Keri Systems is one of the world's largest independent suppliers of access control and integrated security systems. Systems can be scaled to meet requirements of all types, from simple systems for just a few doors to systems with mid-sized, large, and even enterprise requirements, with integrated video, photo badging, biometric, graphic maps, telephone entry, and many other powerful features.

For additional information, contact:

Keri Systems, Incorporated
302 Enzo Drive
Suite 190
San Jose, CA 95138
Phone: +1 408-435-8400
+1 800-260-5265
Fax: +1 408-577-1792
Web: www.kerisys.com
E-mail: sales@kerisys.com

ACCESS CONTROL SOFTWARE

DIVISION 28 - ELECTRONIC SAFETY AND SECURITY

28 10 00 Electronic Access Control and Intrusion Detection

28 13 00 Access Control

28 13 16 Access Control Systems and Database Management

Notes to Specifier:

1. Where several alternative parameters or specifications exist, or where, the specifier has the option of inserting text, such choices are presented in **<bold text>.**

2. Explanatory notes and comments are presented in **colored** text.

ACCESS CONTROL SYSTEM

PART 1 GENERAL

1.01 SUMMARY

A. Section includes an access control system (“ACS”), consisting of a software application, designed in Microsoft's.NET platform and utilizing the Microsoft SQL database engine; the server supporting such application, and all associated field hardware over a TCP/IP-based network.

B. Related Requirements
   1. 08 00 00 Openings (Division 08)
      a. 08 10 10 Doors and Frames
      b. 08 30 00 Specialty Doors and Frames
         1) 08 31 13 Access Doors and Frames
            a) 08 31 13.53 Security Access Doors and Frames
      c. 08 40 00 Entrances, Storefronts, and Curtain Walls
         1) 08 42 00 Entrances
   2. 27 00 00 Communications (Division 27)
      a. 27 15 00 Communications Horizontal Cabling
      b. 27 20 00 Data Communications
         1) 27 24 00 Peripheral Data Communications Equipment
   3. 28 00 00 Electronic Safety and Security (Division 28)
      a. 28 10 00 Electronic Access Control and Intrusion Detection
         1) 28 13 00 Access Control
            a) 28 13 16 Access Control Systems and Database Management
            b) 28 13 19 Access Control Systems Infrastructure
            c) 28 13 26 Access Control Remote Devices
            d) 28 13 43 Access Control Identification Management Systems
      b. 28 23 00 Video Surveillance

1.02 REFERENCES

A. Abbreviations
   1. ADA - Americans with Disabilities Act
   2. AES – Advanced Encryption Standard
   3. AHJ - Authority Having Jurisdiction
   4. APB – Anti Passback
   5. API – Application Programming Interface
   6. DHCP – Dynamic Host Configuration Protocol
   7. EOL - End of Line (resistance)
   8. EVR - Event Video Recorder

9. GMT – Greenwich Mean Time
10. GUI - Graphic User Interface
11. HTML – Hypertext Markup Language
12. IP – Internet Protocol
13. LED - Light Emitting Diode
14. LCD - Liquid Crystal Display
15. LDAP – Lightweight Directory Access Protocol
16. MSDE - Microsoft Database Engine
17. MSQL - Microsoft SQL Server Database Engine
18. NVR - Network Video Recorder
19. ODBC – Open Database Connectivity
20. PDF - Portable Document Format
21. PIN – Personal Identification Number
22. REX – Request to Exit
23. RTF - Rich Text Format
24. SQL – Structured Query Language
25. SMS – Short Message Service
26. TCP - Transmission Control Protocol
27. TIFF - Tagged Image File Format

B. Definitions

1. Anti-Passback - an access control security measure that prevents a cardholder from passing his or her access card to an individual behind them, and allowing them to gain access into a secured zone.
    a. Hard Anti-Passback - requires that the user be "in" the correct anti-passback area when presenting the card for authorization. An incorrect area will be denied access, and an Access Denied - Anti-Passback Violation event will be generated and the system will not allow the cardholder access through the reader. Once this happens, the card will be denied on all other readers with this selection, regardless of area.
    b. Soft Anti-Passback - allows the user access (if the access level for the cardholder is valid) regardless of the current cardholder Anti-Passback area. If the card is presented out of sequence, an Access Granted - Anti-Passback Violation event will be generated and the system will allow the cardholder access through the reader. However, once the cardholder opens the door, the cardholder is now "in" the destination area.
    c. Timed Anti-Passback, Last Valid User - uses just one reader to control an area. Since there is no reader leaving the area, a time limit is selected for anti-passback rules to be applied. This means that the card cannot be used at the reader for the specified time interval after the initial access grant or until the reader has been used by another valid user.
    d. Timed Anti-Passback, Per User - uses just one reader to control an area. Since there is no reader leaving the area, a time limit is selected for anti-passback rules to be applied. This means that the card cannot be used at the reader for the specified time interval after the initial access grant and is on a per user basis. The last valid access at each reader is tracked for each cardholder.

e. Timed Hard Anti-Passback, Soft Anti-Passback - a combination of different anti-passback modes. For the time limit specified, the reader operates in Hard Anti-Passback mode for each cardholder. At the end of the time limit, the reader operates in Soft Anti-Passback mode for each cardholder. This allows for the strictest anti-passback rules to be applied for a specific time, and then the more relaxed rules apply. This mode typically provides the best combination of security and management when applying anti-passback rules

2. Autolock: A mechanism which, when activated, shall cause the pulse time of the corresponding relay and the shunt time for the door-position input to reset when the door closes, overriding the programmed relay pulse time and input point shunt time and re-securing the door.
3. Gateway: Software service that manages communication between the Application Server/PC and the field hardware

