

## 1. SIMS Specification

### Section 17060 Recommended Minimum Specifications

#### Access Control System

### Part 1 GENERAL

#### 1.01 SUMMARY

- A. Drawings and conditions of the contract, including but not limited to General Conditions, and the Special Conditions listed below, apply to work of this section.
  - 1. Supplementary Instructions to Bidders
  - 2. Supplementary Conditions
  - 3. Summary of the Work
  - 4. Project Coordination
  - 5. Cutting and Patching
  - 6. Definitions and Standards
  - 7. Submittals
  - 8. Schedules and Reports
  - 9. Temporary Facilities
  - 10. Security Regulations
  - 11. Safety and Health
  - 12. Products
  - 13. Project Closeout

#### 1.02 SECTION INCLUDES

- A. This performance specification provides the minimum acceptable requirements for the Security Information Management System (SIMS). 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:

- B. The SIMS shall consist of a personal computer-based hardware and software capable of integrating the security functions for: access control, alarm management, photo identification card production, data management, graphics mapping, roll call, muster station, network video recording and interfacing with video systems.
- C. SIMS shall provide access validation and prevent unauthorized access at designated facility portals.
- D. SIMS shall meet all current TSA/TWIC program requirements and allow for future additions
- E. SIMS shall provide alarm/alert notification of access breaches at designated facility portals and other points as desired.
- F. SIMS shall provide the ability to configure global and local macros that execute based on conditions anywhere in the system. This includes hardware control, email, SMS, IM, ASCII output, Anti-Passback (global), and other system functions.
- G. SIMS shall provide data collection and management tools for an access credential database at the facility. All system information shall be stored in a Microsoft SQL database.
- H. SIMS shall include a complete audit trail that tracks all configuration changes for card holders and controllers. Old value, new value and operator making the change must be tracked.
- I. SIMS shall provide the ability to produce instant history reports for all devices and card holders. History report option must be available as part of the configuration editor for all card holders and devices without leaving the edit function.
- J. SIMS shall provide a user configurable user interface. All live events, trace events, alerts and system status shall be provided in grids that can be sized, floated or relocated by the user. User shall be able to specify display colors and be able to sort/group information at will. All user specified user interface configurations shall be stored per user.

- K. SIMS shall not be accessible using web browser technology.
- L. SIMS shall provide integrated Network Video Recording functions.
- M. SIMS shall provide an Event Video Recording (EVR) gateway feature that is native to the application and not integrated from another manufacturer. The EVR feature must store video based on user defined events. The video must clips must include a unique identifier as opposed to relying on a time stamp from a DVR/NVR system. The EVR gateway must support MJPEG video streams. The EVR must also provide an optional video client.
- N. SIMS EVR must provide support for video content analysis features including; loitering, package left behind and people counters.
- O. SIMS shall provide integration with Aimetis Symphony and AIRA V5.
- P. SIMS shall provide integration with EasyLobby visitor management.
- Q. SIMS shall provide Photo Badging and credential management for Facility Employees, Contractors, Visitors and others as required.
- R. SIMS shall provide Graphics Mapping user interface that includes support for video.
- S. SIMS shall provide a video only client for monitoring of surveillance cameras. Video client must provide the ability to pause live video, rewind and fast forward video.
- T. SIMS shall provide full application features across the internet on an encrypted connection without using the less secure internet browser method or Virtual Private Network (VPN) hardware and software.
- U. SIMS shall provide both an integrated and a separate Report Client with integrated Report Designer.
- V. SIMS shall provide a separate roll call client with muster station capability. Roll call and muster areas must be definable as nested areas without the need for exit readers.

- W. SIMS shall provide a complete and detailed context sensitive help file. Help file must include software configuration and all hardware information. Help file must also include a documented API (Application Programmer Interface) that can be used to interface to the SIMS.
- X. SIMS shall provide support for all Mercury Security Controllers including the AP, SCP and EP series controllers
- Y. SIMS application must be a Native Microsoft .NET application and shall not have been ported from a previous operating system. Systems that were not originally developed for the .NET platform are not acceptable.
- Z. SIMS must use Microsoft SQL server and support LDAP and Microsoft Active Directory for database interfaces.
- AA. SIMS shall provide direct support for the Sagem Morpho TWIC readers without the use of third party middleware.
- BB. SIMS shall provide a Situation Manager that allows for definition of 5 threat levels. All system devices must support configuration to allow for different modes of operation based on the Situation Manager setting.

