SECTION 28 05 45

ELECTRONIC ACCESS CONTROL SYSTEM

(Part of the Work for Section 260001)

PART 1 - GENERAL

1.1 GENERAL PROVISIONS

A. Attention is directed to the GENERAL REQUIREMENTS AND COVENANTS - DIVISION I, and the SPECIAL PROVISIONS - DIVISIONS IIA and IIB, which are hereby made a part of this Specification Section.

B. Examine all Drawings and all Sections of the Specifications for requirements and provisions affecting the Work of this Section.

1.2 TRADE CONTRACT REQUIREMENTS

A. Work of this Section is part of the Electrical Trade Contract. Refer to Section 26 00 00 "Electrical Trade Contract Requirements" for additional information about this Trade Contract.

1.3 RELATED DOCUMENTS

A. Drawings and general provisions of the Contract, including General and Supplementary Conditions and Division 01 Specification Sections, apply to this Section.

1.4 SUMMARY

A. The Security Management System (SMS) shall be the key central component for managing physical security. The system shall provide a variety of integrated functions including access control, alarm monitoring, intrusion detection, visitor management and video.

B. Related Sections:

1. Section 08 71 00 Door Hardware
2. Division 21 Fire Suppression
3. Division 26 Electrical
4. Division 27 Communications
5. Division 28 Electronic Safety and Security

1.5 ACTION SUBMITTALS

A. Product Data: For each type of process and factory-fabricated product. Indicate component materials and dimensions and include construction and application details.

B. Field Test Reports:

1. Upon completion and testing of the installed system, test reports shall be submitted in booklet form and electronic media showing field tests performed on, and adjustments made to each component and field tests performed to prove compliance with the specified performance criteria.
2. Indicate and interpret test results in written form and verbally to Engineer for compliance with performance requirements at a pre-scheduled meeting.

C. Battery calculations to show the expected loads and backup duration for power supplies and UPS devices for active AC/ID equipment.

D. Security Subcontractor is responsible to prepare and submit as required to the Authority Having Jurisdiction (AHJ) and information to obtain an Electronic Locking Mechanism

permit.

1.6 SYSTEM COORDINATION

A. The Security Subcontractor shall completely coordinate relevant work of trades/systems including, but not limited to:

1. Door Hardware
2. Fire Alarm System
3. Electrical Systems(s)
4. Telecommunications System(s)

B. Electric Locking Mechanisms

1. The Security Subcontractor and Door Hardware Subcontractor shall coordinate door hardware, door and doorframe design.
2. The Security Subcontractor shall verify specified door hardware is appropriate for the security application and verify the sequence of operations for each access controlled opening.

C. Fire Alarm and Life Safety

1. The Security Subcontractor shall coordinate the (ACS) design with the life safety consultant to ensure compliance with applicable codes and requirements.
2. This includes, but is not limited to:
   a. Fire alarm interface
   b. Fail safe/fail secure locking mechanisms
   c. Delayed egress

D. General Requirements

1. Provide labor, materials, tools, equipment, and services for a complete security system as indicated and in accordance with provisions of the contract documents.
2. Although such work is not specifically indicated, provide supplementary or miscellaneous items, and devices incidental to or necessary for a sound, secure and complete installation.
3. All system devices and components included shall be compatible.
4. Units of the same type of equipment shall be products of a single manufacturer. Material and equipment shall be new and currently in production. Each major component of equipment shall have the manufacturer's model and serial number in a conspicuous place.
5. Provide workstations with the minimum requirements as stated by the manufacturer or the IT department, whichever is greater, based on the design herein and within the Contract Documents.

E. The Electronic Security System (ESS) shall include ACS and IDS sensors in the locations shown on the Contract Drawings. The type, location, quantity and connectivity of these devices for the facility are shown on the Contract Drawings.

F. The ACS and IDS shall be interfaced with the Fire Alarm System (Fire Alarm System by Fire Alarm Subcontractor) as required to comply with building code requirements.

G. The Security Subcontractor shall program the ACS to include graphical maps that present a

dynamic and consolidated view of security applications including:

1. Event Monitoring with Command and Control
    a. View access control (ACS), video, ALPR, intrusion and other events including unlocking doors, controlling cameras and managing alarms.
2. Monitoring and Control
    a. Deploy maps that present a dynamic and consolidated view of security applications
    b. View live or recorded video, ACS events with cardholder pictures, and ALPR hits with license plates
    c. Control cameras and unlock doors
    d. Highlight an area within a map to instantly populate display tiles with associated cameras
3. Embedded Map-Based Alarm Management
    a. When alarms are triggered, operators receive real-time visual cues that instantly draw their attention to the precise location of alarms. Once there, operators can quickly zoom through multiple layers to get a closer and more detailed view with video. Operators respond to alarms, either acknowledging them directly from the map or forwarding them to guarantee a response.
4. Alarm Management
    a. View alarms as they are triggered in real-time directly from your maps
    b. Manage alarms triggered across the facilities, sites, and geographic locations
    c. Receive instant visual notifications the moment alarms are generated
    d. Respond to alarms directly within your maps: acknowledge, forward, or snooze alarms
    e. Asses the validity of alarms on the fly with instant access to correlated video
    f. Centralize map-based alarm management

H. Emergency power will be utilized to power the ACS/IDS system's field panels and control components as required throughout the facility.

I. The ACS supplied by the Security Subcontractor shall support functional integration of subsystems through identified subsystem interfaces as specified herein. This shall include the integration to the Video Management System (VMS) to include video call up and recorded alarm video tagging on the ESS upon 'Door Forced Open' and 'Door Held Open' alarm conditions as well as other programmed event driven events. These may include but not be limited to an invalid access control credential presented at a reader and monitor points which when alarmed, call up video.

J. The ACS shall support point identification from each device, access control transactions, where required, in a distributed processing format and communications interfaces, plus support applicable wiring and cable between devices.

K. Access denial alarms shall be communicated directly to the field control panels. Intrusion alarms on perimeter doors during normal operating hours shall report to the field control panels. alarms, both internal area and point alarms, in addition to card access denials and intrusion

detection points, shall be immediately reported as alarms. Field panels will transmit alarms to the head end immediately.

1.7 GENERAL DESCRIPTION

A. The Security Management System (“SMS”) shall be the key central component for managing physical security access control, video, alarm monitoring, visitor management and selected other functions provided through third party integrations as specified herein.

B. The ACS shall support the following IP-enabled controllers industry standard field hardware platforms:

1. Mercury Security access control product line, controllers and SIO modules

C. The ACS shall be an enterprise class IP-enabled security and safety software solution.

D. Scalability

1. The SMS shall be capable of processing an unlimited number of credential readers, scalable from single site to multiple sites.

E. Database

1. The SMS shall be based upon one or more independent secure SQL database instances, one of which has been designated as the system master.

F. The SMS shall provide a variety of integrated core functions to include:

1. regulation of access and egress

2. provision of identification credentials

3. video management

4. monitoring and managing alarms related to both access control and intrusion

5. visitor management

G. Integrations – The SMS shall employ a RESTful, Web Services API to enable the integration of select third party products and functions with the core functions of the SMS.

H. User Interface

1. The SMS shall provide access to licensed and installed applications through a common browser-based launcher application that can invoke various components and modules of the SMS from a single location, with users able to customize, rearrange, and retain configurations.

a. This launcher shall offer Single Sign On and enable launch of both Windows and browser clients.

I. Communication Security

1. All communication paths within the SMS shall support encryption to provide end-end communication security.

J. User Login and Authentication

1. The SMS shall offer both a native capability to manage system users, as well as the option to authenticate system users through an external Active Directory, LDAP, or OpenID Connect® (OIDC) system. Solutions that do not support OpenID Connection authentication of system users shall not be acceptable. System shall also allow for denial of login after a specified number of failed retries.

2. System shall also log the user out of any browser clients after a specified period of inactivity.

3. Customizable login message and ability to link to external websites or documents.

K. The SMS should provide the ability for control of expiration and complexity for the User Account Passwords internal to the system such that system could comply with existing NIST and NERC guidance.

1. Complexity options to include: Upper/Lower Case, Numeric, Special Characters, Minimum Length, Prohibited List, and Password history

2. Expiration options to include: Number of days as well as administrator enforced update of password.

L. Operational Efficiencies

1. The SMS shall offer a self-service portal for employees to request access and for area owners to approve, hold or deny requested access. This web portal shall also offer administrator-configurable self-service functions for cardholders such as PIN change, setting up a visitor and visit record, and resending a mobile credential to their mobile device.

2. Transactions shall be reportable within the SMS.

3. The SMS shall offer an expedient means to identify access rights provided in violation of corporate policies and to automatically revoke access rights for these violations.

