwich (GRW ) electronic deadbolt.
   1. Provide a programmable stand-alone Electronic Deadbolt that is computer managed. Deadbolt to conform to ANSI A156.5-2000 grade 2 and ANSI/BHMA certified.
   2. Provide programmable electronic with the following:
      a. Time and Date controlled access.
      b. Up to 500 user.
      c. 1000 event Audit Trail report.
      d. 8 time zone capability
      e. Compatible with STRATIS Energy & Access Management & Control System.
   3. Provide deadbolts with standard 2-3/4 inches (70 mm) backset. Provide 2-3/8 inches (60 mm) where noted or if door or frame detail requires. Provide deadbolt with full 1 inch (25 mm) throw. constructed of steel alloy.
   4. Provide entry by a Keyfob that supports aptiQ MIFARE classic, aptiQ DESFire EV1 and aptiQmobile credentials.
   5. Provide power by four (4) AA batteries (included) where if loss of battery power occurs, a 9V battery can be used to jump start the lock and provide access with an assigned credential. Battery life of 2 years in OFF-LINE MODE.

D. **Requirements**
   1. Provide programmable electronic locksets **OPTION**: and deadbolts with the following:
      a. Time and Date controlled access.
      b. Up to 500 user.
      c. 1000 event Audit Trail report.
      d. 8 time zone capability
      e. Compatible with STRATIS Energy & Access Management & Control System.
   2. Provide entry by a Keyfob that supports aptiQ MIFARE classic, aptiQ DESFire EV1 and aptiQmobile credentials.
   3. Provide power by four (4) AA batteries (included), where if loss of battery power occurs, a 9V battery can be used to jump start the lock and provide access with an assigned credential. Battery life of 2 years in OFF-LINE MODE.

E. **Components**
1. Keyfob, 13.56 MHz Smart Credential [OPTION: other credentials are available and need to be coordinated with other credential readers or products being used on the project]
   a. Manufacturer and Product:
      1) Schlage 9651 Keyfob
   b. Requirements:
      1) Access key fobs shall be used with access readers to gain entry to access control portals (e.g. doors, gates, turnstiles) and to hold information specific to the user.
      2) The fob shall function at ISO 14443A standards, provide for a faster data transfer speed. Smart Credentials operate on a 13.56 MHz frequency and utilize high security encrypted data.
      3) The fob shall support MIFARE or MIFARE DESFire EV1 technology.
      4) Presentation to the access control reader at any angle within a minimum distance of one (1) inch shall result in an accurate reading of the fob.
      5) The fob shall be composed of polycarbonate material.

2. Keyfob Construction [OPTION: other credentials are available and need to be coordinated with other credential readers or products being used on the project]
   a. Manufacturer and Product:
      1) Schlage 9651 (CT8X4248) Keyfob
   b. Requirements:
      1) Same smart credential Keyfob as above but pre-configured for construction with locks out of the box.

3. Credential Enrollment Reader
   a. Manufacturer and Product:
      1) Schlage aptiQ MT20W
   b. Requirements:
      1) Unit provides simplified credential enrollment via computer connect. USB connection is for power only, enrollment uses Wi-Fi connection.
      2) Multi-technology enrollment reader is designed to simplify the enrollment of proximity and smart credentials. The reader is powered by a USB cable via computer’s USB port and utilizes a Wi-Fi connection for certain scenarios (enrolling no-tour credentials).
      3) The unit is compatible with smart credentials (MIFARE Classic and FIFARE DESFire EV1), aptiQmobile credentials, PIV credentials and most proximity credentials up to 37-bits. The unit supports no-tour (with supported locks) via aptiQ MIFARE Classic or MIFARE DESFire EV1 credentials.

4. Access Management Software [OPTION: other systems are available and need to be coordinated with other credential readers or products being used on the project]
   a. Manufacturer and Product:
      1) Stratis, Sphere for Schlage
   b. Requirements:
      1) Provide an access management system that is cloud based that can be managed via a computer or tablet.
         a) Task tracking and audits for maintenance
         b) Integrates with property management software platforms
c) No-Tour access control, key replacement does not require touring to enable or invalidate credentials.
d) Replace credentials in less than two minutes.

2) System provides:
a) Fast credentials replacement
b) Issuing maintenance credentials
c) Providing master credential
d) Provides temporary lockout credential.
e) Audit Trail

3) System Requirements:
a) WiFi internet connection for producing credentials.
b) Provide with 7” tablet and programming cables

2.30 ELECTRONIC ACCESS CONTROL LOCKSETS—WIRELESS BORED-TYPE

A. Manufacturers:

B. Product: Schlage ND Series wireless bored-type electronic locksets conforming to the following requirements:

1. ANSI/BHMA A156.2 Series 4000, Grade 1.
3. Certified to UL10C 3 hour rating, ULC-S319, FCC Part15, ADA RoHS, ICC ANSI A117.1
4. Listed, UL 294 - The Standard of Safety for Access Control System Units.
5. Compliant with ANSI/BHMA A156.25 Operation and Security interior operating range of 32 degrees F (0 degrees C) to 120 degrees F(49 degrees C) for interior use only.
7. Compliant with ICC / ANSI A117.1, NFPA 101, NFPA 80 and IBC Chapter 10
8. Provide cylindrical locksets exceeding the ANSI/BHMA A156.2 Grade 1 performance standards for strength, security, and durability in the categories below:

   a. Abusive Locked Lever Torque Test – minimum 3,100 inch-pounds without gaining access
   b. Offset lever pull – minimum 1,600 foot pounds without gaining access
   c. Vertical lever impact – minimum 100 impacts without gaining access
   d. Cycle Test - tested to minimum 16 million cycles with no visible lever sag or use of performance aids such as set screws or spacers.

9. **OPTION Vandlguard/Free-Wheeling:** Provide levers with vandal resistant technology for use at heavy traffic or abusive applications.
11. Emergency Override: Provide mechanical key override; cylinders: Refer to “KEYING” article, herein.
12. Levers:

   a. Vandal Resistance: Exterior (secure side) lever rotates freely while door remains locked, preventing damage to internal locking components from vandalism by excessive force.
   b. Provide lever trim that operates independently of each other.
   c. Style: Sparta[Rhodes][Athens]
d. Tactile Warning (Knurling): Where required by authority having jurisdiction. Provide on levers on exterior (secure side) of doors serving rooms considered to be hazardous.

13. Power Supply: 4 AA batteries

a. Provide battery powered wireless electronic products with the ability to communicate battery status and battery voltage level by means of a mobile app at door and remotely by Partner integrated software.

14. Features:

a. Ability to communicate unit’s communication status.
b. Visual LED indicators that indicate activation, operational systems status, system error conditions and low power conditions.
c. Audible feedback that can be enabled or disabled.

15. Switches:

a. Door Position Sensor – magnet integrated into strike to eliminate additional door prep
b. Interior Cover Tamper Guard
c. Battery Status
d. Request to Exit

16. Credential Reader:

a. Credential Reader Configuration: Provide credential reader modules in the following configurations, as scheduled. 
   1) Proximity, Smartcard via Multi-Technology reader.

b. Credential reader capabilities:
   1) 13.56 MHz Smart card credentials: 
      a) Secure section (Multi-Technology and Smartcard): aptiQ MIFARE Classic, aptiQ MIFARE DESFire EV1
      b) 13.56 MHz Serial number only (Multi-Technology and Smartcard): DESFire CSN, HID iCLASS CSN, MIFARE CSN, MIFARE DESFire EV1 CSN
   2) 125 kHz Proximity card credentials: Schlage, XceedID, HID, GE/CASI, AWID
   3) Multi-Technology readers that read both 13.56 MHz Smart Cards and 125 kHz Prox cards on a battery powered device.

17. Operation: Provide battery powered wireless electronic products able to operate in three possible modes without change to lock hardware.

a. Manual operation – Updates pulled direct from mobile app via BLE when in range of up to 100 feet from mobile device to wireless electronic product.
b. Daily operation –
   1) Updates request by wireless electronic product within 24 hours over Wi-Fi communication, Wi-Fi connection required at the wireless electronic product.
   2) Can be managed by external software.
c. Real-time operation
   1) Updates communicated in real-time via 2.4 GHz communication to gateway in less than 5 seconds.
   2) Wireless electronic products will be connected via integrated 3rd party software.
   3) Wireless electronic products to have real-time bidirectional communication between access control system and wireless electronic products in less than 5 seconds.
d. Remote Commanding by Partner Integrated Access Control Network Software with Real-time operation: Provide battery powered wireless electronic products with wireless gateway allowing activation of remote, wireless access control products, enabling activated wireless electronic products to be locked or unlocked from a centralized location within 5 seconds or less without user interface at the device.

e. Upon Loss of Power to Wireless Electronic Products: Provide battery powered wireless electronic products able to manage access control offline in one of three methods below that can be configured in the field at wireless electronic product by mobile app and remotely by Partner integrated software:

1) Fail locked (secured)
2) Fail unlocked (unsecured)
3) Fail As-Is

g. Upon Loss of Communication Between Wireless Electronic Products and Gateway with Internet Protocol connection to Host for Real-time operation: Provide battery powered wireless electronic products able to manage access control offline with self-contained database inside device until communication can be re-established between Wireless Electronic Product and Host via Gateway.

