MILLENNIUM

SECURE YOUR WORLD

Electronic Access Control System

Specifications for Architects & Engineers

September 2, 2017

Millennium Group Inc.

16 Tech Circle

Natick, MA 017630

PART 1 - GENERAL

1.01 Summary

A. The section includes an Access Control System (ACS) comprised of a server based software application deployed using Microsoft SQL and Microsoft .NET technology, one of more web or client based interfaces for system configuration, operation, management and reporting, TCP/IP based supervisory controllers, TCP/IP or RS-485 based door controllers, and other associated hardware and software components.

1.02 RELATED SECTIONS

Specifier Notes: Edit the following list as required for the project. List other sections with work directly related to the electronic access control system.

A. 08 00 00 Openings (Division 08)
   1. 08 10 10 Doors and Frames
   2. 08 30 00 Specialty Doors & Frames
      a. 08 31 13 Access Doors & Frames
   3. 08 40 00 Entrances, Storefronts and Curtain Walls
      a. 08 42 00 Entrances

B. 27 00 00 Communications (Division 27)
   1. 27 15 00 Communications Horizontal Cabling
   2. 27 20 00 Data Communications
      a. 27 24 00 Peripheral Data Communications Equipment

C. 28 00 00 Electronic Safety & Security (Division 28)
   1. 28 10 00 Electronic Access Control & Intrusion Detection
      a. 28 13 00 Access Control
         i. 28 13 16 Access Control Systems and Database Management
         ii. 28 13 19 Access Control System Infrastructure
         iii. 28 13 26 Access Control Remote Devices
         iv. 28 13 43 Access Control

1.03 REFERENCES

Specifier Notes: This article does not require compliance with standards, but is merely a listing of those used.

A. IEEE 802.3 Ethernet Standards

B. UL 294 (available) - Standard for Access Control System Units

C. Americans with Disabilities Act (ADA)

D. FCC - Code of Federal Regulations, Title 47, Part 15, Class B

E. Federal Information Processing Standards Publication 197 – Advanced Encryption Standard

F. EMC Directive 89/336/EEC

G. International Organization for Standardization - ISO 8601 Data elements and interchange formats – Information interchange – Representation of dates and times

H. NFPA 70: National Electric Code (NEC)

I. NFPA 101: Life Safety Code

J. NFPA 730: Guide for Premises Security

K. NFPA 731: Standard for the Installation of Electronic Premises Security

L.

1.05 DEFINITIONS USED WITH ON-LINE ELECTRONIC ACCESS CONTROL SYSTEM

A. Access Level: A list of access points and the time zone that users will be allowed access.

B. Access Reader: Provides control of the access point by interfacing a card, electronic key, chip, or keypad with the system.

C. Alarm Monitoring: Provides the system a status of the alarm devices.

D. Distributed Architecture: Describes the operation of the system that allows the system to function with its normal routines without communications to the computers.

E. Door Controller: Provides the system the interface of the reader and alarm inputs along with the relay outputs and communicates the information to the computer.

F. Elevator Controller: Restricts user access to the floors by user access group.

G. Operator Log-On: Computer operator that has been granted access to the system software by a user ID and password.

H. Relay Control: Provides control of devices by time zones or linking events by the software.

I. Controller: Provides the interface of 100 DCD's (Door Control Device) and 10 RCD's (Relay Control Device) with the computer.

J. Site Ethernet Interface: Provides TCP/IP connectivity via an Ethernet network with any number of control units.

K. Time Period: Start and end period along with days of the week that can be used to control user access, automatic unlocking access points, alarms inputs, reports, and relay operations.

L. Cardholder: Holder of a card, biometric, or keypad ID.

1.06 SYSTEM GENERAL DESCRIPTION

A. The Electronic Access Control System (EACS) shall be a secure, modular, extendable system designed to control and manage the movement of building occupants. The EACS shall include a centralized Access Management Server configured, monitored and operated from web browsers and software clients located on a common Building Local Area Network (LAN).