C. Reference Standards
1. IEEE 802.3 Ethernet Standards
2. UL 294 (available) - Standard for Access Control System Units
3. Americans with Disabilities Act (ADA)
4. FCC - Code of Federal Regulations, Title 47, Part 15, Class B
5. Federal Information Processing Standards Publication 197 – Advanced Encryption Standard (AES)
6. EMC Directive 89/336/EEC
7. European CE
8. Australian C-Tick
9. Electromagnetic Compatibility Requirements Product Standard EN 55011: 1991
10. International Organization for Standardization - ISO 8601 Data elements and interchange formats – Information interchange – Representation of dates and times
11. ONVIF

1.03 SUBMITTALS

A. Informational Submittals
1. Product Data - Manufacturer’s printed or electronic data sheets
2. Manufacturer’s instructions

B. Closeout Submittals
1. Warranty documentation
2. Manufacturer’s installation, configuration and operation manuals
3. As-built wiring diagrams and system drawings
4. Recommended spare parts list
5. Complete system test reports

1.04 QUALIFICATIONS

A. Installers shall be trained by the Manufacturer to install, configure and commission the access control system.

1.05 LICENSING

A. The ACS software shall be licensed without the use of hardware dongles.

B. The ACS software shall support a minimum of 256 concurrent connected client licenses.

C. The ACS software shall not require more than 1 SQL client license to operate in order to provide up to 16 operator clients.

1.06 WARRANTY

A. Software Support -

B. Manufacturer shall provide a limited "no questions asked" warranty for hardware products to be free of defects in material and workmanship, as follows:

1. Two years – Controller; I/O Expansion Boards; Reader Interface Modules
2. Lifetime - Clam shell card; key ring tag; mullion, Euro, and wall switch readers
3. 1 year on photo imageable cards

END OF SECTION

PART 2 PRODUCTS

2.01 EQUIPMENT

A. Manufacturer: Keri Systems, Incorporated
302 Enzo Drive
Suite 190
San Jose, CA 95138
Phone: +1 408-435-8400
+1 800-260-5265
Fax: +1 408-577-1792
Web: www.kerisys.com
E-mail: sales@kerisys.com

B. Model(s)
1. Software: Doors.NET
2. Hardware
a. NXT Hardware Platform
1) NXT-2D-MSC, NXT-4D-MSC Controllers
2) PXL-500 Controller
3) NXT-4X4, NXT-GIOX I/O Expansion Modules

C. Alternates: Open Platform Authentic Mercury Security Corporation Hardware

2.02 GENERAL DESCRIPTION

A. The access control system (“ACS”) shall be a complete system, consisting of the following
1. Access control software application
2. Server to host the application software
3. Door controllers
4. Input devices to include <card readers> <keypads> <biometric readers>
5. Access cards and tags
6. Request to Exit (REX) Devices and door contact switches

B. The ACS shall provide access validation and prevent unauthorized access at designated facility portals.

C. The ACS shall provide alarm/alert notification of access breaches at designated facility portals and other monitored points.

D. The ACS shall be capable of integrating the security functions for access control, alarm management, photo identification card production, data management, graphics mapping, roll call, muster station, and video.
1. The graphics Mapping user interface shall include integration with digital video.

E. The ACS shall provide a complete and detailed context sensitive help file.
1. The help file shall include:

a. software installation and configuration and all hardware information
b. a documented API (Application Programming Interface) for interface to the ACS

F. The ACS shall be of true multi-user design and capable of simultaneous operations from multiple client interfaces.
1. A user logged onto any one client interface shall not affect the system control by users logged onto other client interfaces.
2. Changes made to the system shall be updated in real-time to other users of the system.

G. Network
1. The ACS software shall enable secure, encrypted connections from remote locations over the Internet without the use of a Web Browser or VPN connections.
2. Protocols
a. Transport layer: TCP
b. Network layer: IP
c. Data Link layer: Ethernet, IEEE 802.3
d. Addressing
1) Gateways and clients: DHCP
2) Controllers: Static – automatically assigned by ACS software

2.03 ACCESS CONTROL SOFTWARE

A. The ACS software shall enable communication and information exchange with microprocessor-equipped controller hardware and peripherals with distributed databases.

B. The ACS software shall be based upon
1. Microsoft's .NET development framework
2. Microsoft SQL database engine
a. Version: Microsoft SQL Server 2005/2008/2008R2 or 2012 or the equivalent SQL Express versions
b. All interaction with the SQL database from the ACS must be performed using stored procedures for increased efficiency and speed.
c. The ACS shall support LDAP and Microsoft Active Directory.

C. Applications
1. The .NET framework shall consist of modular applications including
a. Primary Application Server (the actual access control software program)
b. Hardware Gateway for communication between field hardware and software
c. Standard Operator/User Interface Client
d. Report Client
e. Photo Identification Client
f. Event Video Recorder

g. Global Linkage and Automation service

h. Graphics Mapping Client

2. The ACS shall support the ability to accommodate the Application Server, SQL database, Hardware Gateways and all associated Clients on the same PC or distribute them to separate PCs.

D. Application Server Component

1. The Application Server shall be the only ACS component that communicates with the SQL database.

a. Client PCs shall not have the ability to communicate with the SQL database directly.

2. The Application Server shall be able to communicate with all supported hardware Gateways simultaneously.

3. System Capacities

a. Doors: 65,536

b. Four state supervised inputs: 254,976

c. Relay outputs: 254,464

d. Cardholders: 750,000

4. The software shall have the capability to automatically discover and configure in its database all controllers, expansion boards, interface boards, and readers attached to the system, as well as having the capability to configure them manually.

5. Schedule support – The ACS software shall have the ability to configure schedules as follows:

a. Time schedules per Controller: 255

1) Interval characteristics:

a) Start/stop intervals per schedule: 12

b) Day of week selection

c) Holiday types: 8

b. Holidays: 255

1) Holiday types - Each holiday shall support a type designation and a start date plus the number of days for the holiday to be enforced.

2) Holidays shall have the ability to be configured to extend into the following week, month, or year as desired 8

3) Holidays per type: 32

E. Program Compatibility

1. The ACS software shall provide a multitasking-type environment that allows other Windows compatible programs to run on Client and Server computers concurrently without interrupting or disturbing communications with hardware controllers or operation of the software.

