Add Alternates 1 & 2 Integrated Door Security for Ridgeland High School and Lafayette High School

1 GENERAL

Integrated Door Security Overall Scope of Work

Please refer to the drawing provided for more clarification on the written scope of work below.

RIDGELAND HIGH SCHOOL
This project is to provide manual and scheduled door release of exterior doors securing the doors as much as possible reducing the possibility of unauthorized access during classes while providing as much access for the students as possible during class changes.

The Front and back door from the parking areas (BLUE ARROW) will be locked at all times. A speaker call switch will be installed at the door and when visitors approach they place a call to the communications system console located in the main office. Once the person has been vetted the door will be Released from a simple push button release in the office allowing entry. A IP camera connected to the existing Pelco NVR using a dedicated monitor in the office will provide a visual of the visitor for additional verification.

There are 5 doors (RED ARROWS) that are regularly used by the students during class changes. These doors would be on a schedule that will coincide with the bells. The Door release hardware will be integrated with the new communications system using a networked based switching module that will provide the contact closure necessary to change the state of the doors. This integration would provide the locking and unlocking schedule that will determine whether students have free access or will need to use a card to enter the building. The doors will be on a schedule to unlock prior to the bell ringing and would reengage during classes. If a student needs entry during classes, the teacher would provide the student with a proximity card that would allow the student to enter the building as act as a hall pass. The schedule to lock and unlock the doors will be determined by the communication system to insure doors will be locked and unlocked in perfect synchronization with the bell schedule. The remaining doors would be locked at all times using standard key locks (BLACK ARROWS).

LAFAYETTE HIGH SCHOOL
The Front Office Entrance (BLUE ARROW) and the Attendance Entrance from the student parking areas (ORANGE ARROW) will be locked at all times. A speaker call switch will be installed at each door and when visitors approach they place a call to the main office or the attendance office. Once the person has been vetted the door will be released from a simple push button release in the office allowing entry. A camera using a dedicated monitor in the attendance office can provide a visual of the visitor for additional verification. Due to the proximity of the door in the main office no camera will be installed at that door only an audio station. There is also an existing door release that will be reused for this project

There are 2 doors (RED ARROWS) that are regularly used by the students during class changes. These doors would be on a schedule that will coincide with the bells. The Door release hardware will be integrated with the new communications system using a networked based switching module that will provide the contact closure necessary to change the state of the doors. This integration would provide the locking and unlocking schedule that will determine whether students have free access or will need to use a card to enter the building. The doors will be on a

schedule to unlock prior to the bell ringing and would reengage during classes. If a student needs entry during classes, the teacher would provide the student with a proximity card that would allow the student to enter the building as act as a hall pass. The schedule to lock and unlock the doors will be determined by the communication system to insure doors will be locked and unlocked in perfect synchronization with the bell schedule. The remaining doors would be locked at all times using standard key locks (BLACK ARROWS).

The Access Controlled doors will also feature a prop alarm that will sound after a set amount of time should the door be propped open and left unattended. Include a choice of Key Fob style cards or adhesive "Pucks" that can be attached to existing printed badges already in use by the school staff as well standard cards that can have Walker County credentials printed on them as existing badges are retired. Provide management software licensing for two users.

1.01 SUMMARY

A. The system shall consist of access-control software that enables communication between IBM®-compatible personal computers and microprocessor-equipped smart controllers with distributed databases. The smart controllers make access-control decisions at doors, exits, entrances, etc., and communicate to PCs for programming instructions, event monitoring and record keeping. The controller(s) shall be designed specifically for access-control system applications.

B. The controller(s) shall receive data input from other hardware components of the system, such as readers and relays. All system controllers shall be connected to the system server(s) where event history, cardholder data and system programming data shall reside. The controller(s) shall receive data input from, and provide system data to, the controlling system server(s).

C. This performance specification provides the minimum requirements for the Access-Control system. The system shall include, but not be limited to, all equipment, materials, labor, documentation and services necessary to furnish and install a complete and operational system to include, but not be limited to, the following functions:
Enabling valid access and preventing unauthorized access at facility portals
Enabling alarm/alert notification of access breaches at facility portals and other points as desired
Enabling data collection and management for a cardholder database at the facility

1.02 SECTION INCLUDES

Access Control Software & Related Access Control Hardware

1.03 RELATED REQUIREMENTS

A. All work and materials shall conform to all applicable Federal, State, local and/or municipal codes and regulations governing the installation. If there is a conflict between this specification and the referenced standards, federal, state, local and/or municipal codes, it is the bidder's responsibility to immediately bring the conflict to the attention of the Engineer for resolution. National standards shall prevail unless local codes are more stringent. The bidder shall not attempt to resolve conflicts directly with the local authorities unless specifically authorized by the Engineer.

B. The controllers, reader boards and input/output boards proposed in this specification shall be compliant with UL 294. The supplier shall be responsible for filing of all documents, paying all fees (including, but not limited to plan checking and permit) and securing all permits, inspections and approvals. Upon receipt of approved drawings from the authority having jurisdiction, the supplier shall immediately forward two sets of drawings to the Owner. These drawings shall either be stamped "Approved" or a copy of the letter stating approval shall be included.

E. All controllers and connected boards, readers and the like shall be tested to ensure that a fully functioning system is designed and installed. The system supplied under this specification shall be a microprocessor-based system. The system shall utilize independently addressed, microprocessor-based controllers as described in this specification.

1.05 ALTERNATES

A. Specifications related to the access control are based on Identicard. Alternate products are allowed but must provide strict conformance to this specification and is required to ensure that the installed and programmed system will function as designed, and will accommodate the future requirements and operations of the building owner. All specified operational features must be met without exception.

B. The authorized representative of the manufacturer of the major equipment shall be responsible for the satisfactory installation of the complete system.

C. All equipment and components shall be the manufacturer's current models. The authorized representative of the manufacturer of the major equipment, such as controllers, shall be responsible for the satisfactory installation of the complete system.

D. All controllers and connected boards, readers and the like shall be tested to ensure that the system operates as specified. The system shall utilize independently addressed, microprocessor-based controllers as described in this specification.

E. All equipment and components shall be installed in strict compliance with the manufacturer's recommendations.

G. The acceptability of any alternate proposed system shall be the sole decision of the Owner or his authorized representative.

1.06 REFERENCES

1.06.01 Abbreviations and Acronyms

A. UL® or ULI: Underwriters Laboratories, Inc

B. ADA: Americans with Disabilities Act

C. AFF: Above Finished Floor

D. AHJ: Authority Having Jurisdiction

1.06.02 Definitions

1.06.02.01 Approved

Unless otherwise stated, materials, equipment or submittals approved by the Authority or AHJ.

1.06.02.02 User

An administrator or operator who performs functions in the system in accordance with his/her system permissions and roles, unless otherwise stated.

1.06.03 Reference Standards

The equipment shall comply with the current provisions of the following codes and standards:
<UL 294 - Standard for Access Control System Units>
<List any other relevant and applicable codes below as needed:>
<Factory Mutual (FM) approval>
<Insert AHJ>
<Local codes/standards such as: CSFM (State of California), MEA (New York City), City of Chicago >
<Federal Codes and Regulations>
<Americans with Disabilities Act (ADA)>
<Insert state Accessibility Code, if applies>
<European Union (EU)>
<EMC Directive 89/336/EEC>
<Electromagnetic Compatibility Requirements
Product Standard EN 55011: 1991
Generic Standard EN 50082-2: 1995>

1.07 ADMINISTRATIVE REQUIREMENTS

Preinstallation Requirements: The provider shall submit a detailed project plan that will describe in detail how the provider will approach the project, from inception to finalization.

1.08 SUBMITTALS

A. The contractor shall purchase no equipment for the system specified herein until the owner has approved the project submittals in their entirety and has returned them to the contractor. It is the responsibility of the contractor to meet the entire intent and functional performance detailed in these specifications. Approved submittals shall only allow the contractor to proceed with the installation and shall not be construed to mean that the contractor has satisfied the requirements of these specifications. The contractor shall submit three (3) complete sets of documentation within 30 calendar days after award of purchase order.

B. Each submittal shall include a cover letter providing a list of each variation that the submittal may have from the requirements of the contract documents. In addition the contractor shall provide specific notation on each shop drawing, sample, catalog cut, data sheet, installation manual, etc. submitted for review and approval, of each such variation.

1.14 QUALITY ASSURANCE

A. All equipment and components shall be installed in strict compliance with each manufacturer's recommendations. Consult the manufacturer's installation manuals for all wiring diagrams, schematics, physical equipment sizes, etc., before beginning system installation. Refer to the manufacturer's riser/connection diagram and details for all specific system installation/termination/wiring data.

B. The engineered systems distributor must be licensed in the state of Georgia and have been incorporated in the business in that state for a minimum of 10 years.

1.15 QUALIFICATIONS

A. The contractor shall have successfully installed similar access-control systems on a previous project of comparable size and complexity. The owner reserves the right to reject any control components for which evidence of a successful prior installation performed by the contractor cannot be provided.

B. The contractor shall have in-house engineering and project management capability consistent with the requirements of this project. Qualified and approved representatives of the system manufacturer shall perform the detailed engineering design of central and remote-control equipment. Qualified and approved representatives of the system manufacturer shall produce all controller and equipment drawings and submittals, as well as operating manuals. The contractor is responsible for retaining qualified and approved representative(s) of those system manufacturers specified for detailed system design and documentation, coordination of system installation requirements, and final system testing and commissioning in accordance with these specifications.

1.16 DELIVERY, STORAGE, AND HANDLING

1.16.01 Storage and Handling Requirements

A. The Contractor shall be responsible for all receiving, handling and storage of his materials at the job site.

B. Use of loading docks, service driveways and freight elevators shall be coordinated with the Owner.

C. The Owner will provide the Contractor with a lockable storage space for the Contractor's use during this project. The Contractor shall be responsible for the security of this space.

D. Overnight storage of materials is limited to the assigned storage area. Materials brought to the work area shall be installed the same day, or returned to the assigned storage area, unless previously approved by the Owner.

1.16.02 Waste Management

A. The Contractor shall remove rubbish and debris resulting from his work on a daily basis. Rubbish not removed by the Contractor will be removed by the Owner, and charges for such removal shall be charged back to the Contractor.

B. Removal of debris and rubbish from the premises shall be coordinated with the Owner.

1.17 FIELD CONDITIONS

A. It shall be the Contractor's responsibility to inspect the job site and become familiar with the conditions under which the work will be performed. Inspection of the building may be made by appointment with the Owner. Contractors are requested to inspect the building prior to the pre-bid meeting.

B. All work, except for <INSERT AS APPLICABLE>, may be conducted during normal working hours, 8:00 AM to 5:00 PM, Monday through Friday, by properly coordinating the work with the Owner. Noise restrictions do apply. The core drilling, testing of evacuation signals and other work disruptive to occupants will be prohibited between 6:00 AM and 6:00 PM, Monday through Friday, and will be explained at the pre-bid meeting. <NOTE: Add exclusion as needed for kitchens and other areas>. <OPTIONAL: All system switch-over shall be done during unoccupied hours or over weekends. Contractor is to include, in his base bid, all overtime necessary to complete his work.

C. The Contractor shall be responsible for prior coordination of all work and demolition with the Owner.

1.18 WARRANTY

A. The contractor shall warranty all materials, installation and workmanship for one (1) year from date of acceptance, unless otherwise specified. A copy of the manufacturer's warranty shall be provided with closeout documentation and included with the operation and installation manuals.

B. The System Supplier shall maintain a service organization with adequate spare parts stock within <75> miles of the installation. Any defects that render the system inoperative shall be repaired within 24 hours of the owner notifying the contractor.

2 PRODUCTS

2.01 ACCESS CONTROL SOFTWARE

2.01.01 Manufacturers

A. The manufacturer named herein shall be regularly involved in the design, manufacture or distribution of products specified in this document.

B. All products shall be listed by the manufacturer for their intended purpose.

C. Products manufactured or distributed by IDenticard Systems or equal shall constitute the minimum type and quality of equipment to be installed.

D. The specified PC-based Access Control and Monitoring Software shall be IDenticard Systems or equal.

E. All equipment and components shall be the manufacturer's current model. The authorized representative of the manufacturer of the major equipment shall be responsible for the satisfactory installation of the complete system.

F. The contractor shall provide, from the acceptable manufacturer's current product lines, equipment and components that comply with the requirements of these specifications. Equipment or components that do not provide the performance and features required by these specifications are not acceptable, regardless of manufacturer.

2.01.02 Computer and OS

A. The system shall use a server computer that communicates with a client computer or computers. It shall be possible to install the system software so that one computer functions as server and client.

B. The system uses an IDenticard Windows Service, Database Service and components requiring Internet Information System (IIS). It shall be possible to install the IDenticard Windows Service, Database Service and the components requiring IIS on the same or separate computers within a network.

C. The system server computer shall have a 1.8 GHz (minimum), 2.1 (recommended) or faster processor (Intel® Core 2 Quad or equivalent or higher (recommended) or Intel® Core 2 Duo or equivalent (minimum)), a minimum of 1536 MB or 2 GB (recommended) of RAM, 1 GB of free space on the hard drive for the PremiSys software, plus space for data; a CD-ROM drive or DVD drive or network connection; a 1024 x 768 24-bit video card; and a 10/100Base-T network interface card. The server computer shall have available as well COM ports if needed for the connection of system controllers using serial communications or for connection to third-party devices as described elsewhere in this specification. Any system client computer shall have a 1 GHz or faster processor (Intel Pentium® 4 processor or higher (or equivalent), a minimum of 1024 MB of RAM, 650 MB of free space on the hard drive for the PremiSys LT software, plus space for data; a CD-ROM drive or DVD drive or network connection; a 1024 x 768 24-bit video card; and at least two USB ports for camera and printer.

D. The recommended operating system software for servers with all components installed shall be Microsoft® Windows Server® 2008 (R1 or R2); Microsoft® Windows® 7 Professional; or Microsoft® Windows Server® 2003. The minimum operating system software for servers with all components installed shall be Microsoft® Windows Server® 2003. The minimum operating systems for clients shall be; Microsoft® Windows® 7 Professional or higher; Microsoft® Windows Vista® Business or higher; or Microsoft Windows® XP Professional with Windows® Service Pack 2 or higher. The computer on which the components requiring IIS are installed shall have the Internet Information System (IIS) installed and enabled. All

clients and servers in the system shall have Microsoft® Internet Explorer® 7 and Windows® Media Player.

E. The system shall be compatible with all 64-bit Windows® operating systems, except 64-bit Windows XP®.

F. Additionally, the database installed with the access-control software of this specification shall be Microsoft® SQL Server® 2008 Express R2. If the operating system is 32-bit, the 32-bit version of SQL Server shall be installed; if the operating system is 64-bit, the 64-bit version of SQL Server shall be installed.

G. The system shall be of true multiuser design and capable of simultaneous operations from multiple client interfaces. A user logged onto any one client interface shall not affect the system control by users logged onto other client interfaces.

H. Through optional licensing, the system additionally shall allow hand-held devices based on the Apple® and Android® mobile platforms to serve as clients that are wirelessly connected to the server. The server shall be enabled to communicate with these mobile devices through a licensing process as described elsewhere in this specification. Systems that do not offer such capability to make mobile devices serve as wirelessly connected clients shall be deemed unacceptable.

2.01.03 Installation and Licensing

A. The software installation application shall allow the user/installer to install the product for the first time or install a software upgrade, when new versions of the software are made available. The installation process for these two scenarios shall not vary significantly.

B. The complete software with all components and features shall be installable at one time on one computer, using a full-installation option, by which this one computer becomes a client-server computer. This arrangement shall permit the installation of stand-alone systems. The software installation program shall also offer a client-only option to install remote clients on separate PCs.

C. In addition, the software installation application shall offer to the user installation options to accommodate multiple server configurations. Specifically, the user shall be able to independently install
1) the system's controlling service
2) the system's database service
3) the components the system uses in conjunction with Windows® IIS.
In this way, user shall be able to install these constituents of the complete application on existing, separate servers to accommodate installation sites where, for example, a separate SQL database server already exists, a separate application server is needed and a separate IIS server already exists. The installation application shall be equally capable of allowing two of items a), b) and c) above in any combination, or all three, to be installed on one computer.

D. Licenses shall be activated separately from the software installation.

E. The software shall provide an automatic upgrade alert whereby users attempting to upgrade client stations before the server is upgraded are notified that the server must be upgraded first. An upgrade function shall also be provided that automatically flags users when they log into a client that is running a version of the software older than that on the server. The server shall then be capable of automatically "pushing down" the client software to the client and installing the upgrade on the client.

F. The optional mobile application described elsewhere in this specification shall be "installed" on the server by activating a license on the server that allows the connection and use of the mobile devices. Licenses shall be available that allow connection of one (1) mobile device or ten (10) mobile devices. Multiples of these licenses can be activated as well.

G. Once the license has been activated on the server, each mobile device that the licensing permits shall be configured by the user to connect and communicate to the system server. This configuration shall be done on an individual device by device basis.

2.01.04 Communications: Host

A. The system controllers shall confirm receipt of all commands from the PC to ensure that no system transactions are lost.