1) Wireless electronic product manages access offline with up to 5,000 users and access schedules as provided by Host prior to loss of communication
2) Wireless electronic product captures up to 2,000 audit events from time of communication loss with Host. Audits are transferred to Host upon reconnection of communication via Gateway.

h. Upon Loss of Communication Between Wireless Electronic Products and Gateway with RS-485 connection to Access Control Panel or Host for Real-time operation: Provide battery powered wireless electronic products able to manage access control offline in one of four methods below that can be configured in the field at wireless electronic product by mobile app and remotely by Partner integrated software:

1) Fail locked (secured)
2) Fail unlocked (unsecured)
3) Fail As-Is
4) Fail to Degraded/cache mode utilizing cache memory with following selectable options:
   a) Grant access up to the last 1,000 unique previously accepted User IDs.
   b) Grant access up to the last 1,000 unique previously accepted facility/site codes
   c) Remove from cache previously stored User IDs or facility/site codes that have not been presented to wireless electronic product within the last 5 days.

i. Provide battery powered wireless electronic products able to be remotely configured and managed with Web App, Mobile App, or Partner integrated software.

j. Wireless Transmission:

1) Bluetooth Low Energy (BLE)
2) Wi-Fi 802.11 B & G

k. Data Encryption

1) Encryption: AES-256 bit Key minimum – all BLE communication is AES 256 bit encryption minimum
2) TLS encryption –
   a) Wireless Electronic Product to Cloud – Daily Mode
   b) Gateway to Cloud - Real Time Mode
C. Components

   a. Provide Mobile App for wireless electronic access control products capable of the following minimum requirements.
      1) Add and Configure wireless electronic access control products.
      2) Send updates to wireless electronic access control products.
      3) Add new users and enroll credentials to wireless electronic access control products.
      4) View audits and alerts by wireless electronic access control product.
      5) Perform diagnostics of wireless electronic access control products.
   b. System Requirements: mobile devices, provided by others, require one of the following operating systems.
      1) IOS 7.1 or later
      2) Android 4.4, Kit Kat, or later
      3) Capable of using Allegion Engage Mobile App
   c. Mobile App capable of field configuring electronic access control devices for the following minimum attributes.
      1) Credential reader formats
      2) Unlock Period
      3) Power failure mode
      4) Audible alarm ON/OFF
      5) Battery status
      6) Validate hardware and software revision
      7) Troubleshooting status signals
      8) Door propped open delay

   a. Provide Web App for wireless electronic access control products capable of the following minimum requirements.
      1) Configure wireless electronic products
      2) Add new users and enroll credentials
      3) View audits and alerts by door
   b. System Requirements: computers or other devices, provided by others, require the one of the following browsers.
      1) Internet Explorer 9.0 or later
      2) Chrome 33.0 or later
      3) Firefox 28.0 or later
      4) Safari 7.0 or later

3. Product: Gateway
   a. Provide Gateway for Real-time operation between wireless electronic access control products and Host system that meets the following requirements.
      1) Supports real-time communications to wireless electronic access control product.
      2) Communicates between gateway and host by RS-485, Ethernet (IP/PoE).
      3) Supports up to 10 wireless electronic access control products.
      4) Performs lockdown/unlock command from host to wireless electronic access control product within 5 seconds.
      5) Capable of receiving remote firmware upgrades by mobile app.
      6) Capable of updating the firmware on a linked wireless electronic product.
7) Capable of being powered over Ethernet (PoE) or via an external 12/24 VDC power supply.
8) Supports a remote antenna to extend reach of wireless signal to wireless electronic access control product.
9) Communicates secured data between the gateway and wireless electronic access control products.

2.31 ELECTRONIC ACCESS CONTROL LOCKSETS AND EXIT DEVICE TRIM

A. Manufacturers:


1. Provide bored cylindrical locks conforming to ANSI/BHMA A156.2 Series 4000, Grade 1, non-handed, field-reversible.
2. Backset: [2-3/4-inch (70 mm)][2-3/8-inch (60 mm)][3-3/4-inch (95 mm)][5-inch (127 mm)].
3. Latchbolt Throw: 1/2-inch (13 mm) unless noted otherwise. Provide 3/4-inch (19 mm) throw for UL listing at pairs.
4. Chassis: Standard 161 cylindrical lock prep for 1-3/4-inch (44 mm) doors <insert optional door thickness – maximum of 2-3/4 inches 1/8 inch door increments>

C. Product: Schlage [CO-100-MS][CO-200-MS/MD][CO-220-MS/MD][CO-250-MS/MD] standalone mortise-type electronic locksets.

1. Provide mortise locks conforming to ANSI/BHMA A156.13 Series 1000, Grade 1 Operational, Grade 1 Security, and manufactured from heavy gauge steel, containing components of steel with a zinc dichromate plating for corrosion resistance. Provide lock case that is field reversible for handing without opening case.
2. Backset: 2-3/4-inch (70 mm), nominal.
3. Latchbolt: 3-piece, beveled, stainless steel with 3/4-inch (19 mm) throw and anti-friction latch.
4. Deadbolt: Where deadbolt function is scheduled, provide stainless steel deadbolt interconnected with latch 1-5/8-inch (41 mm) high and 5/8-inch (16 mm) thick with 1-inch throw.
5. Chassis: ANSI/BHMA standard mortise lock prep for 1-3/4-inch (44 mm) doors <insert optional door thickness – maximum of 2-3/4 inches 1/8 inch door increments>


1. Provide exit device trim conforming to ANSI/BHMA A156.25, non-handed, field-reversible.
2. Exit Device Configurations: Exit device lever trim to retract latchbolt for following exit device applications:
   a. Rim
      
      NOTE – The following are applicable to Von Duprin 98/99/22 only.
   b. Surface vertical rod
      
      NOTE – The following are applicable to Von Duprin 98/99 only.
c. Mortise

d. Concealed vertical rod

e. Concealed vertical cables

3. Exit Device Compatibility: Provide exit device trim with universal mounting plate enabling operation as required.

E. Requirements:

1. Provide offline electronic access control products that comply with the following requirements:

   a. Listed, UL 294 - The Standard of Safety for Access Control System Units.
   b. Compliant with ANSI/BHMA A156.25 Grade 1 Operation and Security.
   d. Compliant with ASTM E330 for door assemblies.

2. Functions: Provide functions as scheduled that are field configurable without taking the offline electronic product off the door.

3. Emergency Override: Provide mechanical key override; cylinders: Refer to “KEYING” article, herein.

4. Levers:

   a. Vandal Resistance: Exterior (secure side) lever rotates freely while door remains locked, preventing damage to internal lock components from vandalism by excessive force.
   b. Provide non-handed lever trim that operates independently of non-locking levers.
   c. Style: [Sparta (17)][Rhodes (06)][Athens (07)][Tubular (03)]
   d. Tactile Warning (Knurling): Where required by authority having jurisdiction. Provide on levers on exterior (secure side) of doors serving rooms considered to be hazardous.

5. Power Supply: 4 AA batteries

   a. Provide electronic access control locks and/or exit device trim with the ability to communicate battery status.

6. Features:

   a. Visual tri-colored LED indicators that indicate activation, operational systems status, system error conditions and low power conditions.
   b. Visual bi-colored LED indicator on interior that is capable of indicating secured/unsecured status of device to occupants on interior.
   c. Audible feedback that can be enabled or disabled.
   d. Onboard processor with memory capacity of 2,000 users, 2,000 event audit history, up to 16 time zones and up to 32 calendar events.
   e. Tamper-Resistant Screws: Tamper torx screws on inside escutcheon for increased security.

   EDIT – Select configurations below when CO-220 is specified.

f. Lockdown Function:

   1) Provide electronic access control locks and/or exit device trim with lockdown function with a remote Fob for immediate lockdown of lock restricting entrance to authorized credentials. Free egress always from non-secure side of lock.
2) Provide 1 Remote Lockdown Fob that will be paired to each lock.
3) Provide electronic access control locks and/or exit device trim with lockdown function capable of being paired with up to 10 Remote Lockdown Fobs. Provide one Remote Lockdown Fob to be paired with lock. Remote Lockdown Fob shall be capable of being paired with up to 10 locks. Remote Lockdown Fob shall have one button to initiate lockdown with Paired Lock and a separate button to reset locks that are paired to it from lockdown. Range of Remote Lockdown Fobs up to 75 feet on secured side and up to 25 feet on exterior side of door based upon typical building construction.

7. Switches:
   a. Mechanical Key Override
   b. Door Position Switch NOTE – not used on CO-100 or CO-220

8. Credential Reader:
   EDIT – Select configuration(s) as required.
   a. Credential Reader Configurations:
      1) Proximity. NOTE – not used on CO-100
      2) Proximity and keypad. NOTE – not used on CO-100
      3) Magnetic stripe (swipe type). NOTE – not used on CO-100
      4) Magnetic stripe (swipe type) and keypad. NOTE – not used on CO-100
      5) Keypad.
   b. Credential Reader Capabilities: Provide credential readers capable of operating with the following integrated software partners.
      EDIT – Revise capabilities to suit actual configuration(s)
      1) Magnetic card triple track reader capable of reading tracks 1, 2 or 3 per configuration in field. OPTION 1
      2) Swipe reader capable of reading information along full length of magnetic stripe.
      3) 125 kHz Proximity card or fob credentials: Schlage, XceedID, HID, GE/CASI ProxLite and AWID. OPTION 2
      4) Dual credential reader with keypad plus proximity reader capable of reading card or fob. OPTION 3
      5) 125 kHz Proximity card credentials: Schlage, XceedID, HID, GE/CASI ProxLite and AWID.
      6) 12 button keypad with backlit buttons.
      7) 12 button keypad with backlit buttons. OPTION 4

9. Operation:
   a. Provide electronic access control locks and/or exit device trim with the ability to be configured at door by handheld programming device the length of time device is unlocked upon access grant.
   b. Provide electronic access control locks and/or exit device trim with the ability to communicate identifying information such as firmware versions, hardware versions, serial numbers, and manufacturing dates by handheld programming device.

F. Components
   1. Product: Schlage HHD series with Utility Software.
      REQUIRED for all CO-series
a. Provide Handheld Programming Device for adaptable electronic access control products capable of the following minimum requirements.
   1) Capable of initializing lock and accessories using preloaded software.
   2) Utilized to field configure electronic access control devices, to download firmware updates and door files to device, and to download audit files from device.

2.32 ELECTRONIC ACCESS CONTROL LOCKSETS AND EXIT DEVICE TRIM

A. Manufacturers:

   1. Provide bored cylindrical locks conforming to ANSI/BHMA A156.2 Series 4000, Grade 1, non-handed, field-reversible.
   2. Backset: [2-3/4-inch (70 mm)][2-3/8-inch (60 mm)][3-3/4-inch (95 mm)][5-inch (127 mm)].
   3. Latchbolt Throw: 1/2-inch (13 mm) unless noted otherwise. Provide 3/4-inch (19 mm) throw for UL listing at pairs.
   4. Chassis: Standard 161 cylindrical lock prep for 1-3/4-inch (44 mm) doors. 

C. Product: Schlage [AD-200-MS/MD][AD-250-MS/MD][AD-300-MS/MD][AD-400-MS/MD] adaptable mortise-type electronic locksets.
   1. Provide mortise locks conforming to ANSI/BHMA A156.13 Series 1000, Grade 1 Operational, Grade 1 Security, and manufactured from heavy gauge steel, containing components of steel with a zinc dichromate plating for corrosion resistance. Provide lock case that is field reversible for handing without opening case.
   2. Backset: 2-3/4-inch (70 mm), nominal.
   3. Latchbolt: 3-piece, beveled, stainless steel with 3/4-inch (19 mm) throw and anti-friction latch.
   4. Deadbolt: Where deadbolt function is scheduled, provide stainless steel deadbolt interconnected with latch 1-5/8-inch (41 mm) high and 5/8-inch (16 mm) thick with 1-inch throw.
   5. Chassis: ANSI/BHMA standard mortise lock prep for 1-3/4-inch (44 mm) doors.