B. The Access Management Server shall be deployed on the Microsoft Windows operating system and capable of being run on a dedicated server or a virtual machine and able to support multiple simultaneous users.

C. The EACS shall include either RS-485 or TCP/IP based communication links between system components. Inputs, outputs and peripheral devices shall be connected to peripheral control devices capable of operating with or without connectivity to the Access Management Server.

1.07 SUBMITTALS

A. Shop Drawings
   a. Prior to assembling or installing the EACS, the contractor shall provide complete shop drawings including the following;
      i. Architectural floor plans indicating all system device locations.
      ii. Wiring schematics for all devices including cable types, lengths, routings and termination requirements.
      iii. Complete block diagram of the EACS.
      iv. Detailed drawings showing mounting and fastening methods for system components
      v. System commissioning requirements and report format

B. Product Data
   a. Prior to assembling or installing the EACS, the contractor shall provide the following details for EACS system components
      i. Manufacturers technical specifications and/or data sheets for all system components and accessories including but not limited to server hardware, supervisory and control .devices, access cards and readers and any other equipment provided as part of the SMS
      ii. Detailed requirements for the Access Control Server including processor speed and count, memory requirements, disk storage capacity and Uninterruptible Power Supply/System Backup requirements.

C. Product Manuals
   a. Upon completion of the system installation, the contractor shall make available print or digital versions of the following manuals.
      i. Hardware manual describing the installation, configuration and operation for hardware deployed as part of the EACS installation.
      ii. Software manual describing the proper configuration and operation of the Access Control Server.
      iii. Maintenance manual describing the proper maintenance and repair of the EACS.

D. Warranty & Software Maintenance Agreements
   a. Upon completion of the system installation, the contractor shall make available the manufacturers product warrant and software maintenance agreement.

1.08 QUALIFICATIONS

A. Manufacturer Qualifications:

1. The manufacturer and supplier of all hardware and software components deployed as part of the EACS shall be reputable, established vendors in the industry for not less than ten (15) years and shall have demonstrated the ability to support projects of a similar size and complexity.

B. Installer Qualifications:
   1. Installers shall have a demonstrated history of successfully installing and servicing Electronic Access Control systems of a similar size, scope and complexity.
   2. Installers shall be capable of providing evidence that they are trained and authorized by the EACS manufacturer.
   3. The installer shall retain sufficient personnel, capacity and spare parts to support the ongoing operation of the EACS or demonstrate that such support can be provided by other local service organizations that have also been trained and authorized by the EACS manufacturer.

1.09 DELIVERY, STORAGE, AND HANDLING

A. Delivery: Deliver materials to site in manufacturer's original, unopened containers and packaging, with labels clearly identifying product name and manufacturer.

B. Storage: Store materials indoors, in a clean, dry area in accordance with manufacturer's instructions.

C. Handling: Protect materials and finishes during handling and installation to prevent damage.

1.10 WARRANTY

A. The EACS shall be provided with a 12 month warranty from the date of system registration and shall include software updates for the duration of the warranty period.

END OF SECTION

PART 2 - PRODUCTS

2.01 MANUFACTURER

The Electronic Access Control System (EACS) shall utilize the Millennium Ultra Access Control Server and the complete system shall include supervisory controller and door control devices compatible with Millennium Ultra and manufactured by the Millennium Group Inc.

2.02 EQUIPMENT

A. The following equipment shall be required as the core elements of the EACS and shall be developed and manufactured by the following supplier:

Millennium Group, Inc.
16 Tech Circle
Natick, MA 01760
Phone: (866) 455-5222
Fax: (508) 651-2902
Web Site: www.mgiaccess.com

B. Software shall be Millennium Ultra Version 2.02 or later

C. Supervisory Controllers shall be Millennium E-Series ESCU Site control units

D. Door Controllers shall be Millennium E-Series EDCD Door Control Devices

E. Power Supplies shall be Millennium PS-1 series power supplies

2.03 SYSTEM DESCRIPTION

A. The EACS shall be an integrated system built upon the Microsoft Software platform including the Microsoft Windows/Server operating system, Microsoft SQL Database and Microsoft .NET software framework. The complete system shall include but not be limited to the Access Control Server, supervisory controllers, door controllers, credential readers, door locking and release hardware, power supplies and sufficient credentials for the size and scale of the system deployed

B. The EACS shall allow or deny door or portal entrance to authorized personnel based upon the specific operational configuration and schedule of the deployment

C. The EACS shall prevent access by unauthorized personnel regardless of credential status for doors or portals managed by the EACS.