B. The communications between the host and connected controllers shall be continuously monitored with the host initiating all message exchange sequences. Supervision of system input points shall be provided by the controller. Failure or fault of data connections between the controller(s) and server(s) shall be indicated on the system display on a User Interface PC.

C. It shall be possible in the system to require controllers to confirm with the host computer and its cardholder database that a card presented is a valid card. The host shall respond with a command either to confirm that access should be granted or to deny access, based on information in the cardholder database resident in the host. If this option is not enabled, the normal action of the card presentation being verified against the database on the controller shall be in effect. If this option is implemented in a system, users shall be able to define a timeout value, that is, a length of time that controllers shall wait for the host to respond. If the host does not respond within this set time, the controller shall function normally to either grant access or to deny it.

D. It shall be possible to easily update firmware files on any controller and/or reboot the processor in any controller via software commands from the host.

2.01.05 Communications: Components

A. The software shall support a maximum of 254 channels per system and a maximum of 8 controllers per channel.

B. The system hardware shall support various communication methods for communication among host computers, controllers and I/O components. It shall be possible to use serial RS-232 or serial RS-485 methods as well as TCP/IP over Ethernet methods, with dependence on the communications specifications of the individual controllers. Communications between any controller and its I/O boards shall be via serial RS-485 and/or TCP/IP over Ethernet.

C. It shall be possible for system users to define the number of times the host attempts to retry to connect to a controller before the controller is considered offline by the system. The range of times shall be 0 - 32,767.

D. System integrators shall be able to enable or disable communication to individual I/O boards and select the speed to communication between each. The baud rate of communications among the controllers and I/O boards shall be user-selectable from among the following: 2400; 9600; 19,200 and 38,400. If legacy IDenticard® Series 9000™ hardware is incorporated into the system a specific baud rate must be used (see Legacy Hardware paragraph below).

2.01.06 Downloading

A. System administrators or other authorized users shall be capable of downloading any selected or all system setup parameters and databases to any selected or all system controllers. The system software shall indicate when any download is complete, and it shall be possible to optionally view a log of download details.

B. Certain modules and features in the system shall provide the user with a message or other indication to the user notifying him or her that a download is required for these features' various settings to take effect.

2.01.08 System Security and User Rights

A. For each application-level user of the system, it shall be possible for the administrator to define the user name, enter the full first and last names of the user, and define a password. It shall also be possible to establish activation and expiration dates for the user account in the system. Passwords permissible for use in the software shall conform to default Windows®-based requirements.

B. It shall also be possible for the administrator to use the network user names and passwords of LDAP users.

C. When the software opens, a login window shall appear and prompt the operator to enter his or her system user name and password. If the login attempt fails, the

software shall indicate the nature of the failure, i.e., incorrect password or invalid user name. In addition, each time that this login window appears, it shall display the user name of the last user to log into the system on that computer.

D. The software shall include a system-administration application that allows administrators to manage operator accounts. Administrators shall be able to create groups having specific assigned rights and then to add operators to these groups and manage these groups. The administrators may edit any settings regarding an operator, in accordance with their own administrative rights within the system.

E. It shall be possible to specify particular cardholder record screens to open by default when a specific operator opens a cardholder record without choosing a particular data-entry screen to use.

F. The software shall enable administrators to assign time periods to users, which determine the days and times during which group rights are valid. Time periods can be associated with groups or users. Operators shall be able and need to enter a unique name as part of the definition of any time period.

G. The software shall provide a method to limit the cardholder records a user may view and modify, in accordance with other system permissions. This method, termed cardholder filtering, allows the security administrator to create criteria to filter cardholder records and then assign the cardholder filter to groups of users so that only the records that meet the criteria are displayed for the logged-in users. If no such filter is assigned to a group of users those users shall be able to view all cardholders in the system unless the user belongs to another group that is assigned a cardholder filter. The software shall also provide a means by which users in a group can always see all cardholders; cardholder filtering shall not apply to them.

H. The software shall provide a means to limit the hardware and other system objects that can be accessed in the software by users. This method, termed hardware filtering or permissions, allows the security administrator to "Allow" or "Deny" groups of users specific rights to Add or Edit, View, Delete, or perform Actions on the system objects. If a user belongs to more than one group and one group is denied permission, the Deny permission takes precedence. A user can be allowed or denied any or all of these permissions in any combination to result in the filtering deemed necessary by the security administrator. Systems incapable of filtering hardware from specific users' ability to view, add, edit, delete or perform actions shall be deemed unacceptable.

I. System users who are to use the optional mobile application as described elsewhere in this specification shall be given specific rights to use mobile devices through the mechanism described in Paragraph 4 above. Systems that cannot so limit which users are capable of accessing the mobile application shall be deemed unacceptable. The users with this right shall be able to log into the system using the login that they use at any other client in the system. Users shall be able to enter LDAP logins, if that is how their system has been configured.

J. Administrative system users shall be able to revoke specific licenses assigned to specific devices if needed for security purposes. The access-control program shall provide a means whereby administrative users can view which devices are using licenses and individually revoke any license that should be suspended so as to prevent the device from accessing the system. This right to revoke licenses shall be a separately selectable right available for assignment as needed to administrative users of the system. This right shall be different from the one described in the previous paragraph.

K. It shall be necessary for users to define names for their individual hand-held mobile devices so that the system can recognize the device as a valid system client. As an extra security option the system shall allow the user to define a PIN to use for logging into the mobile device in lieu of entering the user's password.

2.01.09 User Interface

A. The User 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 users complete access on one screen to all system functions and system setup parameters to which the users have rights.

B. Users shall be able to design, store and display multiple, individually created screens used to display cardholder information and data. The system shall support an unlimited number of user-defined screen layouts that shall accommodate the data fields in the system. The system shall additionally be built and delivered with a standard, ready-to-use data-entry screen. This product-standard screen shall be able to be modified and saved under a new screen name by the user.

C. A data-entry screen shall be assignable to a system user for automatic display when that user logs in. It shall be possible to define default screens that always appear when a particular user logs onto the system. The system software shall allow an authorized user to select an appropriate screen layout from a menu on a per-client interface basis.

D. The user interface shall provide windows and other controls for viewing system cardholder activity; monitoring and acknowledging alarms; and monitoring and controlling input points, relays and door configurations.

E. The optional mobile application used with the access control software shall present its own user interface, tailored for use on mobile devices and featuring controls commonly employed on such devices. This mobile user interface shall allow users to work with a limited set of features and modules suitable for mobile devices. The GUI shall appear on the device after the user downloads the mobile application from the relevant platform's online store – the iTunes® store or the Android® Marketplace – after the mobile application server has the relevant licensing and after the device has been configured to communicate to this server.

2.01.10 General Software, GMT, and Time

It shall be possible to retrieve the system time of a host and store it within the controller(s). Users shall be able to assign local and daylight saving time offsets from GMT for use on individual controllers. The system shall be able to support the time functions of controllers across multiple time zones. For transaction logging, the controller shall use the host's system time, which has been synchronized with the GMT; however, transactions appearing in the log can be configured to display time stamps showing local time. The controller shall use this local time, with an optional daylight saving time offset described in this specification, for schedules and time zones.

2.01.11 Access Control Cards

A. The system shall allow data to be entered to stipulate dates for the following parameters: card-activation dates, card-deactivation dates, vacation-start dates and vacation-end dates.

B. It shall be possible in the software to designate a cardholder as exempt from area tracking for antipassback purposes. In addition, cardholders' records can include settings that allow them to benefit from extended time at doors and readers as specified under the Americans with Disabilities Act (ADA).

C. The system shall allow a user to copy a cardholder's card settings to create an additional card for that cardholder. All card settings other than the card number are copied to the additional card.

D. The system shall allow a user to reassign a cardholder's card settings to create a new card for that cardholder. All card settings other than the card number are copied to the new card.

E. The system shall provide the means to assign multiple access control cards to a single cardholder record so that the user is not required to enter duplicate cardholder information for each card.

F. When a user is accessing the system via a hand-held device running the mobile application, the following access card parameters shall be available for editing: active/inactive status; activation and deactivation dates; and access group selection. The mobile device shall be capable of displaying a list of all the cards that a particular cardholder may have. Any of these cards can be selected for editing as described above.

2.01.12 Block Add and Block Update for Cardholders with Cards

A. The system shall provide the means to add a block of cardholder cards in such a way that each card is assigned a card number unique within the system. The user shall be able to select the number of cardholder records to be created in the system.

The user shall be able to select a starting number for the block of cards so that card numbers in the system can be reused. The means shall exist to overwrite cards with the same number and reassign those numbers to the new cardholders if the user selects the option.

B. The system shall provide the means to assign the same settings to all cards for the following fields: activation and inactivation dates; vacation start and end dates; use count settings to be used with use limits as outlined elsewhere in this specification; antipassback settings to be used with antipassback as outlined elsewhere in this specification; ADA (Americans with Disabilities Act) timing settings; access groups as outlined elsewhere in this specification; user levels as outlined elsewhere in this specification. Systems incapable of creating large blocks of cards with such time-saving card-creation capability shall be deemed unacceptable.

C. It shall be possible as well for users to update blocks of existing cards to add new data to them or to edit or delete the data that is already there. The means of accomplishing this block update process shall be essentially identical to that used to add blocks of cards. However, the software shall allow the user to use cardholder searches (described elsewhere in this specification) for defining the block of cards to update. The search criteria can be any values stored in the database of cardholder information, including the card numbers. All card parameters and attributes that are used to create individual cards or blocks of cards shall be available for selection for modification in the block update module.

2.01.13 Global Access Groups

A. The software shall permit the configuration of access groups that consist of doors and/or elevators from multiple controllers and sites. Such access groups shall be termed "Global Access Groups." It shall be possible to create up to 32,000 global access groups in the system.

B. It shall be possible to establish up to 32 access groups per cardholder per controller that designate the permissible readers that cardholders may use and the time zones, or schedules, during which they may be used. By defining the permissible readers, the areas to which each cardholder has access rights shall thereby be defined. This definition of access rights in the system shall allow access to any cardholder if a particular time zone is active at a particular reader, that reader is part of the access group, and all other access-rights tests prove valid for that cardholder.

C. Administrative users of the system shall be able to control which users of the system are permitted to create and delete global access groups, and to assign global access groups to cardholder cards,. These permissions shall be applied on a user-group basis, and so provide the capability to "filter out" specific access groups from view and use by specific users when they are logged into the system.

D. Through the use of the elevator access groups, it shall be possible to define elevator operation for normal business hours, operation after hours, on weekends and during special events. It shall be possible as well to define a "default" floor-access

scheme that controls the access of noncardholders.

E. The software shall provide a means by which users can remove one or more doors and/or elevators from all global access groups in the system.

F. A warning message shall appear to the user when assigning a particular access group to a card causes the limit of 32 access groups per cardholder per controller to be exceeded.

G. A warning message shall appear to a second user who attempts to save configuration changes to an access group that was previously opened by another user and is still open for viewing or editing by that first user. This warning shall alert the second user that his or her modifications to the access group shall not be saved. It is the first user's changes that are saved. The second user shall be free to configure his or her settings at a later time after the first user has finished configuration.

2.01.14 Antipassback, Areas

A. The software shall permit the configuration and use of several forms of antipassback, all under the basic classifications of: 1) Reader-based antipassback, which shall prevent the same card from being used at the same reader within a defined space of time. If a card is presented more than once before the defined time has elapsed, presenting the card shall not permit access to be granted; 2) Area-based antipassback, which shall allow "tracking" of entries into and exits out of defined areas. These area designations shall correspond to an area reference and shall be assigned to door configurations in the software. The door shall have a defined area in which it is located and a defined area into which the door leads. "Hard" antipassback rules shall prevent the user from moving between areas without using the card reader. "Soft" rules shall permit access when those rules are violated, while recording the antipassback violation as a transaction.

B. It shall be possible to "reset" an individual cardholder's antipassback status whenever desired, by granting a "free antipassback pass" to the cardholder, as well as to globally grant "free antipassback passes" that apply to all cards downloaded to a specific controller.

C. Means shall exist in the software to configure up to 128 access areas per controller, these areas being used for antipassback configuration.

D. The system shall be capable of saving the time, date and access-control reader number of the last entry for all cardholders as they move through the access-controlled facility for the purpose of antipassback.

2.01.15 Use Limits

It shall be possible to define for any card in the system a set number of times that the card can be used at readers configured to count card uses. The number of uses

remaining on a card shall be decremented when the card is presented for access at a reader that is configured to be used to implement this feature. It shall be possible to require any system reader to decrement a use count for a card. It shall be equally possible for a card to be used at readers that do not decrement the use count of that card.

2.01.16 Holidays and Time Zones

A. There shall be no limit on the number of time zones and holidays defined in the system other than limits imposed by the amounts of memory allocated and used in controllers in the system.

B. It shall be possible to define blocks of time over the course of one or more days - up to seven days per calendar week - that are used for controlling access and initiating or halting automated operations. These blocks of time are termed time zones and shall consist of one to six individual time intervals that are set to span various hours of the day. It shall be possible to activate or deactivate time zones based on triggers or procedures defined elsewhere in the system software. It shall also be possible to temporarily alter or override time zones using direct commands and/or holidays - days during which the interval is disabled. An inactive time zone shall be automatically activated at the moment any of its intervals becomes active (reaches its start time). An active time zone shall be automatically deactivated at the moment its last active interval becomes inactive (elapses past its end time). Via a direct command from the host to a controller, users shall be able to activate an inactive time zone and deactivate an active time zone, or a time zone can be allowed to return to its normal state (release from override). Users shall also be able set the time zone override to persist until the next direct command, or it can be set to resume automatic control the next time the interval status changes.

C. Holidays shall be configurable in the system to specify exceptions to the day-of-week schedules defined for any time zone. In this way, the holiday shall provide a break in the schedule the time zone creates. Holidays shall be definable by the date and duration of the holiday and its type. It shall be possible to create system holidays that span more than one day. The maximum number of days that can be set up for a holiday duration is 32,767. The holiday type shall be used to group holidays together and to designate schedules that are active when a holiday of a certain type occurs. When a holiday is active, it shall supersede the normal time-zone interval settings.

D. It shall be possible to configure a holiday in such a way as to override all time zones in a system and essentially disable most granting of access and all time-zone dependent functions. In addition, by the assignment of holiday types to intervals in a time zone, it shall be possible to cause the holiday to be in effect for only a portion of a day, allowing partial-day holidays.

E. The user shall be able to select an option within the software that automatically deletes holidays that have passed.

2.01.17 Daylight Saving Time

A. Users shall be able to allow for worldwide time zone offsets and daylight saving time offsets on an individual controller basis. The controllers shall be able to hold 20 date pairs for daylight saving time, allowing the creation of a 20-year span of current and future daylight saving time schedules.

B. The user shall be able to select an option within the software that automatically deletes configurations for daylight saving times that have passed.

2.01.18 Duress Codes

A. The system shall allow the configuration and use of duress codes. Duress codes shall consist of modifying current card numbers in such a way as to make them unique to each cardholder and recognizable system-wide. A duress code that is the same for all cardholders in a system shall be deemed unacceptable.

B. It shall be possible to deny access to an entered duress code on a reader-by-reader basis.

2.01.19 Card Formats

A. Users shall be able to select ABA and Wiegand reader card formats. Up to eight card formats shall be selectable per reader. The software shall accommodate multiple formats to allow the use of badges with different facility codes or different data lengths. These card data formatting capabilities shall allow the use of different reader technologies without modification to the software. The system shall support readers (with or without keypads) using magnetic-stripe, proximity, smart-card and biometric technologies.

B. The software shall allow the configuration of multiple card formats to allow the use of badges with different site/facility codes and/or different data lengths. The maximum value for a facility code shall be 32 bits.

C. The system shall support the use of cards with Wiegand or ABA formats, to accommodate magnetic-stripe, bar-code, smart-card, proximity and other cards.

D. The software shall work with a unique identifier block on the identification card that contains a cardholder ID of up to 19 digits (64 bits), an optional issue code to uniquely identify lost and reissued cards and an optional PIN of up to 15 digits.

2.01.20 User Levels

The software shall allow individual card records to be designated so that selected controller triggers can be linked to those cards. These designations are termed user levels and shall be provided to enable cardholder cards to be used as triggers in triggers and procedures as defined in this specification. It shall be possible to

establish in the software up to 256 user levels, which shall then be capable of being assignable to individual cards. It shall also be possible to assign up to seven user levels to a single card. The software shall allow a single user level to be assigned to more than one card or cardholder. The user shall as well be able to define specific doors within a group of doors at which the triggers shall work.

2.01.21 Photo Recall

A. The system shall provide the means to display a cardholder photo on the system-monitoring screen when the cardholder presents a card at a system reader. The default display is a grid with the most recent cardholder photo in the top left corner and the previous 11 photos displayed as smaller versions in three rows.

B. Users shall be able to create customized photo recall configurations using one of the following layouts: a basic 1x8 grid with all 8 photos the same size; a basic 2x8 grid with all 16 photos the same size; an advanced 3x8 grid with the most recent photo in the top left portion of the screen and the other 20 photos displayed as smaller versions in three rows; an advanced 3x5 grid with the most recent photo in the top left portion of the screen and the other 11 photos displayed as smaller versions in three rows; an advanced 4x5 grid with the two most recent photos in the top left and middle portions of the screen and the other 12 photos displayed as smaller versions in the four rows; an advanced 5x8 grid with the two most recent photos in the top left portion of the screen and the other 2 photos displayed as smaller versions in five rows.