4. The SMS shall offer a browser-based analysis tool that collects system data for comprehensive system health monitoring and displays it on a customizable, intuitive dashboard.

1.8 REFERENCES

A. Abbreviations

1. ACS: Access Control System

2. ADRC: Advanced Dual Reader Controller

3. AES: Advanced Electronic Encryption

4. API: Application Programming Interface

5. DAS: Direct Attached Storage

6. DHCP: Dynamic Host Configuration Protocol

7. DPS: Door Position Sensor

8. DRI: Dual Reader Interface

9. FASC: Federal Agency Smart Credential

10. FASC-N: Federal Agency Smart Credential Number

11. FICAM: Federal Identity, Credential, Access Management

12. FIPS: Federal Information Processing Standard

13. ICM: Input Control Module

14. IP: Internet Protocol

15. ISC: Intelligent System Controller

16. IDRC: Intelligent Dual Reader Controller
17. ISDC: Intelligent Single Door Controller
18. LAN: Local Area Network
19. LDAP: Lightweight Directory Access Protocol
20. NAS: Network Attached Storage
21. NFC: Near Field Communications
22. NVR: Network Video Recorder
23. OCM: Output Control Module
24. ODBC: Open Database Connectivity
25. OPC: OLE for Process Control
26. OSDP: Open Supervised Device Protocol
27. PACS: Physical Access Control System
28. PIV: Personal Identity Verification
29. POE: Power-Over-Ethernet
30. RAM: Random Access Memory
31. REST: Representational State Transfer
32. REX: Request to Exit
33. RFID: Radio Frequency Identification
34. RIM: Reader Interface Module
35. SAN: Storage Area Network
36. SIA: Security Industry Association
37. SMS: Security Management System
38. SQL: Structured Query Language
39. SRI: Single Reader Interface
40. SSL: Secure Sockets Layer
41. TCP: Transport Control Protocol
42. TDE: Transparent Data Encryption
43. TWIC: Transportation Worker Identity Card
44. UPS: Uninterruptible Power Supply
45. VMS: Video Management System

B. Definitions

1. Alarm aggregation: A mechanism of combining several alarms into a single item (group) based on certain criteria.
2. Credential: Data assigned to an entity and used to identify that entity.
3. Designated One Person Control: Requires that a designated cardholder is present before anyone else is allowed to access a certain area.

4. Designated Two Person Control: Requires the presence of two cardholders, designated as special “Team Members”, to restrict individuals from being alone in restricted or highly secure areas as well as restricting the type of personnel allowed in those areas.

5. Devices Global Hard Anti-passback: Once access has been granted via a valid badge presentation, (1) a cardholder cannot present their badge to another entry card reader within the same area without first presenting it to the area's exit card reader, and (2) any attempt to use any card reader in the same area other than exit card reader shall result in access denied and an alarm report.

6. First Card Unlock: Function where a pre-determined time zone activated unlock command is suppressed until a valid credential has been presented and granted access to the portal.

7. Global Soft Anti-passback: As defined in Devices Global Hard Anti-passback with the exception that the cardholder shall be allowed access to a new area for which he is authorized.

8. (Guard) Tour: One or more checkpoints (card readers or alarm inputs) checked during a guard’s predetermined path.

9. Interlock group readers: Configuration for local, but not global, anti-passback whereby only one door may be opened at a time within the area and an alarm is generated for any denied access.

10. Pass-Through: The ability assigned to a person’s credential that allows them to access a door even if in lockdown state.

11. Occupancy Limit: Restricts the number of cardholders that shall be present in an area at any given time.

12. Region: A separate instance of the distributed database.

13. Representational State Transfer (REST): A software architecture style consisting of guidelines and best practices for creating scalable web services.

14. RESTful API’s (Application Programming Interfaces): Term given to Web services using the REST architecture.

15. Runaway detection: A situation when there are more than a specified number of alarms coming from a given device within a specified time interval.

16. Tailgate Control: Triggered when a person receives an access granted, an output will be fired momentarily for a single person or twice for two people, for a maximum duration of one second.

17. Timed Anti-passback: Configurable wait time between an initial badge swipe and the time at which the same badge will be accepted again at the same card reader.

18. Timezones: Time-based periods, encompassing time of day, day of the week and holidays, which are stored on the ISC and control hardware behavior, cardholder access, online mode of the readers, activation of outputs, masking of inputs, and logging events to the database.

19. Two Person Control: Restricts access to certain areas unless two (2) cardholders are present, where the second badge must be presented within a designated time interval of the first to provide access.

C. Reference Standards

1. Underwriters Laboratories

a. UL 294 - Standard for Access Control System Units

b. UL 1076 - Standard for Proprietary Burglar Alarm Units and Systems

c. UL 1981 - Standard for Central-Station Automation Systems

d. UL 1610 - Central Station Automation System Software

2. ISO/IEC 14443-3:2011 – Identification Cards

3. ADA – Americans with Disabilities Act

4. National Fire Protection Association

a. NFPA 70 National Electric Code

b. NFPA 101 – Life Safety Code

c. NFPA 731 - Standard for the Installation of Electronic Premises Security Systems

5. Institute of Electrical and Electronic Engineers

a. IEEE 802.3 Ethernet Standards

6. National Institute of Standards and Technology (NIST)

a. Federal Information Processing Standard Publication 140-2 – Security Requirements for Cryptographic Modules

b. Federal Information Processing Standard Publication 197 – Advanced Encryption Standard

c. Federal Information Processing Standard Publication 201 – Personal Identity Verification

d. SP 800-116 A Recommendation for the Use of PIV Credentials

7. Security Industry Association

a. Open Supervised Device Protocol (OSDP)

8. Video

a. ISO / IEC 10918 – JPEG

b. ISO / IEC 14496 –10, MPEG-4 Part 10 (ITU H.264)

D. Submittals

1. Informational Submittals

a. Product Data

b. Manufacturer product data sheets

c. Manufacturer product instructions, and installation and operating manuals

d. Shop Drawings

i. Complete set of proposed drawings, identifying equipment locations, types of cabling, numbers of conductors, raceway locations, and termination points of each conductor.

ii. Complete listing of proposed devices, indicating interconnection equipment locations and specifying terminal/connecter termination locations.

iii. Operational narrative of each component/system.

2. Closeout Submittals

a. Warranty Documentation:

i. Manufacturer warranty statements for all system components and applicable equipment.

3. Record Documentation:

4. Maintenance Material Submissions:

a. Listing of spare parts required to maintain the system.

5. Closeout Submittals

a. Final listing of doors, locations, and normal status in MS Excel format.

b. Complete set of supplier's operating instructions, installation instructions, and troubleshooting guide, to include but not be limited to instructions for:

c. Schematic drawings depicting type and location of interface equipment/components, 1. number of cables and conductors, raceway locations, types of connectors, circuit requirements and type and dimensions of enclosures.

1.9 QUALITY ASSURANCE

A. Contractor qualifications:

1. Company with a minimum of 2 (two) years system design, engineering supervision, and installation experience in the access control industry.

2. Contractor must be a current, authorized reseller for the SMS product and manufacturer, and provide evidence thereof.

B. Manufacturer Qualifications

1. The SMS Hardware and software manufacturer(s) shall have delivered security management products for at least 10 (ten) years, and shall have a sufficiently large and diverse installed base to ensure competence in delivering, deploying, and supporting systems of this type and scale throughout their expected service life.

C. Units of the same type of equipment will be products of a single manufacturer. Material and equipment will be new and currently in production. Each major component of equipment will have the manufacturer's model and serial number in a conspicuous place.

1.10 PRODUCT DELIVERY, STORAGE, AND HANDLING

A. Acceptance: Upon delivery to the site, Contractor shall inspect all products and materials for any damage.

1.11 PROJECT CONDITIONS

A. Maintain environmental conditions (temperature, humidity, and ventilation) within limits recommended by manufacturer for optimum results.

1.12 MANUFACTURER CAPABILITIES

A. Advanced Services - The SMS Manufacturer shall have an in-house Advanced Services group available to contract for:

1. Professional engineering services to include on-site or remote advanced support, enterprise planning and advanced deployments, system design, supporting software

tools, database migrations and conversions, emergency service, system assessments.

2. Remote Management and Embedded Services to include project management and coordination, contract management, VAR coordination, and Manufacturer resource coordination

3. Custom applications and reports.

B. 3rd Party Product Certification Program

1. The SMS Manufacturer shall have a Partner Program that allows other products to develop interfaces to the Security Platform based on a RESTful Web Services API.

a. Third-party integrations shall have been certified by SMS Manufacturer personnel.

b. Each new revision or version of the third-party system shall be subject to recertification.