### 1.03 MANUFACTURER

- A. The manufacturer named herein shall be regularly involved in the design, manufacture or distribution of products specified in this document. All products shall be listed by the manufacturer for their intended purpose.
- B. Products manufactured or distributed by Keri Systems Inc., shall constitute the minimum type and quality of equipment to be installed.
- C. Manufacturer must have a GSA (General Services Administration) contract in good standing.
- D. All control panels and connected field hardware, 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, 32 bit microprocessor-based controller panels as described in this specification

- E. Manufacturer's software application must be a native Windows .NET framework system initially developed as a .NET application and not converted from a previous generation system.
- F. Systems that can be accessed via web browser shall be deemed not acceptable due to security concerns.

#### 1.04 Alternates

- A. Strict conformance to this specification 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 model. The materials, appliances, equipment and devices shall be tested and listed by a nationally recognized approvals agency for use as part of a protected-premises protective access-control system.
- D. The system shall utilize independently addressed, microprocessor-based controller panels as described in this specification. All equipment and components shall be installed in strict compliance with the manufacturer's recommendations.
- E. The equipment to be supplied will be considered only if it meets all sections of the performance specification. Any deviations of system performance outlined in this specification will only be considered when the following requirements have been met:
  - 1. A complete description of proposed alternate system performance methods with three (3) copies of working drawings thereof for approval by the Owner, not less than ten (14) calendar days prior to the scheduled date for submission of bids.

2. The supplier shall furnish evidence that the proposed or alternate system performance is equal or superior to the system operation stated in the specification. Such evidence shall be submitted to and accepted by the Owner, not less than ten (14) calendar days prior to the scheduled date for submission of bids.
3. The supplier shall submit a point-by-point statement of compliance for all sections in this specification. The statement of compliance shall consist of a list of all paragraphs within these sections. Where the proposed system complies fully with the paragraph as written, placing the word "comply" opposite the paragraph number shall indicate such. Where the proposed system does not comply with the paragraph as written and the supplier feels the proposed system will accomplish the intent of the paragraph, a full description of the function as well as a full narrative description of how its proposal will meet its intent shall be provided. Any submission that does not include a point-by-point statement of compliance as described herein shall be disqualified. Where a full description is not provided, it shall be assumed that the proposed system does not comply.

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

#### 1.05 References

##### A. General (References)

1. 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.

#### 1.06 Access Control

A. The equipment shall comply with the current provisions of the following codes and standards:

1. UL 294 - Standard for Access Control System Units 1076

2. Federal Codes and Regulations
3. Americans with Disabilities Act (ADA)
4. EMC Directive 89/336/EEC
5. Electromagnetic Compatibility Requirements Product Standard EN 55011: 1991

## 1.07 Definitions and Abbreviations

### Definitions

- a. ADA: Americans with Disabilities Act
- b. AHJ: Authority Having Jurisdiction
- c. Approved: Unless otherwise stated, materials, equipment or submittals approved by the Authority or AHJ
- d. Cable-foot / Cable-meter: Length of wire used to connect components; does not necessarily correspond to the physical distance between components
- e. Circuit: Wire path from a group of devices or appliances to a control panel or transponder
- f. GUI: Graphic User Interface
- g. LED: Light Emitting Diode
- h. LCD: Liquid Crystal Display
- i. MSDE: Microsoft® Database Engine
- j. SQL: Microsoft® SQL Server Database Engine
- k. PTR: Printer
- l. UL® or ULI: Underwriters Laboratories, Inc
- m. NVR: Network Video Recorder
- n. EVR: Event Video Recorder
- o. MAPC: Graphics Mapping Client
- p. MAPD: Graphics Mapping Designer
- q. EOL: End of line resistance
- r. MSC: Mercury Security Corporation
- s. KERI: Keri Systems Inc.
- t. E700: Eclipse™ 700
- u. SPM: System Processor Module
- v. DDM: Dual Door Module

- w. ICM: Input Control Module
- x. OCM: Output Control Module
- y. SDM: Single Door Module

## 1.08 System Description

### A. General

1. The Contractor shall furnish all labor, services and materials necessary to furnish and install a complete, functional access-control system (System). The System shall comply in respects with all pertinent codes, rules, regulations and laws of the Authority, and local jurisdiction.
2. It is further intended that upon completion of this work, the Owner shall be provided with:
  - a. Complete information and drawings describing and depicting the entire System as installed, including all information necessary for maintaining, troubleshooting and/or expanding the System at a future date
  - b. Complete documentation of System testing

## 1.09 Description

### A. Provide and install a new access-control system consisting of:

1. Control panels installed in locations specified by Customer
2. Auxiliary components located as shown on the drawings
3. Mullion/Door Frame and Surface Mount Proximity Card Readers and Keypads located as shown on the drawings and detailed on Door Schedule

4. Input points and output relays as required and located in locations specified by Customer.
5. Request to Exit devices as listed on Door Schedule, or shown on drawing.
6. Connections to central server(s) and all system components.