C. Users shall be able to specify the door and/or elevator readers that shall cause a specific customized photo recall layout to display when monitoring and controlling the system. The system shall allow a combination of any or all doors/elevators to be selected in the configuration for the customized layout and such doors/elevators can be from any part of the system.

D. The system shall provide the means to display additional cardholder and card information in a details section of the photo recall display. The specific database fields containing the information shall be selectable by the user upon configuration of the customized photo recall display, including but not limited to the first and last name, card number, phone number, department and automobile information.

2.01.22 Alarm Acknowledgements

A. The software shall provide for alarm management capabilities. It shall be possible to set up system transactions or events to require alarm acknowledgement. The system shall provide user-defined alarm-handling capabilities to include easy-to-use interfaces to create alarm acknowledgement alert messages, acknowledgment response options and priority parameters, and password and comment requirements. Alarm management shall also provide for removing alarm acknowledgements from the user's display.

B. It shall be selectable by the user or administrator to display the alarm-acknowledgement window, and which types of transactions are to be displayed

shall be selectable as well. The alarm acknowledgement window shall be capable of showing all of the columns that appear in the monitor transactions window, and also allow the filtering of specified transactions, the selection of columns to display and the selection of column widths.

C. Fifty user-nameable priority levels shall be available to denote the severity of alarms. Assignment of priority levels to alarms shall provide options to require users to enter notes, usernames and/or passwords to acknowledge and/or clear alarms. In addition, through these priority assignments, users shall have options to acknowledge or clear individual alarms in one step and/or to acknowledge or clear all alarms of priorities so enabled at one time with two clicks. Users' capability to acknowledge and/or clear alarms and the method they may use are determined by permissions assigned in the security administration module of the software to users like any other permission.

D. It shall be configurable in the software to cause the alarm acknowledgement window to immediately appear "on top" of any other Windows® application running on the system computer. The system shall offer means to users to select predefined responses to describe the handling of a particular alarm. These predefined responses shall be configurable in the alarm acknowledgement module

E. The software shall provide a default sound for all alarm acknowledgment alarms. The user may optionally select customized sounds for use with specific alarm acknowledgment priority levels or triggers. The alarm sound for the highest priority level alarm shall "loop" continuously until the alarm is acknowledged and then the next highest priority level alarm will sound.

F. The optional mobile application described elsewhere in this specification shall allow users to acknowledge and clear alarms. "Fresh" alarms shall first appear in a "New" list that users can click to open a detail window where the user can respond to a new alarm as required. Users may need to enter notes (predefined or a free-typed response) or logins as described above, and after doing so, shall be able to acknowledge an alarm. The predefined responses shall be those already set up in the server. After an alarm is acknowledged, it shall disappear from the "New" list and then appear on an "Acknowledged" list. Other users with different rights shall then be able to clear the alarms in the "Acknowledged" list, at which point the alarms shall disappear from both lists. The system shall be capable of requiring notes or logins as described above to clear alarms as well.

2.01.23 Global Triggers and Procedures

A. The software shall permit the configuration of triggers and procedures that consist of points from multiple controllers and sites. Such triggers and procedures shall be termed "Global Triggers and Procedures." The user shall be able to choose whether to configure the individual elements of a trigger and procedure (actions, action groups, procedures and triggers) on an element-by-element basis or to make use of a software wizard that streamlines the configuration process.

B. The software shall provide customizable means by which users can choose an event in the system to trigger an action that the system takes. These triggers and procedures shall provide a means for event-based control as opposed to solely time-based control, although the starting and ending of time zones can be used as triggers. It shall be possible, through the use of user levels as described in this specification, to use card-generated transactions and/or system events as triggers.

C. Procedures shall be available and consist of any configurable system action to be taken in response to the triggering event. Procedures shall have sufficient flexibility so as to permit the configuration of a virtually unlimited number of system actions that can be applied to many procedures. The software shall allow, per controller up to 4096 individual actions to be included in one global action group; up to 4096 global action groups to be incorporated into one global procedure (or a limit of four action groups per procedure, if the action groups are not to cross controllers or sites); and up to 4096 global procedures. There shall be no restriction beyond the system limit given above on the number of action groups in which a single action can be included.

D. It shall be possible when configuring procedures to include a time-delay feature that shall allow the actions of the procedure to temporarily pause. The pause shall be user-configurable from 0 to 16384 seconds. Such action delays shall allow for another action to occur in the system before the system resumes the action of the paused procedure. It shall be possible to abort paused procedures during these action delays. Systems not allowing the configuration of such delay times shall be deemed unacceptable.

E. The elements of triggers and procedures – triggers, procedures, action groups and actions – shall be represented in the software by icons in their relevant configuration windows. Whenever any of these elements contain actions or points that cross controllers, these global groups shall have icons with a distinguishing "globe" icon superimposed on them to distinguish them.

F. Means shall be provided in the trigger-configuration window to allow users to edit or create time zones as defined elsewhere in this specification. These means permit "on-the-fly" editing or creation of time zones when choosing the time zone during which the trigger can occur and/or when choosing a time zone that is to act as a trigger.

2.01.24 Configuring Hardware

A. Through the software application, users shall be able to view the firmware version numbers of any controller in the system.

B. Through the software application, it shall be possible to view the total amount of memory installed in any controller as well as the amount of free memory available for use.

C. It shall be possible for system users to define the number of milliseconds between messages from the host before a controller is considered offline by the

system. The range of milliseconds shall be 10,000-65,000.

D. The system shall support the connection of a virtually unlimited number of controllers when connecting controllers using Ethernet. When connecting via Ethernet the only limits are those imposed by the user's PC memory and speed, network bandwidth and/or IP addresses available for use on the user's network. It shall be possible to connect up to 8 controllers in a "multidrop" configuration per RS-485 serial channel. It shall also be possible to connect one controller per RS-232 serial channel.

E. It shall be possible through the software to disable individual I/O boards in the system for any reason.

F. The hardware boards to which readers are connected shall indicate and generate a transaction in the system if a "forced-open" or "door-ajar" are detected at the door/reader connected to the hardware board.

G. When configuring any item of hardware it shall be possible in the system software to choose the settings of that particular item as the settings "template" that is used by default for the settings of all other items of the same type throughout the system. The user has the capability of temporarily disabling this choice at any time and then later re-enabling it if desired.

H. The user interface shall provide the means to add system objects using the "right-click" method.

I. In the right-hand pane for each tabbed page of the Hardware Configuration window, the user has the option to display the objects as large icons with the object name, as a list of object names with small icons or as a detailed list of names and descriptions of the objects.

2.01.25 Doors and Reader Settings

A. It shall be possible to connect controllers to reader boards so that the system has a maximum of forty (40) readers, including those readers attached to controllers with onboard reader ports.

B. When inputs change state virtually simultaneously, they shall normally be processed sequentially from low input-point numbers to high numbers on any I/O board. However, the software shall provide a setting to reverse the processing sequence of two input points wired as door-position and request-to-exit points to prevent the processing of information in the incorrect order when these two inputs appear to change simultaneously. For example, if the REX input is wired to a higher point number than the door status (door-position input point), the door-open event is processed before the REX, and so the system reports that the door was forced open (the door opens before the REX is received). This setting changes the order in which

these two inputs are processed, to report the events in the proper order.

C. The software shall be capable of permitting readers to support the following basic reader access modes: unlimited access; exit only, no entrance access; disabled; access on valid facility code alone; access on valid card number alone; access on valid PIN code alone; access on valid PIN code AND card number; access on valid PIN code OR card number.

D. The system shall be capable of generating a transaction indicating whether a controlled door was opened and used after a valid card is read and the associated door unlocked.

E. The system shall permit the configuration and use of master and slave readers for use as, for example, "in" and "out" readers for antipassback. The slave reader shall make access requests to the master reader, and the two readers are handled by the software as a single reader.

F. It shall be possible to activate the relay controlling a door lock subsequent to an access-granted for a range of time from 1 to 255 seconds, in one-second increments. It shall also be possible to configure a door-lock relay to energize when activated (termed the "Normal" mode) and to de-energize when activated (termed the "Inverted" mode). In addition, it shall be possible to allow the door to relock as soon as the door opens or upon the door closure.

G. The reader port, door-position-input point and the request-to-exit input point (REX) for a reader-door shall be established by default, when the automatic generation of doors is selected as a part of reader-board setup; however, users of the system shall be able to easily redefine any DPIP or request-to-exit input point they need.

H. The system shall allow alternate readers to be set up to work concurrently with another reader to control one door. An alternate reader shall be useful, for example, as a reader placed higher than the main reader at a parking lot entrance for use by truck drivers whose vehicles are taller than passenger cars.

I. It shall be possible to select in the system whether it is desired to log a transaction indicating that access was granted to a cardholder before the system verifies that the door was actually used. Select this option so that as soon as access is granted, a transaction is logged indicating that the cardholder accessed the area, whether or not the door was used.

J. The system shall allow doors to be configured so as not to energize the door-lock relay upon a REX.

K. The system shall allow doors to be configured so as not to display all change-of-state transactions occurring at the door.

L. The system shall allow doors to be configured so as to require two cards to be presented within 10 seconds of each other at the door's reader for the cardholders to enter or exit.

M. Cardholders shall be able to use the keypad to enter the card numbers at doors that have been configured in the software to allow direct entry of card numbers at keypad readers.

N. It shall be possible to select from three different sets of default settings to control LED action on readers so enabled.

O. The system shall be capable of generating prealarm transactions that can serve as alerts that a door is about to go into a door-ajar state. It shall be possible in the software to specify a defined number of two-second units at which the prealarm should be generated before the door goes into the door-ajar state.

P. It shall be possible to select an antipassback delay to apply to any reader configured for time-dependant antipassback. The range of values in seconds that can be selected is 0-255, in one-second increments.

Q. The system and software shall support the configuration of separate setups for readers and doors so as to comply with requirements provided for under the Americans with Disabilities Act (ADA).

R. It shall be possible in the software to choose alternate door-strike time and held-open time for use as part of a "special door cycle" for ADA compliance. This door-strike time shall range from 0 seconds through 255 seconds. The held-open time shall consist of specifying the number of two-second ticks, and the number of ticks is selectable from the range of 0 through 32757.

S. It shall be possible for the system to log card presentations in a transaction log at a reader which is in an unlimited-access mode.

T. The user shall be able to create global access groups that pair the access-controlled doors of the building with system time zones to specify the doors at which cardholders are permitted access and at which times of the day and days of the week.

2.01.26 Monitor Points

A. Input points shall have standard supervision configurations that allow the input to be wired normally closed or normally open, or to be wired with selective resistance on the point to allow 1000 ohms resistance as the normal state and 2000 ohms as the active state or 2000 ohms resistance as the normal state and 1000 ohms as the active state.

B. Users shall be able to configure custom debounce times and motion-detector delays in the system. The number of successive input scans (debounce) shall have the range of 2-15, and the range of possible motion-detector delays shall be 0-15.

C. The system shall allow the "masking," or shunting, of monitor points to suppress event reporting for changes between active and inactive input conditions. However, it shall be possible as well to allow users to select an option to report changes even when inputs are masked.

2.01.27 Control Points

It shall be possible to set the output points (relays) used as control points (non-door-lock relays) to have "normal" or "inverted" action, as described in this specification. Other actions are as described elsewhere in this specification.

2.01.28 Elevators

A. The system shall accommodate access control at elevators by establishing the floor or floors to which a cardholder may have access from an elevator car. The user shall be able to define within the software which reader or readers are for use inside elevator cars. Feedback to the system on the cardholder's floor selection shall not be provided.

B. Outputs in the system shall be assignable to the floor-selection buttons inside the elevator car, one per access-controlled floor, per car. Although a single floor may be assigned more than one output for more than one car, the system shall allow only those outputs controlling buttons in the elevator car where the cardholder presented the card to work. Regardless of elevator access level assignments (as described elsewhere in this specification), outputs controlling buttons in other elevator cars shall not be affected.

C. The user shall be able to create access groups that pair the access-controlled floors of the building with system time zones to specify the floors to which cardholders are permitted access and at which times of the day and days of the week.

D. Once a cardholder selects a floor in an elevator car, the system shall disable all other valid floor selections for that cardholder to prevent access to unauthorized floors by other people in the car, regardless of whether they are valid cardholders or not.

2.01.29 Global Monitor Point Groups

A. The software shall permit the creation of global groups of monitor points. Users shall be able to select monitor points from any site in the system to create a global monitor point group. These global groups shall have icons with a distinguishing "globe" icon superimposed on them to distinguish them as global features. Specific settings of points in the group shall be able to be changed "on-the-fly" through a

monitor and control means as described in this specification.

B. The software shall provide an easy search feature that allows users to search on a string of characters that occur in any part of the names of any element defining the points in the global group in order to quickly find specific global groups.

2.01.30 Global Control Point Groups

A. The software shall permit the creation of global groups of control points. Users shall be able to select control points from any site in the system to create a global control point group. These global groups shall have icons with a distinguishing "globe" icon superimposed on them to distinguish them as global features. Specific settings of points in the group shall be able to be changed "on-the-fly" through a monitor and control means as described in this specification.

B. The software shall provide an easy search feature that allows users to search on a string of characters that occur in any part of the names of any element defining the points in the global group in order to quickly find specific global groups.

2.01.31 Global Door Groups

A. The software shall permit the creation of global groups of doors. Users shall be able to select doors from any site in the system to create a global door group. These global groups shall have icons with a distinguishing "globe" icon superimposed on them to distinguish them as global features. Specific settings of the doors in the group shall be able to be changed "on-the-fly" through a monitor and control means as described in this specification.

B. The software shall provide an easy search feature that allows users to search on a string of characters that occur in any part of the names of any element defining the points in the global group in order to quickly find specific global groups.

2.01.32 Global Elevator Groups

A. The software shall permit the creation of global groups of elevators. Users shall be able to select elevators from any site in the system to create a global elevator group. These global groups shall have icons with a distinguishing "globe" icon superimposed on them to distinguish them as global features. Specific settings of the elevators in the group shall be able to be changed "on-the-fly" through a monitor and control means as described in this specification.

B. The software shall provide an easy search feature that allows users to search on a string of characters that occur in any part of the names of any element defining the points in the global group in order to quickly find specific global groups.

2.01.33 Global Alarm Point Groups

A. The software shall permit the creation of global groups of doors and monitor points from any site in the system. These global groups shall have icons with a distinguishing "globe" icon superimposed on them to distinguish them as global features. Specific settings of points in the group shall be able to be changed "on-the-fly" through a monitor and control means as described elsewhere in this specification.

B. The software shall provide an easy search feature that allows users to search on a string of characters that occur in any part of the names of any element defining the points in the global group in order to quickly find specific global groups.

2.01.34 Global Elevator Floor Groups

A. The software shall permit the creation of global groups of elevator floors from any site in the system. These global groups shall have icons with a distinguishing "globe" icon superimposed on them to distinguish them as global features. Specific settings of points in the group shall be able to be changed "on-the-fly" through a monitor and control means as described elsewhere in this specification.

B. The software shall provide an easy search feature that allows users to search on a string of characters that occur in any part of the names of any element defining the points in the global group.

2.01.35 Monitoring and Controlling – Access Areas

A. Users shall be able to modify access-area settings during regular operation (as opposed to during configuration) to enable or disable the access area.

B. In the right-hand pane of the Monitor and Control tree window, the user has the option to display the points as large icons with the point name, as a list of point names with small icons or as a detailed list of names and current statuses of the points.

2.01.36 Monitoring and Controlling – Time Zones

A. The software shall allow time-zone actions to be overridden in the following ways: temporarily deactivate the time zone until it would normally change, temporarily activate the time zone until it would normally change, deactivate the time zone until a later overriding command, activate the time zone until a later overriding command; return the time zone to normal, log the time zone state in the transaction log.

B. In the right-hand pane of the Monitor and Control tree window, the user has the option to display the points as large icons with the point name, as a list of point names with small icons or as a detailed list of names and current statuses of the points.

2.01.37 Monitoring and Controlling – Antipassback

A. The software shall permit the generation of commands that disable antipassback restrictions. These commands shall be selectable for application on a per-cardholder basis or for all cardholders in the system. This command shall act as a way of (re)initializing users for area-based antipassback, as described in this specification. After the issuance of this command, which essentially acts as a "free pass" for antipassback, the movements of the affected cardholder(s) are logged and stored by the system. The issuance of this command for all cardholders shall allow all cardholders to be resynchronized with respect to antipassback. Additionally, the software shall permit the generation of a command that moves a cardholder's location to a specific area, on a per cardholder basis.

B. In the right-hand pane of the Monitor and Control tree window, the user has the option to display the points as large icons with the point name, as a list of point names with small icons or as a detailed list of names and current statuses of the points.