2. Interfaces developed shall be tested and certified by the SMS Manufacturer for each new version of product released. The Certification Program shall have integrations which include, as a minimum, Command and Control, Key Management, Fire Detection, Intrusion, Elevator and Critical Communication products, and the capability to integrate with other security and non-security products, as desired by the customer.

C. Global Support Capability

1. The SMS Manufacturer shall have dedicated global support mechanisms in place to provide local support to any installation covered by this specification, regardless of location throughout the world.

2. The SMS Manufacturer shall have multiple independent Value Added Reseller (VAR) options to support customers in each market.

3. The SMS Manufacturer shall have a proven and demonstrable history of deploying Enterprise-scale solutions to Global customers.

1.13 WARRANTY AND SUPPORT

A. Manufacturer shall warrant that the physical media on which the Software is distributed, if applicable, is free from defects in materials and workmanship and that the Software will function in substantial accordance to the Documentation that accompanies the Software for a period of one (1) year from the date of shipment of the Software to the reseller. This limited warranty is void if failure of the Software results from accident, abuse, modification, misapplication, misuse, abnormal use or a virus.

B. Hardware warranties shall be provided by the original manufacturer of the specific hardware device or component.

C. Manufacturer shall offer a supplemental software support program to include software updates and upgrades.

1.14 LICENSE

A. The SMS shall only require a single license key to be present on the database server for the SMS to operate.

1. A license key on the database server shall determine the number of client workstations that shall be able to connect to the SMS and access its functionality.

a. The license key shall either be a physical device or a software license key.

b. License keys shall not be required at the client workstations.

2. The SMS shall allow the SMS user the ability to activate, return, or repair the software license key.

3. The software license shall only be used on a physical computer or in a VMware virtual environment.

1.15 LOCALIZATION (LANGUAGE)

A. The SMS (Security Management System) shall provide language support for interface and database by default or by installation of specific localization packages. Support shall be written using Unicode format and have the capability to support both single-byte and double-byte languages, with the list of languages to available. Localized versions of documentation may be available.

1. Required languages: English

1.16 ARCHITECTURE

A. Open Architecture - The SMS shall support an 'open architecture' allowing for additional support of products outside of the vendor proprietary options.

1. SMS shall support hardware that is non-proprietary such that other vendors could readily offer support for these devices. Access Control Panels that are only supported by a single SMS provider shall not be acceptable.

2. SMS shall support a RESTful Web Services Application Programming Interface (API) that supports the opportunity for 3rd party integration. Access to this API should be managed through a program to ensure that certified integrations utilize this API appropriately.

3. The SMS shall, when possible, leverage open or industry standards for device and system design.

B. System Topology

1. The SMS shall include a central or distributed server component for managing security and any associated integrations.

a. The SMS server shall function as an application server for connectivity of workstation based or browser-based clients for support of configuration and management.

2. An input or output linkage feature shall allow linking of input points to output control points.

3. Tasks shall be accessible from compatible client workstations on the network utilizing any of the following:

a. Traditional client-server architecture, using either Windows clients or browser clients for common day-to-day tasks.

b. Support for federated system architecture (multi-server, multi-database) where the SMS supports the expansion of the system architecture and allows for user deployment based upon their system architectural needs

c. Centralized distribution (publishing) of applications using Windows Terminal Server and Citrix® on Windows, UNIX, Linux or Apple Macintosh based systems through any compatible internet browsers and/or by means of a mobile computing platform or mobile device.

4. Redundancy - The SMS shall support the following means of fault tolerance and SMS redundancy:

a. Hot Standby Servers - A Primary Server shall be the main server that is in use when the SMS is operating under normal conditions, and the SMS shall mirror its database information to a Backup/Secondary Server.

i. Field hardware shall be configured for both the Primary Server and the Backup Server, which shall each recognize the same TCP/IP ISC address on the network.

ii. Upon sensing Primary Server failure, the Backup Server shall automatically initiate itself as the Primary Server and shall begin communication with the Field Hardware.

a) Frequency of check for Primary Server failure: 5 seconds

b) Resynchronization time upon Primary Service restoration: 5 minutes maximum

b. Cluster/Warm Standby - A Primary Server shall be the main server that is in use when the SMS is operating under normal conditions.

i. Field hardware shall be configured for both the Primary Server and the Backup Server, which shall each recognize the same TCP/IP ISC address on the network.

ii. Upon sensing Primary Server failure, the Backup Server shall bring the necessary services online and shall begin communication with the Field hardware.

iii. Shared media devices, either single or dual, shall be employed to house the hard disk used by both servers.

a) Resynchronization time upon Primary Service restoration: 5 minutes maximum

c. Disk Mirroring - This configuration shall allow data to be stored on dual hard disks running simultaneously.

d. RAID Level 10 - The SMS shall offer a Fault Tolerant Redundant Array of Independent Disks Level 10 (RAID Level 10) with a hot standby disk.

i. Redundant components: disk storage, controller channels, high efficiency power supplies

e. Distributed Intelligence - In the event SMS communications is lost or the database server fails, Intelligent System Controllers shall provide complete control, operation and supervision of the system's monitoring and control points.

i. Should the downtime exceed the capacity of the Field Hardware buffer and events are overwritten, an alarm shall appear in the Alarm Monitoring Window notifying the System Operator that events were overwritten.

C. Inter-site Communications

1. The SMS shall support a distributed system (application and database) installation to support geographical or logical separation and management of installations while maintaining a centralized system for reporting.

a. Each distributed system shall support operation of the local clients and hardware, and provide configuration, event, and transactional events to the central system.

b. The SMS shall use a message architecture to transfer necessary incremental credential data from one site to another. This architecture shall provide data queuing, guaranteed delivery, and secure transmission of this data.

D. External Interaction of Data

1. The SMS shall be able to connect to and interface bi-directionally with external data sources utilizing the following methods:

a. ASCII with support for XML formatted text exchange

b. Real-time exchange of data via Active Directory or LDAP

c. Software Application Programming Interface (API)

E. Database - The SMS shall utilize a single supported relational database.

1. Acceptable databases: Microsoft SQL, Oracle

2. Acceptable operating systems: Microsoft Windows Servers or Clients

3. Protection of 'Data at Rest' within the database shall be provided via SQL Transparent data encryption (TDE) and shall be supported to perform real-time I/O encryption and decryption of the database and database log files.

4. The SMS database server shall support an unlimited number of cardholders and visitors limited by the available memory, storage, and processing of the devices. The SMS database server shall support an unlimited number of system events and System Operator transactions in the history file limited only by available hard disk space. The SMS database server shall support an unlimited number of system events and System Operator transactions in the history file limited only by available hard disk space.

5. The SMS shall support bi-directional data interface to external databases in real-time or in a batch mode basis.

a. The SMS shall support a one-step download and distribution process of cardholder and security information from the external database to the SMS database and through the system to Intelligent System Controller (ISC) databases.

b. If a required communication path is broken, the data shall be stored in a temporary queue and shall be automatically downloaded once the communication path is restored.

F. Security

1. Each page in the cardholder record shall be permission protected.

2. Each field in the database shall be permission protected.

3. Communication throughout the SMS shall be AES encrypted, using TLS where practical.

4. All cardholder PIN codes within the system shall be encrypted.

G. A Network Account Management Module shall integrate SMS cardholders with external user network accounts, allowing System Administrators to perform a set of administrative tasks in Windows domains from the System Administration Module, and to create a link between physical access control and logical domains.

H. The SMS shall allow, through standard API toolkits, System Administrators to expose specific SMS data and events that are relevant to IT information or other third-party systems or to allow, System Administrators to accept and process information exposed from the IT

information or other third-party systems.