2. The ACS software shall alert a user to security events as required while other concurrent programs are running.

F. Database

1. The system software shall be capable of stand-alone or Client-Server networked operations utilizing open system architecture and a 32-bit bit ODBC-compliant database.

2. Database structure: Microsoft® SQL Server Express or Microsoft® SQL Server, selectable upon installation with appropriate database drivers automatically installed.
3. Cluster environment: Capable of operating in a Microsoft SQL cluster environment where two redundant servers utilize a shared database cluster.
4. Location separation capability:
    a. Isolation of the ACS database from the application
    b. Hosting of application and database in separate geographical locations
    c. Communication between hosting servers over standard TCP/IP network
5. File and database replication capability:
    a. Via Microsoft SQL Server 2005 update Replication Services and Microsoft File Replication Services
    b. No requirement for proprietary file replication software
6. Timestamps:
    a. Record all transactions with all of the following
        1) GMT timestamp
        2) local time zone timestamp of the controller that generated the transaction
        3) SQL server timestamp when the transaction was inserted into the database.
    b. Format: per ISO 8601

G. System Operators
    a. Number of concurrent operators: up to 256
    b. Security shall be provided through the assignment of operator user names, passwords, and privilege levels.
        1) Passwords assigned to system operators shall allow an operator to log onto any Client interface without affecting system control of current operators logged onto other client interfaces.
    c. Operator rights:
        1) Rights shall be assignable by:
            a) feature
            b) screen or menu item
            c) controller
        2) Rights shall be assignable to any and all system operators, whether individually or as members of a defined group.
        3) It shall be possible to add, remove and edit any operator and operator group rights.
    d. The software shall allow access to designated listings of alarms, readers, relays, schedules, and access levels.
    e. Authorized operators shall be able to view, edit, add, or delete any or all alarms, readers, relays and/or schedules and access levels as their designated privilege level allows.
    f. Operators shall have the capability, within their authorized privilege parameters, to use the same display screen to mask, unmask any alarm point; turn on, turn off, or pulse any relay; or lock, unlock, momentary release or set modes including card only, card or pin, card and pin, or pin only for any card reader.

g. Operator/User Interface – The ACS shall provide an operator configurable and customizable interface.
   1) The operator interface shall provide a hardware configuration tree and filterable display grids to display information to the operator.
      a) All live events, trace events, alerts and system status shall be provided in grids that can be sized, floated or relocated by the user.
   2) The Operator shall be able to specify display colors and be able to sort/group information at will.
   3) The Operator Interface shall incorporate a menu bar with drop-down menus and display icons for full system setup and operation. This menu and these icons shall offer to system operators complete access on one screen to all system functions and system setup parameters to which the users have rights.
   4) Screens that are opened by the operator shall remain open and available via tabs just below the main ribbon for easy accessibility until they are closed by the operator.
   5) The background and text colors for all transaction-display screens shall be customizable for each operator, and it shall be possible to apply filters to display only selected transactions on a transaction-display screen, as described in this specification.
   6) The screen layouts shall provide for viewing system cardholder activity; monitoring and acknowledging alarms; and monitoring and controlling input points, relays and door configurations. Capability to include a site tree per connected hardware gateway for displaying system setup and configuring system parameters shall be provided.
   7) It shall be possible to create tabbed windows in the screen layout to conserve desktop space in the viewing area without in any way restricting the availability of information that can be displayed for the operator.
   8) All operator-specified screen configurations shall be stored per operator such that when the operator logs on, the interface opens in the saved configuration.
      a) The stored operator interface shall include the following:
         i. docking positions and state of all dockable controls
         ii. group sort categories
         iii. direction of all status views
         iv. displayed/hidden columns in all status views

H. General Capabilities – The ACS software shall provide for the following capabilities and functions, as a minimum:
   1. "First Person In" - auto-unlock schedules are not activated until a valid credential has been presented and a door is opened with an access granted transaction.
   2. Roll call - indicates in/out status of cardholders
   3. Mustering – an advanced roll call function that provides for personnel mustering at designated "safe zone" readers in case of emergency evacuation.
   4. Photo recall - recall a stored photo based on a cardholder's credential presentation at any specified reader or readers to allow a positive visual match to be made by a guard or operator monitoring the system.
   5. Supervisor cards - Allow for the creation of supervisor cards such that supervisor cardholders can be configured with the ability to:

a. change reader modes at certain access points
b. globally unlock or lockdown any or all doors on the system
c. grant anti-passback free passes to all cardholders
d. mask or unmask inputs such as door contacts

6. “Two person rule" - require two different valid cards to be presented in succession before access is granted.
7. Credential data formats – allow for multiple data formats and include a format builder to allow operators to create custom formats as required.
8. History and trace functions - allow operators to quickly review past activity and to follow an object's or person's activity going forward, for objects such as users, readers, inputs, and outputs.
9. Customizable Situation Manager - allows instant change of operating parameters of the system to predefined settings in order to respond to changing security threats by clicking a button on the menu ribbon.
    a. The Situation Manager shall be able to instantly trigger a linkage macro that is designed to respond to immediate or perceived threats.
10. Scheduling - The ACS software shall include:
    a. a host scheduler that can be used for some global linkage functions.
    b. an available advanced system calendar to perform various functions including the ability to:
        1) automatically create a full system backup
        2) schedule a full download to the controller network
        3) run and distribute system reports
        4) automatically synchronize server and controller times
        5) schedule execution of any global macro
        6) automatically schedule hardware commands

