SECTION 28 13 00

DOOR ACCESS CONTROL SYSTEM

PART 1 - GENERAL

1.1 SECTION INCLUDES

A. Contractor shall provide a complete, fully distributed, solid state IP network system consisting of a network controller with web based user interface, network connection cards for device termination, door access card readers, request-to-exit devices, door position switches, door release control station, and all associated wiring.

B. Contractor shall provide a complete door lock release system consisting of intercom door stations, a master door lock release panel, a system central controller, and all associated wiring.

1.2 WORK PROVIDED UNDER OTHER DIVISIONS

A. Power circuits, including 120VAC outlets and wiring, shall be provided under Division 26.

B. Raceway and boxes shall be provided under Division 26.

1.3 RELATED SECTIONS

A. Section 26 05 33 – Raceway and Boxes.

B. Section 26 05 19 - Building Wire and Cable.

C. Section 27 10 00 – Structured Cabling System.

1.4 REFERENCES

A. National Fire Protection Association (NFPA): NFPA 70 - National Electrical Code.

B. Underwriters Laboratories Incorporated (UL):

1.5 REGULATORY REQUIREMENTS

A. Comply with requirements of NFPA 70.

B. Comply with applicable UL Standards.

1.6 SYSTEM DESCRIPTION:

A. Door Access Control System: Full-featured, credential-based access control system that runs on a solid state network appliance and is controlled from a standard web browser. System shall provide for the following features:
   1. Provide for door access through the use of HID proximity cards.
   2. Facilitate door status monitoring through the use of door position switches.
   3. Facilitate door egress through the use of request to exit motion devices.

4. Provision of multiple access cards per person and multiple card formats per system.
5. System software shall provide for the following:
    a. Built-in ODBC-compliant database for personnel data.
    b. Facilitate dual reader and keypad support by time and threat level.
    c. Facilitate decoding of unknown card formats.
    d. Store personnel reports of date and time of last card use.
    e. Support photo ID capability.
    f. Provide activation and expiration date and time to the minute.
    g. Provide user-defined data fields and personnel records.

1.7 SUBMITTALS

A. Submit shop drawings and product data under provisions of Division 1 and Section 26 00 00.

B. Provide wiring diagrams, data sheets, and equipment ratings, layout, dimensions, and finishes.

C. Submit manufacturer's installation instructions under provisions of Division 1 and Section 26 00 00.

D. Submit manufacturer's certificate under provisions of Division 1 and Section 26 00 00 that the system meets or exceeds specified requirements.

1.8 PROJECT RECORD DRAWINGS

A. Submit documents under provisions of Division 1 and Section 26 00 00.

B. Record actual locations and devices, and routing of alarm wiring.

1.9 OPERATING AND MAINTENANCE INSTRUCTIONS

A. Provide written operating and maintenance instructions as specified in Section 26 00 00. Include product data and operation/maintenance information for all system components.

B. The Owner may assign personnel to participate with the Contractor during installation. Without delaying work, familiarize the Owner's personnel with the installation, equipment, and maintenance.

C. During tests and adjustments, permit the Owner's personnel to observe. When feasible, explain the significance of each test.

D. Provide sufficient training to personnel selected by the Owner on operation and basic maintenance of all systems and equipment.

E. Employ manufacturer's field representative to demonstrate system operation to designated Owner personnel.

F. Conduct walking tour of project and briefly describe function, operation, and maintenance of each component.

G. Use submitted operation and maintenance manual as reference during demonstration and training.

H. Provide the owner with a training program designed to make all administrative control station users familiar with the operation of the security system.

1.10 COORDINATION

A. The Contractor shall provide all miscellaneous items and accessories required to make the system operational whether or not such items are specifically mentioned in the plans and specifications. It is the Contractor's responsibility to review the architectural, structural, mechanical, and electrical drawings, as well as the specifications, for any details that may impact the installation or provisioning of the system. Any discrepancies discovered shall be brought to the attention of the engineer and Owner.