   1. Provide exit device trim conforming to ANSI/BHMA A156.25, non-handed, field-reversible.
   2. Exit Device Configurations: Exit device lever trim to retract latchbolt for following exit device applications:
      
      NOTE – The following is applicable to Von Duprin 98/99/22 and Falcon 25 Series
      a. Rim
      NOTE – The following is applicable to Von Duprin 98/99/22 only.
   b. Surface vertical rod
NOTE – The following are applicable to Von Duprin 98/99 only.

c. Mortise
d. Concealed vertical rod
e. Concealed vertical cables

3. Exit Device Compatibility: Provide exit device trim with universal mounting plate enabling operation as required.

E. Requirements:

1. Provide adaptable electronic access control products that comply with the following requirements:

   a. Listed, UL 294 - The Standard of Safety for Access Control System Units.
   b. Compliant with ANSI/BHMA A156.25 Grade 1 Operation and Security.
   d. Compliant with ASTM E330 for door assemblies.
   e. Compliant with ICC / ANSI A117.1, NFPA 101, NFPA 80, and Industry Canada IC.

2. Functions: Provide functions as scheduled that are field configurable without taking the adaptable electronic product off the door.

3. Emergency Override: Provide mechanical key override; cylinders: Refer to “KEYING” article, herein.

4. Levers:

   a. Vandal Resistance: Exterior (secure side) lever rotates freely while door remains locked, preventing damage to internal lock components from vandalism by excessive force.
   b. Provide non-handed lever trim that operates independently of non-locking levers.
   c. Style: [Sparta (17)][Rhodes (06)][Athens (07)][Tubular (03)]
   d. Tactile Warning (Knurling): Where required by authority having jurisdiction. Provide on levers on exterior (secure side) of doors serving rooms considered to be hazardous.

5. Power Supply:

   a. Offline – access control rights stored on device and access control rights stored on magnetic stripe credential
      1) Adaptable electronic access control products powered by four AA batteries with options for eight AA batteries or a 12V or 24V DC power supply.
      2) Provide adaptable electronic access control products with the ability to communicate battery status.

   b. Networked – hardwired
      1) Adaptable electronic access control products powered by 12VDC or 24VDC power supply with max current draw not to exceed 250mA.

   c. Networked – wireless
      1) Adaptable electronic access control products powered by four AA batteries with options for eight AA batteries or a 12V or 24V DC power supply.
      2) Provide adaptable electronic access control products with the ability to communicate battery status and battery voltage level by means of a handheld programming device at door and remotely by Partner integrated software.

6. Features:
a. Audible feedback that can be enabled or disabled.

b. Tamper-Resistant Screws: Tamper-resistant Torx screws on inside escutcheon for increased security.

c. Offline – access control rights stored on device
   1) Visual tri-colored LED indicators that indicate activation, additional PIN code credential required, operational systems status, system error conditions and low power conditions.
   2) Visual bi-colored LED indicator on interior that is capable of indicating secured/unsecured status of device to occupants on interior.
   3) Onboard processor with memory capacity of 5,000 users, 5,000 event audit history, up to 16 time zones and up to 32 calendar events.

d. Offline – access control rights stored on magnetic stripe credential
   1) Visual tri-colored LED indicators that indicate activation, operational systems status, system error conditions and low power conditions.
   2) Onboard processor with memory capacity of 10,000 event audit history, up to 16 time zones and up to 32 calendar events.

e. Networked – hardware and wireless
   1) Ability to communicate unit’s communication status.
   2) Visual tri-colored LED indicators that indicate activation, additional PIN code credential required, operational systems status, system error conditions and low power conditions.
   3) Visual bi-colored LED indicator on interior that is capable of indicating secured/unsecured status of device to occupants on interior.

7. Adaptability:

a. Field changeable Reader Modules: Adaptable electronic access control products to have the ability to change credential reader technologies without being removed from door.

b. Offline
   1) Networking Capabilities: Network adaptable without removing device from door. Adaptable electronic access control products to have the ability to be upgraded in the field from a standalone battery powered configuration to a wireless networked configuration without being removed from the door.

c. Networked
   1) Open Architecture: Adaptable electronic access control products manufactured with open architecture characteristics capable of handling new and existing access control software and credential reading technology.

8. Switches: Provide adaptable electronic access control products with the following switches, standard:

a. Door Position Switch
b. Interior Cover Tamper Guard
c. Mechanical Key Override
d. Request to Exit
e. Request to Enter
f. Lock/Unlock Status (Clutch Position).

9. Credential Reader:

   EDIT – Select configuration(s) as required.

a. Offline – access control rights stored on device
1) Credential Reader Configuration: Provide credential reader modules in the following configurations, as indicated in door hardware sets. Multi-tech contactless reader shall be NFC-Compatible and read access control data from both 125 kHz and 13.56 MHz contactless smart cards. The multi-tech contactless reader shall be optimally designed for use in access control applications that require reading both 125 kHz proximity and 13.56 MHz contactless smart cards.

EDIT – Select configuration(s) as required.

a) Proximity, Smartcard via Multi-Technology.
b) Proximity, Smartcard via Multi-Technology and keypad.
c) Magnetic stripe (insertion type).
d) Magnetic stripe (insertion type) and keypad.
e) Magnetic stripe (swipe type).
f) Magnetic stripe (swipe type) and keypad.
g) Keypad.

2) Credential Reader Capabilities: Provide credential readers capable of operating with the following integrated software partners.

EDIT – Select capabilities, as appropriate, based upon reader configuration(s).

a) 13.56 MHz Smart card credentials: NOTE: Multi-tech reader.
   i. Secure section (Multi-Technology and Smartcard): aptiQ MIFARE Classic, aptiq MIFARE DESFire EV1, PIV and PIV-I Compatible
   ii. 13.56 MHz Serial number only (Multi-Technology and Smartcard): MIFARE, DESFire, HID iClass, MIFARE DESFire EV1
   iii. 125 kHz Proximity card credentials: Schlage, XceedID, HID, GE/CASI ProxLite and AWID. NOTE: Multi-tech reader.

b) Multi-Technology readers that read both 13.56 MHz Smart Cards and 125 kHz Prox cards. NOTE: Multi-tech reader.
c) Dual credential reading capabilities credential card or fob and PIN. NOTE: Credential reader combined with keypad.
d) 12 button keypad with backlit buttons.
e) Magnetic Card Reader:
   i. Full insertion or swipe reader capable of reading information along full length of magnetic stripe.
   ii. Magnetic card triple track reader capable of reading tracks 1, 2 or 3 per configuration in field.

b. Offline – access control rights stored on magnetic stripe credential

1) Credential Reader Configuration: Provide credential reader modules in the following configurations, as indicated in door hardware sets.

a) Magnetic stripe (insertion type).
b) Magnetic stripe (insertion type) and keypad.
c) Magnetic stripe (swipe type).
d) Magnetic stripe (swipe type) and keypad.

2) Credential Reader Capabilities: Provide credential readers capable of operating with the following integrated software partners.

a) Magnetic card triple track reader capable of reading tracks 1, 2 or 3 per configuration in field.
b) Dual credential reader with Keypad plus Magnetic card triple track reader capable of reading tracks 1, 2 or 3 per configuration in field.
   i. Reading capabilities of credential card and PIN
   ii. [Full insertion][Swipe] reader capable of reading information along full length of magnetic stripe.
   iii. 12 button keypad with backlit buttons.
c. Networked – hardwired

1) Credential Reader Configuration: Provide credential reader modules in the following configurations, as indicated in door hardware sets. Multi-tech contactless reader shall be NFC-Compatible and read access control data from both 125 kHz and 13.56 MHz contactless smart cards. The multi-tech contactless reader shall be optimally designed for use in access control applications that require reading both 125 kHz proximity and 13.56 MHz contactless smart cards.

**EDIT – Select configuration(s) as required.**

a) Proximity, Smartcard via Multi-Technology.
b) Proximity, Smartcard via Multi-Technology and keypad.
c) Magnetic stripe (insertion type).
d) Magnetic stripe (insertion type) and keypad.
e) Magnetic stripe (swipe type).
f) Magnetic stripe (swipe type) and keypad.
g) Keypad.

2) Credential Reader Capabilities: Provide credential readers capable of being configured at lockset with handheld programming device and remotely operated with the following integrated software partners.

**EDIT – Select capabilities, as appropriate, based upon reader configuration(s).**

a) 13.56 MHz Smart card credentials: **NOTE: Multi-tech reader.**
   i. Secure section (Multi-Technology and Smartcard): aptiQ MIFARE Classic, aptiq MIFARE DESFire EV1, PIV and PIV-I Compatible
   ii. 13.56 MHz Serial number only (Multi-Technology and Smartcard): MIFARE, DESFire, HID iClass, MIFARE DESFire EV1
   iii. 125 kHz Proximity card credentials: Schlage, XceedID, HID, GE/CASI ProxLite and AWID. **NOTE: Multi-tech reader.**

b) Multi-Technology readers that read both 13.56 MHz Smart Cards and 125 kHz Prox cards. **NOTE: Multi-tech reader.**
c) Dual credential reading capabilities credential card or fob and PIN. **NOTE: Credential reader combined with keypad.**
d) Magnetic Card Reader:
   i. **[Full insertion][Swipe]** reader capable of reading information along full length of magnetic stripe.
   ii. Magnetic card triple track reader capable of reading tracks 1, 2 or 3 per field configuration by handheld programming device at lockset and remotely by Partner integrated software.
e) 12 button keypad with backlit buttons.

d. Networked – wireless

1) Credential Reader Configuration: Provide credential reader modules in the following configurations, as indicated in door hardware sets. Multi-tech contactless reader shall be NFC-Compatible and read access control data from both 125 kHz and 13.56 MHz contactless smart cards. The multi-tech contactless reader shall be optimally designed for use in access control applications that require reading both 125 kHz proximity and 13.56 MHz contactless smart cards.

**EDIT – Select configuration(s) as required.**

a) Proximity, Smartcard via Multi-Technology.
b) Proximity, Smartcard via Multi-Technology and keypad.
c) Magnetic stripe (insertion type).
d) Magnetic stripe (insertion type) and keypad.
e) Magnetic stripe (swipe type).
f) Magnetic stripe (swipe type) and keypad.
g) Keypad.

2) Credential Reader Capabilities: Provide credential readers capable of being configured at lockset with handheld programming device and remotely operated with the following integrated software partners.