I. Door and I/O Configuration
1. The ACS software shall support configuration and support for all industry standard reader types and peripheral hardware.
2. Reader types - The ACS software shall allow for selection of reader type, including
    a. Wiegand/Proximity (1 wire LED)
    b. Wiegand/ Proximity 1 wire LED / 4 bit keypad
    c. Wiegand/ Proximity (2 wire LED) / 4 bit keypad
    d. Wiegand/ Proximity (1 wire LED) / 8 bit keypad
    e. Wiegand/ Proximity (2 wire LED) / 8 bit
    f. Biometric

g. Keri NXT Proximity
h. Keri MS Series Proximity

3. Door Configuration - Through the door configuration interface of the ACS software, the user shall be able to configure, monitor and control the hardware components in the software for any door or access control point in the system, including the following:
   a. door position switches
   b. request to exit (REX) devices and all associated door hardware
   c. door strike times
   d. individually assign input points and relays through the software to readers to permit door monitoring and door-lock control
   e. reassignment of door function inputs and relays to general purpose inputs and outputs, and auxiliary general purpose I/O to door I/O
   f. held open times and ADA timing – allow the operator to type in the exact time in hours, minutes and seconds
      1) It shall not be acceptable to use drop down values or inputs in seconds only.
      2) Maximum duration: 36 hours, 24 minutes, 30 seconds with a 2 second resolution.
   g. manual opening, closing, or masking of a door or group of doors
   h. viewing doors that have been configured
   i. editing existing door configurations
   j. deleting door configurations from the system
   k. global lock, unlock, lock out and lock down
      1) specifiable global lock and unlock lockout and lockdown, permitting users to rapidly lock all doors, selected doors or a single door to prevent entry and/or egress
         a) Systems unable to affect a rapid, comprehensive lock out and lock down of any or all doors shall be unacceptable.
      2) configure the lockout parameters such that designated cardholders may override the lockout/lockdown command(s) and retain entry access at the locked-out doors
         a) Systems that are not capable of easily conferring cardholder-by-cardholder permissions to override lockout or that confer such permissions only on a cardholder-group basis shall be unacceptable.
      3) lock, lockout, or lockdown via a panic button, keypad, card reader, or other external device tied to the system
      4) enablement of administrators or authorized users to lock out doors without allowing any cardholder(s) to exercise override privileges
         a) Systems incapable of establishing lockout without override at any single door, combination of doors or all doors shall be unacceptable.
      5) software-selectable autolock on a per door basis
   l. Man-traps and Sally ports - when two doors so configured, only one of those shall be permitted to be open at any one time, and access shall be denied through the other
4. Linkage Macros - The ACS software shall provide a linkage macro tool that allows a user to define input/output linkages which link any system transaction or event (trigger) such as schedule change, input state change, door or user group action, alarm acknowledgement or user command

to a user defined series of actions (procedures) including initiation of other user defined action lists, relay control, door mode control, alarm generation, schedule enable/disable and ASCII-text out to a 3rd party system or device.

a. The linkage macros shall have the ability to be created both to function within a controller and its connected hardware without requiring PC intervention (input/output linkages), as well as system events that are software and PC-generated.
    1) The response time when linking inputs and outputs within any specific controller shall not exceed 1 second.
b. The ACS software shall provide an easy-to-use tool for configuring these linkage macros that allows operators to create them "on the fly to meet current or future function requirements.
c. Each controller shall support at least 1000 user defined linkage macros with 100 instructions per macro, with a greater number possible via controller memory allocation.

J. Listings and Groups
1. The ACS software shall allow access to listings of all or selected individual or groups of inputs via operator permission, alarms, readers, relays, schedules and access levels.
2. Administrators and authorized operators shall be able to view, edit, add, or delete any or all alarms, readers, relays and/or schedules and access levels, which shall have the capability of being grouped for display, configuration, automation, and control.
3. Administrators and authorized operators shall have the capability to use the same display screen to mask, unmask any alarm point; turn on, turn off, or pulse any relay; or lock, unlock, momentary release or set modes including card only, card or pin, card and pin, or pin only for any card reader.
    a. This ability shall be available for groups of inputs, outputs, and readers.
4. Manual control for these functions shall be available via right-click menus.
5. Cardholders shall be assignable to user groups.

K. Monitoring and Message Filters
1. Screens - The ACS software shall provide screens for operators to view system activity in real time.
2. The ACS software shall support the use of multiple display monitors.
3. Customization
    a. Events of different types shall be customizable via application of text and background colors for easier identification in the monitoring screen.
    b. The operator shall have the ability to define custom Filters for filtering information displayed on a transaction screen and a separate filter for filtering the display of cardholder images in the Roll Call window.
        1) The Filters option shall be
            a) applicable per device and per user
            b) capable of displaying available event messages
        2) Filters can be capable of being defined and saved for defined functions.
            a) The system shall maintain the capability of recording into the historical file all transactions into history in the presence of filters for real time monitoring.

L. Alarm Management – The ACS system shall allow for the following alarm management capabilities:

1. Set up any system transaction or event to display as an alarm and to require alarm confirmation and acknowledgement, or not as needed
2. Operator ability to set alarm priorities from over a range of 255 values, with the highest priority alarms displaying at the top of the monitoring screen
3. Alarm-handling capabilities that include interfaces to create predefined customizable or operator-annotated alarm acknowledgement messages
4. Custom color coding assignable for displaying different alarm events for easy operator recognition and handling
5. Alerts - event or alarm configuration to trigger an email or SMS alert
6. Linking of audio WAV files to the generation of defined alarms with immediate audible alerts upon alarm, customizable on an event by event basis

M. Elevator Control - Elevator control shall be user configurable using an available elevator control software module to provide the following functions:
1. Provide the authorized operator with the ability to enable floor call buttons based on card access by certain user groups
2. Enable the floor buttons assigned to the user group to which the card holder is assigned when that cardholder uses the elevator reader
3. Enable designated relays on the controller and/or output boards that are in series with the elevator cab floor buttons to allow floor access