1.17 CORE FUNCTIONALITY

A. Access Control - access granted or denied decisions, define access levels, and set time zones and holidays. The SMS shall support features such as area control (two-man control, hard, soft, and timed anti-passback), database segmentation, and time zone or holiday overrides

1. Configuration

a. Credentials

i. SMS credential management functionality shall allow:

a) enrollment of cardholders via traditional thick client and/or by a browser-based credential application for the storage of cardholder records in the database

b) formatting of cardholder records

c) capturing of images, biometric data, and signatures

d) user-defined fields in the cardholder record

e) issuance / reissuance of traditional plastic badges and/or mobile credentials using information in the cardholder record. It shall be possible to print to a designated, configured badge printer from both browser-based and Windows clients. This mechanism shall be based on a print server architecture supported by the SMS. Solutions requiring a printer directly connected to the device on which the browser client is used shall not be acceptable.

f) import or export of cardholder data from internal or third-party systems

1. data delimiter: definable

2. import-export filters: selectable

g) assignment and modification of access rights and levels

h) definition of cardholder escort requirements

i) cardholder use limits

j) user definition of extended individual strike and door held open times

k) deactivation of credential following a period of non-use

l) furnishing and management of digital certificates for smart cards

m) searching for records and images based on any fields in the database

ii. Field types: text, date, numeric, drop-down lists

b. Access Levels shall consist of a combination of readers and timezones.

i. Minimum number of supported access levels per controller: 32,000

ii. Minimum number of supported access levels per badge: 255

iii. Card readers shall be assignable to any or all access levels.

iv. Each access levels shall have the option for “First Card Unlock”.

v. Temporary access levels - Within the constraint of number of access levels, the SMS shall have provision for access levels with definable start and end dates.

vi. Precision access levels - Beyond the constraint of number of access levels, the SMS shall be able to assign access levels with unlimited card reader and timezone combinations.

vii. Access Groups - The SMS shall provide for access groups, assignable to an alphanumeric name, containing up to 32 access levels.

viii. Timezones - Pre-defined card reader settings shall have the flexibility to be overridden or modified for locking state and required authentication means.

c. Holidays shall be assignable via an embedded calendar with an alphanumeric name and to individual timezones.

i. Minimum number of holiday assignments: 255

ii. Number of holiday group types: 8

iii. Repeat frequency: annual

iv. Daylight Savings Time: definable for automatic time conversion

v. Span: configurable for multiple days

d. Timezones

i. The SMS shall be capable of creating timezones, each with intervals assignable to any day of the week.

a) number of timezones: 255 minimum

b) Intervals: 6 minimum

ii. Timezones shall be allowed to belong to any or all access levels so that the time zone only has to be defined once.

e. Scheduling - The SMS shall have a scheduling utility to allow System Administrators to schedule actions to occur on a one-time or a recurring basis and to maintain a log of actions executed.

f. Field Hardware

i. The SMS shall allow for a Windows-based configuration of the following types of field devices which participate in the access control function:

a) Intelligent System Controllers (ISC’s)

b) Input Control Modules (ICM’s)

c) Output Control Modules (OCM’s)

d) Access card readers

e) Integrated lock-readers

ii. The SMS shall provide a device discovery utility to aid in

configuration.

a) Scope: local subnet or multiple subnets

b) Display categories: brand, discovery service, device status, device type

c) Available functions: ping, reboot, default password check, version discovery, launch device web server, save credentials, update IP address

iii. When a field hardware device is configured, the device shall appear in a graphical system overview tree and be available in drop down lists which support operator access.

iv. The SMS shall have the ability for bulk add, modify, and delete privileges for ISCs and card readers to allow for the ease of addition and maintenance of themes.

v. The System Administrator shall have the ability to group field devices into monitor zones.

vi. System status update frequency shall be configurable.

g. Alarm Masking Groups - System Administrators shall be able to create groups of alarm inputs that enable them to mask or unmask multiple Input Control Module inputs and card reader inputs simultaneously.

i. Alarm Masking Groups shall be able to be masked or modified as a group or as individual points.

ii. Alarm masking shall support two-man control.

iii. Number of Alarm Masking Groups: maximum 64 per ISC

iv. Alarm inputs: maximum 128 per Alarm Masking Group

h. Event Linkage - The SMS shall support a global linkage feature whereby any input or output or event shall be linked to any other input or output or event., with the following additional characteristics:

i. support global I/O function lists, consisting of sequences of up to six actions

ii. association with panel areas

i. Graphical Maps - The SMS shall support graphical maps that display device or group status, function lists and video cameras dynamically in real-time, and support the following:

i. graphical maps are available via traditional thick client and/or through a browser-based monitoring application

ii. configuration to appear on command or when specified alarms are acknowledged

iii. graphical map creation software that allows the import of map backgrounds from supported file formats

iv. associate various maps with each area to provide for the creation of a map hierarchy

v. user-defined text and icons

vi. configuration of map icon shape and color to represent the state of

the associated device

vii. pan and zoom capability is supported for Maps when viewing through the browser-based client

2. Badging - SMS badging functionality shall allow for the creation of different badge types based on a database field, the linking of that field to a badge type to automate the process of credential production, and the use of security colors, chromakey, and ghosting, to allow quick identification of personnel access authority.

a. The SMS shall have the ability to create and maintain badge designs, with tools and support for image import and export, ghosting, signature capture, bar code, and smart card chips.

i. Image formats: all standard industry image formats

ii. Support image processing and effects with a pre-defined effects gallery.

iii. A badge layout and creation module shall support custom badge designs by the User.

iv. Additional badging related functionality shall include the following:

v. assignment of access levels and access groups, including bulk assignment, modification or deletion of access levels

vi. custom badge layout

vii. mobile and remote badging

viii. printing: print limits, batch printing

ix. magnetic stripe encoding using any of three tracks

x. support for all industry standard bar code formats

b. Credential images shall be digitized using industry standard JPEG image compression and printed using a high quality and direct card printing process.

c. The System Operator shall have the following functions available when enrolling cardholders: choose a badge type, select access levels, enter personal identification numbers (PIN), and/or any other user-defined fields.

d. A badge form shall keep a complete history of every badge that was assigned to the cardholder's record to include cardholder badge ID, issue code, badge type, badge status, activation and deactivation dates and times, PIN numbers, embossed numbers, and anti-passback information.

3. Ingress and Egress

a. Individual Use

i. Access Cards

a) Card types supported:

1. Proximity - 30 mil thickness, ISO compliant

2. smart cards - contact and contactless

a) MIFARE - 1 kB (8 kb) and 4 kB (32 kb)

b) DESfire

c) HID iCLASS

d) U.S. Government FIPS 201 and HSPD-12 compliant, including TWIC

3. PIV standard formats

4. Mobile Credentials to be installed and used from a smart phone

b) Data formats supported:

1. Magnetic stripe - with card number, facility code, and issue code combinations up to nine-digit card number and two-digit issue code

2. Wiegand - all industry standard variations

3. HID Corporate 1000 - 32 bit and 48 bit

4. 200 bit BCD FASC-N output of FASC-N readers

5. 75-bit Wiegand Binary output of GSA approved FASC-N readers

6. Custom

c) The SMS shall support the provisioning and usage of Mobile Credentials.

1. Mobile Credentialing shall be configurable from the SMS to include:

a) Name for the credential service

b) URL for issuing credentials

c) Requirements for certificate-based authentication and/or username password to access web portal

d) Supported mobile credentials:

1. LenelS2 - BlueDiamond

2. HID Mobile Access on Origo

e) The SMS shall support desktop smart encoding and inline smart encoding for relevant affected reader technologies.

f) The SMS shall support a card reader cipher mode, emulating the presentation of a card credential by manually entering their badge ID.

g) The SMS shall support a configurable denied access attempts counter for each card reader.

h) Extended Held-Open Time - Authorized cardholders shall have the ability on demand to extend the time for which a door is help open after access is granted for up to 30 minutes.

i) An alarm shall be generated upon an attempt to use any badge that is not marked active in the SMS.

ii. Biometrics shall provide multi-factor (or alternate) identification through the measurement and comparison of human characteristics including fingerprints, hand geometry, iris imaging, and facial features. The SMS shall have the capability to verify the identity of enrolled individuals using products from approved manufacturer partners.

a) Capture of biometric data (template) shall be accomplished via the biometric device or associated reader.

b) Cardholder biometric data (template) storage means: smart card; in access controller; in the biometric partner database.

iii. Request to Exit (REX) - The SMS shall be able to provide an event when a REX is initiated.

iv. The SMS provides the ability to alert the System Operator when a cardholder does not present their credential at a required location in a designated period of time.

v. Pre-Alarm - The SMS shall support a card reader pre-alarm feature which sounds a tone prior to a door held open alarm for a configurable period.

a) The SMS shall allow operator response instructions to be specified for each type of alarm and delivered via text and/or audio.

b. Area Control - The SMS shall implement area control implementing functionality affecting more than one person, and have the following elements:

i. Global and Local Hard Anti-passback

ii. Global and local Soft Anti-passback

iii. Timed Anti-passback

iv. Two Person Control

v. Designated One Person Control

vi. Designated Two Person Control

vii. Tailgate Control

viii. Occupancy Limit

ix. Interlock group readers

c. Mustering - The SMS shall provide a mustering function to automatic register cardholders that are on site during an incident.

i. Muster Mode shall mean that an incident has occurred and an evacuation is required of one or more a Hazardous Locations.

a) Triggers

1. automatic: occurrence of a designated hardware event

2. manual: by System Operator

b) Reset: manual by System Operator or Automatic based on Global I/O

d. Hazardous Location (s) shall be defined using entry and exit readers associated with the location.

i. One or more safe locations shall be designated for each a Hazardous Location.

ii. Entry and exit card readers shall be provisioned at each portal with the requirement that a badge always be used to enter or exit Hazardous and Safe Locations.

e. Muster Alarm and Reporting

i. When a Hazardous Location is in Muster Mode, all associated Alarm Monitoring Workstations shall be notified with a breakthrough notification and Muster Reporting shall be active.

ii. Live Muster Report

a) display the last location of each cardholder based on card swipe.

b) activation:

1. immediately upon entering into Muster Mode

2. after a specified time period from Muster Mode activation

3. after the number of personnel in the Hazardous Location reaches a given count.

c) configurable for automatic refresh time and automatic end

f. Muster Status Reporting: individual cardholders in Hazardous Location

g. Live Hazardous Location and Safe Location Reports: cardholder listing and record selection

h. Operator Display

i. Hazardous Locations and Safe Locations shall be placed on graphical maps' System Hardware Status Tree as Area Icons with associated head counts.