**EDIT – Select capabilities, as appropriate, based upon reader configuration(s).**

a) 13.56 MHz Smart card credentials: **NOTE: Multi-tech reader.**
   i. Secure section (Multi-Technology and Smartcard): aptiq MIFARE Classic, aptiq MIFARE DESFire EV1, PIV and PIV-I Compatible
   ii. 13.56 MHz Serial number only (Multi-Technology and Smartcard): MIFARE, DESfire, HID iClass, MIFARE DESFire EV1

b) 125 kHz Proximity card credentials: Schlage, XceedID, HID, GE/CASI ProxLite and AWID. **NOTE: Multi-tech reader.**

c) Multi-Technology readers that read both 13.56 MHz Smart Cards and 125 kHz Prox cards. **NOTE: Multi-tech reader.**

d) Dual credential reading capabilities credential card or fob and PIN. **NOTE: Credential reader combined with keypad.**

e) 12 button keypad with backlit buttons.

f) Magnetic Card Reader:
   i. **[Full insertion][Swipe]** reader capable of reading information along full length of magnetic stripe.
   ii. Magnetic card triple track reader capable of reading tracks 1, 2 or 3 per field configuration by handheld programming device at lockset and remotely by Partner integrated software.

10. Operation:

a. Offline – access control rights stored on device
   1) Provide adaptable electronic access control products with the ability to be configured at door by handheld programming device the length of time device is unlocked upon access grant.
   2) Provide adaptable electronic access control products with the ability to communicate identifying information such as firmware versions, hardware versions, serial numbers, and manufacturing dates by handheld programming device.

b. Networked – hardwired
   1) Adaptable electronic access control product system interface:
      a) EDIT - Select interface option.
      b) Wiegand or Clock & Data via PIB300 (Panel Interface Board). **OPTION 1**
      c) Directly via RS485. **OPTION 2**
   2) Adaptable electronic access control products to have real-time bidirectional communication between access control system and lock.
   3) Credential Verification Time: less than 1 second.
   4) When Utilized with Partner Integrated Access Control Network Software With Remote Commanding Capability: Provide adaptable electronic access control product with the ability to be remotely locked down or unlocked within 10 seconds or less, without user interface at the device.
   5) Upon Loss of Power to Device: Provide adaptable electronic access control product with the ability to manage access control offline in one of three methods below that can be configured in the field at lockset by handheld programming device and remotely by Partner integrated software:
      a) Fail locked (secured)
      b) Fail unlocked (unsecured)
      c) Fail As-Is
Upon Loss of Communication Between Device and Network: Provide adaptable electronic access control product with the ability to manage access control offline in one of four methods below that can be configured in the field at device by handheld programming device and remotely by Partner integrated software:

a) Fail locked (secured)
b) Fail unlocked (unsecured)
c) Fail As-Is
d) Fail to Degraded/cache mode utilizing cache memory with following selectable options:
   i. Grant access up to the last 1,000 unique previously accepted User IDs.
   ii. Grant access up to the last 1,000 unique previously accepted facility/site codes.
   iii. Remove from cache previously stored User IDs or facility/site codes that have not been presented to lock within the last 5 days.

7) Provide adaptable electronic access control product with the ability to be configured at door by handheld programming device and remotely by Partner integrated software the length of time device is unlocked upon access grant.

8) Provide adaptable electronic access control product with the ability to communicate identifying information such as firmware versions, hardware versions, serial numbers, and manufacturing dates by handheld programming device and remotely by Partner integrated software.

c. Networked – wireless
1) Adaptable electronic access control product system interface:
   a) EDIT - Select interface option.
   b) Wiegand or Clock & Data via PIM400-TD2 (Panel Interface Module).

   OPTION 1
   c) Directly via RS485. OPTION 2
2) Adaptable electronic access control products to have real-time bidirectional communication between access control system and lock.
3) EDIT – Wake on Radio feature is for battery-powered devices.
4) Remote Commanding By Partner Integrated Access Control Network Software: Battery-powered lockset shall have “Wake on Radio” feature causing activation of remote, wireless access control devices, enabling activated devices to be configured, locked or unlocked from a centralized location within 10 seconds or less without user interface at the device.
5) Local Commanding: Provide adaptable electronic access control product with the ability to be configured, locked or unlocked locally by handheld programming device, in real-time.
6) When Utilized with Access Control Network Software With Remote Commanding Capability: Provide adaptable electronic access control product with the ability to be remotely locked down or unlocked within 10 seconds or less while battery powered without user interface at the device.
7) Real-time response of battery powered device capable of being configured at door by handheld programming device and remotely by Partner integrated software.
8) Upon Loss of Power to Device: Provide adaptable electronic access control product with the ability to manage access control offline in one of three methods below that can be configured in the field at device by handheld programming device and remotely by Partner integrated software:
   a) Fail locked (secured)
   b) Fail unlocked (unsecured)
   c) Fail As-Is
9) Upon Loss of Communication Between Device and Network: Provide adaptable electronic access control product with the ability to manage access control offline
in one of four methods below that can be configured in the field at lockset by handheld programming device and remotely by Partner integrated software:

a) Fail locked (secured)
b) Fail unlocked (unsecured)
c) Fail As-Is
d) Fail to Degraded/cache mode utilizing cache memory with following selectable options:
   i. Grant access up to the last 1,000 unique previously accepted User IDs.
   ii. Grant access up to the last 1,000 unique previously accepted facility/site codes
   iii. Remove from cache previously stored User IDs or facility/site codes that have not been presented to lock within the last 5 days.

10) Provide adaptable electronic access control product with the ability to be configured at door by handheld programming device and remotely by Partner integrated software the length of time device is unlocked upon access grant.

11) Provide adaptable electronic access control product with the ability to communicate identifying information such as firmware versions, hardware versions, serial numbers, and manufacturing dates by handheld programming device and remotely by Partner integrated software.

12) Wireless Transmission:
   a) Modulation: 900 MHz spread spectrum, direct sequence, 10 channels.
   b) Encryption: AES-128 bit Key minimum.

F. Components

1. Product: Schlage HHD series with Utility Software.

   REQUIRED for all AD-series

   a. Provide Handheld Programming Device for adaptable electronic access control products capable of the following minimum requirements.
      1) Capable of initializing lock and accessories using preloaded software.
      2) Utilized to field configure electronic access control devices, to download firmware updates and door files to device, and to download audit files from device.

2. Product: Schlage PIB300-2D Panel Interface Board.

   OPTION for AD-300 series no substitute

   a. Provide Panel Interface Board for hardwired adaptable electronic access control products capable of the following minimum requirements.
      1) Used to connect hardwired adaptable electronic access control products to the access control board or reader interface board, where Wiegand or Clock & Data protocol is required.
      2) Applicable Standards:
         a) Listed, UL 294 - The Standard of Safety for Access Control System Units.
         b) Compliant with NEMA 1, 4, 4X, 6.
         d) Compliant to ASTM E3300 and IC (Canada).
      3) Power Supply: 12VDC or 24VDC.
      4) Status Indicators: 13 LEDs minimum.

3. Product: Schlage PIM400-485 or PIM400-TD2 Panel Interface Module as required.

   OPTION for AD-400 series no substitute

   a. Provide Panel Interface Module for wireless adaptable electronic access control products capable of the following minimum requirements.
1) Used to connect wireless adaptable electronic access control products to the access control board or reader interface board [where Wiegand or Clock & Data protocol is required].

2) Distribution:
   a) General: Provide one (1) panel interface module per sixteen (16) electronic access control devices, subject to the following limitations:
      i. Panel interface module is located on the same floor as associated electronic access control devices.
      ii. Panel interface module is located up to 200-feet (60m) indoor range with normal building obstructions; or up to 1000-feet (300m) with unobstructed, clear line-of-sight of associated electronic access control device(s).
   b) Where panel interface module cannot comply with general distribution requirements for associated electronic access control devices, provide additional modules, as required.
   c) General: Provide one (1) panel interface module per two (2) electronic access control devices, subject to the following limitations:
      i. Panel interface module is located on the same floor as associated electronic access control devices.
      ii. Panel interface module is located up to 200-feet (60m) indoor range with normal building obstructions; or up to 1000-feet (300m) with unobstructed, clear line-of-sight of associated electronic access control device(s).
   d) Where panel interface module cannot comply with general distribution requirements for associated electronic access control devices, provide additional modules, as required.

3) Applicable Standards:
   a) Listed, UL 294 - The Standard of Safety for Access Control System Units.
   b) Compliant with NEMA 1, 4, 4X, 6; 294
   c) Certified compliant with FCC Part 15 and RoHS.

4) Power Supply: 12VDC or 24VDC.

5) Wireless Transmission:
   a) Modulation: 900 MHz spread spectrum, direct sequence, 10 channels.
   b) Encryption: AES-128 bit Key minimum.


   **OPTION for AD-400 series no substitute**

   a. Provide Panel Interface Module for wireless adaptable electronic access control products capable of the following minimum requirements.

      1) System Description – General
         a) Intelligent controller shall provide decision making, event reporting, and database storage for hardware platform. Reader interface shall provide control for up to 16 wireless access points in paired and or alternate reader configurations.
         b) Controller shall communicate with the host via on-board 10BaseT/100BaseTX Ethernet port.
         c) Card data, PIN data, Door position and Request to Exit shall all be reported to wireless access control remote device.

      2) Distribution:
         a) General: Provide one (1) panel interface module per sixteen (16) electronic access control devices, subject to the following limitations:
            i. Panel interface module is located on the same floor as associated electronic access control devices.
            ii. Panel interface module is located up to 200-feet (60m) indoor range with normal building obstructions; or up to 1000-feet (300m) with
unobstructed, clear line-of-sight of associated electronic access control device(s).

b) Where panel interface module cannot comply with general distribution requirements for associated electronic access control devices, provide additional modules, as required.

3) Applicable Standards:
   a) Listed, UL 294 – The Standard of Safety for Access Control System Units, when connected to a UL 294-listed power supply.
   b) Certified compliant with:
      i. FCC Part 15, Class C.
      ii. NIST Encryption
      iii. IC (Canada)
      iv. RoHS

4) Power Input:
   a) Power over Ethernet (PoE) power input 12.95 watts, compliant to IEEE 802.3af.
   b) Twelve volts of direct current (12VDC) ±10% 400 mA minimum from a UL294 listed power supply to achieve UL294 Listing.
   c) No additional wiring requirements such as RS-485 or RS-232.

5) Wireless Communication:
   a) Transmission/Encryption: AES-128 bit Key
   b) 900MHz spread spectrum modulation, direct sequence, 10 channels, field configurable Dynamic Channel Switching.
   c) Up to 200’ with normal building obstructions or up to 1000’ feet in clear line of sight.