N. Cardholders/Credentials
1. The ACS software user interface shall provide the ability to add, edit, activate, deactivate and/or delete individual card or cardholder records.
2. Enrollment and configuration functions:
   a. ability to block enroll credentials for large populations
   b. individual credential enrollment, with the capability of presenting credentials to an enrollment reader
   c. assignment of up to 30 card numbered credentials to a single card holder record
   d. configure credentials to automatically activate and/or expire based on
      1) a future date and time, or
      2) a designated number of uses
   e. capture a photo using a digital camera or retrieve a stored photo file for inclusion in individual new or existing card or cardholder records, such photos to be displayable in the cardholder record, printable on a photo ID badge, and made part of the card and cardholder record
   f. via a cardholder entry screen shall provide tabbed pages to allow a system user to:
      1) digitally store the photo in over 39 different formats including BMP, GIF, JPG, and TIF and export the selected image to any of the 39 formats
      2) configure and assign virtually unlimited access groups, which consist of a time schedule or time schedules and a reader group or groups
      3) provide separate drop-down calendar controls for use in assigning future card-activation and card-expiration dates (temporary credentials)
      4) enter cardholder names, user group membership, access level information, a personal identification number (PIN), company information and user defined custom data fields

5) enable anti-passback override
6) set cardholder ADA/DDA information
7) set VIP status
8) view data concerning the recent transaction for the cardholder in the system
9) enable PIN exempt override

g. display of cardholder information in both individual record form and in filterable spreadsheet or "grid" format that allows for mass viewing, searching, sorting, and editing

h. configuration of user requirements, as follows:
1) use of more than one credential (dual verification), such as the use of a card plus a PIN or card plus biometric verifications
2) select individual users or user groups to be PIN-exempt
3) set a card + PIN rule to apply only during predefined days and hours during the week

3. Badging
a. the ACS shall allow creation and saving of an unlimited number of photo/graphic badge templates
b. the ACS shall allow any or all of the following elements to be employed together in card design that can be used to create individual, cardholder-specific cards or identification badges:
1) captured or retrieved cardholders' photos that are part of the cardholder database
2) graphics, logos or other images
3) static data that is duplicated on each card printed
4) variable data from the cardholder database that is specific to each card printed
5) bar codes
c. it shall be possible for customers to create card designs that employ:
1) choice of vertical orientation or horizontal orientation with optional card rotation
2) dual-sided printing
3) predefined or custom dimensions
4) cardholder photos, with optional borders, with ability to rotate the image, select border color and width and adjust the image brightness
5) bitmaps or JPEGs of logos, designs, pictures and other graphics, including a card background color or graphic, all with definable dimensions
6) text using the design font selections available in Windows with ability to vary text formatting
7) slots for insertion of clips, lanyards, or similar
8) bar codes associated with database fields that are to be selected from a drop-down list that includes database fields and a constant or separator
a) The user shall have the capability to select the field length, use of padding, padding characters, position, rotation, ratio, height, size and readability of text appearing with the bar code.
d. The ACS software shall be capable of allowing unlimited individual badge designs to be designed, created and previewed before saving.

e. The ACS software shall allow for on-screen printer selection from a drop-down list that displays all installed print drivers within Windows.

f. The customer shall be able to define logical arguments based on selected database information that may vary from card record to card record. It shall be possible to define different bitmap images to appear on the printed card as a result of the application logic, which uses the specific data from the database as the criterion for displaying or not displaying the image.

4. Cardholder Database functions:

a. provide pages in the cardholder database module to allow custom fields to be saved to the cardholder database

b. display custom fields on a custom tabbed page

c. allow users to:

1) rename each field and its accompanying label

2) enter and save existing data into the custom field, or delete the data from the field

d. provide a page in the cardholder database module to permit template definitions that can be easily assigned to new card holders in order to reduce data entry time

e. have the ability to display cardholders in a sortable and filterable grid

O. Anti-Passback - The ACS shall support the following modes of anti-passback:

1. Soft Anti-Passback
2. Hard Anti-Passback
3. Timed Anti-Passback

a. the following modes of timed anti-passback shall be supported:

1) Last Valid User

2) Per User

3) Timed Hard Anti-Passback, Soft Anti-Passback

b. the ACS software shall allow the operator to type in the exact time in hours, minutes and seconds

1) It shall not be acceptable to use drop down values or inputs in seconds only.

2) Maximum value: 18 hours, 12 minutes, 16 seconds

3) Resolution: 1 second

P. Graphics Mapping Client – The following functions shall be supported:

1. Vector based mapping

a. bitmap images shall not be used

2. Retention of aspect ratios upon map re-sizing
3. Display floor view, unit view and sensor view on a single screen, without requiring the operator to switch to alternate views

Q. Video Management and Recording

1. The ACS shall provide an available video-only client for monitoring of surveillance cameras, with the ability to pause live video, rewind and fast forward recorded video.
2. The ACS shall provide an available event video recording (EVR) solution for video management with the following characteristics:

1) seamless integration with ACS
2) built on a Microsoft.NET framework
3) user friendly with the complexity and sophistication hidden from the user to provide a uniform, simple look and feel
4) available video analytics that can detect and prevent threatening events in real-time to include loitering, package left behind and people counting
5) storage of video based on user defined events
6) maintenance of forensic integrity without a requirement for accurate time synchronization between the video server, access control server, and field hardware
    a) video clips shall include a unique system generated identifier
7) ONVIF compliant
8) support for MJPEG and H.264 video streams

R. Third Party System Integration - The ACS software shall provide the ability to transmit ASCII codes from the primary field panel to 3rd party systems.
    1. The ACS shall provide a linkage editor that allows the authorized user or system administrator to define the ASCII strings that will be sent to 3rd party equipment such as CCTV systems, DVRs and other security equipment based on user commands or system initiated events that have been defined by the user.
    2. The ACS shall provide integration with the EasyLobby visitor management system.