4. Guard Tour

a. A tour shall consist of a series of checkpoints that shall include card readers and/or alarm inputs.

b. Each tour shall be assigned to one or more alarm monitoring Workstations indicating from where automatic tours are to be launched.

c. Tour checkpoints shall be assigned minimum and maximum times within which to be reached.

d. The SMS shall handle both scheduled and random tours.

e. Scheduled tours shall have an Alarm Monitoring Window pre-departure notification.

f. Tours will have the option of being linked to live video.

g. Guard tours shall capable of being monitored through a tracking window including tour details and status.

h. The SMS shall support aggregation of tours into tour groups.

5. Elevator Destination Dispatch

a. SMS shall support network/data level integration to elevator destination dispatch systems

b. Access control information shall be shared with the elevator destination dispatch system as needed to facilitate the access control decision

6. Direct Wired Elevator Control - The SMS shall provide elevator control using standard access control field hardware that will permit the restriction of cardholder access to certain floors while also allowing general access to other floors, with the following additional functions:

a. Allow, at the elevator, the use of any card reader and card reader modes used on any other card reader in the SMS

b. Track which floor was selected by an individual cardholder for auditing and reporting purposes

c. Provide an option where the floors of a building are able to be configured into logically divided sections (floor groups) to prevent passenger requests between designated sections.

7. Field Devices

a. Interface

i. The SMS shall be equipped with the access control field hardware required to receive alarms and administer access granted or denied decisions.

ii. The SMS shall be capable of interfacing with the following field devices:

a) Devices without Lenel Part Numbers

1. Intelligent System Controllers (ISC)

2. Intelligent Single Door Controller (ISDC)

3. Intelligent Dual Reader Controller (IDRC)

4. Advanced Dual Reader Controller (ADRC)

5. Input Control Module (ICM)

6. Output Control Module (OCM)

7. Single Reader Interface Module (SRI)

8. Dual Reader Interface Module (DRI)

9. Reader Interface Module (RIM)

10. Access Control Network Door Controllers or Network Controller/Readers

11. Power over Ethernet Plus (PoE+) Enabled Dual Door Interface

12. Network Adapters

13. Communication Star Multiplexer

14. RS-485 Interface Module
15. Network ready power supplies and enclosures
    a) On-demand and scheduled testing of system standby battery sets
    b) Reports and alert notifications to the SMS and the database
    c) UL Listed prewired system enclosures with LenelS2 connectors
    d) Compatibility with enclosure wire duct systems for wire protection and integrity
    e) Modularity of system power components for expansion and configuration
    f) A minimum MTBF of 80,000 hours for reliability
16. Dual Reader Interface (DRI)
17. Intelligent, wireless, and combination locks

b) Devices with Lenel Part Numbers

1. Intelligent System Controllers (ISC)
    a) LNL-X3300
2. Intelligent Single Door Controller (ISDC)
    a) LNL-X2210
3. Intelligent Dual Reader Controller (IDRC)
    a) LNL-X2220
4. Advanced Dual Reader Controller (ADRC)
    a) LNL-X4420
5. Input Control Module (ICM)
    a) LNL-1100-S3
6. Output Control Module (OCM)
    a) LNL-1200-S3
7. Single Reader Interface Module (SRI)
    a) LNL-1300-S3
8. Dual Reader Interface Module (DRI)
    a) LNL-1320-S3
9. Power over Ethernet Plus (PoE+) Enabled Dual Door Interface
    a) LNL-1324e
10. Communication Star Multiplexer
    a) LNL-8000

11. Network ready power supplies and enclosures shall provide:
(reference Appendix E)

a) On-demand and scheduled testing of system standby battery sets

b) Provide reporting of battery life “out of tolerance”

c) Reports and alert notifications to the SMS and the database

d) UL Listed prewired system enclosures with Lenel connectors

e) Compatibility with enclosure wire duct systems for wire protection and integrity

f) UL Listed modularity of system power components for expansion and configuration

g) A minimum published MTBF of 80,000 hours for established reliability

12. Intelligent, wireless, and combination locks

c) Migration boards

d) The SMS must be able to retrieve device serial numbers from field hardware, excluding card readers, biometric readers, and keypads.

b. Data download

i. The SMS shall provide for the downloading of data to the ISCs. Downloads shall load SMS information (timezones, access levels, alarm configurations, etc.) into the ISC’s first, followed by cardholder information and card reader configurations.

ii. Information on cardholder status, badge status, timezones or access levels shall download in real time as they are added, modified, or deleted from the SMS.

c. Permission control - The SMS shall allow System Administrators to set permission control for individual devices within a monitoring zone for command override.

d. Device grouping - The SMS shall support device grouping for uniform command and control of groups of devices within the system.

e. Card readers

i. Options to include:

a) User commands

b) Door strike, REX and DPS functionality

c) Duress actions

d) Alarm masking

e) Logging requirements

f) Selection as “In” or “Out” reader

g) Use limits

ii. The SMS shall provide connectivity to, proximity/mobile ready, Smart Card and smart card/mobile ready readers which provide continuous supervision and monitoring of reader processor and wiring integrity by means of a non-proprietary communications protocol standard.

iii. The SMS shall support encrypted reader to panel communications using the SIA OSDP Secure Channel protocol.

a) OSDP File Transfer capabilities shall be supported

b) Flexible support for OSDP manufacturer specific commands shall be provided. It shall be possible to send commands based on a schedule or manually.

f. Input Control Modules (ICM’s) options to include:

i. Alarm masking

ii. Local linkage of inputs and outputs

iii. Output activation rules

iv. Input configuration for Guard Tour

v. Entry (latched, not latched) and Exit delay modes

g. Intelligent System Controller (ISC) capabilities shall include:

i. Administrator functions to group, add, modify or delete ISC’s in the system

ii. Ability to update firmware or replace hardware while maintaining complete hardware and data configuration settings

iii. A distributed intelligence redundancy mode, whereby the ISC, configured with a UPS battery to maintain the unit for 24 hours, participates with other ISC's to provide complete control, operation and supervision of the system’s monitoring and control points in the event of SMS server failure.

a) cardholder capacity: configurable up to 1,000,000

b) event capacity: configurable up to 50,000

h. A system Operator shall have the option to manually control the output points or input points connected to the SMS.

i. The SMS shall support a real-time graphical system status tree or list window that graphically depicts configured field hardware devices.

8. Distributed Access Level Management

a. The SMS shall provide a browser-based interface for the assignment of access rights to individuals or groups of cardholders, using a simple user-interface paradigm suitable to general employee use, and not requiring specialized training on the SMS

b. The SMS administrator shall have the ability to designate for which areas a manager has assignment rights. These rights shall then be reflected in the browser interface accessible by the area manager, such that only areas for which they have authority are available for assignment.

c. The browser-based tool for access rights assignment by area managers shall have the ability to search for cardholders and to view cardholder details, constrained by the permissions of the manager

B. Alarm Monitoring - The SMS will provide the ability to monitor system and device Alarms/Events, Field Hardware Command and Control and Status Monitoring and system support functions, for the use of the operators of the system.

1. The SMS shall provide monitoring options through workstations installed or browser-based clients.

2. An Alarm Monitoring window shall provide System Operators information about the time, location, and priority of an alarm and provide the ability to sort pending and new alarms based on event detail.

a. Detail shall include at a minimum: Date/Time, Description, Priority, Controller, Device, and person.

3. Alternate alarm view windows shall be available to support: Alarm or Badge Activity Monitoring, Event Tracing (Live/Historical), and Alarms Pending Response

a. Operators shall be able to acknowledge alarms from any alarm view window.

4. Monitor support shall include the ability to view live and recorded surveillance video and link video to alarm events.