D. Operators of the EACS shall be capable of accessing routine functions such as adding new cardholders, removing cardholders, running reports or monitoring system access events, status and alarms from either a web browser interface or a software client installed on a local computer

E. The EACS system shall be expandable and scaleable to support an unlimited number of sites, doors and cardholders and capable of supporting multiple operators.

2.04 ACCESS CONTROL SERVER SOFTWARE – MILLENNIUM ULTRA

A. On-Line Electronic Access Control System: Millennium Ultra.
   1. System shall have capability to perform:
      a. Access control configuration & monitoring
      b. Alarm monitoring.
      c. Programmable relay control.
      d. Real time event viewing
      e. Elevator control.
      f. Database backup and support functions
      g. System configuration and troubleshooting
      h. Extended functionality through optional manufacturer supplied and 3rd party integrations

B. Computer System Characteristics:
   1. An off-the-shelf stand-alone computer or readily available server.
   2. Processor: 2.8 GHz or faster, 64 bit
   3. RAM: 8 GB minimum.
   4. Upgrades: System hardware shall allow computer upgrades without replacement of system hardware.
   5. Communication: TCP/IP
   6. Hard Drive: 120GB for storage of events that have occurred on system.
   7. Printer: Support any Windows installed printer for reports.
   8. Operating System: Windows 7, 8, 8.1, Server, VMWare or MS Hyper-V

C. Software:
   1. Server: 64 bit
   2. Client: application or Web Browser based, have extensive context sensitive on-line help, and provide familiar icon-driven, tabbed dialog menu options. Supports all common browsers including Internet Explorer, Edge, Firefox, Chrome, and Safari.
   3. Client require operator logon to function.

D. Database:
   1. Supplied with full support of Microsoft SQL 2012 –2014 database server application to allow archiving of history, database repair functions, and import/export.
   2. Support near-real-time import and export of data.
   3. Support automatic update of user access rights as a result of the import process.
   4. Allow for a unique industry standard ISO card number to be generated on demand as part of import process.
   5. Provide a tenant feature; allows specific system entities in the database to be seen and manipulated only by certain "Tenant". Such entities can be cardholders, operators, sites and elevator floors. When the database is divided into spheres of control in this way, operators in a given tenant will control data such as sites, doors, cardholders for their own tenant(s) only. The database itself is complete, but views are generated such that what the operator can view, add, modify, delete or print reports, is limited by the Tenant(s) to which they have rights to as well as by Operator level.

E. Operators:

1. Limits system operation by different operator levels.
2. Assign individual operator passwords for logging on.
3. Custom configured operator levels. Operators may have rights to view, add, change, delete, or execute program features.
4. Provide an automatic operator logoff delay.