6) Enclosure:
   a) Certifications: NEMA 1, 4, 4X, 12, 13.
   b) Size: 10.43-inches (265mm) high; 7.28-inches (185mm) wide; 3.79-inches (96mm) deep.

7) Environmental Conditions:
   a) Operational Temperature: 32-deg F (0-deg C) to 150 F (66-deg C).
   b) Operating Humidity: Ten to ninety-five percent (10–95%) relative humidity, non-condensing (RHNC).

8) Connectivity:
   a) Primary Port: 10/100 Ethernet
   b) External RJ-45 connector for direct connection on exterior of enclosure.
   c) External USB connector for direct connection on exterior of enclosure.
   d) Option to connect to external remote antenna to enable additional wireless applications including extended distances and navigation of radio frequency barriers.

9) Door Control: Up to sixteen (16) physical barriers can be controlled wirelessly.

10) Access Control Capabilities:
    a) 240,000 Cardholder capacity
    b) 50,000 Transaction buffer
    c) 32 Access Levels per cardholder
    d) 19 digit (64-bit) user ID and 15 digit PIN numbers maximum
    e) Activation and Deactivation dates
    f) If/Then Macro capability

11) Card Formats:
    a) Eight active card formats per intelligent controller
    b) 19 digit (64-bit) User ID and 15 digit PIN numbers maximum
    c) PIV-II, CAC, TWIC card compatible

12) Card Reader Functions
    a) Multiple card format support by reader
    b) Paired reader support
    c) Elevator support
**2.33 ACCESS CONTROL READER**

A. Manufacturers and Products:


B. Requirements: Read Only Multi-technology Contactless reader

1. Access control card readers shall be as manufactured by a global company who is a recognized leader in the production of access control devices. Card reader manufactured for non-access control applications shall not be acceptable

2. Multi-technology contactless reader shall read access control data from both 125 kHz and 13.56 MHz contactless smart cards and NFC-compatible. The multi-technology contactless reader shall be optimally designed for use in access control applications that require reading both 125 kHz Proximity and 13.56 MHz contactless smart cards by providing:

   a. Configuration allows reader to be enabled to read smart, proximity or both technologies at the same time.
   b. A migration platform to upgrade from the most popular 125 kHz proximity technologies to MIFARE or MIFARE DESFire EV1 by reading both 125 kHz proximity technology and 13.56 MHz contactless smart card technology.
   c. Guaranteed compatibility to read all standard data formats ensuring card-to-reader interoperability in multi-location installations and multi-card/reader populations.
   d. Secure access control data exchange between the smart card and the reader utilizing diversified keys and mutual authentication sequences.
   e. Universal compatibility with most access control systems.
   f. Ease of installation through industry standard wiring methods.
g. Compatibility with legacy 125 KHz proximity access control formats (all standard formats up to 37 bits, including HID Corporate 1000 formats).

h. Optimal read range and read speed for increased access control throughput.

i. Global availability.

j. Product construction suitable for both indoor and outdoor applications.

k. Customizable behavior for indicator lights and beeper.

3. Multi-technology contactless reader shall comply with the following 13.56MHz-related standards to ensure product compatibility and predictability of performance:

   a. ISO 14443

4. Multi-technology contactless reader shall be configurable to read 13.56 MHz data simultaneously from the following cards (multiple credential support based on reader configuration):

   a. Secure support - Mifare DESFire EV1 with PACSA, Mifare Classic, FIPS 201 PIV Credential.
   b. UID/CSN Support – DESFire Classic V0.06, HID iClass, ISOX (my-d).

5. Multi-technology contactless reader shall be configurable to read data from any compatible 125 kHz technology simultaneously with 13.56 MHz data. Compatible 125 kHz technologies include:

   a. XCEEDID/Schlage/HID Prox (format in the card – formats up to 37-bits supported).
   b. AWID PROX (SAME AS LENEL PROX - format in the card – formats up to 42-bits).
   c. GE PROX - two possible format options.

6. Multi-technology contactless reader shall provide the ability to read card access data stored in the secure access control sector/application area of the ISO 14443 XceedID MIFARE or MIFARE DESFire EV1 card.

7. The Multi-technology contactless reader shall be configurable to provide multiple hierarchical degrees of key compatibility for accessing the smart card access control data. Compatibility shall be provided for the following key structure options:

   a. Compatibility with the default manufacture’s key structure to ensure convenient off the shelf compatibility with manufacture’s cards and readers.
   b. Compatibility with custom keys managed by manufacturer which provide a site-specific, unique, protected key structure.
   c. Compatibility with high security customer managed custom keys.

8. The Multi-technology contactless reader shall be configurable to provide compatibility with all standard Prox formats up to 37 bits (including Corporate 1000®).

9. Multi-technology contactless reader shall allow the reader firmware to be upgraded in the field without the need to remove the reader from the wall through the use of factory-provided device.

10. Multi-technology contactless reader shall be suitable for global deployment by meeting worldwide radio and safety regulatory compliance including:

    a. FCC Certification (US)
    b. CE (EU)
    c. C-tick (Australia, New Zealand)
    d. R&TTE Directive (15EU)
    e. UL294 (US)
    f. ULC-S319
Multi-technology contactless reader shall be fully compliant with Restriction of Hazardous Substances directive (RoHS) restricting the use of specific hazardous materials found in electrical and electronic products.

Multi-technology contactless reader shall provide universal compatibility with most access control systems by outputting card data in compliance with the SIA AC-01 Wiegand standard.

Multi-technology contactless reader shall allow for secure installation practices through mounting methods utilizing tamper resistant screws.

Multi-technology contactless reader shall provide the ability to transmit an alarm signal via and integrated optical tamper switch if an attempt is made to remove the reader from the wall. The tamper switch shall be programmable to provide a selectable action to provide a selectable action compatible with various tamper communication schemes provided by access control panel manufacturers. The selectable action shall include one of the following:

a. The reader open collector line changes from a high state (5V) to a low state (Ground).

b. If utilizing OSDP Protocol reader shall report a tamper condition via RS485.

Multi-technology contactless reader shall provide the ability for mounting to standard electrical boxes through the use of universal international mounting holes.

Multi-technology contactless reader shall be provided with a full potted assembly.

Multi-technology contactless reader shall be provided with a quick connect wire harness.

The Multi-technology contactless reader shall provide customizable reader behavior options either from the factory, or defined in the field through the use of pre-configured command cards. Reader behavior programming options shall include:

a. LED & Audio configurations.
b. Ability to disable reading of specific card technologies or frequencies.
c. ISO 14443/15693 CSN output configuration.
d. Wiegand output spacing and timing.

Multi-technology contactless reader shall provide the following programmable audio/visual indication:

a. An audio beeper shall provide tone sequence to signify: access granted, access denied, power up, and diagnostics.
b. A light bar shall provide clear visual status (red/green/amber).

Multi-technology contactless reader shall be designed for low current operation to enable migration from most legacy proximity applications without the need to replace existing access control panels and/or power supplies. Contactless smart card power requirements shall be:

a. Operating voltage: 5 – 16 VDC, reverse voltage protected. Linear power supply recommended.
b. Current requirements: 125 mA DC, 140 mA PEAK @ 12 VDC

Multi-technology contactless reader shall meet the following physical specifications:

a. Dimensions: 5.91” x 1.72” x 0.84” (15 cm x 4.4 cm x 2.1cm)
b. Weight: 9.6 oz. (272.15 g)
c. Material: UL94 Polycarbonate
22. Multi-technology contactless reader shall meet the following environmental specifications:
   a. Operating temperature: -31 to 151 degrees F (-35 to 67 degrees C)
   b. Operating humidity: 5% to 95% relative humidity non-condensing
   c. Weatherized design suitable to withstand harsh environments
      1) Certified rating of IP65

23. Multi-technology contactless reader cabling requirements shall be:
   a. Cable distance: (Wiegand): 500 feet (150m)
   b. Cable type: 5-conductor #22 AWG
   c. Standard reader termination: 18" (0.5m) wire harness

2.34 ACCESS CONTROL READER

A. Manufacturers and Products:

B. Requirements: Read Only Multi-technology Contactless reader
   1. Access control card readers shall be as manufactured by a global company who is a
      recognized leader in the production of access control devices. Card reader manufactured
      for non-access control applications shall not be acceptable.
   2. Multi-technology contactless reader shall read access control data from both 125 kHz
      and 13.56 MHz contactless smart cards and NFC-compatible. The multi-technology
      contactless reader shall be optimally designed for use in access control applications that
      require reading both 125 kHz Proximity and 13.56 MHz contactless smart cards by
      providing:
         a. Configuration allows reader to be enabled to read smart, proximity or both
            technologies at the same time.
         b. A migration platform to upgrade from the most popular 125 kHz proximity
            technologies to MIFARE or MIFARE DESFire EV1 by reading both 125 kHz proximity
            technology and 13.56 MHz contactless smart card technology.
         c. Guaranteed compatibility to read all standard data formats ensuring card-to-reader
            interoperability in multi-location installations and multi-card/reader populations.
         d. Secure access control data exchange between the smart card and the reader utilizing
            diversified keys and mutual authentication sequences.
         e. Universal compatibility with most access control systems.
         f. Ease of installation through industry standard wiring methods.
         g. Compatibility with legacy 125 KHz proximity access control formats (all standard
            formats up to 37 bits, including HID Corporate 1000 formats).
         h. Optimal read range and read speed for increased access control throughput.
         i. Global availability.
         j. Product construction suitable for both indoor and outdoor applications.
         k. Customizable behavior for indicator lights and beeper.
   3. Multi-technology contactless reader shall comply with the following 13.56MHz-related
      standards to ensure product compatibility and predictability of performance:
         a. ISO 14443
4. Multi-technology contactless reader shall be configurable to read 13.56 MHz data simultaneously from the following cards (multiple credential support based on reader configuration):
   a. Secure support - Mifare DESFire EV1 with PACSA, Mifare Classic, FIPS 201 PIV Credential.
   b. UID/CSN Support – DESFire Classic V0.06, HID iClass, ISOX (my-d).

5. Multi-technology contactless reader shall be configurable to read data from any compatible 125 kHz technology simultaneously with 13.56 MHz data. Compatible 125 kHz technologies include:
   a. XCEEDID/Schlage/HID Prox (format in the card – formats up to 37-bits supported).
   b. AWID PROX (SAME AS LENEL PROX - format in the card – formats up to 42-bits).
   c. GE PROX - two possible format options.