5. Monitor support shall include options for comparison of the in-person cardholder to their stored image either in person or via live video. Cardholder Verification and Video Verification.

6. The SMS shall allow a System Operator to:

a. monitor alarms in their assigned monitor zone and to perform field device control actions on specified devices in that zone from either thick client, web client or mobile client platform

b. delete the alarm from the alarm monitoring window without acknowledging the alarm

c. enter and edit an Acknowledgement note detailing the cause of specified alarms and the actions taken

d. activate, deactivate, or pulse outputs configured and associated with a card reader

e. mask or unmask each individual card reader door forced open alarms, door held open alarms, and associated auxiliary alarm inputs

f. display a cardholder record with the stored cardholder’s image

g. verify that a person using a credential matches their stored photo

h. open multiple cardholder verification windows to cover multiple readers at the same time

i. initiate several traces of cardholders, assets, and/or field hardware devices while monitoring alarms

j. initiate an historical trace for a device, specifying a date and time range

k. filter alarms from the trace window to include access granted, access denied, system, duress, and area control alarms and by alarm source

l. perform a trace on any ISC, ICM, Alarm Input, Credential, Intrusion Detection

Device, Monitor Zone, or card reader

m. manually override card readers, alarm points, and relay outputs

n. combine, enable, or disable alarms for aggregation

o. acknowledge or delete a group of aggregated alarms

p. view runaway devices

7. System Administrators capabilities shall include:

a. set permission control for individual devices within a monitoring zone for command override

b. assign default monitor zones to monitoring workstations

c. option to define monitor zones to include sub devices of an ISC

d. configure how the SMS handles the annunciation of alarms on an individual alarm or event basis

e. set display parameters for unacknowledged alarms

8. Notifications - Upon alarm, the SMS shall allow for:

a. automated sending of texts or e-mail messages

b. forwarding alarms to another location

9. Annunciation - The System Administrator shall have the ability to configure how the SMS handles the annunciation of alarms on an individual basis.

a. These attributes and actions shall be assignable on a ‘global’ basis to all devices that share an alarm description.

10. System Administrators shall be able to route and re-route device alarms and events to defined monitoring client workstations on the network, regardless of where the alarm is generated in the field.

11. A real-time graphical system status tree on the screen shall indicate the status of devices to reflect secured, unsecured, in alarm, or offline and provide command and control functions for authorized users.

12. Output control operations shall be available to lock, unlock or pulse control points.

13. An automatic cardholder call-up feature shall allow the quick search and display of images in the database.

14. Logging

a. All alarms and events in the SMS shall, by default, always be recorded in the database.

i. System Administrators shall have the ability to select on a time zone basis, the times required for the SMS to log specific events to the database.

ii. System Administrators shall have the option for Alarm or Events to be set to log or not to log particular alarms or events by individual reader or input.

b. A System Operator journal shall be available to log important daily events.

15. A trace function shall be available for System Operators to locate and track activity on specific cardholders, assets, video cameras, or card readers. An image

comparison feature must be provided for use in conjunction with a CCTV interface.

16. The SMS shall support a Test Mode for Alarm Inputs, Door Forced Open, and Access Grants to verify that all inputs within the group are operational.

C. Intrusion Detection

1. The intrusion detection function shall employ keypad used in conjunction with a card reader, both supplied from the Manufacturer.

2. The Alarm Monitoring interface shall be able to control the intrusion detection function.

3. Intrusion zone point types:

   a. 24-hour point

   b. Interior point

   c. Perimeter point

4. Arming options:

   a. Exit delay

   b. Entry delay

   c. Forced

5. Actions under User command:

   a. Disarmed

   b. Disarmed Fault

   c. Armed Away

   d. Armed Stay

   e. Armed Instant

   f. Forced Armed Away

   g. Force Armed Stay

   h. Force Armed Instant

   i. Entry Delay

   j. Exit Delay

   k. Alarm

   l. After Alarm

   m. Chime

   n. Silence

6. System Administrators shall have the ability to define Alarm Mask Groups for sets of points to be treated as an intrusion area.

   a. Indication of events from these points shall be masked (disarmed) or unmasked (armed).

7. The SMS shall support Intrusion Mask Groups to contain individually configured intrusion points and to have the capability reporting of arming mode and state for the group.

a. Within the configuration of the Intrusion Mask Group, the initial power up state of the Intrusion Mask Group shall be definable as one of the following states:

i. Disarmed

ii. Armed Away

iii. Armed Stay

iv. Armed Stay Instant

8. Alarms shall be reported for the intrusion mask group by the SMS based on the current arming mode and state of the intrusion mask group.

D. Visitor Management System

1. The SMS shall have an integral Visitor Management traditional client or browser-based client to provide the following functionality:

a. Allow an operator to enroll, schedule, assign to an employee, capture photos, capture signature, assign access levels, sign in or out, and track visitors as they move throughout the facilities

b. Support for enrollment at a desktop computer, portable computer, or mobile device

c. Support for bulk visitor import from CSV or spreadsheet files.

d. An invitation email shall be automatically transmitted to the visitor without additional operator intervention. Invitation shall include:

i. Visit details including date, time, host and location

ii. PDF417 barcode instantly readable by the visitor check-in system

iii. Ability to include invitation in Apple Wallet

a) A wallet card for the invitation

b) Date, time and location information shall be provided to allow for user notification

e. Provide visitor data and image capture / import capability as well as image edits using pre-defined effects, Chroma key (background transparency) and aspect ratio settings

f. Allow for re-assignable badges and sticker badges

g. Provision visitor credentials and maintain visitor data, including credentials and visit history, in the SMS database to minimize re-entry of data.

h. Search for visitor records and images using any fields in the database relevant to them.

i. Assign visitors to existing valid cardholders with email notification

j. Pre-schedule visits/events

k. Visitor sign-in and sign-out at a desktop computer, portable computer, or a tablet

2. The system shall support the use of a browser-based self-service portal to create a Visit Event that will include the visitor(s) record creation or modification.

a. Any cardholder with permissions shall be able to create a visit using a self-

service portal to self-enroll visitors and create/manage events.

b. The Host application shall allow any Cardholder with appropriate permissions to use their Directory Account to log in and create the Event/Visit record to include:

i. Visitor Name, email, phone and other personal information

ii. Purpose

iii. Sign-in location

3. The Visitor Management System shall provide a visit status user interface to include:

a. in-progress visits, including overstayed visits

b. pending visits, including late visitors

c. completed visits

4. Self-Service app

a. The Visitor Management System shall have a self-service iPad-based visitor app which allows visitors to:

i. sign themselves into or out of events without assistance from a front desk attendant

ii. sign in/sign out a pre-registered visit or a “walk-up” visit

iii. update personal information (including photo capture)

iv. view and complete pre-recorded video content during the sign-in process (example: safety or security procedures or guidelines)

v. sign or accept up to seven documents (example: non-disclosure agreements)

vi. print an adhesive-backed paper badge with latest photo and other pertinent information via supported printer devices

b. Allow for customizations related to end-user branding (logos or colors) to facilitate inclusion in the environment

c. Upon Sign In and Sign Out, an email, which can include a captured image of the visitor, shall be sent to notify host and security personnel of a signed in or signed out visitor.

d. Administration of the self-service app shall allow for custom configurations of:

i. App Theme Color, Logos, and custom messages to be defined by customer

ii. Required documents (up to 5) such as a Non-Disclosure Agreement (NDA) or Privacy Agreement and associated acceptance and signature requirements.

a) Such documents shall be available records stored in the database.

b) Records stored shall be stamped with visitor name, time of visit and contact information

c) An Administrator shall set the renewal period for updating a photo, required signed or completed documentation based

on Visit Type

iii. The administrator may also save a VSS image or “Pre-Set” of a configured VSS iPad and store it into the SMS database.

a) When new Check-In locations are created, the user may download the image or Preset that is stored in the SMS database

e. Visitor self-service application must be a native iOS application that automatically launches on iPad startup, and cannot be terminated or exited by the visitor.

E. Third Party Application Programming Interface (API)

1. Software Integrations

a. Software integrations shall be based upon a RESTful Web Services API.

b. Access control integrations shall provide for the following functionality:

i. Full Alarm Management - Send and Receive and Acknowledge alarms

ii. Full identity/card management (add/modify/delete) identities, cards, visitors, access permissions, etc.

iii. Main command and control operations including - Set Reader modes

iv. Add/modify/delete of operator/user permissions of the system

v. Access to device and other security system configuration (e.g. panels, readers, segments, badge types, etc.)

vi. API support for the same functions as used by manufacturer’s browser clients, such that it is possible to implement the same features and functions as the manufacturer, but in custom applications or integrations.