F. Software Functions and Options:
   1. Software to provide support for the following:
      a. Unlimited number of users.
      b. Each Site Control Unit: 100 access readers, 10 Relay Output boards
      c. Up to 1,000 site controllers.
      d. Number of Tenants: Unlimited.
      e. Number of Access Levels: Unlimited (6 per card).
   2. Support multiple access reader technologies and protocol on same system simultaneously.
   3. Support simultaneously 2 custom ABA formats and 2 Wiegand formats for access readers.
   4. Support combination access readers with one Wiegand output. Support custom Wiegand outputs from 0 to 50bits, including 32 bits, 37 bits, HID Corporate 1000 program, and Motorola 27 bits.
   5. Support Suprema fingerprint readers
   6. Support user pin number along with a card that is enabled by a time period.
   7. Support a door pin number that is enabled by a time period.
   8. Able to accept any facility code of card provided. (0 to 31bit facility code)
   9. Not allow duplication of Employment ID.
   10. Option to rename fields on the cardholder page.
   11. Allow up to three cards to be programmed per cardholder.
   12. Support “disable card” function for each access card.
   13. Support anti-passback modes
   14. Support a door control device address and text description name in a field minimum of 19 characters.
   15. Support 2 relays included with each door control device.
   16. Support unlocking a strike/magnetic lock automatically in accordance with a programmable time period.
   17. Support unlocking a strike/magnetic lock device at a defined time, but only after first valid user accesses access reader.
   18. Notify when status of a door or relay controller changes because of a communication or device problem.
   19. Support programmable reports viewed on monitor or printed.
   20. Provide capability of sorting history events by time, dates, cardholders, access readers, and operators.
   21. Ability to preprogram dates for Daylight Savings Time.
   22. Support relays that can be programmed to operate by a time period, alarms, or by events linked to access points.
   23. Have the Owner’s name encrypted and displayed on monitor.
   24. Capability to automatically archive transaction data and be able to select dates of data being archived.
   25. Provide communication to sites using TCP/IP.
   26. Advise and display on computer monitor status of door and relay controller(s) if communication or power is lost on system.

G. Software Optional Functions

1. Support system lockdown on programmable Threat Levels.
2. Support system lockdown by pre-programming access point (device) groups. Support linking any system alarm point or action with lockdown function.
3. Support system Toggle function allowing first valid card to unlock and hold unlock. The next valid card will lock the door. This function can be set to follow a schedule.
4. Support 3rd party integrations including
    a. March Networks IP based video security solutions
    b. Assa Abloy IN120 based Wireless door solutions
    c. Assa Abloy VINGCard door management solutions
    d. DMP XR Series Intrusion systems

Specifiers note: Supported 3rd part integrations are constantly evolving. Contact the Millennium Group for the latest list of supported integrations

H. Alarm Monitoring Software:
1. Support a minimum of 7 supervised alarm inputs per door control unit with time period disable feature, and a programmable shunt delay timer from 0 to 255 seconds.
2. Supervision of alarm points can be either two (Alarm, Reset) or four states (Alarm, Reset, Open, Shorted) determined at software configuration.
3. Provide a forced-door entry alarm and a door ajar alarm. Forced-door alarm shall have a shunt delay timer of 0 to 255 seconds. Ajar alarm shall have a programmable delay timer of 1 to 255 minutes.
4. Support adding comments to the alarm/events.
5. Support prioritizing of alarms to 100 levels.
6. Support linking specific alarms to relay control devices.
7. Require acknowledgment text so personnel monitoring alarms shall provide response information.
8. Include an alarm monitor application separate which shall display alarms graphically in the priority with which they were programmed. Application shall be able to be run from any Windows based computer. Allow Alarm acknowledgment from any computer with synchronization between operators.
9. Provide alarm monitor with capability to display a user portrait in response to valid or invalid access attempts.

I. Scheduler; integrated software:
1. Fully configurable integrated module allowing scheduled actions for any access points of the system, overriding the normal door unlock/lock set up
2. Unlimited number of schedules supported
3. Configurable actions;
    a. Unlock – Lock
    b. Shunt alarms

J. System Hardware:
1. System components to include Site Controllers, Door Controllers, Power Supplies, optional Relay controllers, optional Elevator Controllers,
2. System shall be able to be configured from 1 to 100 access readers for each site control unit.
3. Controllers shall store basic parameters, including real-time clock, for a minimum of 24 hours, in case of AC loss of power and battery backup is exhausted.
4. System shall use a fully-distributed architecture in which system alarms, access, relays, and elevator control shall continue to function in a normal mode without computer communications.