## SCHEDULE 1 - **Integrated Security Management Operations**

### 1. Personal Computers

- 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. All Server and Client computers shall be off-the-shelf IBM®-compatible personal computers with components that have been certified by Microsoft Windows Hardware Quality Labs (WHQL).
- b. Any Server computer shall have Quad Core Intel® Xeon® Processor / 2.5GHz or faster processors, a minimum of 4 GB of RAM, 250 GB hard drive, CDR and a 10/100/1000 Base T network interface card. Any Client computers shall have Quad Core Intel® Xeon® Processor / 2.0 GHz or faster processors, a minimum of 2 GB of RAM, 1 GB free space on hard drive and a 10/100/1000 Base T network interface card.

### 2. Control Panels

- a. All control panels shall be non-proprietary versions of Mercury Security Corporation AP, SCP or EP series panels. Panels shall not have proprietary firmware or chips installed.
- b. Control panels shall be intelligent and fully stand alone processor capable. Controllers shall make all local access control and alarm decisions without host server dependency.
- c. All panels shall support flash memory to facilitate firmware updates.
- d. Controller shall provide FIPS 197 AES 128 Bit encryption.

### 3. System Software

- a. The operating system software for servers shall be Microsoft® Windows® XP Professional with Service Pack 2 or Microsoft® Windows® Vista Ultimate or later and with .Net Framework 1.1 and .Net Framework 2.0. The operating system software for clients shall be Microsoft® Windows® XP Professional or Microsoft® Windows® Vista Ultimate.
- b. The integrated security management software shall be Keri Eclipse™ 700.
- c. The SIMS shall be licensed without the use of hardware dongles.

- d. The SIMS software shall not be accessible via web browsers.
- e. The SIMS shall have a minimum of 16 concurrent client licenses.
- f. The SIMS shall not require more than 1 SQL client user license to operate.
- g. The SIMS shall use “Stored Procedures” for communications with the SQL database for increased efficiency and stability.

#### 4. Databases / Redundancy

- a. The system software shall be capable of stand-alone or Client-Server networked operations utilizing open system architecture and a 32-bit ODBC-compliant database.
- b. The software installation application shall allow the user/installer to select between a Microsoft® SQL Server Express or Microsoft® SQL Server database structure. The appropriate database drivers shall be automatically installed.
- c. The SIMS shall be capable of operating in a Microsoft SQL Cluster environment where two redundant servers utilize a shared database cluster. Cluster management should be provided by industry standard Microsoft clustering service and should not require any proprietary clustering software.
- d. It shall be possible to isolate the SIMS database from the application including running the application and database in separate geographical locations and communicating over standard network infrastructure to provide maximum flexibility and conformance to IT data center standards.
- e. The SIMS shall be capable of utilizing file and database replication using Microsoft SQL Server 2005 Replication Services and Microsoft File Replication Services in providing distributed database replication across multiple regional servers allowing for endless expansion. File replication should be provided by industry standard Microsoft File Replication Services and shall not require any proprietary file replication software. Database replication should be provided by industry standard Microsoft SQL Server 2005 Replication agent.
- f. The system software shall record all transactions with a GMT timestamp, Local time zone timestamp of the primary controller that generated the transaction, and the SQL server timestamp when the transaction was inserted into the database.
- g. All timestamps must be in the ISO 8601 format.

## 5. System Security

- a. User logins that incorporate passwords and other administrative controls available in the system shall protect the system software, database and data distributed to the controller panels from unauthorized access.
- b. User Rights
  - 1) The software shall permit assignment of rights to system features on a feature-by-feature basis to any and all system users, whether individually or as members of a defined user group. It shall be possible to add, remove and edit any user and user group rights.
- c. Passwords assigned to system users shall allow a user to log onto any Client interface without affecting system control of current users logged onto other client interfaces.

## 6. Network Communication

- a. The software shall enable PC communication to any System Processor Modules (SPMs) over a LAN and/or WAN using Ethernet protocol. The software shall allow the user to perform all system functions in a LAN/WAN environment as are possible when panels are hardwired directly to the PC.
- b. The software shall enable secure, encrypted connections from remote locations over the Internet without the use of a Web Browser or VPN connections. Web Browser user interfaces are unacceptable.

## 7. Polling

- a. The software shall provide a multitasking-type environment that allows other Windows®-compatible programs to run on Client and Server computers without interrupting or disturbing communications with the network of E700 Panels or operation of the software. The system software shall always be capable of alerting a user to security events as required while other programs are running.