2.01.38 Monitoring and Controlling – Doors

A. The software shall allow users to send commands to a door in the system through a system "monitor and control" means in such a way that the door can be momentarily unlocked. The door still shall be monitored for door-ajar conditions. Any granted cardholder access that occurs during this time shall be logged. These momentary unlock commands shall be available to the user from a dialog box where door parameters may be changed for just this command.

B. It shall also be possible for a user to momentarily unlock a door in one click from a shortcut menu, unlocking the door for its default unlock (strike) time. Additional one click options from the shortcut menu shall be: unlock (free access); lock (return the door to its default access mode); photo recall (opens a photo recall window filtered for the door); and schedule (opens a setup window for one-time lock and unlock settings).

C. It shall be possible to open a dialog box allowing users to change the mode of a door "on the fly" through a system "monitor and control" means in such a way that the following reader modes can be obtained: unlimited access; exit only with no entrance; disabled; access on valid facility code alone; access on valid card number alone; access on valid PIN code alone; access on valid PIN code AND card number; access on valid PIN code OR card number. Via a shortcut menu, users shall also be able to quickly unlock a door and/or lock it using the default lock mode configured for the door.

D. Users shall be able to send commands to a door through a system "monitor and control" means in such a way that the door-position input can be set to mask or unmask (disarm or arm, respectively) the specific door point. Setting a mask suppresses alarm conditions when the input is active, and clearing the mask restores the "visibility" of the alarm in the system. It shall also be possible to view the status of the door, that is, whether or not the door-position input is active and whether or not the point is masked, through this "monitor and control" means.

E. Users shall be able to send commands in the system in such a way that the "door forced open" events at any door are "masked," that is, the appearance of these events in the transaction log is suppressed.

F. Users shall be able to send commands in the system in such a way that the "door-ajar" events at any door are "masked," that is, the appearance of these events in the transaction log is suppressed.

G. Any changes made to door settings using the "monitor and control" method shall be overwritten and the original settings restored when the relevant controller is reset in the system and the controller's database is downloaded to that controller with the original hardware configuration settings.

H. In the right-hand pane of the Monitor and Control tree window, the user has the option to display the points as large icons with the point name, as a list of point names with small icons or as a detailed list of names and current statuses of the points.

2.01.39 Monitoring and Controlling – Global Door Groups

A. The software shall allow users to send commands to a global group of doors in the system through a system "monitor and control" means in such a way that all doors in the global group can be momentarily unlocked. The doors still shall be monitored for door-ajar conditions. Any granted cardholder access that occurs during this time shall be logged. These momentary unlock commands shall be available to the user from a dialog box where door group parameters may be changed for just this command. It shall also be possible for a user to momentarily unlock a door group in two-clicks from a shortcut menu, unlocking the doors in the group for the individual default unlock (strike) time of each door in the group.

B. It shall be possible to open a dialog box allowing users to change the mode of all doors in the global group "on the fly" through a system "monitor and control" means in such a way that the following reader modes can be achieved: unlimited access; exit only, no entrance access; disabled; access on valid facility code alone; access on valid card number alone; access on valid PIN code alone; access on valid PIN code AND card number; access on valid PIN code OR card number. Via a shortcut menu, users shall also be able to quickly unlock a door group and/or lock it using the individual default lock mode set for each door in the group.

C. Users shall be able to send commands to all doors in the global group through a system "monitor and control" means in such a way that the door-position input can be set to mask or unmask (disarm or arm, respectively) the door points in the global group. Setting a mask suppresses alarm conditions when the inputs are active, and clearing the mask restores the "visibility" of the alarms in the system.

D. Any changes made to settings for the doors in the global group using the "monitor and control" method shall be overwritten and the original settings restored when the relevant controller is reset in the system and the controller's database is

downloaded to that controller with the original hardware configuration settings.

E. In the right-hand pane of the Monitor and Control tree window, the user has the option to display the points as large icons with the point name, as a list of point names with small icons or as a detailed list of names and current statuses of the points. These global groups shall have icons with a distinguishing "globe" icon superimposed on them to distinguish them as global features.

2.01.40 Monitoring and Controlling – Elevators

A. The software shall allow users to send commands to reconfigure selected elevator characteristics and settings "on the fly" through a system "monitor and control" means. These reconfigurable settings shall include the following, among others: disabling the elevator reader (no access); permitting unlimited access; granting access to any card with a valid facility code; requiring presentation of both a card and PIN; and requiring presentation of a card or PIN.

B. A user shall be able to send a command to temporarily energize the elevator buttons for a specific floor or for all floors to allow an occupant of the elevator to select one of those floors.

C. Any changes made to elevator configurations using the "monitor and control" method shall be overwritten and the original settings restored when the relevant controller is reset in the system and the controller's database is downloaded to that controller with the original hardware configuration settings.

D. In the right-hand pane of the Monitor and Control tree window, the user has the option to display the points as large icons with the point name, as a list of point names with small icons or as a detailed list of names and current statuses of the points.

2.01.41 Monitoring and Controlling – Global Elevator Groups

A. The software shall allow users to send commands to a global group of elevators in the system through a system "monitor and control" means in such a way to temporarily energize the elevator buttons for all floors on all elevators in the group or for all floors on one elevator in the group, to allow an occupant of the elevators to select any of those floors. Users shall optionally be allowed to send a command to the global group of elevators to energize the elevator button for a specific floor on one elevator in the group to allow an occupant of the elevator to select that floor.

B. It shall be possible to change the mode of all elevators in the global group "on the fly" through a system "monitor and control" means in such a way that the following reader modes can be achieved: disabling the elevator readers (no access); permitting unlimited access; granting access to any card with a valid facility code; requiring presentation of both a card and PIN; and requiring presentation of a card or PIN.

C. Any changes made to settings for the elevators in the global group using the "monitor and control" method shall be overwritten and the original settings restored when the relevant controller is reset in the system and the controller's database is downloaded to that controller with the original hardware configuration settings.

D. In the right-hand pane of the Monitor and Control tree window, the user has the option to display the points as large icons with the point name, as a list of point names with small icons or as a detailed list of names and current statuses of the points. These global groups shall have icons with a distinguishing "globe" icon superimposed on them to distinguish them as global features.

2.01.42 Monitoring and Controlling – Monitor Points

A. The software shall allow users to send commands to a selected monitor point in the system through a system "monitor and control" means. These commands shall consist of setting or clearing the mask (disarming or arming, respectively, the point) for the specific monitor point. Setting a mask suppresses alarm conditions when the input is active, and clearing the mask restores the "visibility" of the alarm in the system. It shall also be possible to view the status of the monitor point, that is, whether or not the input is active or inactive, through this "monitor and control" means.

B. Any changes made to monitor point settings using the "monitor and control" method shall be overwritten and the original settings restored when the relevant controller is reset in the system and the database is downloaded to that controller with the original hardware configuration settings.

C. In the right-hand pane of the Monitor and Control tree window, the user has the option to display the points as large icons with the point name, as a list of point names with small icons or as a detailed list of names and current statuses of the points.

2.01.43 Monitoring and Controlling – Global Monitor Point Groups

A. The software shall allow users to send commands to a monitor point group consisting of monitor points and doors (on one controller) through a system "monitor and control" means. These commands shall consist of setting or clearing the mask for all monitor points and door position inputs in the group. Setting a mask suppresses alarm conditions when the inputs are active, and clearing the mask restores the "visibility" of the alarms in the system.

B. The software shall allow users to view the status of the monitor point group, that is, whether or not any inputs are active, through this "monitor and control" means.

C. Any changes made to monitor point and door settings using the "monitor and control" method shall be overwritten and the original settings restored when the relevant controller is reset in the system and the database is downloaded to that

controller with the original hardware configuration settings.

D. In the right-hand pane of the Monitor and Control tree window, the user has the option to display the groups as large icons with the group name, as a list of group names with small icons or as a detailed list of names and current statuses of the groups. These global groups shall have icons with a distinguishing "globe" icon superimposed on them to distinguish them as global features.

2.01.44 Monitoring and Controlling – Alarm Point Groups

A. The software shall allow users to send commands to an alarm point group consisting of monitor points and doors (from any controller in the system) through a system "monitor and control" means. These commands shall consist of setting or clearing the mask for all monitor points and door position inputs in the group. Setting a mask (disarming) suppresses alarm conditions when the inputs are active, and clearing the mask (arming) restores the "visibility" of the alarms in the system. It shall also be possible to send other commands to arm or disarm active or inactive points only if one or more points are active or inactive, respectively.

B. The software shall allow users to view the status of the alarm point group, that is, whether or not any inputs are active, through this "monitor and control" means.

C. Any changes made to monitor point and door settings using the "monitor and control" method shall be overwritten and the original settings restored when the relevant controller is reset in the system and the database is downloaded to that controller with the original hardware configuration settings.

D. In the right-hand pane of the Monitor and Control tree window, the user has the option to display the groups as large icons with the group name, as a list of group names with small icons or as a detailed list of names and current statuses of the groups. These global groups shall have icons with a distinguishing "globe" icon superimposed on them to distinguish them as global features.

2.01.45 Monitoring and Controlling – Control Points

A. The software shall allow users to send commands to a selected control point in the system through a system "monitor and control" means. These commands can be entered through a dialog box and shall consist of turning the control point on (energizing a relay with normal function or de-energizing a relay with inverted function), turning it off (de-energizing a relay with normal function or energizing a relay with inverted function), pulsing the control point in a single pulse of 0-32,767 seconds; or pulsing the control point repeatedly (if the control point is not a relay on legacy hardware), with on-times and off-times in 0.1-second steps and a selectable repeat count, and with all repeated-pulse setting values ranging from 0 to 255. Actions for off, on, pulse for a default duration and pulse for a custom duration (0 to 32,767 seconds) shall be selectable in two clicks using a shortcut menu.

B. The software shall allow users to view the status of the control point, that is, whether or not the point is energized, through this "monitor and control" means.

C. Any changes made to control point settings using the "monitor and control" method shall be overwritten and the original settings restored when the relevant controller is reset in the system and the database is downloaded to that controller with the original hardware configuration settings.

D. In the right-hand pane of the Monitor and Control tree window, the user has the option to display the points as large icons with the point name, as a list of point names with small icons or as a detailed list of names and current statuses of the points.

2.01.46 Monitoring and Controlling – Global Control Point Groups

A. The software shall allow users to send commands to a global group of control points in the system "on the fly" through a system "monitor and control" means. These commands shall be identical in initiation and function to those available for single control points as described above in this specification, except that pulsing for a default duration shall consist of each individual control point in the group pulsing for its own configured default duration.

B. Any changes made to the settings for the control points in the global group using the "monitor and control" method shall be overwritten and the original settings restored when the relevant controller is reset in the system and the database is downloaded to that controller with the original hardware configuration settings.

C. In the right-hand pane of the Monitor and Control tree window, the user has the option to display the points as large icons with the point name, as a list of point names with small icons or as a detailed list of names and current statuses of the points. These global groups shall have icons with a distinguishing "globe" icon superimposed on them to distinguish them as global features.

2.01.47 Monitoring and Controlling – Photo Recall

A. The system shall provide the means to view a cardholder photo when a card is presented at a reader in the system. This photo recall window shall have a default configuration as well as options to configure customized photo recall layouts, as outlined elsewhere in this specification.

B. The user shall be able to enlarge any photo in the photo recall display by moving the mouse cursor over the photo in the layout.

C. The system shall automatically display a red border around a photo to visually identify the photo as representing a card that was denied access at a reader configured for the photo recall display.

D. The user shall be able to expand the photo recall display to view additional cardholder and card information as selected for the customized photo recall configuration. The user shall additionally have the option to open the specific cardholder record directly from the photo recall window.

E. The software shall allow a user to display in the photo recall window the doors and time zones to which a cardholder has rights when that cardholder's card is presented at a reader.

2.01.48 Monitoring and Controlling – Procedures

A. The software shall enable users to alter how procedures resulting from triggers are executed through a system "monitor and control" means. These means shall allow procedures to be aborted, executed or resumed. Aborting a procedure shall stop a procedure during a delay action (in other words, while it is delayed) and all subsequent actions after the delay. Executing a procedure shall cause all the actions in the procedure to occur. Resuming a procedure shall execute actions remaining in a procedure if the procedure is in a delay.

B. Changes made to the system through triggers and procedures using the "monitor and control" method shall be overwritten and the original settings restored when the relevant controller is reset in the system and the database is downloaded to that controller with the original hardware configuration settings.

C. In the right-hand pane of the Monitor and Control tree window, the user has the option to display the points as large icons with the point name, as a list of point names with small icons or as a detailed list of names with optional descriptions of the points. These global procedures shall have icons with a distinguishing "globe" icon superimposed on them to distinguish them as global features.

2.01.49 Monitoring and Controlling – Transactions

A. The software shall provide a monitor-transactions window that reports all system events and activity, such as access-granted and access-denied transactions, alarm states, door activity, change-of-state information and the like. The transactions appearing in this window shall not only report system events, but their appearance shall define the starting point of system triggers that initiate system actions via the triggers and procedures as defined in this specification.

B. Users shall be able to configure the monitor-transaction window to display all or selected columns of information and/or to otherwise filter the display of information in the window, as described below. This configuration shall be selectable by means of the user's login, and it shall be possible for any login to have its own configuration. Systems incapable of such configuration of the monitor-transaction window shall be deemed unacceptable.

C. The software shall allow users to define the number of rows of transactions to display in the window, as well as selecting whether the most recent transaction appears at the top or at the bottom of the list in the window.

D. The software shall allow users to define the transaction source(s) of the displayed transactions, for example, whether all transactions appear or only those from I/O boards, or only those relating to access areas, etc. Users shall also be able to exclude from display in the monitor transactions window certain kinds of transactions, specifically, 1) request-to-exit transactions, 2) "Trigger Active" transactions, 3) "Execute Procedure" transactions, 4) "Resume Procedure" transactions and 5) "Procedure with No Actions" transactions.

E The software shall allow users to define the site(s), channel(s), and controller(s) whose transactions are to be displayed in the monitor-transactions window. This feature shall allow only user-specified information to be displayed in the window.

F. The software shall allow users to customize the color and text used to display each type of transaction in the system making the transactions more visually-identifiable and text-specific for the users monitoring the system.

2.01.50 Monitoring and Controlling – User Commands

A. Users shall be able to use keypads connected into the system for the purpose of sending commands to the controllers. These commands shall be either commands that allow a cardholder number to be entered at the keypad (see elsewhere in this specification), or user commands that trigger a specific action in the system.

B. It shall be possible to send user commands as numeric codes entered through a card-reader keypad to the controllers to trigger procedures (as described in this specification) in the system. The numeric code shall be entered as part of a trigger for a trigger and procedure action. User commands shall be capable of ranging from 1 to 8 digits in length.

2.01.51 Monitoring and Controlling – Component Status

Windows for the individual controllers and boards in the monitor and control "module" of the software shall permit selection and display of configurations, capacities, firmware versions, online and offline status, status of these controllers and boards as well as their individual components, (such as relays on these boards or controllers.)

2.01.52 Reports and Journals

A. The software shall provide the user with the capability to configure, customize and generate reports of system transactions, hardware and access-setting configurations, cardholders, etc. It shall be possible to output generated reports to a local or network printer or in any of the following ways (output file types in

parentheses): Microsoft® Excel spreadsheets (.xls), Adobe® PDFs (.pdf), Microsoft® Word documents (.doc), Crystal Report files (.rpt), or Rich Text files (.rtf) openable by most word processors. Users shall be able to export the generated report using an intuitive file name of their own devising. When the report is displayed on the screen, the generated report shall appear in a window with a toolbar that will allow the user to scroll to the next or a previous page, go directly to the first or last page, jump to a specific page of the report, search for user-specified text anywhere in the report, and zoom in or out on the report page. Systems unable to provide such print previewing capabilities shall be unacceptable.

B. Users shall be able to generate the following system reports:
Cardholders Report
Cardholders – Access Rights Report
Transaction History Report
Transaction History Report with Device Links
Alarm Acknowledgements Report
Access Groups Report
Sites Report
Channels Report
Controllers Report
I/O Boards Report
Inputs Report
Outputs Report
Monitor Points Report
Alarm Point Groups Report
Control Points Report
Readers Report
Readers – Access Rights Report
Doors Report
Door Groups Report
Elevators Report
Elevator Groups Report
Triggers and Procedure
Access Areas Report
Time Zones Report
Holidays Report
Card Formats Report
Maps Report
Daylight Saving Time Report
Print Journal Report
Custom Report

C. The Cardholders report shall offer two modes of presentation: a list view and a detail view. The list view shall present a user-configurable display of information, and such information can be selected from among any fields in the cardholder database. The Detail view shall present a predefined layout of specific information. Both report modes shall be capable of displaying cardholder record information for all cardholders or those meeting specific user-defined search criteria. The amount of

information displayed in the report shall depend on the size of the page and the widths of the columns in the report as selected by the user.

D. The Transaction History Report With Device Links shall have a format different from the other reports and be more like a spreadsheet in its structure. This report shall show only those transactions generated by points linked to a camera as part of the Exacq® video plug-in. For each entry in the report there shall be a hyperlink to the recorded video from the primary camera assigned to the point generating the transaction (described elsewhere in this specification). The report shall offer the same search, or filtering, criteria available for the other reports. The report shall be exportable as an Excel file without the links for printing or saving purposes.