6. Multi-technology contactless reader shall provide the ability to read card access data stored in the secure access control sector/application area of the ISO 14443 XceedID MIFARE or MIFARE DESFire EV1 card.

7. The Multi-technology contactless reader shall be configurable to provide multiple hierarchical degrees of key compatibility for accessing the smart card access control data. Compatibility shall be provided for the following key structure options:
   a. Compatibility with the default manufacture’s key structure to ensure convenient off the shelf compatibility with manufacture’s cards and readers.
   b. Compatibility with custom keys managed by manufacturer which provide a site-specific, unique, protected key structure.
   c. Compatibility with high security customer managed custom keys.

8. The Multi-technology contactless reader shall be configurable to provide compatibility with all standard Prox formats up to 37 bits (including Corporate 1000®).

9. Multi-technology contactless reader shall allow the reader firmware to be upgraded in the field without the need to remove the reader from the wall through the use of factory-provided device.

10. Multi-technology contactless reader shall be suitable for global deployment by meeting worldwide radio and safety regulatory compliance including:
    a. FCC Certification (US)
    b. CE (EU)
    c. C-tick (Australia, New Zealand)
    d. R&TTE Directive (15EU)
    e. UL294 (US)
    f. ULC-S319
    g. IC (Canada)
    h. FIPS201 / PIV I
    i. IP65

11. Multi-technology contactless reader shall be fully compliant with Restriction of Hazardous Substances directive (RoHS) restricting the use of specific hazardous materials found in electrical and electronic products.

12. Multi-technology contactless reader shall provide universal compatibility with most access control systems by outputting card data in compliance with the SIA AC-01 Wiegand standard.

13. Multi-technology contactless reader shall allow for secure installation practices through mounting methods utilizing tamper resistant screws.
14. Multi-technology contactless reader shall provide the ability to transmit an alarm signal via an integrated optical tamper switch if an attempt is made to remove the reader from the wall. The tamper switch shall be programmable to provide a selectable action to provide a selectable action compatible with various tamper communication schemes provided by access control panel manufacturers. The selectable action shall include one of the following:

a. The reader open collector line changes from a high state (5V) to a low state (Ground).
b. If utilizing OSDP Protocol reader shall report a tamper condition via RS485.

15. Multi-technology contactless reader shall provide the ability for mounting to standard electrical boxes through the use of universal international mounting holes.

16. Multi-technology contactless reader shall be provided with a full potted assembly.

17. Multi-technology contactless reader shall be provided with a quick connect wire harness.

18. The Multi-technology contactless reader shall provide customizable reader behavior options either from the factory, or defined in the field through the use of pre-configured command cards. Reader behavior programming options shall include:

a. LED & Audio configurations.
b. Ability to disable reading of specific card technologies or frequencies.
c. ISO 14443/15693 CSN output configuration.
d. Wiegand output spacing and timing.

19. Multi-technology contactless reader shall provide the following programmable audio/visual indication:

a. An audio beeper shall provide tone sequence to signify: access granted, access denied, power up, and diagnostics.
b. A light bar shall provide clear visual status (red/green/amber).

20. Multi-technology contactless reader shall be designed for low current operation to enable migration from most legacy proximity applications without the need to replace existing access control panels and/or power supplies. Contactless smart card power requirements shall be:

a. Operating voltage: 5 – 16 VDC, reverse voltage protected. Linear power supply recommended.
b. Current requirements: 160 mA DC, 195 mA PEAK @ 12 VDC

21. Multi-technology contactless reader shall meet the following physical specifications:

a. Dimensions: 5.1" x 3.25" x 0.83" (12.9 cm x 8.3 cm x 2.1 cm)
b. Weight: 9.6 oz. (272.15 g)
c. Material: UL94 Polycarbonate
d. Plastics: Consist of three-piece design with mounting plate, potted case and aesthetic cover.
e. Color: Black, Gray, Brown or Cream as approved by the project architect.

22. Multi-technology contactless reader shall meet the following environmental specifications:

a. Operating temperature: -31 to 151 degrees F (-35 to 67 degrees C)
b. Operating humidity: 5% to 95% relative humidity non-condensing

23. Multi-technology contactless reader cabling requirements shall be:
a. Cable distance: (Wiegand): 500 feet (150m) 
b. Cable type: 5-conductor #22 AWG  
c. Standard reader termination: 18” (0.5m) wire harness

2.35 ACCESS CONTROL READER

A. Manufacturers and Products:

B. Requirements: Read Only Multi-technology Contactless reader
   1. Access control card readers shall be as manufactured by a global company who is a recognized leader in the production of access control devices. Card reader manufactured for non-access control applications shall not be acceptable.
   2. Multi-technology contactless reader shall read access control data from both 125 kHz and 13.56 MHz contactless smart cards and NFC-compatible. The multi-technology contactless reader shall be optimally designed for use in access control applications that require reading both 125 kHz Proximity and 13.56 MHz contactless smart cards by providing:
      a. Configuration allows reader to be enabled to read smart, proximity or both technologies at the same time.
      b. A migration platform to upgrade from the most popular 125 kHz proximity technologies to MIFARE or MIFARE DESFire EV1 by reading both 125 kHz proximity technology and 13.56 MHz contactless smart card technology.
      c. Guaranteed compatibility to read all standard data formats ensuring card-to-reader interoperability in multi-location installations and multi-card/reader populations.
      d. Secure access control data exchange between the smart card and the reader utilizing diversified keys and mutual authentication sequences.
      e. Universal compatibility with most access control systems.
      f. Ease of installation through industry standard wiring methods.
      g. Compatibility with legacy 125 KHz proximity access control formats (all standard formats up to 37 bits, including HID Corporate 1000 formats).
      h. Optimal read range and read speed for increased access control throughput.
      i. Global availability.
      j. Product construction suitable for both indoor and outdoor applications.
      k. Customizable behavior for indicator lights and beeper.
   3. Multi-technology contactless reader shall comply with the following 13.56MHz-related standards to ensure product compatibility and predictability of performance:
      a. ISO 14443
   4. Multi-technology contactless reader shall be configurable to read 13.56 MHz data simultaneously from the following cards (multiple credential support based on reader configuration):
      a. Secure support - Mifare DESFire EV1 with PACSA, Mifare Classic, FIPS 201 PIV Credential.
      b. UID/CSN Support – DESFire Classic V0.06, HID iClass, ISOX (my-d).
5. Multi-technology contactless reader shall be configurable to read data from any compatible 125 kHz technology simultaneously with 13.56 MHz data. Compatible 125 kHz technologies include:
   a. XCEEDID/Schlage/HID Prox (format in the card – formats up to 37-bits supported).
   b. AWID PROX (SAME AS LENEL PROX - format in the card – formats up to 42-bits).
   c. GE PROX - two possible format options.

6. Multi-technology contactless reader shall provide the ability to read card access data stored in the secure access control sector/application area of the ISO 14443 XceedID MIFARE or MIFARE DESFire EV1 card.

7. The Multi-technology contactless reader shall be configurable to provide multiple hierarchical degrees of key compatibility for accessing the smart card access control data. Compatibility shall be provided for the following key structure options:
   a. Compatibility with the default manufacture’s key structure to ensure convenient off the shelf compatibility with manufacture’s cards and readers.
   b. Compatibility with custom keys managed by manufacturer which provide a site-specific, unique, protected key structure.
   c. Compatibility with high security customer managed custom keys.

8. The Multi-technology contactless reader shall be configurable to provide compatibility with all standard Prox formats up to 37 bits (including Corporate 1000®).

9. Multi-technology contactless reader shall allow the reader firmware to be upgraded in the field without the need to remove the reader from the wall through the use of factory-provided device.

10. Multi-technology contactless reader shall be suitable for global deployment by meeting worldwide radio and safety regulatory compliance including:
    a. FCC Certification (US)
    b. CE (EU)
    c. C-tick (Australia, New Zealand)
    d. R&TTE Directive (15EU)
    e. UL294 (US)
    f. ULC-S319
    g. IC (Canada)
    h. FIPS201 / PIV I
    i. IP65

11. Multi-technology contactless reader shall be fully compliant with Restriction of Hazardous Substances directive (RoHS) restricting the use of specific hazardous materials found in electrical and electronic products.

12. Multi-technology contactless reader shall provide universal compatibility with most access control systems by outputting card data in compliance with the SIA AC-01 Wiegand standard.

13. Multi-technology contactless reader shall allow for secure installation practices through mounting methods utilizing tamper resistant screws.

14. Multi-technology contactless reader shall provide the ability to transmit an alarm signal via and integrated optical tamper switch if an attempt is made to remove the reader from the wall. The tamper switch shall be programmable to provide a selectable action to provide a selectable action compatible with various tamper communication schemes provided by access control panel manufacturers. The selectable action shall include one of the following:
    a. The reader open collector line changes from a high state (5V) to a low state (Ground).
    b. If utilizing OSDP Protocol reader shall report a tamper condition via RS485.
15. Multi-technology contactless reader shall provide the ability for mounting to standard electrical boxes through the use of universal international mounting holes.

16. Multi-technology contactless reader shall be provided with a full potted assembly.

17. Multi-technology contactless reader shall be provided with a quick connect wire harness.

18. The Multi-technology contactless reader shall provide customizable reader behavior options either from the factory, or defined in the field through the use of pre-configured command cards. Reader behavior programming options shall include:
   
   a. LED & Audio configurations.
   b. Ability to disable reading of specific card technologies or frequencies.
   c. ISO 14443/15693 CSN output configuration.
   d. Wiegand output spacing and timing.

19. Multi-technology contactless reader shall provide the following programmable audio/visual indication:
   
   a. An audio beeper shall provide tone sequence to signify: access granted, access denied, power up, and diagnostics.
   b. A light bar shall provide clear visual status (red/green/amber).

20. Multi-technology contactless reader shall be designed for low current operation to enable migration from most legacy proximity applications without the need to replace existing access control panels and/or power supplies. Contactless smart card power requirements shall be:
   
   a. Operating voltage: 5 – 16 VDC, reverse voltage protected. Linear power supply recommended.
   b. Current requirements: 125 mA DC, 140 mA PEAK @ 12 VDC

21. Multi-technology contactless reader shall meet the following physical specifications:
   
   a. Dimensions: 5.1” x 3.25” x 0.83” (12.9 cm x 8.3 cm x 2.1cm)
   b. Weight: 11.2 oz. (317.51 g)
   c. Material: UL94 Polycarbonate
   d. Plastics: Consist of three-piece design with mounting plate, potted case and aesthetic cover.
   e. Color: Black, Gray, Brown or Cream as approved by the project architect.