## SCHEDULE 2 - **Minimums and Maximums**

### 1. Architecture

- a. The system software shall be a native Windows .NET framework application and run on IBM compatible Personal Computers using

the Microsoft Windows XP Professional or Microsoft® Windows® Vista Ultimate operating system.

- b. The .NET framework shall consist of modular applications including a primary Application Server, Hardware Gateway, standard user interface Client, Report Client, Photo Identification Client, Event Video Recorder, Global Linkage Service, Graphics Mapping Client and shall utilize Microsoft SQL Server Express or Microsoft SQL Server 2005.
- c. The application server shall be the only component of the SIMS that communicates with the SQL database; Client PCs shall not communicate with the SQL database directly.
- d. All interaction with the SQL database from the SIMS must be performed using stored procedures for increased efficiency.
- e. The system shall be able to operate on a single PC or multiple PCs.
- f. The system shall support the ability to separate the Application Server, SQL database, Hardware Gateway and all associated Clients to separate PCs.
- g. System shall support the use of DHCP addressing for all gateways and all clients.

## 2. Capacities

- a. The system software application server shall be capable of controlling/monitoring up to 16,384 doors, or 254,976 four state supervised inputs or 254,464 relay outputs.
- b. Each Application Server shall be able to communicate with up to 32 Gateways concurrently.
- c. Application Servers shall be able to communicate with AP, SCP and EP series Gateways simultaneously.
- d. Each Gateway shall be able to communicate with up to 256 AP, SCP or EP series System Processor Modules (SPM) concurrently.
- e. The software shall support up to 8 site codes per SPM.
- f. Each site code shall be configured independently with a value range from 0 to 999,999,999,999.
- g. The system shall support card numbers with a value range from 1 to 999,999,999,999,999.

- h. The system shall support the use of PIN digits in a PIN only mode, Card or PIN mode, or Card and PIN mode at selected readers. The PIN digit assigned to a cardholder shall be capable of different lengths for each cardholder with a range of 0 to 15 digits. Leading zero PIN digits shall be supported.
- i. Each SPM shall support the connection of up to 64 card readers.
- j. Each SPM shall support up to 1000 user defined linkage macros with 100 instructions per macro. The total number of macros shall be configurable based on available memory at the SPM.
- k. The system shall provide 255 time schedules and 255 holidays per primary field panel. Each time schedule shall support 12 intervals with each interval having a start time, end time, day of week selection, and up to 8 holiday types. Each holiday shall support a type designation and a start date plus the number of days for the holiday to be enforced. Holidays shall have the ability to be configured to extend into the following week, month, or year as desired.
- l. The system shall support user definable EOL for each input point in the system including reader door contact and request to exit inputs. The EOL shall include a minimum and maximum resistance value for both the active and inactive states of the input. In addition to the normal status changes between the inactive and active states, the system shall report the following conditions: open circuit, shorted circuit, grounded circuit, EOL tolerance. In the event the circuit resistance cannot be classified due to rapid changes in the circuit resistance, a non-settling error shall be reported.
- m. The system shall have the ability to support up to 256 Client work stations on a LAN/WAN/Internet connection.
- n. The system shall support configuration of Gateway computers for connection to the field panels. Each field panel Gateway shall support up to 56 primary field panels to support up to 512 card reader connections. The system shall support the capability to configure the Gateway, Database Server, Application Server and Client GUI on a single PC, or distributed in a network environment.

### SCHEDULE 3 - **Anti-passback**

#### 1. Anti-passback

- a. The system shall support 5 modes of anti-passback as follows:

- 1) Soft Anti-Passback - This selection allows the user access (if the access level for the cardholder is valid) regardless of the current cardholder Anti-Passback area. If the card is presented out of sequence, an Access Granted - Anti-Passback Violation event will be generated and the system will allow the cardholder access through the reader. However, once the cardholder opens the door, the cardholder is now "in" the destination area.
- 2) Hard Anti-Passback -This selection requires that the user be "in" the correct anti-passback area when presenting the card for authorization. An incorrect area will be denied access, and an Access Denied - Anti-Passback Violation event will be generated and the system will **not** allow the cardholder access through the reader. Once this happens, the card will be denied on all other readers with this selection, regardless of area.
- 3) Timed APB, Last Valid User -This selection uses just one reader to control an area. Since there is no reader leaving the area, a time limit is selected for anti-passback rules to be applied. This means that the card cannot be used at the reader for the specified time interval after the initial access grant or until the reader has been used by another valid user. The system software shall allow the operator to type in the exact time in hours, minutes and seconds. It shall not be acceptable to use drop down values or inputs in seconds only. The maximum value shall be 18 hours, 12 minutes, 16 seconds with a 1 second resolution.
- 4) Timed APB, Per User - This selection uses just one reader to control an area. Since there is no reader leaving the area, a time limit is selected for anti-passback rules to be applied. This means that the card cannot be used at the reader for the specified time interval after the initial access grant and is on a per user basis. The last valid access at each reader is tracked for each cardholder. . The system software shall allow the operator to type in the exact time in hours, minutes and seconds. It shall not be acceptable to use drop down values or inputs in seconds only. The maximum value shall be 18 hours, 12 minutes, 16 seconds with a 1 second resolution.
- 5) Timed Hard APB, Soft Anti-Passback - This selection is a combination of different anti-passback modes. For the time