5. Site controller shall be able to communicate to computer via TCP/IP, either on-board or with an optional interface.
6. Site controller shall have a local relay to monitor status of communications with door control units. In case of device failure relay will open, providing a means of triggering an external monitoring device.
7. Site, door, relay, and elevator controller features shall have capability to be field upgraded by a firmware change. Such firmware upgrades shall be offered as needed to registered users on an exchange basis.
8. Door controller shall support any Wiegand standard based readers in any bit format up to 50 total; bit patterns fully programmable within software.
9. Supported reader types to include but are not limited to: Wiegand, Mag stripe, Bar Code, Proximity, Keypad, Biometrics, combination keypad with Wiegand/Proximity/Magnetic stripe.
10. Door control Unit shall be able to be programmed for custom ABA formats from the software, including ability to ignore user specified characters in format.
11. Door control Unit shall be programmable to accept either normal or inverted strobe signals from ABA format readers.
12. Door control Unit shall be programmed for appropriate access reader technologies.
13. Site controller shall buffer the last 2,000 events from door controllers when computer communications has been lost or terminated.
14. Each door control Unit shall buffer an additional 2,000 events when site controller buffer has filled.
15. All system control Units shall have a built-in tamper alarm to detect when a cover to the controller is removed.
16. Door Control Unit shall include:
    a. Request to Exit input.
    b. Single reader input.
    c. Function at full capacity without communications to computer, and buffer events up to a maximum of 2,000 during this period.
    d. Continue to function on battery backup at a minimum of 9 V DC.
17. Door and relay control Unit shall have Form C dry contact configuration.
18. Door and relay control Unit shall have relays with a minimum current rating of 24 V DC at 2 A with solid-state automatically resettable overcurrent protection for contacts.
19. Door control Unit shall have a relay that can be programmed by software for: Valid User, Auto Activate, First User Auto Activate, Any User, Rejected User, Dual Custody (2 valid token to be presented within 5 sec), or Alarm Options.
20. Relay control Unit shall have relays that can be configured by software for Time Zone Activation, Timed Activation, Timed Released, First Event Activation, and First Event Released and Last Person Out.
21. Relay on door controller shall have a programmable timer and settings in software for strike and magnetic lock operation.
22. Site controller to door control Unit communication shall conform to EIA RS-485 with a recommended total cable length of 5,000 feet (1,524 m).
23. Power Supply:
    a. Battery backup capable of providing power for system during temporary AC power outage.
    b. Provide an output to notify system when there is a loss of AC power.

K. System Access Readers:

1. Wiegand Output Format Readers: Output of 26-bit Wiegand format or a custom bit configuration from 13 to 50 with configurable facility codes
2. Example supported reader types include but are not limited to: Proximity, Mag Stripe, Bar Code, Wiegand, Keypad, Biometrics, combination keypad with Wiegand/Proximity/Magnetic stripe.
3. ABA Format Readers: ABA, ABA inverted.

L. E-Series Door Control Device (EDCD):
1. Description:
    a. Designed to control a single access point.
    b. Contains a real-time clock and sufficient memory to provide access control independent of main PC.
    c. Transaction history shall be automatically buffered when not on line with PC.
    d. Priority event buffer assures alarms are annunciated in a timely manner even if history buffer is full.
2. Power: 9 to 14 V DC, supplied by central power supply; 80 to 110 mA, depending upon reader technology. Accessory relays require additional 20 mA each.
3. Power Protection: Reverse polarity, over voltage, transient.
4. Reader Technologies Supported: Wiegand card (any bit format up to 50), ABA/ISO Track 2, proximity, keypad, combination reader/keypad, biometrics.
5. Reader Interfaces Supported: clock/data, clock/data inverted, Wiegand.
6. History Buffer: 2,000 transactions.
7. Priority Event Buffer: 100 transactions.
8. On-Board Memory and Clock Backup: 24 hours minimum.
9. Maximum Users Stored in Memory: either 10,000 or 60,000, depending on hardware.
10. Alarm Input Points: 7 total, 2-wire supervised, 2 or four state selectable (EOL resistor) including built-in door contact monitoring.
11. Alarm Input Monitoring Circuit: Analog to digital conversion.
12. Tamper Alarm: On-board switch.
13. Output Relays: 2 each with Form C contacts rated 2 A, 30 V.
14. Output Relay Contact Protection: Solid-state polymeric resettable.
15. Connectors: 5 mm plug-on screw terminal.
16. Address Switches: Rotary, direct-reading 00 to 99.
17. Communications: Multi-drop RS-485, proprietary protocol.
18. Operating Environment:
    a. Between 14 degrees F and 104 degrees F (-10 degrees C and 40 degrees C).
    b. Less than 90 percent noncondensing humidity.
19. Support T-TAP, Daisy Chained or in a Star Topology connectivity