22. Multi-technology contactless reader shall meet the following environmental specifications:
   
   a. Operating temperature: -31 to 151 degrees F (-35 to 67 degrees C)
   b. Operating humidity: 5% to 95% relative humidity non-condensing
   c. Weatherized design suitable to withstand harsh environments
      1) Certified rating of IP65

23. Multi-technology contactless reader cabling requirements shall be:
   
   a. Cable distance: (Wiegand): 500 feet (150m)
   b. Cable type: 5-conductor #22 AWG
   c. Standard reader termination: 18” (0.5m) wire harness

2.36 ACCESS CONTROL READER

A. Manufacturers and Products:

B. Requirements: Proximity Card Reader

1. Access control card readers shall be as manufactured by a global company who is a recognized leader in the production of access control devices. Card reader manufactured for non-access control applications shall not be acceptable.
2. Provide surface mounting style 125 KHz proximity card readers suitable for door or window mullion mounting.
3. The reader shall be capable of reading access control data in standard Wiegand formats up to 37 bits in length from any XceedID Proximity card or equivalent, outputting the data in the following configuration:
   a. The card reader shall output credential data in compliance with the SIA AC-01 Wiegand standard, compatible with all standard access control systems.
4. Proximity card readers shall provide the following programmable audio/visual indication:
   a. A buzzer shall provide an audible tone upon successful power up/self-test, good card read, or whenever the beeper control line is asserted by the host.
   b. A tri-color, red/green/amber LED shall light upon successful power up/self-test, good card read, or whenever the LED control line(s) are asserted by the host.
   c. The reader shall have individual control lines for the buzzer, and for red and green LED indication. When the LED control lines are asserted simultaneously, an amber LED indication will occur.
5. The reader shall have a configurable hold input, which when asserted shall either buffer a single card read or disable the reader, until the line is released. This input may be used for special applications or with loop detectors.
6. Typical proximity card read range shall be up to:
   a. Prox ISO Card: 2.5 – 5" (6.5 – 12.5 cm)
   b. Prox Clamshell Card: 3.5 – 4.0" (9.0 – 10.0 cm)
   c. Prox Keyfob/Tag: 1.25 – 1.75" (3.2 - 4.5 cm)
7. Proximity card readers shall meet the following physical specifications:
   a. Dimensions: 4.26 x 1.72 x 0.84" (10.8 x 4.4 x 2.1 cm)
   b. Weight: 7.2 oz (204.16 g)
   c. Material: UL94 Polycarbonate
   d. Three-part design with back plate, potted reader and aesthetic cover.
   e. Color: Black, Gray, Brown or Cream as approved by the project architect.
8. Proximity card readers shall meet the following electrical specifications:
   a. Operating voltage: 5 – 16 VDC, reverse voltage protected. Linear power supply recommended.
   b. Current requirements: 65 mA DC, 110 mA DC Peak @ 12 VDC.
9. Proximity card readers shall meet the following certifications:
   a. FCC Certification (US)
   b. CE (EU)
   c. C-tick (Australia, New Zealand)
   d. R&TTE Directive (15EU)
   e. UL294 (US)
   f. CAN/ULC-S319
   g. IC (Canada)
10. Proximity card readers shall meet the following environmental specifications.
a. Operating temperature: -31 to 151 degrees F (-35 to 67 degrees C)
b. Operating humidity: 5% to 95% relative humidity non-condensing
c. Weatherized design suitable to withstand harsh environments
   1) Certified rating of IP65

11. Proximity card readers cabling requirements shall be:
   a. Cable distance: (Wiegand): 500 feet (150m)
   b. Cable type: 5-conductor #22 AWG
   c. Standard reader termination: 18” (0.5m) wire harness

2.37 ACCESS CONTROL READER

A. Manufacturers and Products:

B. Requirements: Read Only Smart Contactless reader
   1. Access control card readers shall be as manufactured by a global company who is a recognized leader in the production of access control devices. Card reader manufactured for non-access control applications shall not be acceptable.
   2. Smart contactless reader shall read access control data from both 125 kHz and 13.56 MHz contactless smart cards and NFC-compatible. The Smart contactless reader shall be optimally designed for use in access control applications that require reading 13.56 MHz contactless smart cards by providing:
      a. Configuration allows reader to be enabled to read smart.
      b. Guaranteed compatibility to read all standard data formats ensuring card-to-reader interoperability in multi-location installations and multi-card/reader populations.
      c. Secure access control data exchange between the smart card and the reader utilizing diversified keys and mutual authentication sequences.
      d. Universal compatibility with most access control systems.
      e. Ease of installation through industry standard wiring methods.
      f. Optimal read range and read speed for increased access control throughput.
      g. Global availability.
      h. Product construction suitable for both indoor and outdoor applications.
      i. Customizable behavior for indicator lights and beeper.
   3. Smart contactless reader shall comply with the following 13.56MHz-related standards to ensure product compatibility and predictability of performance:
      a. ISO 14443
   4. Smart contactless reader shall be configurable to read 13.56 MHz data simultaneously from the following cards (multiple credential support based on reader configuration):
      a. Secure support - Mifare DESFire EV1 with PACSA, Mifare Classic, FIPS 201 PIV Credential.
      b. UID/CSN Support – DESFire Classic V0.06, HID iClass, ISOX (my-d).
   5. Smart contactless reader shall provide the ability to read card access data stored in the secure access control sector/application area of the ISO 14443 XceedID MIFARE or MIFARE DESFire EV1 card.
6. The Smart contactless reader shall be configurable to provide multiple hierarchical
degrees of key compatibility for accessing the smart card access control data.
Compatibility shall be provided for the following key structure options:

   a. Compatibility with the default manufacture’s key structure to ensure convenient off
      the shelf compatibility with manufacture’s cards and readers.
   b. Compatibility with custom keys managed by manufacturer which provide a site-
      specific, unique, protected key structure.
   c. Compatibility with high security customer managed custom keys.

7. Smart contactless reader shall allow the reader firmware to be upgraded in the field
   without the need to remove the reader from the wall through the use of factory-provided
device.

8. Smart contactless reader shall be suitable for global deployment by meeting worldwide
   radio and safety regulatory compliance including:

   a. FCC Certification (US)
   b. CE (EU)
   c. C-tick (Australia, New Zealand)
   d. R&TTE Directive (15EU)
   e. UL294 (US)
   f. ULC-S319
   g. IC (Canada)
   h. FIPS201 / PIV I
   i. IP65

9. Smart contactless reader shall be fully compliant with Restriction of Hazardous
   Substances directive (RoHS) restricting the use of specific hazardous materials found in
   electrical and electronic products.

10. Smart contactless reader shall provide universal compatibility with most access control
    systems by outputting card data in compliance with the SIA AC-01 Wiegand standard.

11. Smart contactless reader shall allow for secure installation practices through mounting
    methods utilizing tamper resistant screws.

12. Smart contactless reader shall provide the ability to transmit an alarm signal via and
    integrated optical tamper switch if an attempt is made to remove the reader from the wall.
    The tamper switch shall be programmable to provide a selectable action to provide a
    selectable action compatible with various tamper communication schemes provided by
    access control panel manufacturers. The selectable action shall include one of the
    following:

    a. The reader open collector line changes from a high state (5V) to a low state
       (Ground).
    b. If utilizing OSDP Protocol reader shall report a tamper condition via RS485.

13. Smart contactless reader shall provide the ability for mounting to standard electrical
    boxes through the use of universal international mounting holes.

14. Smart contactless reader shall be provided with a full potted assembly.

15. Smart contactless reader shall be provided with a quick connect wire harness.

16. The Smart contactless reader shall provide customizable reader behavior options either
    from the factory, or defined in the field through the use of pre-configured command cards.
    Reader behavior programming options shall include:

    a. LED & Audio configurations.
    b. Ability to disable reading of specific card technologies or frequencies.
    c. ISO 14443/15693 CSN output configuration.
    d. Wiegand output spacing and timing.
17. Smart contactless reader shall provide the following programmable audio/visual indication:
   a. An audio beeper shall provide tone sequence to signify: access granted, access denied, power up, and diagnostics.
   b. A light bar shall provide clear visual status (red/green/amber).

18. Smart contactless reader shall be designed for low current operation to enable migration from most legacy proximity applications without the need to replace existing access control panels and/or power supplies. Contactless smart card power requirements shall be:
   a. Operating voltage: 5 – 16 VDC, reverse voltage protected. Linear power supply recommended.
   b. Current requirements: 65 mA DC, 110 mA PEAK @ 12 VDC

19. Smart contactless reader shall meet the following physical specifications:
   a. Dimensions: 4.26” x 1.72” x 0.84” (10.8 cm x 4.4 cm x 2.1 cm)
   b. Weight: 7.2 oz. (204.16 g)
   c. Material: UL94 Polycarbonate
   d. Plastics: Consist of three-piece design with mounting plate, potted case and aesthetic cover.
   e. Color: Black, Gray, Brown or Cream as approved by the project architect.

20. Smart contactless reader shall meet the following environmental specifications:
   a. Operating temperature: -31 to 151 degrees F (-35 to 67 degrees C)
   b. Operating humidity: 5% to 95% relative humidity non-condensing
   c. Weatherized design suitable to withstand harsh environments
      1) Certified rating of IP65

21. Smart contactless reader cabling requirements shall be:
   a. Cable distance: (Wiegand): 500 feet (150m)
   b. Cable type: 5-conductor #22 AWG
   c. Standard reader termination: 18” (0.5m) wire harness

2.38 ACCESS CONTROL CREDENTIALS

A. Manufacturer and Product:
   1. Scheduled Manufacturer and Product: aptiQ XF9551.

B. Requirements:
   1. Provide access control credentials ISO 14443A compliant and GSC-IS® certified compatible with access control readers that allow authorized entry and hold information specific to the user.
   2. Provide credentials that have an ISO MIFARE microprocessor, function at 13.56 MHz, 8kbits of memory, open memory architecture, and a passive design requiring no batteries.
   3. Provide credentials made of a composite material for added durability that have a read range of up to 4 inches, support up to a 40 bit format.
   4. Credentials presented to the access control reader at any angle within a minimum distance of one 1-inch shall result in an accurate reading of the card.
2.39 WIRELESS READER INTERFACE

A. Manufacturer and Product:
   1. Scheduled Manufacturer and Product: Schlage WRI400.

B. Requirements:
   1. Provide a wireless reader interface where specified that communicates data via 900MHz back to either a PIM400-485 or PIM400-TD2 which are hardwired to the Access Control Panel (ACP) where all access and specific reporting decisions are made and recorded.
   2. Provide a wireless reader interface compatible with most of the popular Wiegand or Clock and Data format readers.
   3. Wireless reader interface shall include:
      a. Visual LED Indications
         1) WRI400 cover is monitored by a tamper switch
      b. Encryption
         1) Each RF transmission is encrypted with AES-128 bit keys
      c. Reader Interfaces Support
         1) Wiegand (data1/data0) up to 255bits
         2) Magnetic Stripe (clock & data) up to 255bits
      d. Form C Relay Outputs
         1) Strike Relay
         2) Auxiliary Output Relay
      e. Signal Inputs
         1) Request-to-Enter
         2) Request-to-Exit
         3) Door Position Switch
         4) Reader Tamper 1
         5) Reader Tamper 2

2.40 ELECTRIC STRIKES

A. Manufacturers and Products:
   1. Scheduled Manufacturer and Product: Von Duprin 6000 series

B. Requirements:
   1. Provide electric strikes designed for use with type of locks shown at each opening.
   2. Provide electric strikes UL Listed as burglary-resistant.
   3. Where required, provide electric strikes UL Listed for fire doors and frames.
   4. Provide fail-secure type electric strikes, unless specified otherwise.
   5. Coordinate voltage and provide transformers and rectifiers for each strike as required.