limit specified, the reader operates in Hard Anti-Passback mode for each cardholder. At the end of the time limit, the reader operates in Soft Anti-Passback mode for each cardholder. This allows for the strictest anti-passback rules to be applied for a specific time, and then the more relaxed rules apply. This mode will provide the best combination of security and management when applying anti-passback rules. . The system software shall allow the operator to type in the exact time in hours, minutes and seconds. It shall not be acceptable to use drop down values or inputs in seconds only. The maximum value shall be 18 hours, 12 minutes, 16 seconds with a 1 second resolution.

## **SCHEDULE 4 - Door Configuration**

### **1. Door Configuration**

#### **a. Door Hardware**

- 1) The system software shall support configuration of a wide variety of doors and support for all industry standard reader types and peripheral hardware. The system software shall allow for selection of reader type and include selections for: Magnetic Stripe, Magnetic Stripe w/Keypad, Magnetic Stripe no Keypad (2 wire LED), Wiegand/Prox 1 wire LED, Wiegand/Prox 1 wire LED / 4 bit keypad, Wiegand/Prox 2 wire LED / 4 bit keypad, Wiegand/Prox 1 wire LED / 8 bit keypad, Wiegand/Prox 2 wire LED / 8 bit keypad and ORIS 200 readers.
- 2) The system software shall provide direct enrollment support for Bioscrypt V-Series fingerprint readers. Direct storage of templates on SPMs as well as no separate 485 network for Bioscrypt is required.
- 3) The system software shall provide for configuration and setup of door position switches, request to exit (REX) devices and all associated door hardware.
- 4) The system software shall provide for the configuration of door strike times, help open times and ADA timing by allowing the operator to type in the exact time in hours, minutes and seconds. It shall not be acceptable to use drop down values or inputs in seconds only. The maximum value shall be 36 hours, 24 minutes, 30 seconds with a 2 second resolution.
- 5) Through the door configuration interface, the user shall be able to set up, monitor and control the security hardware components in the software for any door or access-control point

in the system. The interface shall also allow the user to see doors that have been configured, edit existing door configurations and delete door configurations from the system.

- 6) Door configurations shall provide the system with flexible and specifiable lockout capabilities that enable users to rapidly lock all doors, selected doors or even a single door to prevent entry. Systems unable to affect a rapid, comprehensive lock out at all doors, any-sized group of doors or a pinpointed, single door in a system shall be unacceptable. It shall be possible to configure the lockout parameters so that designated cardholders may override the lockout command(s) and retain entry access at the locked-out doors. Systems that are not capable of easily conferring cardholder-by-cardholder permissions to override lockout or that confer such permissions only on a cardholder-group basis shall be unacceptable. The software shall also enable administrators or authorized users to lock out doors without allowing any cardholder(s) to exercise override privileges. Systems incapable of establishing lockout without override at any single door, combination of doors or all doors shall be unacceptable.

## SCHEDULE 5 - **Relay Assignment**

### 1. Relay Assignment

- a. It shall be possible to individually assign input points and relays through the software to readers to permit door monitoring and door-lock control. "Autolock" shall be software-selectable on a per-reader basis and when activated shall cause the pulse time of the corresponding relay and the shunt time for the door-position input to reset when the door closes, overriding the programmed relay pulse time and input point shunt time and re-securing the door. Systems that are not capable of "autolock" shall be unacceptable.
- b. It shall be possible to configure additional input points and output relays to program user defined applications aside from door control. A system that does not provide a linkage macro tool that allows the user to define input/output linkages that can be triggered from a card read, user command, input point and computer manual control shall be unacceptable.

## SCHEDULE 6 - **Point Groups**

### 1. Point Groups

- a. The software shall allow access to listings of all alarms, readers, relays, schedules and access levels. Administrators and authorized users shall be able to view, edit, add, or delete any or all alarms, readers, relays and/or schedules and access levels.
- b. Administrators and authorized users shall also have the capability to use the same display screen to mask, unmask any alarm point; turn on, turn off, or pulse any relay; or lock, unlock, momentary release or set modes including card only, card or pin, card and pin, or pin only for any card reader. In addition, the two card requirement and biometric verify requirement shall be able to be set on or off.