1.11 WARRANTY

A. The Contractor shall warranty all electronic components for five (5) years and workmanship and labor for a period of one (1) year from the date of system acceptance or beneficial usage by the Owner. Neither the final payment, nor any provisions in the contract documents shall relieve the Contractor (or General Contractor) of the responsibility for faulty materials and/or workmanship for a period of one year. This Contractor shall remedy any defects due thereto, and pay for any damage to work resulting therefrom.

PART 2 - PRODUCTS

2.1 DOOR ACCESS CONTROL SYSTEM

A. Products specified herein are referenced by *S2 Security Corporation* model numbers. Equal products by other manufacturers will also be accepted, providing the Contractor demonstrates to the Engineer full equivalency of system components and operating characteristics:

B. Operational Architecture:
   1. Network:
      a. The network appliance shall be capable of running on an existing TCP/IP network and shall be accessible, configurable, and manageable from any network connected PC with a browser. Browser access for configuration and administration of the system shall be possible from a PC on the same subnet, through routers and gateways from other subnets, and from the Internet. Control and management of the system shall therefore be geographically independent.
      b. IP video cameras, video storage subsystems, VoIP intercoms, and other network connected storage systems shall be usable by the system via TCP/IP communications over the network.
      c. Security of the data communicated over the network to and from the browser, network controller, and nodes shall be protected by encryption (SSL 128-bit) and authentication (SHA-1).
      d. No separate networking shall be required.
   2. Hardware:

a. At the top of the hardware tiers shall be the Network Controller. Embedded on the network controller are an operating system, a web server, security application software, and the database of personnel and system activity.
b. The middle hardware tier shall be the Network Node. The network node shall make and manage access control decisions with data provided by the network controller, and it shall manage the communication between the network controller and application blades connected to the system's inputs, outputs, and readers.
c. The bottom hardware tier is the Application Blades. Four unique application blades shall be available.
d. An Access Blade shall support two readers, four supervised inputs, and four relay outputs.
e. An Alarm Input Blade shall support eight supervised inputs.
f. A Relay Output Blade shall support eight relay outputs.
g. A Temperature Blade shall support eight analog temperature sensor inputs.
h. This modular design shall make it possible, even during network downtime, for the system to continue to manage access control, and store system activity logs. When network connectivity is reestablished, the system activity logs shall be automatically reintegrated.
i. Each NetDoor MicroNode shall function as a node and as an access control blade. In addition each MicroNode shall support one temperature input.
j. No separate PC client or PC server hardware shall be required.

3. Software:
a. The database tier shall use PostgreSQL. PostgreSQL is a full featured, high performance database management system that supports ODBC. This shall provide a small footprint, low administration, and high reliability relational database that is embedded without requiring the use of a separate PC server.
b. The web server tier shall be based on GoAhead's embedded web server. This shall provide a graphically rich security management application through a standard web browser.
c. The security application software tier shall contain the business logic. This application shall also be embedded on the network device and requires no additional memory or processing power.
d. This three tiered embedded software design shall run within an embedded Linux operating system and shall require no client side software other than a web browser.
e. Only a browser, shall be required for a base system.

C. Functional Capabilities:
1. The System shall integrate in the browser interface the access control, alarm monitoring, camera and video monitoring, intercom, and temperature monitoring applications. The system shall also maintain a database of system activity, personnel access control information, and system user passwords and user role permissions.
2. Access Control Features:
a. Multiple access levels and cards per person.
b. 128-bit card support.
c. Detailed time specifications.
d. Multiple card formats for mixed card populations.
e. Activation/expiration date/time by person with one minute resolution.
f. Access level disable for immediate lockdown.
g. Use of Threat Levels to alter security system behavior globally.

h. Multiple holiday schedules.
i. Timed unlock schedules.
j. Scheduled actions for arming inputs, activating outputs, locking and unlocking portals.
k. Card enrollment reader support.
l. Photo ID creation support.
m. Counted-use access control.
n. Timed anti-passback.
o. Dual reader portal support
p. 26-bit Wiegand keypad PIN support
q. 8-bit burst keypad support
r. Integration with supported alarm panels.
s. First-in unlock rule.
t. Up to 60,000 person records.