E. The Reports feature used for cardholder reports shall allow users to define single- or compound-search, or filtering, criteria to apply to determine the names of cardholders that appear in either a list report or detailed report. These searches shall be based on any field in the cardholder database. It shall be possible to save search criteria for later use. It shall also be possible to sort the records in the report in ascending or descending order based on data appearing in one or more selected fields in the cardholder database, such as last name, department, school grade and the like.

F. The Reports feature used for system and hardware reports shall also allow users to define single- or compound-search, or filtering, criteria to apply to determine which system components or settings appear in the report. These searches shall be based on the fields in the database relevant to the selected module report. It shall be possible with these reports as well to save search criteria for later use. Records in the report shall be sortable in ascending or descending order based on data appearing in one or more selected fields in the system database.

G. There shall be a user-selectable option in the Reports window to prevent the database fields that do not contain data from appearing in the list of fields available for use as search criteria. This option shall be activated by default in the software, so unused fields do not appear as columns in the report. This feature allows a user to find the fields needed for the report criteria more quickly and easily. The user shall be free to deactivate this option and so allow all of the database fields to appear and be available for selection.

H. Users shall be able to include selected header information to appear at the tops of generated reports. Capability shall exist as well to include custom logos or other image files as part of the header information. All reports shall have default descriptive names; however, it shall be possible for users to change the name of the report as it appears in the report header "on the fly."

I. Users shall be able to save the report search criteria for any system reports and generate the report using that search criteria at a future time. Saved search criteria are saved per user and reports using the saved criteria can be used by the user to generate a report from any client in the system.

J. Users shall be able to save the report search criteria along with customized report layouts for the following system reports: Cardholders; Cardholder - Access Rights; Transaction History; Readers - Access Rights; and Print Journal reports. These reports are saved per user and can be generated at any time with the saved settings by the user while logged into the system at any client in the system.

K. For those reports whose layouts are savable as described immediately above, it shall be possible to use the SMTP Mail Server plug-in (described below) to create template e-mails to be sent to definable addressees with the reports as attachments. Users shall be able to specify the source address(es), the direct addressee(s), the carbon-copy addressee(s) and the blind-copy addressee(s), as well as customize the subject line and body of each e-mail. The output format of the attached report shall be selectable from between a PDF file and a Microsoft Excel® file. After this e-mail is defined by the user, the user shall then be able to create a schedule for its distribution. The scheduling means used for this distribution is as described below in this specification. This means shall allow the report to be sent once on a user-selected date and time or on a regular and repeated basis that the user defines, with an updated report sent each time. The user shall have the option of creating the e-mail and its distribution schedule in either the Report module or in the Scheduler module. The procedure used to create the schedule shall be the same for both options. Users shall be able to configure multiple e-mail and schedule combinations.

L. Viewing and creating reports shall be limited by a user's hardware filtering permissions and/or cardholder filters as described elsewhere in this specification.

M. Administrators shall be able to configure the software to provide user journals that identify any system users who add, modify or delete hardware configurations, cardholder information and/or cardholders' card data. The journals shall show the system name of the user, the date and time of the activity, the hardware components and/or fields that were affected, and whether affected items were created, modified/updated or deleted. It shall be possible to display the journal on the computer monitor, to export it to a Microsoft® Excel file for saving, archiving and/or printing, or to permanently delete it.

2.01.53 Mantraps

A. The software shall provide the user with the capability to set up access-controlled areas as mantraps or airlocks. The mantrap capability shall accommodate two scenarios: a) an area bounded by more than one door, but only one door leading into this area or out can be open (undergoing an access-granted-door-open cycle) at one time; b) an area serving as an airlock where one or more doors can lead into the area and one or more doors lead out, but no door leading out can ever be open at the same time when any number of the doors leading in are open (undergoing an access-granted-door-open cycle). Likewise, when any number of the doors leading out is open, no door leading in can be open.

B. It shall be possible to configure and use the mantrap capability without using antipassback in a system and vice versa. In addition, mantrap and antipassback

functions shall not interfere with one another.

C. When areas are configured for mantrap and antipassback functions, mantrap restrictions shall always be processed and implemented before the antipassback restrictions.

2.01.54 Scheduler

A. The software shall provide the user with the capability to schedule archiving of transactions, backups of the system and cardholder databases, imports of data from external data sources, one-time door lock and unlock events, and e-mailing certain system reports.

B. One-time unlock-lock, one-time lock-unlock or one-time lock-only door events can be scheduled for a single door at a single time and date. The user shall be able to schedule the event from a scheduling window or shall be able to right-click a door to schedule an event while in the Monitor and Control task.

C. Transaction archiving, data backups and data imports can be scheduled from the scheduling window or from the respective feature window as one-time events or as recurring events.

D. Recurring events can be scheduled as often as once every minute or as infrequently as once every 60 years.

E. Schedules for recurring events can be based on years, months, weeks, days, hours or minutes. These units of time can be used as specific dates (for example, the 16th day of the month) or as relative dates (for example, the first Friday of the month.)

F. Systems incapable of scheduling these system functions and events with such a range of flexibility shall be deemed unacceptable.

2.01.55 Peripherals

The system shall allow the use of commercial, off-the-shelf printers for printing of system activity reports.

2.01.56 Mapping

A. The system shall support an unlimited number of graphic files used as maps.

B. The system shall support the following graphic-file types for use as maps: bitmap (.bmp), enhanced metafile (.emf), graphics-interchange format (.gif), JPEG (.jpg), portable network graphics (.png), TIFF (.tif) and Windows® metafile (.wmf).

C. It shall be possible to display maps at the same time that other system windows (transaction windows, alarm acknowledgement windows and the like) appear on the

screen.

D. Icons on the map shall be dynamic, that is, they shall be capable of changing their appearance in response to changes in the state of the hardware that they represent.

E. It shall be possible for users to zoom in on and out from any map.

F. The system shall provide a default library of multiple icons representing access-control functions.

G. The system shall support the addition of multiple customized icons designed and devised in third-party software programs such as Microsoft® Paint and the like.

H. The system shall provide an easy drag-and-drop means to drag hardware icons from a system hardware configuration window onto any desired map to create a dynamic icon that represents and displays the state of the hardware component represented on the tree. As a result, users shall be able to monitor the system and also control the components via the dynamic icons. Software that does not incorporate such a simple means to create dynamic icons on a map shall be deemed unacceptable.

I. Maps in the software shall allow the system name of a hardware component to be displayed above or below the dynamic icon representing that particular component on the map. It shall as well be possible not to display a name. Icons on maps shall be capable of being individually resized and rotated.

2.01.57 ASCII Commands

A. The system software shall provide a module with which users can set up devices that receive ASCII commands to function. Such devices shall be made available to the software through a plug-in and are the external equipment of various third-party manufacturers. It shall be possible to activate these ASCII commands via a trigger and procedure, as described elsewhere in this specification. In this way, any system event or transaction or combinations of transactions shall be configurable to trigger a response by the third-party equipment through an action.

B. Users shall be able to configure the system to communicate with these devices via either Ethernet connections or hard-wired serial connections to a COM port on the system server computer. It shall be possible to allow only certain groups of users to view, use, etc., these configured devices by means of hardware permissions, as described elsewhere in this specification.

C. As part of the configuration of ASCII commands, it shall be possible to manually enter ASCII code strings provided by any third-party manufacturer to control these devices. In strings used to send text messages to pagers and the like, users shall be able to include variable placeholder text. The variable placeholders shall "stand in" for specific transaction information, such as transaction date and time, or the card number or cardholder's name, in the configured ASCII string. However, the

placeholders shall be replaced by the actual data from the transaction when the string is sent to the device.

D. The module shall provide a means by which users can test the commands after configuration so they do not have to generate a triggering transaction in the system on purpose in order to verify that the command is sent to the device.

E. When the system event chosen as the trigger occurs, the software shall automatically generate the ASCII code strings to control the functions of the selected device.

F. Means shall be provided in the software to easily view the license status of this plug-in and the number of licenses that are available in the system for use, if applicable. The method of displaying and working with this information shall not differ from that used for other similar plug-ins. This licensing information shall be stored on the server to allow ease of maintenance.

2.01.58 SMTP Mail Server

A. The system software shall provide a module with which users can set up an SMTP server to permit sending e-mail messages in response to system transactions and events. Such devices shall be made available to the software through the SMTP plug-in. The mail server and any attendant equipment shall be provided by various third-party manufacturers. It shall be possible to activate these e-mail messages via a trigger and procedure, as described elsewhere in this specification. In this way, any system event or transaction or combinations of transactions shall be configurable to trigger a response by the third-party equipment through an action.

B. Users shall be able to configure the system to communicate with the server over the Internet. It shall be possible to allow only certain groups of users to view, use, etc., this server by means of hardware permissions, as described elsewhere in this specification.

C. As part of the configuration of the SMTP server, it shall be possible to manually enter template e-mails that incorporate the following fields: To, From, Reply To, Subject and Body. In the Subject and Body fields, users shall be able to include variable placeholder text. The variable placeholders shall "stand in" for specific transaction information, such as transaction date and time, or the card number or cardholder's name, in the subject or body of the e-mail message. However, the placeholders shall be replaced by the actual data from the transaction when the message is sent to its recipient(s).

D. The module shall provide a means by which users can test-send e-mails after configuration to obviate generating a triggering transaction in the system on purpose in order to verify that the e-mail is sent to the desired recipient(s).

E. When the system event chosen as the trigger occurs, the software shall automatically generate the e-mail and send it to the server. It shall be possible for system administrators and integrators to incorporate the extensions of mobile-phone carriers in the e-mail addresses to allow the e-mail messages to be sent to e-mail/text-enabled mobile phones.

F. Means shall be provided in the software to easily view the license status of this plug-in and the number of licenses that are available in the system for use, if applicable. The method of displaying and working with this information shall not differ from that used for other similar plug-ins. This licensing information shall be stored on the server to allow ease of maintenance.

2.01.59 Schlage® Door Locks

A. The system shall provide means for configuring the Panel Interface Module (PIM) for communication with the PremiSys IP Controller, both described elsewhere in this specification. The PIM shall be viewed by the software as an I/O board to which readers are connected. The addition of the PIM shall automatically create 16 readers that are available for manual inclusion in doors. As the doors are created from manual assignment of these readers, the software shall automatically assign the door-position input points and request-to-exits (REXes) for each door. These associated-point assignments shall not be modifiable.

B. The reader(s) used for the doors shall be configurable to match whichever of the several interchangeable reader units that plug into the lock unit is used on that particular door.

C. The hardware components of these door locks, the lock relays and all points shall function as do other such components in the system. There shall be no appreciable difference in how these components respond to monitor and control functions and/or how they are reported in transaction windows or appear in maps.

2.01.60 TWIC Card Enrollment and Use

A. The access control system shall allow the use of Transportation Worker Identification Credential (TWIC) cards for access control. Users shall be able to use current configuration screens available in the software to easily modify system and hardware settings so as to accommodate TWIC cards and readers.

B. It shall be possible to enroll the cards with their cardholder data into the system using third-party software and third-party enrollment readers. The system shall permit the data from the enrollment process to be "pushed down" to the cardholder database in the access control system of this specification. The system shall automatically determine with any card enrolled whether to create a new cardholder record or to update an existing cardholder record.

2.01.61 Onscreen Help Manual

Selectable from the main menu of the software shall be a printable portable document file containing detailed instructions and background on the setup and operation of the system hardware components and a context-sensitive Help manual.

2.02 THIRD-PARTY SOFTWARE INTEGRATIONS

2.02.01 Video Integration

A. The system software shall provide an optional module with which users can view security cameras on third-party DVR video servers. Such cameras shall be made available to the software through a plug-in and are the external equipment of various third-party manufacturers. It shall be possible to view live cameras and recorded clips in the system.

B. The following control commands shall be executable by a system user, and executable via a trigger and procedure: display live video; display video clip; create video clip; go to preset; display live video & create video clip. Via trigger and procedure, system events or transactions or combinations of transactions shall be configurable to trigger a response by the third-party camera equipment.

C. The system software shall allow one or more cameras to be associated with individual doors, control points, and monitor points. A camera icon shall automatically overlay device point icons having one or more associated cameras. It shall be possible with one click to view all live cameras associated with a device point.

D. It shall be possible to place and rotate camera icons representing third-party cameras on dynamic maps. A live camera view shall open with one-click on the camera icon.

E. The system software shall allow 30 second pre- and post-recorded video clips to be viewed from the monitor transaction screen for system events generated by device points with associated camera(s). System events for camera-associated devices shall be indicated by a camera icon in a device column next to the event listed in the transaction screen.

F. The system software shall allow a user to replay recorded clips and to use the following viewing speed controls: play in reverse 2x; play in reverse 1x; play at normal speed; play forward 1x; play forward 2x.

G. The system software shall allow a user to mark a segment of a recorded clip and export the selected segment to a .PS or .AVI file format. The user shall be able to enter a file name and select a location where the file will be saved. The user shall be able to select a specific frame within a recorded clip and do the following: save image; copy image to clipboard; and print image.

H. System users who are to use the optional mobile application as described elsewhere in this specification shall be able to view live cameras on mobile devices. Systems that do not have the option to view live integrated video server cameras through a mobile application shall be deemed unacceptable.

I. Means shall be provided in the software to easily view the license status of this plug-in and the number of licenses that are available in the system for use, if applicable. The method of displaying and working with this information shall not differ from that used for other similar plug-ins. This licensing information shall be stored on the server to allow ease of maintenance.

J. The video server shall be <exacqVision®, version 5.0.2.34218, manufactured by Exacq® Technologies> <Avigilon Control Center ACC 4, version 4.12 or higher, manufactured by Avigilon®> <GeviScope/GSCView™; version 6.0 or higher; manufactured by GEUTEBRÜCK®> <CompleteView™ ONE, Pro, or Enterprise; version 4.1; manufactured by Salient> <XProtect™ Smart Client 2013; Corporate/2013 version; manufactured by Milestone®> <DX Video Recorders, Digital Sentry, DVR5100, Endura, or EnduraXpress; manufactured by Pelco®> <Victor; version 4.02 or higher; manufactured by American Dynamics®>.

2.03 DATABASE MANAGEMENT

2.03.01 Databases

A. A cardholder database shall contain all data relating to cardholder records, including information related to the creation of photo identification badges. The user shall be able to create, delete, or modify certain database tables and create or delete fields in selected tables in the cardholder database. It shall be possible for system users to add custom tables and fields to the cardholder database to accommodate the needs of a particular system set of cardholders.

B. A separate system database shall store all information and parameters needed for the functioning of the access system. This system database shall not be generally accessible by system users or administrators.

C. The system and cardholder databases shall be Microsoft® SQL databases, and the system software shall use Microsoft® SQL Server 2008. The software installation application shall allow the user/installer to install SQL Server 2008 if SQL Server 2008 is not already installed on the system computer or network.

D. The modules provided by the system software application shall be the sole means by which users work with and manage the data in any of the tables in the cardholder database. Use of a third-party means outside the system application to manage the data in the cardholder-information database shall not possible without the risk of the loss of data integrity and compromised stability of the system. No means within the software application shall be provided for users to work with the system database

tables.

2.03.02 Data Importer

A. The system shall provide a means and process to transfer cardholder information saved in another database to the cardholder database in the badging system. This process is referred to in this specification as "data importing." The source database can be in one of the following formats: Microsoft® SQL, Microsoft® Access or a delimited file such as a .csv or .txt file. Data from a Microsoft® SQL database can be imported using SQL database tables or SQL views.

B. The system shall support data imports from multiple source databases into the system cardholder database.

C. The system shall be sufficiently flexible to allow the user to import any number of fields from multiple database tables into the system cardholder database. The user shall be allowed to create customized lookup tables and customized fields in an extended cardholder table for the purpose of importing and/or entering cardholder data. The system shall allow the user to create fields in those tables using any of the following Microsoft® SQL data types: BigInt, Binary, Bit, ,Char, DateTime, Decimal, Float, Image, Int, Money, NChar, NText, NVarChar, Real, UniqueIdentifier, SmallInt, SmallMoney, Text, Timestamp, TinyInt, VarBinary, VarChar, Xml, Udt, Structured, Date, Time, DateTime2, and DateTimeOffset.

D. The importing process shall allow the user to update cardholder information from the source database once or repeatedly through manual or scheduled updates.

E. The software shall provide a method to schedule regular data importing as described elsewhere in this specification.

2.03.03 Backup/Restore

A. The software shall allow the user to easily back up the system data and cardholder data. The user shall be able to choose whether or not to back up cardholder photos and signatures, and/or transactions.

B. The software shall provide the user with the capability to easily restore the backed-up data to the system to replace current system and cardholder data, if such a need arises. To preserve database integrity the system shall incorporate logic to automatically prevent users from restoring a database from an earlier version of the software.

C. The software shall provide a method to schedule regular backups as described elsewhere in this specification.

2.03.04 Photo and Signature Storage

It shall be possible for the user to designate whether the captured cardholder photos and/or signatures are stored as BLOB data in the database or as individual photo and/or signature files in a user-defined location. If they are stored as individual photo and/or signature files, the user shall define a file storage path to a local client folder or to a shared network folder, as described elsewhere in this specification.