S. Reports - The ACS shall include a built-in report function that allows the configuration of reports based on selected system parameters.
    1. The ACS shall provide the ability to produce instant history reports for all devices and card holders.
    2. A history report option shall be available as part of the configuration editor for all card holders and devices without leaving the edit function.
    3. The report function shall use simple selection criteria utilizing check boxes and drop down menus.
    4. Reports shall be obtained by any of the following methods, some by using the optional Report Client:
        a. view on the screen
            1) support a search function for user entered text
        b. print
        c. export to a file the following formats:
            1) RTF
            2) PDF, with the following options:
                a) Assignment of the Owner Password
                b) Assignment of the User Password
                c) 40-bit,128-bit or no Encryption
                d) Allow/disallow printing
                e) Allow/disallow modify contents
                f) Allow/disallow copy

g) Allow/disallow modify annotation

3) HTML

4) Microsoft Excel Worksheet (XLS)

5) TIFF

6) Text delimited file

5. Reports shall be generated on demand or on a schedule with capability for automatic or manual email to a distribution list when the System Calendar is in use.
6. Advanced report design function - The ACS software shall include an option for more advanced report design functionality, to include the capability to design all system reports with the capability to:
   a. define report type
   b. add selected fields
   c. define report headers and footers
   d. add logos and images
   e. include pre-defined reports for cardholder listings, system messages, and history and alarm messages
7. Audit – The ACS shall include a complete audit trail that tracks all configuration changes for operators, card holders and controllers.
   a. old value, new value and operator making the change shall be logged

2.04 SERVERS

A. ACS Software Server (PC)

1. CPU: Quad Core Intel Xeon 64-bit processor, 2.5 GHz or higher
2. Operating system: Windows 8.1 Professional, Windows 10 Professional, or greater Windows Server revisions 2012, 2012 R2, 2016 or greater
3. RAM: 8 GB minimum
4. On-board storage: 500 GB minimum
5. Ethernet Port: 10/100/1000 Base-T (RJ-45)
6. Serial Port: RS-232 or USB, but not required if using TCP/IP
7. Database: Microsoft SQL Express Server 2016 or greater
8. .NET Framework: Microsoft.NET Framework 4.6.2 or greater

B. Client PC’s

1. The ACS shall have the ability to support up to 256 Client work stations on a LAN/WAN/Internet connection.
2. CPU: Quad Core Intel Xeon 64-bit processor, 2.0 GHz or higher
3. Operating system: Windows 8.1 Professional, Windows 10 Professional, or greater Windows Server revisions 2012, 2012 R2, 2016 or greater
4. RAM: 4 GB minimum
5. On-board storage: 160 GB minimum available
6. Ethernet Port: 10/100/1000 Base-T (RJ-45)

7. Video Card:
   a. Resolution: 1280 x 1024 minimum supported
   b. RAM: 64 MB minimum

A video plug in card as specified above is required with video integration.

C. Gateway Computers - The ACS shall support configuration of Gateway computers for connection to field controllers to meet IT infrastructure requirements.

D. The ACS shall support the capability to configure the Gateway, Database Server, Application Server and Client GUI on a single PC, or distributed in a network environment.

2.05 FIELD HARDWARE AND PERIPHERAL DEVICES

A. Controllers

1. Controllers shall make access control decisions at doors, exits, and entrances etc., and communicate to PCs for programming instructions, event monitoring and record keeping.
   a. The controllers shall receive data input from other peripheral hardware components of the system, such as readers, input devices and relays.
   b. All system controllers shall be connected to the system server(s) where event history, cardholder data and system programming data shall reside.
   c. The controllers shall receive data input from, and provide system data to, the controlling system server(s) as part of the system polling process.
2. The controllers shall be designed specifically for access control system applications.
3. Controllers shall be intelligent and fully stand alone processor capable.
4. Controllers shall be available in two door and four door versions.
   a. Controllers shall allow access and egress readers to occupy the same reader port, effectively doubling the controller capacity when both access and egress are required.
5. Controllers shall make all local access control and alarm decisions without host server dependency.
6. All panels shall support flash memory to facilitate firmware updates.
7. Encryption – The controller shall provide the capability for FIPS 197 AES 128 Bit encryption.
8. Site codes - The ACS software shall support up to 8 site codes or formats per controller.
   a. Each site code shall be configured independently with a value range from 0 to 999,999,999,999.
9. Card numbers - The system shall support card numbers with a value range from 1 to 999,999,999,999,999.
10. PIN digits
    a. The ACS shall support the use of PIN digits in a PIN only mode, Card or PIN mode, or Card and PIN mode at selected readers.
    b. The PIN digit assigned to a cardholder shall be capable of different lengths for each cardholder with a range of 0 to 15 digits.
    c. Leading zero PIN digits shall be supported.

11. Reader interfaces
    a. The ACS shall support controller types that have the ability to connect up to 1, 2, 4 or 8 readers, depending upon configuration, firmware and reader type.
    b. The controller-reader communication shall be via a high security 64 bit encrypted format that also provides for reader supervision via an RS-485 connection.
    c. The controller will support interfaces to the following types of readers:
        1) Up to 64 bit Wiegand
        2) Bar Code with Wiegand output
        3) Keypad with Wiegand output
        4) Biometric with Wiegand output
        5) Electronic Discharge or Touch Memory Devices with Wiegand output
        6) Keri Systems MS Series Proximity Reader
    d. The controller shall provide reader status supervision.
12. Cardholders
    a. Each controller shall store no less than 48,000 and up to 100K cardholders/users and 10,000 events, with memory configurable to increase or decrease these capacities.
    b. The controller shall be configurable such that only events designated by a system administrator or operator are stored.
    c. Should the event buffer become full, each controller shall delete events only as needed on a first in, first out basis.
1. Each Controller's memory shall operate independently of all other Controllers. Memory shall be configurable for the number of cardholders, the size of each cardholder record related to cardholder options, and the number of offline transaction storage.
13. Linkage macros
    a. Each controller shall support at least 1000 user defined linkage macros with 100 instructions per macro, with a greater number possible via controller memory allocation.
        1) The total number of macros shall be configurable based on available memory at the controller.