3. Alarm Monitoring Features:
   a. User interface securely access under encrypted password control.
   b. Integrated real time IP, DVR, and NVR cameras with stored video replay for events.
   c. A monitoring desktop that integrates video, system activity logs, floor plans, ID photos, and alarm notifications.
   d. Integrated alarm monitoring and event management with alarm panels.
   e. Integrated alarm inputs from the Video Management System.
   f. Alerts delivered to browsers, email, and cell phones.
   g. Graphic floor plans with active icons of security system resources.
   h. System user permissions to grant whole or partial access to system resources, commands, and personal data.
4. Camera and Video Monitoring Features:
   a. Real time video monitoring displays, including multiple cameras simultaneously.
   b. Video switching based on access activity or event activation.
   c. Video Management System integration including digital recording of events.
   d. Support for multiple DVR and NVR systems.
   e. Multiple supported cameras.
   f. Recall of photo ID and real time image for comparison.
   g. Full monitoring through a web browser interface.
   h. System user permissions to grant whole or partial access to system cameras and video resources.
5. Security Database Features:
   a. Record recall by vehicle tag, name, or card.
   b. SQL capability and ODBC compliance.
   c. Optional storage and recall of ID photos and personal/emergency data.
   d. Storage of system user passwords and permissions.
   e. System user permissions to grant whole or partial access to system resources, and personal data.
   f. Pre-defined reports on system configuration, system activity history, and people.
   g. English-based query language for instant custom reports.
   h. Custom Report writer interface that allows the interactive creation of custom reports. Reports may be saved for later reuse. No third party software such as Crystal Reports shall be necessary.
   i. Periodic backup to onboard flash ROM and optional network attached storage (NAS), including FTP servers.

D. System Capacities:

1. The system shall have up to the following capacities for each solid-state network controller:

a.	Network nodes	32
b.	Access control readers:	448 maximum, 140 certified
c.	Access cards:	60,000+
d.	Card formats	32
e.	Alarm input points:	500
f.	Control point outputs:	500
g.	Temperature monitor points:	500
h.	IP, DVR, and NVR cameras:	limited only by license
i.	Intercom stations:	16
j.	Online event history log:	4 to 10 million records (depending upon configuration and transaction types)
k.	Ethernet switch ports:	2
l.	Time specifications	512
m.	Time spec groups	64
n.	Time specs per group	8
o.	Threat Levels	8
p.	Threat Level Groups	32
q.	Holidays	30
r.	Access levels per person	16
s.	Cards per person	100
t.	Report Groups	50
u.	Camera Groups	50
v.	Concurrent system users	10

2. The system shall have up to the following single network node capacities, although all maximums cannot be achieved at the same time:

a.	Application blades:	7
b.	Access control readers:	14
c.	Access levels	512
d.	Portals	14
e.	Portal groups	64
f.	Reader groups	64
g.	Input groups	64
h.	Output groups	64
i.	Elevators	14
j.	Floor groups	32
k.	Alarm input points:	56
l.	Control point relay outputs:	56
m.	Temperature monitor points:	56
n.	Credential storage:	20,000
o.	Event log records:	27,000

2.2 DOOR ACCESS CONTROL SYSTEM EQUIPMENT

A. Network Controller

1. *S2 Security Corporation* S2NC Network Controller (standard)
   a. Provide wall mount enclosure.