## SCHEDULE 7 - **Filters**

### 1. Filters

- a. The system software shall provide the user with Filters for filtering information displayed on a transaction screen and a separate filter for filtering the display of cardholder images in the Roll Call window as described in this specification. The Filters option shall be per device and per user and capable of displaying concise, standard or diagnostic levels of information. It shall be possible to filter out or not filter out any or all system events and messages in the system as required. The system shall still be capable of recording all transactions in history even if filters are created and used.

## SCHEDULE 8 - **Alarm Management**

### 1. Alarm Management

- a. The software shall provide for alarm management capabilities. It shall be possible to set up any system transaction or event 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.
- b. The software shall permit the linking of audio WAV files to the generation of a defined alarm. The playing of the WAV file shall provide immediate audible alerts of a defined alarm.

## SCHEDULE 9 - **Event Linkages**

### 1. Event Linkages

- a. The system software shall provide the capability to link any system transaction or event such as: schedule change, input, door or user group action, alarm acknowledgement or user command to a user defined series of actions including initiation of other user defined action lists, relay control, door mode control, alarm generation, schedule enable/disable and ASCII-text out to a 3<sup>rd</sup> party system or device. The software shall provide an easy-to-use tool for configuring these event links. The authorized system user shall be able to define system actions to occur as a result of the user specified conditions. All user defined linkage macros must reside and execute in the system field panel and not at the computer. All linkages must be able to operate when the host PC is not connected. Systems that do not allow users to easily link any system generated activity as a trigger condition for the user defined action lists that operate at the field panel shall be unacceptable.

#### SCHEDULE 10 - **Cardholder Database**

1. Cardholder Database
  - a. It shall be possible through the software's User Interface to add, edit, activate, deactivate and/or delete individual card or cardholder records. The software shall in all instances support the maximum number of cardholders that are stored in the memories of all the SPMs installed and used. It shall also permit assignment of up to 30 card number credentials to a single card holder record to facilitate assignment of multiple cards to a single cardholder, if desired.
  - b. A cardholder entry screen shall provide tabbed pages to allow a system user to:
    - a) Capture a photo using a digital camera or retrieve a stored photo file for inclusion in individual new or existing card or cardholder records. Photos shall be displayable in the cardholder record and printable on a photo ID badge, and they shall be made part of the card and cardholder record
    - b) Digitally store the photo in over 39 different formats including BMP, GIF, JPG, and TIF and export the selected image to any of the 39 formats.
    - c) Configure and assign virtually unlimited access groups, which consist of a time schedule and a reader group
    - d) Provide separate drop-down calendar controls for use in assigning card-activation and card-expiration dates
    - e) Enter cardholder names, user group membership, access level information, a personal identification number (PIN), company information and user defined custom data fields
    - f) Enable anti-passback override

- g) Set cardholder ADA information
- h) VIP status
- i) View data concerning the recent transaction for the cardholder in the system
- j) Enable PIN Exempt override

SCHEDULE 11 - **Databases**

The system software shall use the Microsoft® SQL Server 2000/2005 or Microsoft® SQL Server 2005 Express. The software installation application shall allow the user/installer to install the appropriate database if it is not already installed on the system computer or network. The appropriate drivers shall be automatically installed as part of the installation.

SCHEDULE 12 - **Multiple Users**

The system shall provide for multiple concurrent users. The system shall allow via a license process for 16 users per license.

SCHEDULE 13 - **Hardware Gateways**

The system shall be architected so that it can operate on a single computer or multiple computers depending upon the size of the system. The system shall support the use of Hardware Gateway computers that can be configured to communicate with up to 256 Eclipse™ SPMs.

SCHEDULE 14 - **Graphics Mapping Client**

The system shall provide a Graphics Mapping Client. The mapping client shall support vector based mapping. Bitmap image icons are not acceptable. If maps are resized they must retain aspect ratios. The mapping client must display a floor view, unit view and sensor view on a single screen. The system shall not require the operator to switch to alternate views.

SCHEDULE 15 - **Event Video Recorder**

The system shall provide an open architecture event video recording solution for video management. The EVR must employ seamless integration and be built on a Microsoft .NET framework. EVR must be user friendly with the complexity and sophistication hidden from the user to provide a uniform, simple look and feel. EVR shall be an advanced Open IP-Surveillance module with integrated video analytics that can detect and prevent threatening events in real-time. It shall simultaneously enable digital video recording from network, mega-pixel and analog devices, intelligent video analysis and remote access to live and recorded images from any networked computer.