2. Hardware Integrations

a. Hardware integration shall be based upon native API plug-ins that allow for 3rd parties to map their hardware into the access system to extend the supported device set including but not limited to, Fire, Intrusion, Intercom, Video, Cameras, Readers, etc.

b. Integration shall provide full support for alarms, hardware status, and command and control for integrating third-party devices into the alarm monitoring software

c. Video integration shall allow for both third-party video to be integrated into the SMS as well as SMS video to be accessed by a third-party

F. Video

1. Integrated Video Management System (VMS)

a. An integral VMS shall provide video response options upon alarm events to include:

i. auto-launch

ii. change camera resolution and/or frame rate

iii. activation and positioning of PTZ camera

iv. event monitoring

v. display of alarm location on multimedia graphical maps

vi. event investigation

vii. automatic archive of event video for selected alarm types

viii. instant replay of up to 5 (five) minutes of video must be provided

ix. to protect privacy, role-based restrictions shall be provided on the ability of an operator to search recorded video beyond a specified age

b. Windows Client capabilities:

i. export of security evidence clips in industry standard formats

ii. switching between live and recorded video

iii. 2-way audio support

iv. search recorded video by specific badge or alarm point

v. operation using same user SMS authenticated credentials

vi. shall provide instant rewind capability

c. Browser video viewing capabilities:

i. browser clients shall not require additional software or plug-in installation

ii. view live and recorded video

iii. automatic display of event linked video in a 2x2 matrix format, including playback controls and event handling

iv. calendar-based recorded video search

v. operation using same user SMS authenticated credentials

vi. ability to organize multiple camera tiles into multiple layouts for convenient monitoring, such as 2 x 2, 3 x 3, 1 + 5, 1 + 8

vii. control for PTZ cameras and client presets

viii. step-through recorded video in forward or reverse, with speed control

ix. display interactive hardware tree with device status

x. support for monitor zones and user permissions

xi. digital pan and zoom

xii. audio support

xiii. snapshot capture and save

xiv. video clip export

2. Integrated Network Video Recorder

a. Supported resolutions: QVGA (320 x 240) to 20 Megapixel (5472x3648)

b. Recording modes: continuous, time-lapse, event-driven, synchronized audio and video

c. Storage options: Direct Attached Storage (DAS), Network Attached Storage (NAS), and Storage Area Networks (SAN).

1.18 EXTENDED CAPABILITIES - The SMS shall allow for the inclusion of additional capabilities.

A. Advanced Unified Client

1. The SMS shall support an advanced unified client (AUC) application for the purpose of monitoring access control events and activity, digital video, and data from third party sources.

2. The AUC shall allow for customizable layouts of up to 400 cells.

a. Each cell can be populated with content, including the following content types:

i. Video streams

ii. Automatic display and management of video related to alarms, including multiple video sources per alarm. Video replay controls shall be available.

iii. Access control activity

iv. Cardholder activity with images

v. Static images [.jpg and .png]

vi. Video clips [MP4 and MOV]

vii. Date and time

viii. Weather

ix. Traffic

x. Information from private and public RSS feeds

xi. Twitter® feeds

xii. Internet TV

xiii. Web content

xiv. Text

xv. Maps

xvi. Content with door and camera objects overlayed, allowing status and door control

3. The AUC shall support the Windows® and macOS® operating systems.

4. The AUC shall support multiple monitors.

5. The AUC shall allow management of SMS events, including:

a. Display of linked cardholders and video recordings

b. Operator instructions

c. Acknowledgements

d. Marking in progress

e. Adding notes

f. Clearing completed events from the display

6. The AUC shall allow for display of recent activity of a cardholder linked to an access control transaction.

7. The AUC shall provide the ability to search for cardholder records in the SMS system, and to view, edit, and add cardholder records, based on the user's permissions on these systems.

8. The AUC shall support the ability to play backward, forward, pause, or capture a snapshot directly from the live video stream in an AUC cell.

9. The AUC shall allow for display of recorded video linked to access control transactions.

10. The AUC shall support forensic video searching and video exporting, video search by date and time, or by access control event (alarm).

11. The AUC shall support exporting video from one or more cameras. The video export shall support MOV and MPEG-4 file formats.

12. The AUC shall allow for display of access control and video information from the following sources:

    a. Supported SMS's

        i. LenelS2 OnGuard® version 7.5 or later

    b. Supported VMS's with event linking

        i. LenelS2 Network Video Recorder (LNVR) version 7.5 or later

        ii. Milestone® XProtect® Systems Professional+ (2020-R2), Expert (2020-R2), and Corporate (2020-R2)

    c. Supported VMS's without SMS event linking

        i. LenelS2 NetVR™ version 1.7 or later

        ii. Lenels2 VRx™ version 5.0 or later

        iii. Avigilon® ACC5 and ACC6

        iv. exacqVision® version 7.0 or later

        v. VideoInsight 7.9.0.503

B. Conversions and Migrations - Manufacturer shall offer the capability to migrate systems from the following manufacturers (equipment)

1. Mercury®

2. Honeywell®

3. GE Security® / Infographics® ACU

4. GE Security® / CASI® - M Series

5. Johnson Controls® - Tyco® (Software House®)

C. U.S. Federal Government

1. The SMS shall be compliant with US Federal Government Personal Identity Verification Authentication Standards for readers and credentials as defined in FIPS 201-2 to include the following criteria:

    a. The solution proposed must be listed on the FICAM (Federal Identity, Credential, Access Management) Approved Products List.

b. The solution proposed must support certificate authentication of the FIPS-201 credentials at each entry, through a connection from the SMS components to the Federal Bridge. Systems that rely on an additional hardware component whose primary function is solely the validation of credentials shall not be acceptable.

c. Cryptographic portion of the SMS approved through the NIST FIPS 140-2 cryptographic validation program.

D. Policy Compliance and Enforcement tool

1. The SMS shall have a browser-based analysis tool to ensure that the SMS is correctly configured to enforce corporate security policies.

2. A SMS policy manager shall be an application with the following capabilities:

a. Incorporate a flexible policy editor that allows the administrator to define complex security policies without having experience programming the SMS.

b. Allows or disallows exemptions on a per-policy basis.

c. Facilitates automatic or manual correction of policy violations.

d. Incorporates auditing and reporting capabilities to meet compliance in regulated industries.

e. Processes multiple violations simultaneously with bulk operations.

E. Web Access and Trending for Comprehensive Health Monitoring (WATCH)

1. The SMS shall provide a self-monitoring tool for SMS system application, database, and communications servers.

a. The monitoring tool shall constantly measure key performance indicators (KPI's) of the system servers, and provide a browser-based portal for viewing, analyzing, and understanding system operations.

b. An overview screen of SMS server operation shall be available, as shall individual screens for each server.

c. Monitoring shall default to a current-time view, with an option to specify a time window to understand system performance and metrics during the specified time window.

d. The SMS shall allow thresholds to be set for key performance indicators and for other system measurements and monitors, and for email notifications to be automatically generated when thresholds exceed or fall below configurable limits.

e. The SMS shall push relevant system health data to a cloud-based remote health monitoring site, providing automated notifications.

F. Cardholder Self Service browser-based portal

1. The SMS shall allow cardholders to log into a browser-based interface to self-execute common tasks, including:

a. Enrolling visitors and scheduling visits in the SMS visitor management system

b. Requesting access either from a list of allowed access levels and readers, or from a log of doors where access was attempted but denied.

c. Changing their cardholder PIN number for the SMS

d. Requesting a re-send of the cardholder's mobile credential

2. The Cardholder Self-Service tool shall generate email to notify approvers when access has been requested, and cardholders shall be notified automatically of the disposition of an access request.

3. It shall be possible for the system administrator to enable or disable each of the self-service capabilities listed above.

G. Console for Launching Common Functions

1. The SMS shall include a launcher application that can be used from a web browser and launch various components and modules of the SMS from a common location.

a. The launcher application shall operate on a variety of platforms, including but not limited to Windows, Mac, and IOS, and shall feature a responsive user interface that adapts to the resolution, screen size, and aspect ratio of the device from which it is launched.

b. When invoked from a Windows-based computer, the launcher application shall support both Windows applications and browser-based applications.

c. Common applications shall be prepopulated in the launcher, but it shall be possible to integrate other browser-based applications by URL, to allow additional security application to be easily accessed by the operator.

d. It shall be possible to rearrange the applications in the launcher on a particular device, and have that arrangement remembered automatically for future sessions.

e. The launcher shall manage the login of system users, such that logging in to the launcher authenticates the logged in user for other system functions during that session.

f. The launcher shall display available OnGuard clients, browser clients, and user selected reports and dashboards

H. Smartphone-based Mobile Credential Support

1. The SMS user screens shall include the ability to issue, modify and revoke smartphone-based mobile credentials. Solutions requiring "dual-enrollment" of mobile credentials in a cloud or web app as well as the SMS are not acceptable.