2.03.05 Photo- and Signature- File Sharing

A. The system shall allow the user to store photo and signature files in a local folder on the client or in a network folder. The user shall be able to choose the type of image file for photo storage and industry-standard image file types shall be supported. The system shall support: CALS Raster Image (*.CALS); Encapsulated Post Script (*.EPS); GEM Image (*.IMG); JPEG Image (*.JPEG); LEAD Compressed (*.CMP); Macintosh Paint (*.MAC); Microsoft Paint (*.MSP); PCX Image (*.PCX); Photoshop 3.x Format (*.PSD); Portable Network Graphics (*.PNG); SUN Raster Image (*.RAS); Truevision Targa (*.TGA); Uncompressed TIFF (*.TIF); Windows Bitmap (*.BMP); Windows(r) Metafile (*.WMF); WordPerfect Graphic (*.WPG).

B. It shall be possible to use a module in the software to create a file-naming scheme that is based on the names of cardholder-record fields in the database. Using this scheme, it shall be possible to identify the cardholder depicted in the photo file by the file name.

C. The user shall be able to select any number of data fields to use in the photo file name and to incorporate any field separator supported by the Windows® operating system. This photo file-naming scheme shall support multiple photo controls on the screen.

D. The user shall be able to define a file path for storing the signature file. It shall additionally be possible to use a module in the software to create a file-naming scheme that is based on the names of cardholder-record fields in the database. Using this scheme, it shall be possible to identify the cardholder whose signature appears in the signature file by the file name.

E. The user shall be able to select a field in the database for storing the entire file path name and file name in text form, for example, \\Server\ Photos \Doe, Jane, S, 1234 - PhotoShare.jpg.

F. The user shall be able to select a field in the database to store the entire signature path and file name in text form, for example, \\Server\ Signature\Doe, Jane, S, 1234 - SignatureShare.sig.

2.03.06 Archiving and Purging Transactions

A. The software shall allow system administrators and users to archive history transactions as a file on a local or network folder. It shall be possible to archive all transactions as of the time when the archive is configured or to delimit a time period

whose transactions alone shall be archived. It shall be possible to view archived transactions by generating an archive report from the archive file similar to the report-generation process described in this specification.

B. It shall be possible to optionally purge transactions after they are archived so that the database "space" is made available for the writing of future transactions and other data. It shall be possible to purge all transactions as of the time when the archive and purge is configured or to delimit a time period whose transactions alone shall be archived and purged.

C. The software shall provide a method to schedule regular archiving and purging as described elsewhere in this specification.

2.04 IDENTIFICATION BADGING SOFTWARE

2.04.01 Screen Designs - Default Designs and Basic Designing

A. The badging software shall provide "ready-made" screen layouts that contain all controls needed for basic system function such as viewing cardholder records and entering cardholder data. The system additionally shall allow users to create an unlimited number of user-defined screen designs that shall accommodate cardholder data fields.

B. The user shall be able to modify the default "ready-made" screen layouts, including removing the controls from the screen to make the space available for new controls or selecting different database fields to display data in the default controls. It shall be possible to save a modified screen design as a new template using a "Save As" command.

C. The badging software shall provide means to design and create screen designs used to enter and display cardholder information on a computer. The software shall save and store screen designs in such a way that when they are created, modified or deleted on one client or workstation, the changes are reflected in all workstations, when a networked version of the software is installed and used. It shall be possible as well to have more than one screen design open for editing at one time on a single client's screen.

D. The user shall be able to choose "Save" or "Save As" commands when saving any screen design.

2.04.02 Screen Designs –Control Adding and Positioning

A. The user shall be able to add controls associated to data fields to a screen design, using one of the following methods: following a system-provided screen-design wizard, choosing individual database fields, or choosing individual control types. Following the wizard or choosing individual database fields shall by default also add individual labels for the selected fields. By default these labels shall display the

names of the fields when the labels first appear, but the user shall be able to modify or delete the labels as desired.

B. After a control has been added to a screen design the user shall be allowed to change the database field associated to the control.

C. In screen design, the designer module shall offer a means by which controls placed on the design produce inherent alignment tools that automatically guide the user should he or she wish to align the control with other controls in the design.

D. The system shall employ standard alignment tools to align multiple controls in screen designs.

E. The user shall be able to position controls utilizing the arrow keys on the keyboard.

F. All shape controls shall be capable of complete, 0°-360° rotation in varying increments, depending on the control, on the screen design.

G. It shall be possible to use "drag-and-drop" techniques when working with all controls on a screen design.

H. It shall be possible to position and resize controls in screen designs by clicking and dragging them. There shall be a properties page for each control where the user can manually enter a position and size for one or more selected controls. It additionally shall be possible for a user to position and size several controls in exactly the same place in order to layer graphic files that are tied to logic statements.

I. It shall be possible to select a control on the screen design and move that control to the front of the design (on the top layer compared to all other controls) or send that control to the back of the design (on the bottom layer compared to all other controls.)

J. There shall be no limit to the number of controls a user can place on a screen design other than the limits imposed by the size of the controls and the dimensions of the design.

2.04.03 Screen Design – Control Formatting

A. The badging software shall employ tools for formatting fonts, setting font types and sizes, aligning text, aligning objects, selecting multiple objects on the screen, changing layer order of objects, rotating text, and accomplishing the following functions: undo, cut, copy, paste and delete.

B. Users shall be able to choose a background color or background graphic to apply to controls placed on the screen. The capabilities for color or image display shall be a function of the control on the screen.

2.04.04 Screen Designs - Text Boxes

A. Text boxes, or edit controls, shall be used for capturing variable information for a cardholder and allow the user to add, edit, or delete information within the edit field. The user shall be able to associate fields within the cardholder database to any selected edit field in the screen design.

B. The user shall be able to resize the edit control on the screen to allow multiple lines of text. The system shall enable users to configure the control to automatically wrap the text to the next line as the user enters it.

C. Text boxes shall be configurable to mimic a "password" field to display a character other than that actually entered in the text field, for the purpose of hiding the actual text from view.

D. It shall be possible to apply automatic formatting in the form of a mask to any text box control used in a screen design. The user shall be able to choose a mask to accept and display only numeric digits and no alphabetic or special characters in the field; to display text in sentence case; to display text in all uppercase; to display text in all lower case; to accept and display numeric text using Social Security number formatting in which the proper hyphens are automatically inserted into the entered number; or not to automatically format (apply a mask to) the field at all.

2.04.05 Screen Designs - Labels

A. Labels shall be configurable for displaying read-only text that cannot be edited in the data-entry screen. The text can be user-definable static text or variable text associated to data fields within the database.

B. The user designing the screen shall be able to add, edit, or delete static text in the label. Once the label control is placed on the screen design, the user also shall be able to type directly in the control to modify the text.

C. The user shall be able associate the label to a field in the database if the label is to display variable text from each cardholder record.

D. The user shall be able to resize the label control on the screen to allow multiple lines of text, and it shall be possible for the text to automatically wrap to the next line when multiple lines of text are used.

E. It shall be possible to apply automatic formatting in the form of a mask to any label control used in a screen design. The user shall be able to choose to display only numeric digits and no alphabetic or special characters in the field; to display text in sentence case; to display text in all uppercase; to display text in all lower case; to display numeric text using Social Security number formatting in which the proper hyphens are automatically inserted into the entered number; or to not automatically

format (apply a mask to) the field at all.

2.04.06 Screen Designs –List Boxes, Combo Boxes, and Check Boxes

A. The badging software shall allow the inclusion of list boxes, combo boxes and check boxes in screen designs, and these controls shall have features, functions and characteristics like those of corresponding controls found in Microsoft® Access®.

B. It shall be possible to define any combo box or list box in a screen design to use a database table to provide the values appearing in the drop-down list.

C. The software shall provide the option to sort the order of the list of values so that the values display in an alphanumeric order instead of the entry order.

2.04.07 Screen Design – Photo Controls

A. The system shall provide a photo control that when placed on a screen design allows a cardholder photo to be displayed on a screen design. Any screen design shall support multiple photo controls. There shall be no limit to the number of photo controls a user can place on a screen design other than the limit imposed by the size of the controls and the dimensions of the design.

B. The user shall be able to choose the name of the database field to associate with the photo control.

C. It shall be possible to exactly specify the photo-control location on the screen design by entering pixel values into a property control.

D. For each photo control appearing on a screen design, the user shall be able to select the camera device to be used for photo capture via that individual photo control. It shall be possible to assign different photo-capture devices to each and every photo control in a screen design.

2.04.08 Screen Design – Signature Controls

The system shall have a Signature control that allows the user to include a signature as part of the screen design and to capture cardholders' signatures in the corresponding data-entry screen. There shall be no limit to the number of signature controls a user can place on a screen design other than the limit imposed by the size of the controls and the dimensions of the design.

2.04.09 Screen Design – Image Controls

A. It shall be possible to place and configure multiple image controls in the screen design that allow the user to define image files to be displayed on the screen. There shall be no limit to the number of image controls a user can place on a screen design other than the limit imposed by the size of the controls and the dimensions of the

design.

B. The user shall additionally be able to define logic statements that determine when each image is displayed on the screen, based on values in specific user-defined database fields on a cardholder-by-cardholder basis.

C. The user shall be able to define multiple images to display within one image control based on bitmap logic statements. In this case only one image file will be displayed at a time per logic statement.

D. The user shall be able to click and drag the corner of any image control placed in a screen design in order to resize the control. When the user resizes the image control using a corner "handle," the system shall maintain the aspect ratio the image had before a corner was clicked.

2.04.10 Screen Design – Tabbed Pages

A. The user shall be able to add, remove, resize, and position tabbed pages on the cardholder record screen. The user shall be able to name all tabbed pages, as well as define a background color and style for each individual tabbed page.

B. The tabbed pages shall be collected in a set for placement on the screen design. The number of sets of tabbed pages shall be limited only by the dimensions of the sets and the dimensions of the screen as designed.

C. If the number or size of the tabs exceeds the size of the tab control then the system shall automatically display scroll arrows for the user to scroll to see all tabs.

2.04.11 Screen Design – Subform Controls

A. The system shall provide subform controls that the user can add to the screen and associate to a user-configured data table within the main database.

B. A default Automobiles table shall be provided in the system for optional association with this subform control in data-entry screens to allow the entry of cardholder automobile information.

2.04.12 Screen Design – Tab Order

A. An administrative user shall be able to set the tab order for all controls in such a way that a data-entry user can use the keyboard to move from one field to the next, allowing fields that do not require data entry to be skipped.

B. The user shall be able to modify the tab order. The default tab order shall be the sequence in which the controls were added to the screen. The user shall be able to change the tab order of the fields in the screen design by altering the TabIndex

property for each control.

C. It shall be possible to exclude individual controls from the tab order sequence.

2.04.13 Card Design - Templates

A. The badging software system shall provide all current card definitions in its as-shipped state.

B. The user shall be able to select a card definition template for use in the creation of a new card design. It shall be possible also to save new card designs that can serve as the basis for later card designs.

C. The user shall be able to create a new card design, modify an existing card design or delete a card design.

D. The user shall be able to select, per card design, if the card is a duplex card, which is a card that is printed on both sides.

E. The user shall be able to select the design for the back of the card by choosing a card design in the system by name.

F. The system shall provide a default template for a photo directory, also known as a "facebook." The system shall also provide default templates for role-recognition cards that are used with identification badges for enhanced visual differentiation.

2.04.14 Card Design – Default Designs and Basic Designing

A. The badging software shall provide "ready-made" card designs that contain all controls needed for basic system function such as viewing and printing a cardholder badge. The system additionally shall allow users to create an unlimited number of user-defined card designs.

B. The user shall be able to modify the default "ready-made" card designs, including removing the controls from a design to make the space available for new controls or selecting different database fields to display data in the default controls. It shall be possible to save a modified card design as a new template using a "Save As" command.

C. The badging software shall provide means to design and create card designs used to print cardholder information on a badge. The software shall save and store card designs in such a way that when they are created, modified or deleted on one client or workstation, the changes are reflected at all workstations, when a networked version of the software is installed and used.

D. The user shall be able to choose "Save" or "Save As" commands when saving any card design.

E. The card-design frame shall display horizontal and vertical rulers as a design aid. When any control is selected within the design window, the position of the leftmost edge of the control shall be indicated on the horizontal ruler at the top. The position of the uppermost edge of the control shall be indicated on the vertical ruler at the left.

F. Users shall be able to choose either inches and decimal fractions of inches or millimeters as the measurement units displayed on the ruler.

G. The software shall provide the capability to zoom in on and zoom out of the design window.

H. The card-design preview shall display any graphics files and static text as they appear. Logic-based graphics and photos shall have standard nonspecific representations. Variable text shall be displayed using the database field name, and the text attributes of the variable text in the data-entry screen shall be represented in the display of the field name.

2.04.15 Card Design – Control Adding and Positioning

A. The user shall be able to add controls directly to a card design by one of two methods: choosing any individual control to place on the design and then selecting the database field whose data should display in that control or choosing the name of the database field and then selecting either a label, picture box, or signature control to display that data on the card design.

B. After a control has been added to a card design the user shall be allowed to change the database field associated to the control.

C. Users shall be able to use "drag-and-drop" techniques to position and resize all controls on a card design. The software shall also provide a properties page applicable to each control in which page the user can manually enter a position and size for that control or for multiple selected controls. It additionally shall be possible for a user to position and size several controls in exactly the same place, if desired for the option of layering graphic files that are tied to logic statements.

D. When in a card design, the user shall be able to use "snap-to-grid" functionality, which, when enabled, causes a control placed on the workspace to automatically reposition itself to the closest grid point and align the top-left corner of the control with that grid point. It shall be possible to use snap-to-grid without the grid being displayed.

E. The system shall employ alignment tools to align multiple controls.

F. The user shall be able to position controls utilizing the arrow keys on the keyboard.

G. It shall be possible to exactly specify the control location on the card design by entering values into a property control.

H. Users shall be able to choose the measurement units from among a) inches and decimal fractions of inches or b) millimeters, whichever is chosen for display on the ruler.

I. The user shall be able to center a field on the card design between the left and right edges and/or between the top and bottom edges.

J. It shall be possible to select a control on the card design and move that control to the front of the design (on the top layer compared to all other controls) or send that control to the back of the design (on the bottom layer compared to all other controls.)

2.04.16 Card Design – Labels

A. The system shall have a label control that allows the user to display static or variable text on the card design.

B. The system shall have a compound label control that allows the user to display multiple database fields in the same control. The user shall also be able to add static text before or after any data field, as well as between two data fields in the compound label control.

C. The user shall be able to select the font and font attributes for any label. Font setting options shall include font type and size; left/right justification; typeface features, including boldface, italics and underline; and font color. It shall be possible to select the font color from the Windows® color palette. When date/time data is to be printed on the card using the label control, the user shall be able to choose from multiple date/time formats to display the date/time.

D. There shall be no limit to the number of label controls a user can place on a card design nor shall there be any limit to the number of database fields or static text entries that can be incorporated into the label other than the limit imposed by the size of the controls and the dimensions of the design.

2.04.17 Card Design - Photos

A. The system shall have a photo control that allows the user to place a photo on the card design. There shall be no limit to the number of photo controls a user can place on a card design other than the limit imposed by the size of the controls and the dimensions of the design.

B. The user shall be able to easily select either a database or fileshare photo field to associate to the photo control.

C. The photo control shall have a default aspect ratio of 1:1.25, but this aspect ratio shall be modifiable by the user designing the card design. The default or selected aspect ratio of the photo control shall serve as the aspect ratio of the crop box used as part of photo capture described in this specification.

2.04.18 Card Design - Images

A. The system shall have an image control that allows the user to place an image in the form of a graphics file on the card design. There shall be no limit to the number of image controls a user can place on a card design other than the limit imposed by the size of the controls and the dimensions of the design.

B. The user shall be able to browse to the computer or server location where the graphic file is stored to incorporate the image into the card design.

C. The user shall be able to grab a corner of the graphic in order to resize it, but the system shall preserve the aspect ratio of the imported graphic.

D. The user shall be able to define multiple images to display within one image control based on bitmap logic statements as described elsewhere in this specification, and only one image file is displayed at a time on the card design, per image control.

2.04.19 Card Design - Signature Controls

A. The system shall have a signature control which allows the user to incorporate a signature on the card design. There shall be no limit to the number of signature controls a user can place on a card design other than the limit imposed by the size of the controls and the dimensions of the design.

B. The user shall be able to easily select either a database or fileshare signature to associate to the signature control.

C. The user shall be able to adjust the line width that is used to display the signature on the card design.

2.04.20 Card Design - Bar Code Controls

A. The system shall have a bar-code control that allows the user to display encoded static or variable text on the card design.

B. The bar-code control provided by the software shall offer all the configuration fields and means needed to set up and correctly print any of the predominating bar-code types currently found on the market. It shall also be possible for users to

define human-readable characters and select their position with respect to the bar code.

C. The user shall be able to choose one or more fields from the database to provide the data that is displayed as the bar code. The user shall also be able to add fixed or static text before, between, or after any data field selected to display in the bar code. The user shall be able to edit any static text contained as part of the bar-code control definition without having to delete the entire control and starting over.