## **PART 2 - Products**

### **2.1 Manufacturers**

#### **2.1.1 Manufacturer**

Acceptable manufacturers of access-control systems include:

Keri Systems Inc..

#### **Accepted Alternates:**

The specified PC-based Access Control and Monitoring Software shall be Eclipse™ 700 from Keri Systems Inc. The hardware panels for Eclipse™ 700 are the Mercury Security AP and EP/SCP series panels. These panels will be referred to as the Eclipse™ 700 panels throughout the specification.

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

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.

## **2.2 Components and Functions**

### **2.2.1 General**

#### **2.2.1.1 General**

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

The SPMs and Modules shall receive data input from other hardware components of the system, such as readers, input devices and relays. All system panels shall be connected to the system server(s) where event history, cardholder data and system programming data shall reside. The SPMs shall receive data input from, and provide system data to, the controlling system server(s) as part of the system polling process.

The system shall be of true multi-user 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. In addition, changes made to the system shall be updated in real-time to other users of the system.

### **2.2.2 Components - Access Control**

#### **2.2.2.1 Power Supply**

The Eclipse™ 700 Panels (SPMs, Door Modules, and Input or Output Modules) in the system shall be powered by a 12-VDC power supply with battery backup charger.

Upon failure of normal power to the SPM and Modules, the panel shall be temporarily powered from four (4) to six (6) hours by a backup 12 VDC gel-cell battery. The transition to the battery backup power shall be automatic to prevent the loss of transactions or notification of any alarm, trouble or operator acknowledgment signals during the transition. Readers powered by the SPMs shall be temporarily powered by the backup battery. Readers and other peripheral devices with separate power supplies shall not be provided backup power via the panel backup battery. The duration of operation shall be a function of the number of equipment connected to the panel and the individual power requirements of that equipment.

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

#### **2.2.2.2 Installation**

The software shall incorporate an installation feature that allows simple PC-by-PC loading of the system software, database and panel services and any client (User) interfaces.

#### **2.2.2.3 Services**

The system shall employ a minimum of one (1) Application service, one (1) Database service, (1) Hardware Gateway service and one (1) User Interface.

#### **2.2.2.4 User Interface**

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.

The background and text colors for all transaction-display screens shall be customizable for each user, and it shall be possible to apply filters to display only selected transactions on a transaction-display screen, as described in this specification.

The screen layouts shall provide for viewing system cardholder activity; monitoring and acknowledging alarms; and monitoring and controlling input points, relays and door configurations. Capability to include a site tree per connected hardware gateway for displaying system setup and configuring system parameters shall be provided. It shall be possible to create tabbed windows in the screen layout to conserve desktop space in the viewing area without in any way restricting the availability of information that can be displayed for the user.

The user interface will provide a hardware configuration tree and display grids to display information to the user. The hardware configuration tree shall display 1 gateway at a time for configuration while actively monitoring all system gateways.

The user interface shall store the screen layout on a per login basis to include the following: docking positions and state of all dockable controls, group sort categories and direction of all status views, displayed/hidden columns in all status views.

#### **2.2.2.5 Peripherals**

The system shall allow the use of commercial, off-the-shelf printers and digital cameras for the capture of identification photos and printing of identification badges and system activity reports.

#### **2.2.2.6 Selectable Wiegand/Magstripe Card Formats**

Users shall be able to select up to eight (8) Wiegand® or magnetic stripe formats per E700 main controller that are used by the system's Wiegand® or magnetic stripe readers. Each format selected shall have a different bit length and an offset parameter that automatically adds the offset to the card number. After these Wiegand® formats have been selected, the panel shall automatically recognize the format used by a Wiegand® reader

communicating to it.

The system shall provide an easy to use interface that allows an authorized user or system administrator to select formats from a list or to create custom formats for use with the system.

Systems that do not include the format editor or offer the selection of eight (8) different Wiegand® bit formats per site and do not provide the capability to use cards utilizing the eight (8) different Wiegand® bit formats selected shall be unacceptable.

#### **2.2.2.7 ASCII Output**

The system software shall provide the ability to transmit ASCII codes from the primary field panel to 3<sup>rd</sup> party systems. The system shall provide a linkage editor that allows the authorized user or system administrator to define the ASCII strings that will be sent to 3<sup>rd</sup> party equipment such as CCTV systems, DVRs and other security equipment based on user commands or system initiated events that have been defined by the user.

Systems that do not provide the capability to initiate ASCII commands from the primary field panel that are defined by an authorized user or system administrator shall be deemed unacceptable.