M. E-Series Site Control Unit (ESCU):
1. Description:
    a. Designed to control a maximum of 100 door controllers and a maximum of 10 relay controllers.
    b. Normally used for a single site or building, contains a real-time clock and sufficient memory to supervise site.
    c. Maximum of 1,000 site controllers can be addressed in a system.
    d. Transaction history is automatically buffered when not on line with PC.
    e. Priority event buffer assures alarms are annunciated in a timely manner even if history buffer is full.
    f. On-board switches select operational modes.

2. Power: 9 to 14 V DC, supplied by central power supply; 50 mA standby, 90 mA maximum.
3. Power Protection: Reverse polarity, over voltage, transient.
4. PC to SCU Communications Interface: RS-232, RS-485 4-wire, or TCP/IP.
5. SCU to DCD Communications Interface: RS-485 multi-drop 2-wire.
6. Supervisory Relay: Rated 2 A, 30 V Form C. Opens on-site fault.
7. History Buffer: 2,000 transactions.
8. Priority Event Buffer: 100 transactions.
9. On-Board Memory and Clock Backup: 24 hours minimum.
10. Alarms: Lost AC input.
11. Tamper Alarm: On-board switch.
12. Connectors: 5 mm screw terminal.
13. Address Switches: Rotary, direct-reading 000 to 999.
14. Operating Environment:
    a. Between 14 degrees F and 104 degrees F (-10 degrees C and 40 degrees C).
    b. Less than 90 percent noncondensing humidity.
15. Support T-TAP, Daisy Chained or in a Star Topology connectivity

N. Relay Control Device (RCD):
1. Power: 9 to 14 V DC, supplied by central power supply; 35 mA standby current, 20 mA additional for each relay activated.
2. Memory and Clock Backup: 24 hours minimum.
3. Relay Outputs: 7 Form C contacts, rated 30 V DC maximum at 2 A.
4. Supervisory Function: Relay 0 on first board installed. Opens on system fault.
5. Communications: Multi-drop RS-485, proprietary protocol.
6. Tamper Alarm: On-board switch.
7. Configuration Jumpers: J3, relay polarity select all 16 relays; J5, relay override select.
8. Address Switch: Rotary, direct-reading 0 to 9.
9. Operating Environment:
    a. Between 14 degrees F and 104 degrees F (-10 degrees C and 40 degrees C).
    b. Less than 90 percent noncondensing humidity.

O. Power Supply:
1. Power: [120 V AC, 60 Hz, 2 A, unswitched] [240 V AC, 50 Hz, 1 A, unswitched (export)].
2. Fuses: 2 A AC input slow-blow, 1 A AC input (export), 8 A (battery output protection).
3. Output: 13.8 V DC nominal, 5 A maximum.
4. Battery Backup: 2 gelled lead acid cell, 6 V DC, 8.0 Ah, supplied with power supply.
5. Alarm Outputs: Cover tamper switch and AC or power supply failure (dry contacts).