2.41 MAGNETIC LOCKS

A. Magnetic Locks - Surface Type: [OPTION – Choose one of the following paragraphs]
1. Manufacturers:
   a. Scheduled Manufacturer and Product: Schlage M490P Series

2. Manufacturers:
   a. Scheduled Manufacturer and Product: Schlage M450P Series

3. Manufacturers:
   a. Scheduled Manufacturer and Product: Schlage M420P Series

4. Requirements:
   a. Provide magnetic locks conforming to ANSI/BHMA A156.23 classification criteria including minimum holding force of 1500 LBF [1000 LBF][500 LBF]. Provide magnetic locks equipped with SPDT Magnetic Bond Sensing device, where specified, to monitor whether sufficient magnetic holding force exists to ensure adequate locking and SPDT Door Status Monitor device, where specified, to monitor whether door is open or closed. Provide bond sensors fully concealed within electromagnet to resist tampering or damage.
   b. Provide fasteners, mounting brackets, and spacer bars required for mounting and details.
   c. Provide power supply recommended and approved by manufacturer of magnetic locks.
   d. Where magnetic locks are scheduled, provide complete assemblies of controls, switches, power supplies, relays, and parts/material recommended and approved by manufacturer of magnetic locks for each individual leaf. Switches control both doors simultaneously at pairs. Locate controls as directed by Architect.
   e. Cylinders: Refer to “KEYING” article, Section 08 71 00.

B. Magnetic Locks - Shear Type:

1. Manufacturers and Products:
   a. Scheduled Manufacturer and Product: Schlage GF3000 DSM/MBS Series

2. Requirements:
   a. Provide shear magnetic locks conforming to ANSI/BHMA A156.23 classification criteria including minimum holding force of 1200 LBF [3000 LBF].
   b. Provide shear magnetic locks equipped with SPDT Magnetic Bond Sensing device to monitor whether sufficient magnetic holding force exists to ensure adequate locking and SPDT Door Status Monitor device to monitor whether door is open or closed. Provide bond sensors fully concealed within electromagnet to resist tampering or damage.
   c. Provide fasteners, mounting brackets, and spacer bars required for mounting and details.
   d. Provide power supply recommended and approved by manufacturer of shear alignment magnetic locks.
   e. Where shear magnetic locks are scheduled, provide complete assemblies of controls, switches, power supplies, relays, and parts/material recommended and approved by manufacturer of shear alignment magnetic locks for each individual leaf. Switches control both doors simultaneously at pairs. Locate controls as directed by Architect.
   f. Cylinders: Refer to “KEYING” article, Section 08 71 00.

C. Magnetic Locks - Movement Exit Delay System:
1. Manufacturers and Products:
   a. Scheduled Manufacturer and Product: Schlage M490DE series

2. Requirements:
   a. Provide movement exit delay systems complete with initiation device, magnetic lock, alarm, authorized reset/momentary release device, logic timer, and alarm output contacts.
   b. Provide movement exit delay system that meets NFPA 101 Life Safety Code governing delayed egress, IBC and/or other local and national fire codes acceptable to authority having jurisdiction as required.
   c. Provide magnetic locks conforming to ANSI/BHMA A156.23 classification criteria including minimum holding force of 1500 LBF.
   d. Provide magnetic locks equipped with SPDT Magnetic Bond Sensing device to monitor whether sufficient magnetic holding force exists to ensure adequate locking and SPDT Door Status Monitor device to monitor whether door is open or closed. Provide bond sensors fully concealed within electromagnet to resist tampering or damage.
   e. Provide tamper proof fasteners, mounting brackets, and spacer bars required for mounting and details.
   f. Provide power supply recommended and approved by manufacturer of delayed egress magnetic locks.
   g. Where exit delay systems are scheduled, provide complete assemblies of controls, switches, power supplies, relays, and parts/material recommended and approved by manufacturer of exit delay system for each individual leaf. Switches control both doors simultaneously at pairs. Locate controls as directed by Architect.
   h. Cylinders: Refer to “KEYING” article, Section 08 71 00.

2.42 POWER SUPPLIES

A. Manufacturers and Products:
   1. Scheduled Manufacturer and Product: Schlage or Von Duprin PS900 series

B. Requirements:
   1. Provide power supplies, recommended and approved by manufacturer of electrified locking component, for operation of electrified locks, electrified exit devices, magnetic locks, electric strikes, and other components requiring power supply.
   2. Provide appropriate quantity of power supplies necessary for proper operation of electrified locking components as recommended by manufacturer of electrified locking components with consideration for each electrified component using power supply, location of power supply, and approved wiring diagrams. Locate power supplies as directed by Architect.
   3. Provide regulated and filtered 24 VDC power supply, and UL class 2 listed.
   4. Options:
      a. Provide power supply, where specified, with internal capability of charging sealed backup batteries 24 VDC, in addition to operating DC load.
      b. Provide sealed batteries for battery back-up at each power supply where specified.
      c. Provide keyed power supply cabinet.
   5. Provide power supply in an enclosure, complete, and requiring 120VAC to fused input.
6. Provide power supply with emergency release terminals, where specified, that allow release of all devices upon activation of fire alarm system complete with fire alarm input for initiating “no delay” exiting mode.

2.43 DOOR POSITION SWITCHES

A. Manufacturers:

1. Scheduled Manufacturer: Schlage 679 Series

B. Requirements:

1. Provide recessed (679 Series) or surface mounted (7766) type door position switches as specified.
2. Coordinate door and frame preparations with door and frame suppliers. If switches are being used with magnetic locking device, provide minimum of 4 inches (102 mm) between switch and magnetic locking device.
SPECIFICATION PARAGRAPHS: PART 3 - EXECUTION

For proper coordination, it is recommend the following paragraphs be included in Part 3 – Execution of your access control specification section (28 10 00).

3.03 INSTALLATION

A. Wiring: Coordinate with Division 26, ELECTRICAL sections for:
   1. Conduit, junction boxes and wire pulls.
   2. Connections to and from power supplies to electrified hardware.
   3. Connections to fire/smoke alarm system and smoke evacuation system.
   4. Connection of wire to door position switches and wire runs to central room or area, as directed by Architect.
   5. Testing and labeling wires with Architect’s opening number.

B. Power Supplies: Locate power supplies as indicated or, if not indicated, above accessible ceilings or in equipment room, or alternate location as directed by Architect.
   1. Configuration: Provide [one power supply for each door opening][least number of power supplies required to adequately serve doors] with electrified door hardware.

3.05 FIELD QUALITY CONTROL

A. Architectural Hardware Consultant: Engage qualified independent Architectural Hardware Consultant to perform inspections and to prepare inspection reports.
   1. Architectural Hardware Consultant will inspect electrified access control door hardware and state in each report whether installed work complies with or deviates from requirements, including whether electrified access control door hardware is properly installed and adjusted.

3.06 ADJUSTING

A. Initial Adjustment: Adjust and check each operating item of electrified access control door hardware to ensure proper operation or function of every unit. Replace units that cannot be adjusted to operate as intended.
   1. Electric Strikes: Adjust horizontal and vertical alignment of keeper to properly engage lock bolt.
COORDINATION WITH DIVISION 08

It is strongly recommended that a meeting with the hardware consultant, security consultant, architect, owner, and other stakeholders takes place to coordinate the requirements of the door hardware section and the access control section of the specifications. This meeting is an integral part of ensuring that all parties are openly communicating and that the design intent is maintained throughout the design and construction process. All door hardware items, whether electronic or mechanical, should be listed in the door hardware groups. If any door hardware items are integrated with the access control system, then the verbiage “Specified under Section 28 10 00, Access Control” should be inserted after the item in the door hardware groups. The article pertaining to that item should then be included in the appropriate Division 28 section.
OPERATIONAL DESCRIPTIONS AND RISER DIAGRAMS

Operational descriptions are required for each opening where electrified hardware is to be applied. These descriptions follow each hardware set in Section 08 71 00. It is important that these operational descriptions are reviewed by the owner, architect, door hardware consultant, and security consultant to ensure they are correct.

Example:

Door normally closed and locked. Authorized access by valid credential, which unlocks outside lever and shunts door position switch. Operation of inside lever shunts door position switch to allow free egress. Free egress always allowed.

Riser diagrams convey information about the location of electrified access control components around a particular door opening. They also convey the approximate path wiring will need to take to connect the components. The number of wires and their gauges is also important to include in these diagrams. These diagrams need to be coordinated and shared with the electrical engineer, low voltage contractor, life safety consultant, door hardware consultant, security consultant, and the architect.

Example:
CONTACT INFORMATION

Allegion is committed to providing the support you need to properly specify and coordinate our access control products. Want to reach us? Here’s how…

Additional resources

Product Information and Learning
- Allegion Website
  www.allegion.com/us
- I Dig Hardware Blog
  www.idighardware.com
- Online Courses
  www.allegion.com/us/onlinecourses
- Application and Installation Videos
  http://us.allegion.com/training/Pages/videos.aspx
- YouTube
  SchlageAD and Schlage Security Channels
- Electronics Mobile App
- Electronic Lock Configurator
  https://elock.allegion.com

News
- Twitter
  www.twitter.com/allegionus
- Integration Insider Newsletter
  us.allegion.com/communities/integrator/resources/Pages/newsletter.aspx

Support
- Online Schlage Electronics Support
  us.allegion.com/irst/service_support
- Technical library
  www.schlage.com/support

Customer Care, Sales and Technical Support
1.877.671.7011