2.04.21 Card Design – Magnetic-Stripe Controls

A. The system shall support magnetic-stripe encoding on Track 1, Track 2, and Track 3 or any combination thereof. The user shall define on a per card design basis which track(s) to use.

B. Any field or fields in the database may be incorporated to provide data to form the string for encoding. The user shall be able to select the field(s) and their lengths. The user shall also be able to add fixed or static text before, between, or after any data field selected to encode in the magnetic stripe.

C. The user shall be able to select a character to use for left padding or right padding, or it shall be possible to choose no padding in the encoding string.

2.04.22 Card Design – Drawing and Shape Controls

A. Drawing tools – line, square and ellipse - shall be available for the user when creating card designs.

B. All shape controls shall be capable of complete 0°-360° rotation on the card design.

C. The system shall allow users to move a control to the topmost layer or to the bottommost layer of fields and controls on the card design.

2.04.23 Navigator

A. The badging software shall incorporate an easy-to-use module that enables the user to "navigate" the cardholder records. This module shall mirror visual and classification features found in, for example, Windows® Explorer. The user shall then be able to select from displayed lists of cardholder records the record to open. This navigating module shall display groups of cardholder records as a "tree" of folders on one side of the window and the contents of the selected folder on the right side.

B. The user shall be able to change the view to display thumbnails, cardholder details or a simple list of cardholder names. The list view shall show the first and last names of all records included in the selected group from the tree. The details view shall show the first and last names of all records and optionally up to two other fields

of information to display in columns. The thumbnails view shall show the first and last names of all records and optionally display a thumbnail of the photo assigned to each record. Through system configuration the user shall be able to choose which field is associated with the photo that is displayed as the thumbnail.

C. It shall be possible to organize the records by user-definable folders. The user shall have the ability to configure the system to automatically create folders based on values entered into a database field.

D. The software shall display up to 100 cardholder records per "folder page" in the navigation window and provide the means to scroll to subsequent and previous pages as well as jump to a specific numbered page within the user-defined folder. The user additionally shall be able to easily advance to the next cardholder record on the page or move back to the previous cardholder record without closing the data-entry screen.

E. The user shall be able to adjust the vertical splitter located between the folder tree and the list view of records.

F. The user shall be able to size the columns using a click-and-drag method. The system shall maintain the column headings until modified by the user. The user shall be able to click on a column heading, and the system shall sort the records based on the column. Clicking a second time on the same column heading shall sort the records in the reverse order.

G. The user shall have the ability to use a search function that allows the user to locate record(s) based on one or more search criteria. The user shall be able to define which database field(s) the Search function uses for the search. It shall be possible to select to display or hide unused cardholder database fields in the search control so that a user can more quickly and easily find the fields needed for the search criteria. The user shall be able to search for specific cardholder records and then work with only the cardholder records that the search returns. If more than one record matches the search criteria, the system shall display all the results. The user shall then be able to open a single record in the cardholder record screen. The user shall, however, be able to scroll through the records listed from within the cardholder record screen.

H. The user shall have the ability to use a "quick search" feature that allows the user to search for a specific cardholder while another cardholder record is open. The user shall be able to free-type characters into a search field to match data in the first name, last name and/or card number fields of the system database. If no records match the criteria, the user is prompted to revise the search. If more than 100 records match the criteria, the user is prompted to enter additional criteria. If fewer than 100 records match the criteria, the cardholder names are listed. The user can then select the cardholder name in the list to open that cardholder record.

I. There shall be a user-selectable option in the Navigator Search window to prevent the database fields that do not contain data from appearing in the list of fields available for use as search criteria. This option shall be activated by default in the software. The user shall be free to deactivate this option and so allow all of the

database fields to appear and be available for selection.

J. The system shall employ a right-click shortcut menu from the navigation screen to allow the user to open a record, delete a record, send a card-print for a record to a batch, force a card to print immediately when it would normally be batched, or allow the card to be printed in a specific position on a sheet of card stock used to print multiple cards. It shall be additionally possible to "lasso" multiple records and effect all of these functions, except opening a record, on the selected records.

2.04.24 Cardholder Records

A. The system shall provide simple means to allow a user to open a new, blank cardholder record and to edit an existing record. When the user has changed the record but has not saved it, the system shall prompt the user to save the record before the user closes the record.

B. There shall be controls for moving through records of a single folder one at a time (first to last or vice versa) in a cardholder record screen.

C. It shall be possible to allow a user to delete a record from the system with a few mouse clicks. The system shall prompt the user to confirm that the record is to be deleted.

D. The system shall permit the connection of an enrollment reader to the client PC to allow the numbers encoded onto certain proximity or smart cards to be automatically entered into cardholder records.

E. It shall be possible to create cardholder records using an import function described elsewhere in this specification.

F. It shall also be possible to create a block of cardholders with a specified range of card numbers using a block/add function described elsewhere in this specification.

G. The system shall provide a report module that allows cardholder reports to be run, as described elsewhere in this specification.

2.04.25 Cardholder Records in the Mobile Application

A. The mobile application, described elsewhere in this specification, shall allow users to alphabetically display all the cardholders in the system, a letter of the alphabet at a time. Users shall be able to select a letter from an alphabetic search carousel and then see a complete listing of all the cardholders whose last names begin with that letter. When the user taps a name in the list, a cardholder record for the selected cardholder shall open on the device. Alternatively, the user can search for an individual cardholder through a standard mobile search control, and the record opens on the screen after the user taps the found record.

B. The open cardholder record on the mobile device shall display the following information: last and first names, photo, job title, department, card number(s) of the card(s) assigned to the cardholder, whether the card(s) is (are) active and optionally the license plate number(s) of the cardholder's car(s).

C. Clicking the image of the card in the cardholder record display shall open the cardholder's card record. The open card record on the mobile device shall display the following information: first and last names of the cardholder, the card number, whether the card is active, any activation or deactivation dates assigned to the card and any access groups assigned to the card. Users shall be able to edit the active attribute, the dates and the access groups using the mobile device. Systems unable to provide such breadth of editing capability shall be deemed unacceptable.

D. It shall be possible to enter the data for new cardholders directly into the system using the mobile application running on the device. Users shall be able to enter data for all the attributes mentioned above for cardholders, except vehicles, and for cards, except the card number, via the mobile application in lieu of a standard client.

2.04.26 Photo Capture

A. The system shall provide a means for incorporating the use of a digital camera for the purpose of capturing photos of cardholders so as to integrate the photo as part of the cardholder's record in the database. The system shall additionally provide fields necessary for the user to specify the format, characteristics and other parameters the photo shall have on the screen and the card. It shall also be possible to control the camera and configure certain camera settings within the software, depending on the model of camera.

B. The system shall support multiple cameras connected for photo capture. It shall be possible to associate different cameras with different photo controls on the cardholder screen.

C. The system shall allow new cameras to be added to the system without the necessity to install a new build of software.

D. The system shall support TWAIN, WIA, and WEBCAM devices for photo capture. In addition, the badging software shall provide fields necessary for the user to set up the desired connection to the selected camera(s) and communications speed when applicable. It shall be possible to directly control any supported and connected digital cameras for photo capture.

E. From the cardholder record screen the user shall be able to do one of the following using the photo control: select a capture source, select a capture device, capture a photo, adjust the photo and optionally apply the floating head characteristic described in this specification, delete the photo, import an existing photo, and perform a quick-capture function that immediately takes the cardholder's photo and displays it

in the cardholder's record without any intermediate steps or screens.

F. To import a photo already stored on the computer or network, it shall be possible through the badging software to browse to the photo-file location and preview a photo before importing it into a cardholder record. The user shall be able to crop the photo as part of the importing process.

G. The user shall be able to make adjustments or enhancements to improve photo quality using the badging software. The badging software shall contain industry-standard photo adjustments, including the capabilities to rotate a photo left, right, or upside-down and to create vertical and horizontal mirror images of the original photo.

H. The user shall be able to save a set of adjustment settings to be applied to other photos, termed a "preset." The user shall be able to name presets to be able to select them at a later time. The user shall also be able to save any one of these presets as the default to be applied to all photos when they are captured. The user shall be able to select a named preset, and the system shall automatically adjust the photo in accordance with the settings defined in the preset. The user shall additionally be able to delete a default preset and choose a different preset at any time.

I. During the photo-capture or -import process the user may choose to save the photo to the cardholder record or to restart the process to capture or import a new photo for the cardholder.

J. Once the image is captured, the user shall be able to crop the photo with additional options of zooming in on the photo; moving the frame over the photo to capture a different area of the photo within the frame; or rotating the photo left or right.

K. The system shall be capable of automatically locating the head of the subject to center the crop frame around it. The user shall be able to turn this feature on or off.

L. The user shall be able to save the photo as what is termed a "floating head," a photo of the subject in which no background is included in the photo. This feature – also known as IntelliChrome or ChromaKey – allows the picture to be placed over a background like a company logo in the card design. The user shall be able to adjust the sensitivity of this feature for eliminating the background.

M. If the user chooses Delete Photo the system shall prompt the user to confirm the action. If the action is confirmed then the system shall delete the photo.

N. The mobile application, described elsewhere in this specification, shall provide an interface between any camera built into the device and the system to allow users to capture cardholder photos and enter these photos into the corresponding cardholder's record. After a user captures a cardholder's photo, he or she shall be able to zoom in or out on the subject, move the image to center it in the photo window and then to use the

photo.

2.04.27 Signature Capture

A. When a screen design includes the use of a signature control, the user shall be able to connect a signature-capture device to use to capture signatures via the control. When the user chooses to capture a signature, the cardholder shall "write" his or her signature using the configured device, and the badging software shall store the signature as part of the cardholder record.

B. The user shall be able to assign a pen width to define the appearance of the signature on the screen.

C. Using the signature control in the cardholder record screen, the user shall be able to delete a signature, capture a signature or import a signature.

D. If the user chooses to delete the signature, the system shall prompt the user to confirm the deletion. If the user confirms the deletion, then the system shall delete the signature.

E. The user shall be able to import a JPEG signature image (.JPG file) into a cardholder record. The user shall be able to browse to the file location before importing it.

2.04.28 Badge Logic

A. The software shall provide the means for a user to create condition statements and group them into badge logic sets. The user can then apply a logic set to a data-entry screen so that the data for each cardholder record, when opened using that data-entry screen, automatically determines the card design used to print that cardholder's badge.

B. Badge Logic statements, once created, shall be usable more than once. It shall not be necessary for the user to build the same badge logic set for use in different data-entry screens.

C. The user shall be able to specify a default card design that is to be used when no badge logic criteria is met for the logic set applied to a data-entry screen.

D. When the user creates a screen design, the software shall prompt the user to select a badge logic set to associate to the design.

E. The software shall provide a centralized location in the system for adding or modifying the condition statements that are used to create the badge logic sets. This logic builder will allow the user to easily create individual logic statements as part of the logic set.

F. The user shall be able to choose any field(s) within the database and build a logic expression using operators such as "<," ">," "=," "Like," "Not Null" or "Is Null" along with a value. Each statement shall be capable of containing a virtually unlimited number of criteria defined by the user.

G. It shall be possible for a user to select to print a cardholder card using a card design different from the design designated by the badge logic for the data-entry screen in which the cardholder record is opened. Additionally, the logic set assigned to the data-entry screen that is the default screen for the logged-in user shall be the logic set used to determine the card design printed when the user chooses to print a specific cardholder's badge without opening the record in the data-entry screen.

2.04.29 Bitmap Logic

A. It shall be possible to use bitmap logic on screen and card designs to display graphics that are selected based on data entered by the users in data-entry screens. For example, when a user selects "First Responder" as the cardholder status during data entry, the system shall be configurable to display on the data-entry screen and/or the cardholder's card an image representing that status.

B. The software shall provide the means for a user to create condition statements and group them into bitmap logic sets. The user can then apply a logic set to an image control used in a data-entry screen or a card design so that the data for each cardholder record, automatically determines a specific image that should appear in such an image control to which the logic is applied.

C. The software shall provide a centralized location in the system for adding or modifying the condition statements that are used to create the badge logic sets. This logic builder will allow the user to easily create individual logic statements as part of the logic set.

D. The user shall be able to specify an optional default image that is to be displayed in the image control on the data-entry screen when no bitmap logic criteria is met for the logic set applied to the image control.

E. The user shall be able to choose any field(s) within the database and build a logic expression using operators such as "<," ">," "=," "Like," "Not Null" or "Is Null" along with a value. Each statement shall be capable of containing a virtually unlimited number of criteria defined by the user.

F. Logic statements, once created, shall be usable more than once. It shall not be necessary for the user to build the same bitmap or badge logic set for use in multiple data-entry screens or card designs.

2.04.30 Card Printing

A. The user shall be able to associate a printer or print server to each card design. The system shall allow a card-print command to be sent from any client station for printing a card or cards on the client or server's local printer or on a network printer.

B. The user shall be able to assign any available printer to a card design to be used as the default printer for that card design. The system shall allow a user to select a different printer for use at the time a card is printed if the assigned default printer is not available from the client PC or if such printer is offline.

C. The badging software shall support all industry-standard printers. The software shall be capable of managing multiple printers throughout the system.

D. The user shall be able to preview the card. It shall be possible for the user to view the back of the card, if a dual-sided PVC printer is being used. The user shall also be able to print the card from the preview window. The preview shall display how the card will appear after it is printed. It shall be possible as well to zoom in on and out from the previewed card.

E. The system shall calculate when to print based on card count settings for the card template, the number of cards waiting to be printed and any other settings made in the system.

F. The user shall be able to force the printing of one or more cards without having to meet a requirement to completely "fill" a sheet of card stock before the printer can begin to print.

G. Using the mobile application as described elsewhere in this specification, users shall be able to print the selected card, a single card at a time, of a cardholder whose record is open on the mobile device. The printers available for printing from the mobile device shall be the same Windows printers that have already been selected and set up on the mobile server computer. The user shall be able to select the printer to use from all of those available. The card shall then print at the selected printer.

2.04.31 Print-Queue Management

A. The system shall allow the user to print a cardholder card directly from the navigation window or optionally from the individual cardholder record. The user shall be able to print cards using the following options: batch-print using badge logic as described elsewhere in this specification, batch-print using any card design, print-to-position using a multiple-position card design, or select any card design to use to print any badge or badges immediately.

B. The system shall provide a process by which card-print jobs are queued so that the user shall be able to change the order of the card-print jobs, pause or resume the print queue, hold all or specific cards to prevent printing until released by the user, release all or specific cards to begin printing when system conditions are met, delete

all or specific cards before printing, or preview individual cards.

C. The system shall provide a means so that the queue threshold of the physical printer can be increased or decreased in order to optimize print-job flow to the Windows® print queue.

D. The system shall provide a means so that a user with rights to manage documents for a specific printer shall be able to pause and/or purge print jobs in the print queue for that Windows® printer.

2.05 ACCESS CONTROL HARDWARE

2.05.01 Manufacturers

A. The manufacturer named herein shall be regularly involved in the design, manufacture or distribution of products specified in this document.

B. All products shall be listed by the manufacturer for their intended purpose.

C. Products manufactured or distributed by IDenticard Systems shall constitute the minimum type and quality of equipment to be installed.

D. The specified hardware to be used with the Access Control and Monitoring Software shall be hardware designed for use with IDenticard® <PremiSys™ > software by IDenticard Systems.

E. All equipment and components shall be the manufacturer's current model. The authorized representative of the manufacturer of the major equipment, such as controllers, shall be responsible for the satisfactory installation of the complete system.

F. The contractor shall provide, from the acceptable manufacturer's current product lines, equipment and components that comply with the requirements of these specifications. Equipment or components that do not provide the performance and features required by these specifications are not acceptable, regardless of manufacturer.

2.05.02 IP Controller

A. The IP Controller shall be of a distributed database design and provide access control, alarm monitoring and time zone control for both access to and egress from selected areas. The IP Controller shall process all data transmitted to and from the I/O boards connected to it. The controller shall use 12 VDC for power and be intended for use in low voltage, Class 2 circuits only.

B. Memory on the IP Controller shall be as follows: 1 MB SRAM for transactions and new card information; 16 MB non-volatile flash memory for card and system information; 32 MB SDRAM for system firmware and database storage for the

application. A 3-volt lithium coin cell shall provide SRAM and clock backup.

C. Two-way communications between the controller and the host computer shall be via a primary Ethernet 10/100Base-T interface or the optional serial RS-232 or RS-485 ports. An Ethernet port and a serial port for RS-232 or RS-485 connections shall be built-in on the controller. When Ethernet is the connection means, the number of controllers possible in a system shall be limited only by the network capacity and bandwidth. When using RS-485 connectivity the system shall allow multi-drop communication on a single bus of up to 4,000 feet (1,200 m). It shall be possible to connect up to eight controllers per host computer port when using RS-485 connections. When using RS-232 connections the system shall allow one controller per computer port. Communication between the controller and host shall be selectable from among the baud rates 2400, 9600, 19,200, 38,400 and 115,200.