14. Inputs (other than Readers)
    a. All inputs shall be protected against power surges by diodes.
    b. Supervision of system input points shall be provided by the control panel.
    c. User definable EOL resistance values shall be configurable for every input in the system including reader door contacts and request to exit inputs.
        1) The EOL shall include a minimum and maximum resistance value for both the active and inactive states of the input.
    d. In addition to the normal status changes between the inactive and active states, the system shall report the following conditions:
        1) open circuit
        2) shorted circuit
        3) grounded circuit
        4) EOL tolerance
            a) In the event the circuit resistance cannot be classified due to rapid changes in the circuit resistance, a non-settling error shall be reported.
    e. Each controller shall have a dedicated tamper input.
15. Outputs
    a. Level: 10 amp @ 125 VAC maximum
    b. Type: dry circuit, single pole, double throw relay
    c. Functions:
        1) application of power to an electric locking device, automatic gate, door operator, or annunciator
        2) shunting an alarm
        3) other general purpose function triggered by an input or software event
    d. All outputs shall be protected against power surges by MOVs and resistor snubber circuits.
16. Memory
    a. The controller's memory shall be non-volatile (supported by a lithium battery) with an expected life of 5 years.
    b. The controller shall send a notification to the Server Software when the lithium battery power approaches a state where it can no longer back up the memory.
17. Controllers shall be protected by a self-resetting, thermal fuse as well as diode protection.
18. Failures - Failure or fault of power supply to panels(s) or data connections between the panel(s) and server(s) shall be indicated on the system display of an operator's screen.
19. Indicator LED's:
    a. RS-485 network activity
    b. TCP/IP network
        1) Activity
        2) Speed
    c. Power fault for over voltage and reverse voltage

d. Reset indication for Controller memory
e. Relay energized

20. Environmental
    a. Operating temperature: 32º F to 150º F (0º C to 65º C)
    b. Relative Humidity: 0 – 90%

B. Telephone Entry Panels - The ACS shall have the capability to support integrated telephone entry panels to allow visitors access via telephone
   1. The telephone entry panel shall function similarly to an intercom system to allow occupants to grant visitor access from their telephone, but utilize the facility's phone lines instead of requiring dedicated hard wiring.
   2. The telephone entry panels shall have a scrollable electronic display with the tenant/occupant names that, when selected, can be called with the push of a button.
      a. The tenant/occupant shall be able to grant access by pressing a pre-programmed button on their telephone.
      b. A second button shall be available to control another relay.
      c. Directory code length: up to 6 digits
      d. Phone number length: 7-15 digits
   3. The telephone entry panels shall display up to 3 scrolling messages for visitor instructions or other information.
   4. The telephone entry panels shall have the capability of being fitted with a camera to allow the tenant/occupant to view the visitor.
   5. The telephone entry panels shall have a "no phone line" option for use in areas that incur a toll charge for local calls.
   6. The following telephone entry panel options shall be available:
      a. Up to 250 occupants/tenants, with a 4 line, 20 characters per line display.
      b. Up to 750 occupants/tenants, with a 4 line, 20 characters per line display.
      c. Up to 5000 occupants/tenants, with 10 line display.
   7. Material: durable brushed stainless steel.

C. Input/Output Expansion – shall be available via add-on modules for controllers.
   1. Inputs shall be configurable as standard door I/O (REX and door contact) or used as general purpose inputs.
      a. Input type: Dry Contact
   2. Outputs shall be configurable for monitoring, alarm management, I/O linking and other functions.
      a. Output type: Form C Relay rated at 10A @ 125 VAC
   3. Modules shall be available as in the following configurations:
      a. 4 input/4 output
      b. Expansion motherboard capable of accepting up to 8 modules, each with either 8 inputs or 8 outputs per module.

Keri Systems expansion modules are the NXT-4X4 4 input/4output unit and the NXT-GIOX system capable of accepting a combination of 8 NXT-8IN 8 input or NXT-8OUT 8 output modules.

Keri Systems 2-door controller, Model NXT-2D-MSC is capable of accepting a total of two expansion modules of either type, for a potential total of 128 combined inputs and outputs.

Keri Systems 4-door controller, Model NXT-4D-MSC is capable of accepting a total of two expansion modules of either type, for a potential total of 256 combined inputs and outputs.

D. Proximity Readers
   1. The interface to the Controller will be on the supervised, encrypted, 9 bit RS-485 bus and shall require only a 4 conductor cable for all Reader functionality including dual color LED control and beeper control.
      a. The Reader shall be supervised by the Controller with a regular “heartbeat” capable of responding within 1 second if the Reader goes offline.
   2. The Readers shall read encrypted Proximity Cards.
   3. When connected to the Controller, presentation of a card or tag shall produce an audible beep from the Reader and will change the color of the Reader LED, as follows:
      a. Amber: power is on and the Reader is in its ready state.
      b. Green: access is granted.
      c. Red: access is denied.
   4. Accidental or intentional transmission of radio frequency signals into the Reader shall not compromise the security of the access control system
   5. All proximity readers shall be of a weatherproof, potted, rugged design.
   6. Operating temperature: at least -40ºF to 150ºF (-40ºC to 65ºC)
   7. Power options
      a. Directly from the controller, with current not to exceed 120 mA
      b. Independently from the controller
   8. The following reader styles shall be available:
      a. Mullion – for mounting directly on a standard metal mullion doorframe
         1) Dimensions: 3.75” h by 1.60” w by 0.625” d (9.5 cm h x 4.1 cm w x 1.6 cm d)
         2) Read range with standard Proximity Card: up to 4” (10 cm)
      b. Euro - a single gang mount, wall switch reader for mounting onto a metal or plastic European electrical junction box or on a non-metallic flat surface.
         1) Dimensions: 3.25” h by 3.25” w by 0.625” d (8.3 cm h x 8.3 cm w x 1.6 cm d)
         2) Read range with standard proximity card: up to 5” (12.5 cm)
      c. Wall switch – a single gang mount, wall switch reader for mounting onto a metal or plastic USA electrical junction box or on a non-metallic flat surface.

a) Dimensions: 4.18” h by 2.95” w by 0.625” d (10.6 cm h x 7.5 cm w x 1.6 cm d)

b) Read range with standard proximity card: up to 6” (15 cm)

d. Other - As needed, the ACS shall have the capability of accepting inputs from Readers with Wiegand outputs such as Biometric Readers, Vehicle Readers, other proximity devices, swipe, optical, or contact readers.