P. Elevator Control Unit (ECU):
1. Description:
    a. Designed to provide access control for a maximum of 16 floors.
    b. Each site controller can support a maximum of 4 Elevator Control Units, giving a maximum of 64 floors per Site Controller.
    c. Each group of elevator control units supports a maximum of 10 elevator readers.
2. Power: [120 V AC, 60 Hz, 1 A, unswitched] [220 V AC, 50 Hz, 1 A, unswitched (export)].
3. Power Supply Output: 5 V DC, 1 A, for local circuit board only.
4. Memory and Clock Backup: 24 hours minimum
5. Relay Outputs: 16 Form C.
6. Contact Ratings: 5 A, 30 V DC; 10 A, 125 V AC; 6 A, 277 V AC.
7. Normal Mode: Energized.

8. Override Input: Normally closed.
9. Unit Address: 4 position dip.
10. Alarm Inputs: 4 unsupervised.
11. Tamper: Built-in switch with activation spring.

Q. Elevator Control Device (ECD):
   1. Description:
      a. Designed to mount inside an elevator car.
      b. Contains reader and communications circuitry to interface with elevator control unit.
      c. Maximum of 10 elevator control devices can be used for each site controller.
   2. Power: 9 to 14 V DC, supplied by power cube (local) or central power supply; 80 to 110 mA depending upon reader technology.
   3. Power Protection: Reverse polarity, over voltage, transient.
   4. Reader Technologies Supported: Wiegand card (any bit format up to 50), ABA/ISO track 2, proximity, keypad, biometrics.
   5. Reader Interfaces Supported: clock/data, clock/data inverted, Wiegand.
   6. Connectors: 5 mm plug-on screw terminal.
   7. Address Switches: Rotary, direct-reading 0 to 9.
   8. Communications: Multi-drop RS-485, proprietary protocol.
   9. Operating Environment:
      a. Between 14 degrees F and 104 degrees F (-10 degrees C and 40 degrees C).
      b. Less than 90 percent noncondensing humidity.

R. Site Ethernet Interface (SEI):
   1. Description: Designed to provide communications between Millennium Windows PC and site control unit(s) by means of Ethernet networks utilizing TCP/IP protocol.
   2. Power: 12 to 15 V DC, supplied by either central power supply or auxiliary power supply; 800 mA maximum.
   3. IP Address Setting: Software through RS-232 port.
   4. Data Backup: Nonvolatile memory.
   5. Network Interface: 10 base T, AUI.
   6. SCU Interface: RS-232-C, 9,600 baud.
   7. Communications Protocol (Network): TCP/IP.
   8. Communications Protocol (SCU Interface): Proprietary.
   9. Operating Environment:
      a. Between 32 degrees F and 104 degrees F (0 degrees C and 40 degrees C).
      b. Less than 90 percent noncondensing humidity.

END OF SECTION

PART 3 EXECUTION

3.01 EXAMINATION

A. Examine areas to receive electronic access control system. Notify Architect if areas are not acceptable. Do not begin installation until unacceptable conditions have been corrected.

3.02 INSTALLATION

A. Install electronic access control system in accordance with manufacturer's instructions.
B. Install system at locations as indicated on the [drawings] [Electronic Access Control System Schedule].
C. Install door hardware as specified in Section 08710.
D. Install electrical wiring to on-line system components as specified in Section 16100.
E. Use manufacturer’s supplied hardware.
F. Replace defective or damaged components as directed by the Architect.
G. Furnish to the Owner all required keys and keycards.

3.03 FIELD QUALITY CONTROL

A. Test completed installation to verify each component of electronic access control system is properly installed and operating.

3.04 ADJUSTING

A. Adjust electronic access control system as required to perform properly.
B. Adjust locksets for smooth operation without binding.

3.05 CLEANING

A. Clean surfaces in accordance with manufacturer's instructions.
B. Use cleaners approved by manufacturer, as some cleaners may damage keylok/keyreaders.
C. Do not use abrasive cleaners.

Specifier Notes: The following is optional. Delete if not required.

3.06 DEMONSTRATION

A. Provide a maximum of 2 consecutive days of on-site service by manufacturer.
    1. Demonstrate system to Owner’s personnel.
    2. Train Owner’s personnel in proper operation and maintenance.