D. The IP Controller shall be connectable to a variety of system I/O boards that act as interfaces between the controller and auxiliary access-control and door hardware such as locks, input devices and switches. These I/O boards shall include reader boards, input boards and output boards, as well as multiplexer boards. All communications lines to I/O boards shall be supervised in the system, and transactions shall be provided in the system to alert the operator of offline or disconnect statuses. Communications between any controller and its I/O boards shall be via serial RS-485 and/or TCP/IP over Ethernet. It shall be possible to connect up to 64 I/O boards to a single IP Controller, with a maximum of 32 boards on each of two I/O ports provided on the controller. It shall also be possible for each IP Controller to receive data from a maximum of 64 readers. Communication between the controller and I/O boards shall be selectable from among the baud rates 2400, 9600, 19,200 and 38,400.

E. The IP Controller shall be capable of providing redundant communications to the host computer for use in the event that the primary Ethernet connection to the host is lost. The user shall be able to choose the secondary Ethernet connection using the serial port configurable as an RS-232 interface or an RS-485 interface as the means for redundant communication.

F. Any controller within the network of controllers shall have an address that is different from any other on the same port of the PC. The IP Controller's address shall be selected by means of a configuration Web page stored on the IP Controller and accessed through a Web browser using a default IP address.

G. The IP Controller shall have a dedicated input point for optional connection to a controller enclosure tamper switch and another dedicated input point for optional connection to a power-loss monitoring device. Systems requiring use of one of the available system input points for this monitoring shall be unacceptable.

H. The system shall allow the incorporation of a rechargeable battery as part of the power supply to provide full functionality for the controller, system communications and board-powered readers in the event of a power failure.

I. IP Controllers shall be housed in heavy-gauge steel enclosures with hinged front doors. Conduit knockouts shall be available on sides and backs of the enclosures.

2.05.03 Two-Reader Controller

A. The Two-Reader Controller shall be of a distributed database design and provide access control, alarm monitoring and time zone control for both access to and egress from selected areas. The Two-Reader Controller shall process all data transmitted to and from the I/O boards connected to it. The controller shall use 12 VDC for power and be intended for use in low voltage, Class 2 circuits only.

B. Incorporated on the Two-Reader Controller shall be memory as follows: 1 MB SRAM for transactions and new card information; 16 MB non-volatile flash memory for card and system information; 16 MB SDRAM for system firmware and database storage for the application. A 3-volt lithium coin cell shall provide SRAM and clock backup.

C. Two-way communications between the controller and the host computer shall be via a primary Ethernet 10/100Base-T interface or the optional serial RS-232 port. The Ethernet port and a serial port for RS-232 connections shall be built-in on the controller. When Ethernet is the connection means, the number of controllers possible in a system shall be limited only by the network capacity and bandwidth. When using RS-232 connections the system shall allow one controller per computer port. Communication between the controller and host shall be selectable from among the baud rates 2400, 9600, 19,200, 38,400 and 115,200.

D. The Two-Reader Controller shall provide two reader ports built into the controller. Such reader ports shall support up to two (2) reading devices of the same or different technologies.

E. The Two-Reader Controller shall be connectable to a variety of system I/O boards that act as interfaces between the controller and auxiliary access-control and door hardware such as locks, input devices and switches. These I/O boards shall include reader boards, input boards and output boards, as well as multiplexer boards. All communications lines to I/O boards shall be supervised in the system, and transactions shall be provided in the system to alert the operator of offline or disconnect statuses. Communications between any controller and its I/O boards shall be via serial RS-485 and/or TCP/IP over Ethernet. It shall be possible to connect up to 32 I/O boards to a single Two-Reader Controller. It shall also be possible for each Two-Reader Controller to receive input from a maximum of 64 readers, including readers connected to the two reader ports built into the controller. Communication between the controller and I/O boards shall be selectable from among the baud rates 2400, 9600, 19,200 and 38,400.

F. The Two-Reader Controller shall be capable of providing redundant communications to the host computer for use in the event that the primary Ethernet connection to the host is lost. The serial RS-232 interface serves as the means for

redundant communication.

G. Any controller within the network of controllers shall have an address that is different from any other on the same port of the PC. The Two-Reader Controller's address shall be selected by means of a configuration Web page stored on the Two-Reader Controller and accessed through a Web browser using a default IP address.

H. The Two-Reader Controller shall provide eight (8) supervised inputs for use as door-position inputs, request-to-exit inputs etc. The states of the inputs shall be as follows: normally open; normally closed; 1 K normal, 2 K active; and 2 K normal, 1 K active. It additionally shall be possible to set the debounce and hold times for each input on the board. It shall be possible to set all input configuration via the system software.

I. Held-open times – the time during which a door may be held open without generating a system alarm – for inputs on the board assigned as door-position points shall be software-selectable in two-second increments between 2 and 65,534 seconds.

J. All input points shall have a corresponding LED on the board that indicates the state of the point.

K. The Two-Reader Controller shall also provide two Form-C, noninductive relay outputs for door-lock control or alarm signaling. Control of the relays shall be software-assignable to be triggered by card presentations, time zones and/or other system actions. The contact ratings shall be 5 A at 30 VDC. The relays shall be configurable for normal (relay energized when "on") or inverted (relay de-energized when "on") action. Pulse time of a relay used as a door-lock relay shall be software-selectable between 1 and 255 seconds.

L. It shall be possible via the system software to link an input or relay on the Two-Reader Controller to cause an action on any other relay in the system and to select the action that a linked relay will take when the triggering input or relay is activated.

M. The Two-Reader Controller shall have a dedicated input point for optional connection to a controller enclosure tamper switch and another dedicated input point for optional connection to a power-loss monitoring device. Systems requiring use of one of the available system input points for this monitoring shall be unacceptable.

N. The system shall allow the incorporation of a rechargeable battery as part of the power supply to provide full functionality for the controller, system communications and board-powered readers in the event of a power failure.

O. Two-Reader Controllers shall be housed in heavy-gauge steel enclosures with hinged front doors. Conduit knockouts shall be available on sides and backs of the

enclosures.

2.05.04 PoE One-Door Reader Controller

A. The PoE One-Door Reader Controller shall be of a distributed database design and provide access control, alarm monitoring and time zone control for both access to and egress from selected areas. The PoE One-Door Reader Controller shall use quick-disconnect terminal blocks for all interconnections to the interface. The PoE One-Door Reader Controller shall be intended for use in low voltage, Class 2 circuits only.

B. Memory on the PoE One-Door Reader Controller shall be as follows: 1 MB SRAM for transactions and new card information; 16 MB non-volatile flash memory for card and system information; 16 MB SDRAM for system firmware and database storage for the application.

C. Two-way communications between the controller and the host computer shall be via a primary Ethernet 10/100Base-T interface. The Ethernet port shall be built-in on the controller. The number of controllers possible in a system shall be limited only by the network capacity and bandwidth.

D. The PoE One-Door Reader Controller shall provide two reader ports built into the controller. Such reader ports shall support up to two (2) reading devices. These reading devices are intended to control one door. It shall be possible to connect up to 16 PoE One Door Reader Boards to a single PoE One-Door Reader Controller via the Ethernet. When 16 of only PoE One Door Reader Boards are connected, it shall be possible for each PoE One-Door Reader Controller to receive input from a maximum of 17 readers, including a reader connected to the reader port built into the controller. It shall be possible to connect up to 8 of any of the other I/O boards cited in this specification to a single PoE One-Door Reader Controller using RS-485 communications downstream from the controller. When 8 "other I/O boards" are connected, it shall be possible to additionally connect up to 8 PoE One-Door Reader Boards to the controller.

E. Any controller within the network of controllers shall have an address that is different from any other on the same port of the PC. The PoE One-Door Reader Controller's address shall be selected by means of a configuration Web page stored on the PoE One-Door Reader Controller and accessed through a Web browser using a default IP address.

F. The PoE One-Door Reader Controller shall provide two (2) supervised inputs for use as a door-position input and a request-to-exit input. The states of the inputs shall be as follows: normally open; normally closed; 1 K normal, 2 K active; and 2 K normal, 1 K active. It additionally shall be possible to set the debounce and hold times for each input on the board. It shall be possible to set all input configuration via the system software.

G. Held-open times – the time during which a door may be held open without generating a system alarm – for the input on the board assigned as the door-position point shall be software-selectable in two-second increments between 2 and 65,534 seconds.

H. All input points shall have a corresponding LED on the board that indicates the state of the point.

I. The PoE One-Door Reader Controller shall also provide two Form-C, noninductive relay outputs for door-lock control or alarm signaling. Control of the relays shall be software-assignable to be triggered by card presentations, time zones and/or other system actions. The contact ratings shall be 2 A at 30 VDC. The relays shall be configurable for normal (relay energized when "on") or inverted (relay de-energized when "on") action. Pulse time of a relay used as a door-lock relay shall be software-selectable between 1 and 255 seconds.

J. It shall be possible via the system software to link an input or relay on the PoE One-Door Reader Controller to cause an action on any other relay in the system and to select the action that a linked relay will take when the triggering input or relay is activated.

K. The PoE One-Door Reader Controller shall have a dedicated jumper-like input for optional use to indicate tamper status.

L. The PoE One-Door Reader Controller shall allow the controller to be powered over the Ethernet connection or via a separate 12-VDC power supply to the board. The input power shall be passed through to the reader terminal block (port) and shall be available for powering a reader.

M. The system shall allow the incorporation of a rechargeable battery as part of the power supply to provide full functionality for the controller, system communications and board-powered readers in the event of a power failure.

N. PoE One-Door Reader Controller shall be mounted in a three-gang junction box with an optional magnetic tamper switch.

2.06 CARD READERS

2.06.01 Manufacturers

A. The manufacturers named herein shall be regularly involved in the design, manufacture or distribution of products specified in this document.

B. All products shall be listed by the manufacturer for their intended purpose.

C. Products manufactured or distributed by IDenticard Systems, Inc., a Brady Worldwide company, shall constitute the minimum type and quality of equipment to

be installed.

D. The authorized representative of the manufacturer of the major equipment, such as controllers, shall be responsible for the satisfactory installation of the complete system.

E. The contractor shall provide, from the acceptable manufacturer's current product lines, equipment and components that comply with the requirements of these specifications. Equipment or components that do not provide the performance and features required by these specifications are not acceptable, regardless of manufacturer.

2.07 ID / TECHNOLOGY CARDS

2.07.01 IDentiPROX™ Cards

A. Identification cards shall be issued to each system user and provide the functions as detailed in this specification. The credit-card sized proximity identification card shall be thin and flexible, and shall contain an integrated circuit connected to an antenna.

B. The core layer of the card shall consist of this antenna printed using conductive ink on the inside surface of an inner layer and electrically connected to an integrated circuit chip. The outside Teslin® surfaces of the card stock itself shall envelop the chip and antenna, and the front and/or back of the card itself shall be capable of receiving printing by the manufacturer, or not printed at all, per customer requirements before lamination.

C. The laminate sleeve shall be laminated onto the outside surfaces of the Teslin® card during final lamination at the manufacturer's facility. The outside surfaces of this laminate shall readily accept the inks used by standard commercially available PVC-card printers utilizing dye-sublimation or thermal-transfer printing.

D. The completed laminated basic card shall then be printable on any standard PVC card printer to enable the card to be personalized with individual cardholder data, such as name, grade, photo and the like. The completed card shall provide the durability and security features of state-of-the-art laminated smart cards with the flexibility and ease of PVC-card customization.

E. The card dimensions shall be 2.125" x 3.370" x 0.030" ± 0.003" (5.4 x 8.6 x 0.076 ± 0.0076 cm).

F. The integrated circuit chip shall be an HID®-compatible card of ISO composite, and shall have the following features: high gloss image grade, lifetime warranty, and the card material shall be available as PVC laminate or composite 60/40% polyester/PVC.

G. The contactless MIFARE® smart identification card shall be Item IDPROX-[ ], manufactured by IDenticard® Systems.

2.08 CARD PRINTERS

2.08.01 IDenticard® Smart IDcard Printer

A. The printer shall be capable of producing multicolor identification cards on PVC cards and composite cards. The printer shall also be capable of single-sided printing< or duplex printing, allowing the front and back of the card to be printed before the card exits the printer>. The printer shall be capable of printing in one color with overlay (resin black and overlay panel (KO)), four-color (yellow, magenta, cyan, black) with resin black and overlay panel (YMCKO), or four-color with a UV panel and overlay panel (YMCKFO). The printer shall also be capable of printing black as a single color (K). The resolution shall be 300 dpi (11.8 dots/mm) print resolution. The printer shall accommodate the standard card stock size CR-80 – 3.375" L x 2.125" W (85.6 mm L x 54 mm W) as well as the ISO 7810 size – 2.12" x 3.38" (54 mm x 86 mm), and the printer shall accommodate card thicknesses of 10-45 mil. In addition, the printer shall be able to print on plain plastic blanks, on card media incorporating a magnetic stripe or smart cards that meet standard chip-position requirements. The printer feed hopper capacity shall be 90 cards and the output stacker capacity shall be 40 cards. An optional encoder shall allow the printer to simultaneously encode cardholder or other data on a magnetic stripe at the time at which the card is printed.

B. It shall be possible to connect the printer to a controlling PC running a Windows® 2000, Windows® 2003, Windows® XP or Windows® Vista operating systems via a USB 2.0 interface.

C. The printer shall be an IDenticard® Model <SMART SE (single-sided printer)> <SMART-DUAL SE (duplex printer)> <SMART3 SE (single-sided printer with three-track encoder)> <SMART-DUAL3 SE (duplex printer with three-track encoder>, manufactured by IDP Corporation.

3 EXECUTION

3.01 ACCEPTABLE INSTALLERS

The following Security Contractors have been pre-approved to bid on this project:

A. < >
B. < >
C. < >

3.02 EXAMINATION

It is up to the Contractor to examine the site to verify the conditions prior to bidding on the project.

3.03 PREPARATION

A. The Contractor shall order all required parts and equipment upon notification of award of the work.

B. The Contractor shall bench test all equipment prior to delivery to the job site.

C. The Contractor shall verify the availability of power where required. If a new source of power is required, a licensed electrician shall be used to install it.

D. The Contractor shall arrange to obtain all programming information including access times, free access times, doors, operator levels, etc.

3.04 INSTALLATION

3.04.01 General

A. The Contractor shall coordinate with the [CLIENT]'s IT Department for interface with their LAN system.

B. The Contractor shall carefully follow the instructions in the manufacturers' Installation Manual to insure all steps have been taken to provide a reliable, easy to operate system.

C. The Contractor shall coordinate with the [CLIENT]'s Architectural Hardware Consultant to interface with all electric locks.

D. The Contractor shall perform all work as indicated in the drawings and specifications.

E. The Contractor shall install the appropriate cable from the I/O boards to readers, door contacts, request-to-exit devices, and electric locks at each door.

F. All communications cables shall be kept away from power circuits.

G. The Contractor shall install the power supply(s) for electric locks in locations where they cannot interfere with other operations.

H. The Contractor shall also execute adequate testing of the system to ensure proper operation.

3.04.02 Conductors and Raceway

A. The entire system shall be installed in a skillful manner in accordance with approved manufacturer's installation manuals, shop drawings and wiring diagrams. The contractor shall furnish all conduit, wiring, outlet boxes, junction boxes, cabinets, enclosures and similar devices necessary for the complete installation. All wiring shall be of the type required by the NEC and approved by local authorities having jurisdiction for the purpose.

B. Any shorts, opens, or grounds found on new or existing wiring shall be corrected prior to the connection of these wires to any panel, component or field device.

C. The contractor shall neatly tie-wrap all field-wiring conductors in the spaces provided in the controller-panel enclosures and secure the wiring away from all circuit boards and control equipment components. All field-wiring circuits shall be neatly and legibly labeled in the controller as needed. No wiring splices shall be permitted in a controller enclosure. There shall be no components mounted in any PremiSys enclosure other than those specified by the manufacturer.

3.04.03 Test and Inspection

A. All wiring shall be tested for continuity, shorts and grounds before the system is activated.

B. All test equipment, instruments, tools and labor required to conduct the tests shall be made available by the installing contractor.

C. The system, including all its sequence of operations, shall be demonstrated to the Owner<, his representative and any relevant local inspector>. In the event the system does not operate properly, the test shall be terminated. Corrections shall be made, and the testing procedure shall be repeated until it is acceptable to the Owner, his representatives and relevant inspector(s).

D. At the final test and inspection, a factory-trained representative of the system manufacturer shall demonstrate that the system functions properly in accordance with these specifications. The representative shall provide technical supervision, and shall participate during all of the testing for the system.

E. A letter from the Contractor shall be provided to certify that the system is installed entirely in accordance with the system manufacturer's recommendations and within the limitations of the required listings and approvals, that all system hardware and software has been visually inspected and functionally tested by a manufacturer's certified representative, and that the system is in proper working order.

3.04.04 Training

A. The System Supplier shall schedule and present a minimum of two (2) hours of documented, formalized instruction for the building owner, detailing the proper

operation of the installed System.

B. The instruction shall be presented in an organized and professional manner by a person factory-trained in the operation and maintenance of the equipment and who is also thoroughly familiar with the installation.

<C. The instruction shall cover the schedule of maintenance required by _____ and any additional maintenance recommended by the system manufacturer.>