2. The SMS shall use a cloud-based mobile credential issuance and management mechanism to allow for shared mobile credential accounts, use of various or mixed mobile credential ecosystems, and updates to mobile credential support without updating the installed SMS software.

3. The system shall have the ability to create a custom email template that will be sent to the cardholder.

4. Email shall include link to download the mobile credential application, instructions to install and configure the mobile app, and a one-time password to authenticate the mobile application to the credential server.

5. A System Administrator with appropriate user permissions shall have the ability to create a friendly name for each mobile reader, to be displayed in the mobile app.

I. Third Party Integrations

1. The SMS shall support multiple certified integrated third-party interfaces with hardware and software vendors to include the following functional areas:

a. Command and control

b. Communications

c. Elevator

d. Fire alarm

e. Identity and access management

f. Intercom

g. Intrusion detection and alarm

h. IP video cameras

i. Key management

j. License plate recognition

k. Monitoring and dispatching

l. RFID

m. Readers

n. Recording appliances

o. Sensor inputs

p. Time and attendance

q. Video analytics

r. Video management systems

2. The SMS shall provide a set of standard RESTful Web Services Application Programming Interfaces (API's) and supporting documentation that allows hardware manufacturers and software application developers to interface their products into the SMS.

3. Third party interfaces shall be integrated to provide a single graphical user interface, single source code base, and a single database for configuration, alarm, and event storage.

a. The SMS shall allow alarms and events from the third-party systems to report into the same main Alarm Monitoring window as access control alarms.

b. Third-party hardware alarms and events shall be stored in the SMS database for audit trail and reporting purposes.

4. Data available through these interfaces shall be organized for optimum performance with one application accessing a single bank of data.

5. Any changes to system hardware shall be instantly available across the entire SMS.

J. The SMS shall support OPC, BACnet and SNMP protocols.

1. An industry standard OPC Server utility shall allow the export of SMS alarms and events to industry standard OPC Clients.

1.19 COMMUNICATIONS

A. The SMS shall communicate with the ISCs via TCP/IP through IPv4 or IPv6 protocols. The network connection shall be configurable to be initiated either by the system to the controller in the field, or from the controller in the field to system.

1. In the case where all field deployed devices are with private network boundaries, the preferred connection is from the system to controller.

2. In the case where field deployed controllers are outside the private network, and use the public internet for connection, then controllers should initiate connection to the system.

3. The system shall be capable of supporting both communications methods within the same overall system.

B. Download communication between the SMS and the ISC shall be fully multi-tasking and shall not interfere with operational functions.

C. Upon loss of communications between the SMS Server and an ISC, an alarm shall be created with a time stamp.

1. Upon re-established communication, the SMS and the ISC shall automatically re-synchronize from the point of communication loss without operator intervention.

2. The SMS shall support Dual Path communications between the SMS Server and the ISC's to allow for a fully functional redundant communication path.

a. During a fail over period, the ISC shall periodically check to see if the primary path has been re-established and will automatically switch back upon a successful connection.

b. Alarms shall be generated upon loss or restoration of communications.

D. Encryption - The SMS shall provide encrypted communication capabilities as follows:

1. Credentials to Reader: DESFire EV1 or EV2, or HID iCLASS or SEOS

2. Reader to Downstream Panels: OSDP Secure Channel Encryption

3. Downstream Panels to ISC: AES-128 bit or AES-256 bit

4. Data on ISC: AES-256 bit Encryption of Data at Rest

5. ISC to SMS Server: AES-128 bit or TLS1.2 with AES-256 bit

6. SMS Server to Client: HTTPS

7. Client to Printers and Badge Encoders: Encrypted encoder communications

1.20 SYSTEM MANAGEMENT

A. System Configuration - The SMS shall provide system icons and/or menu selections for each function requiring configuration of SMS options or peripherals including client workstations, field hardware, network functions, communications, and reports.

1. A set-up assistant utility shall be available for the initial system configuration prior to first log in.

2. The SMS shall support configuration setup wizards to guide System Administrators through the configuration of the access control module of the system.

B. In addition to capabilities previously mentioned herein, System Administration capability shall include the following:

1. Customize cardholder, asset, and visitor forms.

2. Import customized map backgrounds and custom icons.

3. Bulk delete cardholder records.

4. Limit System Operator functions and actions, including searching the database.

5. Configure client workstation applications and settings.

6. Assign System Operator passwords, log on credentials and permissions and provide operator history.

C. The SMS shall provide support for single sign-on capability, whereby System Administrators or System Operators may authenticate into SMS applications using their Windows domain account.

D. System Administrative tasks including defining client workstation and Operator permissions, access groups, time zones, reports, and maps shall be available from any client workstation on the network.

E. Graphical Features

1. The SMS shall display a graphical representation of configured field hardware (including ISCs, fire panels, intrusion detection devices, personal safety devices, intercom systems, and Central Station alarm receivers), digital video hardware, access levels, time zones, access groups, holidays, and card formats.

2. System Administrators shall be able to modify a device that is depicted on the graphical system overview tree or see its properties by double-clicking on the related icon, causing the SMS to bring them to the appropriate form.

F. The SMS shall provide context-sensitive help files to guide System Administrators and System Operators in configuration and operation.

G. Logging - The SMS shall provide full System Operator activity tracking/logging of critical keyboard functions to include date/time, Operator, activity program, function, and database changes.

1. System Operator functions to log shall include System Operator login and System Operator logout; Additions, Changes, and Deletions to Cardholder Management; New Badge, Print Badge, and Update Badge.

2. Configuration changes to log shall include all functional modules within the SMS.

3. The SMS shall log activity of System Operators performing SMS alarm monitoring including alarms acknowledged, alarms cleared, output control activity, trace, and other functions.

H. Reporting - The SMS shall provide rich reporting of system data.

1. an industry standard, off the shelf, custom report writer, allowing the creation of custom reports.

2. Capability shall be provided to view, export, schedule, email, print and modify reports through a web browser, including the ability to add user-defined fields to a report.

3. Reports are stored on the SMS and are able to be viewed from client workstations or web browsers with proper permissions and network access.

4. The SMS shall allow reports to be generated manually or based on system events or user-defined schedules.

I. Archiving - The SMS shall allow System Administrators to archive offline history files. Offline files shall include access events and System Operator transactions that have been purged from the reportable database.

1.21 HARDWARE REQUIREMENTS

A. The Manufacturer shall publish a summary of recommended server hardware to accommodate the performance requirements of the SMS server software.

B. The SMS server software shall be capable of running in a virtual or cloud environment.

1.22 DELIVERY, STORAGE, AND HANDLING

A. Deliver materials in manufacturer's labeled packages. Store and handle in accordance with manufacturer's requirements, in a facility with environmental conditions within recommended limits.

1.23 PROJECT CONDITIONS

A. Inspect locations where installation work will be performed and verify that conditions found are in accordance with the Contract Drawings and are acceptable for installation work. Report discrepancies in writing to the Engineer requesting clarification.

B. Maintain environmental conditions (temperature, humidity, and ventilation) within limits recommended by manufacturer for optimum results. Do not install products under environmental conditions outside manufacturer's absolute limits.

PART 2 - PRODUCTS

2.1 ACCEPTABLE MANUFACTURERS

A. Manufacturer

1. LenelS2

2. No Substitutions Allowed

B. Security Management Software

1. OnGuard

2. No Substitutions Allowed

C. Software Version

1. Enterprise

2. No Substitutions Allowed

PART 3 - EXECUTION

3.1 Installers

A. Contractor installation personnel shall be trained and certified by the SMS manufacturer and have a valid, current certification at the time of installation.

B. Contractor installation personnel shall comply with all applicable state and local licensing requirements.

3.2 Preparation

A. The network design and configuration shall be verified for compatibility and performance with the SMS.

B. The network configuration shall be tested and qualified by the Contractor prior to system installation.

C. Server performance parameters shall be compared with Manufacturer requirements for the SMS.

3.3 Installation

A. Contractor shall follow manufacturer published installation and configuration instructions and guidelines.

B. System shall be configured in accordance with manufacturer-supplied hardening guide. SMS systems for which the manufacturer does not provide a hardened installation option shall not be acceptable.

C. Systems installed in a cloud environment shall be configured in accordance with manufacturer-supplied guidelines outlined in a cloud deployment guide. SMS systems for which the manufacturer does not provide a cloud deployment option shall not be acceptable.

3.4 Storage

A. Server and system hardware devices and components shall be stored in an environment where temperature and humidity are in the range specified by the Manufacturer.

END OF SECTION