B. Network Nodes
   1. *S2 Security Corporation* S2NN Network Node
      a. Provide wall mount enclosure.

C. Proximity Card Reader
   1. Manufacturers:
      a. *ASSA ABLOY* (model 6005B)
      b. Substitutions: Or Approved Equal.
   2. Description: HID Proximity Card Reader with multiple configuration options. The proximity card reader shall be compatible with all standard access control systems, and shall have the capability to read HID cards with formats up to 85 bits. Typical maximum read range shall be up to 1.0".

D. Proximity Access Card
   1. Manufacturers:
      a. *ASSA ABLOY* (model 1386)
      b. Substitutions: Or Approved Equal.
   2. Description: The programmable access card shall include proximity technology and photo identification. It shall support formats up to 85 bits, with over 137 billion codes.

E. Proximity Access Key
   1. Manufacturers:
      a. *ASSA ABLOY* (model 1346)
      b. Substitutions: Or Approved Equal.
   2. Description: The proximity keyfob shall have compatibility with all HID proximity readers and provide an external number for easy identification and control. It shall support formats up to 85 bits, with over 137 billion codes.

F. Motion Sensing Door Release
   1. Manufacturers:
      a. *Dortronics* (model 6612)
      b. Substitutions: Or Approved Equal.
   2. Description: Passive infrared motion sensing door release with adjustable timed relay output.

G. Door Contact Switch
   1. Manufacturers:
      a. *GE Security* (model 1078C)
      b. Substitutions: Or Approved Equal.
   2. Description: Recessed steel door 3/4" diameter contact with wire leads.

2.3 SYSTEM WIRING

A. CAT5e cable shall be as specified in Section 27 10 00.

PART 3 - EXECUTION

3.1 EXAMINATION

A. Verify that field measurements, surfaces, substrates and conditions are as required, and ready to receive Work.

B. Report in writing to Architect prevailing conditions that will adversely affect satisfactory execution of the Work of this Section. Do not proceed with Work until unsatisfactory conditions have been corrected.

C. By beginning Work, Contractor accepts conditions and assumes responsibility for correcting unsuitable conditions encountered at no additional cost.

3.2 INSTALLATION

A. Install system according to applicable codes, and manufacturer's published instructions.

B. Comply with UL Standard 681.

C. Number of Conductors: As recommended by system manufacturer for functions indicated.

D. Splices, Taps, and Terminations: Make splices, taps, and terminations on numbered terminal strips in junction, pull and outlet boxes, terminal cabinets, and equipment enclosures.

E. Identification of Conductors and Cables: Color-code conductors and apply wire and cable marking tape to designate wires and cables so media are identified and coordinated with system wiring diagrams.

F. Install card readers at locations indicated on Drawings and verified by Owner through Project Clerk. Install card readers 48” AFF

G. Grounding: Ground system components and conductor and cable shields to eliminate shock hazard and to minimize ground loops, common mode returns, noise pickup, cross talk, and other impairments.

H. Install exit detectors immediately above door frame. Provide all necessary wiring and connections to make a complete and functioning system, including the electric door locks and door position switches that are furnished by the Door Hardware supplier.

3.3 FIELD QUALITY CONTROL

A. Manufacturer's Field Services: Provide services of factory-authorized service representative to supervise field assembly and connection of components and system pre-testing, testing, adjustment, and programming.

B. Inspection:
   1. Inspect equipment installation, interconnection with system devices, mounting locations, and mounting methods.
   2. Verify that units and controls are properly installed, connected, and labeled and that interconnecting wires and terminals are identified.

C. Pre-testing: Align and adjust system and perform pre-testing of components, wiring, and functions to verify conformance with specified requirements. Correct deficiencies by replacing malfunctioning or damaged items with new items. Retest until satisfactory performance and conditions are achieved.

D. Acceptance Operational Tests:
   1. Perform operational system tests to verify conformance with specifications. Test modes of system operation.
   2. Provide minimum 10 days notice of acceptance test performance schedule to Architect who will coordinate with Owner.

E. Re-testing: Correct deficiencies and retest until total system meets the requirements of Specifications and complies with applicable standards.

END OF SECTION 28 13 00