E. Locks - The ACS shall be capable of managing wireless locks. Aperio locks from Assa Abloy and Allegion AD 300 and 400 Series, NDE/LE in online mode via panel interface module, and NDE/LE and Control Smart Locks in offline mode shall be supported.

1. The management of offline NDE, LE, and Control Locks must have the capability of supporting both simple Time Schedules as well as Access Groups so that users can easily be assigned access to multiple doors.
2. When managing offline NDE, LE, and Control Locks, the mobile application must support database caching so as not to require an IP connection for lock database synchronization when uploading or downloading to and from the lock.
3. Is capable of using a WiFi direct module with NDE and LE locks, and can be configured to call in to the host system twice daily on a per lock basis.
4. Has the ability to allow the site administrator to view and set the firmware level for each lock type. NDE and LE locks using a Wifi direct module can automatically ensure each lock is at a specified firmware version, otherwise notification will be given on web and mobile devices that there are locks that are not at the recommended firmware revision.
5. Capable of supporting a single credential (card or tag) for wired card readers and battery powered locks
6. Support Data on Card for Access Groups involving off line locks
7. Support Data on Card for individual access for offline locks
8. NOT require annual / monthly ongoing fees for lock licensing
9. Archive events using a FIFO (First In, First Out) buffer, storing a user configurable number of transactions with a default of 4 million records, and an optional retention cap (i.e., only store last 90 days of events)
10. Support manual operation of offline locks via mobile app / operator permission
11. ACS manufacturer shall support the Allegion MT-20W, write capable (encoding) reader

F. The duration of operation shall be a function of the amount of equipment, connected to the panel and the individual power requirements of that equipment, and the battery amp hour rating.

G. Power Supplies - The controllers and other hardware components (Readers, Input or Output Modules) in the system shall be powered by a 12-VDC power supply with battery backup charger.

1. The main controller shall be powered from 12VDC and draw no more than 650 mA at 12VDC when all outputs LEDs and communication busses are fully active.
2. Expansion boards shall be capable of drawing 12 VDC power from the main controller or of being powered locally.
3. The primary high security reader types’ current draw shall not exceed 120 mA at 12VDC and shall be capable of drawing 12 VDC power from the controller or of being powered locally.
4. Upon failure of normal power to the controller and modules, the hardware shall be temporarily powered from four (4) to six (6) hours by a backup 12 VDC gel-cell battery. The transition to the

battery backup power shall be automatic to prevent the loss of transactions or notification of any alarm, trouble or operator acknowledgment signals during the transition.

5. Readers powered by the controllers shall be temporarily powered by the backup battery. Readers and other peripheral devices with separate power supplies shall not be provided backup power via the panel backup battery.
6. The duration of operation shall be a function of the amount of equipment, connected to the panel and the individual power requirements of that equipment, and the battery amp hour rating.

Specifier should determine stand-by time based on equipment used and applicable regulations.

---

7. Uninterruptible power sources (UPSs) shall be used with the Server and Client computers used in the system.

H. Access Credentials

1. The system shall accept user credentials of various types, including proximity and swipe cards, PINs, and biometrics.
2. Proximity cards and tags shall be uniquely encoded and not sensitive to facility code matching or other limiting factors.
3. The following types of proximity credentials shall be available:
   a. Clamshell Card
      1) Color: white with imprinted encoded number and date code
      2) Dimensions (l x w x d): 3.38” x 2.13” x 0.065” (8.6 cm x 5.4 cm x 178 mm)
      3) The card shall have a slot punch for attachment to a badge clip.
   b. ISO Card
      1) Color: white with imprinted encoded number and date code
      2) Dimensions (l x w x d): 3.38” x 2.13” x 0.031” (86 mm x 54 mm x 0.08mm)
      3) The card shall be capable of accepting a direct print of photo and other graphics from a dye-sublimation printer.
      4) The card shall be optionally available with a standard high coercivity three track magnetic stripe.
      5) The card shall have an available area for a slot punch for attachment to a badge clip.
   c. Key Ring Tag
      1) Color: light gray with imprinted encoded number and date code
      2) Dimensions (l x w x d): 1.57” x .98” x 0.157” (40 mm x 25 mm x 4 mm)
      3) Shape: teardrop, with a riveted eyelet, allowing the tag to be attached to a key ring.
   d. Adhesive Patch - An adhesive tag or "patch" that adheres to a wallet, cell phone, photo badge, or another access credential

2.06 COMMUNICATIONS

A. IP Network – IP network communication shall be used for communication between servers and controllers.
   1. The IP network shall support 10/100/1000 Base-T Ethernet communication and auto MDI/MDIX.
   2. The access control system shall support the following network protocols:
      a. TCP
      b. UDP
      c. NTP
   3. Connectors: RJ-45 and terminal block

B. RS-485 - communication between Controllers, their Expansion Modules, and the high security Proximity Readers shall be via a supervised, encrypted, 9 bit RS-485 bus.
   1. Supported distance: 500 feet (150 m)

END OF SECTION

PART 3 EXECUTION

3.01 INSTALLERS

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

3.02 EXAMINATION

A. Network - All network connections to the access control system shall be tested for proper levels of performance.

3.03 STORAGE

A. The system shall be stored in an environment compliant with the equipment manufacturers' recommendations.

3.04 PREPARATION

A. IP addressing shall be coordinated with the Owner's responsible IT personnel.

3.05 INSTALLATION

A. Installers shall follow all Manufacturer published installation instructions and guidelines.

B. All wires shall be run through conduit to prevent failure caused by rodent damage.

END OF SECTION