#### **2.2.2.8 Card Design**

It shall be possible to create and save an unlimited number of card template designs. Systems that do not permit users to create and save multiple custom card designs shall be unacceptable. The system shall allow any or all of the following elements to be employed together in card design that can be used to create individual, cardholder-specific cards or identification badges:

- Captured or retrieved cardholders' photos that are part of the cardholder database
- Graphics, logos or other images
- Static data that is duplicated on each card printed
- Variable data from the cardholder database that is specific to each card printed

- Bar codes

It shall be possible for users to create card designs that employ:

- A choice of vertical orientation or horizontal orientation with optional card rotation
- Dual-sided printing
- Predefined or custom dimensions
- Cardholder photos, with optional borders. It shall be possible to rotate the image, select border color and width and adjust the image brightness
- Bitmaps or JPEGs of logos, designs, pictures and other graphics, including a card background color or graphic, all with definable dimensions
- Text using the design using font selections available in Windows®. It shall be possible to vary the formatting of this text.
- Slots for insertion of clips, lanyards, etc.
- Bar codes associated with database fields that shall be selected from a drop-down list that includes not only the database fields but also a constant or separator. The user shall have the capability to select the field length, use of padding, padding characters, position, rotation, ratio, height, size and readability of text appearing with the bar code.

The system software shall be capable of allowing unlimited individual badge designs to be designed and created. It shall be possible to preview the design before saving. The software shall allow for on-screen printer selection from a drop-down list that displays all installed print drivers within Windows®.

The user shall be able to define logical arguments based on selected database information that may vary from card record to card record. It shall be possible to define different bitmap images to appear on the printed card as a result of the application this logic, which uses the specific data from the database as the criterion for displaying or not displaying the image. In this way, logos or color-coding can be used to identify cardholders having, for example, the same department assignments, shifts, job assignments or the like.

#### **2.2.2.9 Card Printing**

The software shall permit the printing of identification cards using selected designs as described in this specification

#### **2.2.2.10 Custom Pages and Fields**

The software shall provide pages in the cardholder database module to allow custom fields to be saved to the cardholder database. These fields shall be displayed in the software on a custom tabbed page that can be added for display in the cardholder database interface in the software. It shall be possible for users to:

- Rename each field and its accompanying label
- Enter and save existing data into the custom field, or delete the data from the field

Systems that do not support the creation of user-defined fields in the cardholder database GUI or of user-defined fields in that database for display in the GUI shall be unacceptable.

#### **2.2.2.11 Card Templates**

The software shall provide a page in the cardholder database module to permit template definitions that can be assigned to new card holders.

#### **2.2.2.12 Gateway List**

A Gateway list window shall be available to allow SPMs to be edited, or deleted within the system software. It shall also be possible to easily display in the status of other hardware such as card readers and alarm inputs.

#### **2.2.2.13 Reports**

The system software shall include a built in Report Designer. The Report Designer shall not be Crystal Reports. The system report

designer will provide the capability to design all system reports with the capability to:

- Define report type
- Add selected fields
- Define report headers and footers
- Add logos and images

The system will include pre-defined reports for cardholder listings, system messages, and history and alarm messages.

Reports may be viewed on-screen, printed, or exported to a file. While in display mode, the system shall support a search function for user entered text.

The system shall support exporting of the reports to the following formats:

- a) Rich Text Format (RTF)
- b) Portable Document Format (PDF)
- c) HTML
- d) Microsoft Excel Worksheet (XLS)
- e) Tagged Image File Format (TIFF)
- f) Text delimited file

The system shall also support the followings options when exporting a Portable Document File (PDF) format:

- a) Assignment of the Owner Password
- b) Assignment of the User Password
- c) 40-bit, 128-bit or no Encryption
- d) Allow/disallow printing
- e) Allow/disallow modify contents
- f) Allow/disallow copy
- g) Allow/disallow modify annotations

Systems that do not provide the capability to export an encrypted, password protected Portable Document File (PDF) shall be deemed unacceptable.

#### **2.2.2.14 Elevator Control**

Elevator control shall be user configurable using the linkage macro system. The Eclipse™ 700 provides the flexibility to connect to elevator systems using either the Output Control Module (OCM) or the ASCII out capability of the System Processor Module (SPM). The system software shall provide the authorized user or system administrator with the ability to enable floor call buttons based on card access by certain user groups. When a card holder uses the elevator reader, the system linkage macro will enable the floor buttons assigned to the user group to which the card holder is assigned. The system can either enable the relays on the OCM that are in series with the elevator cab floor buttons or send a user defined ASCII stream across an RS-232 connection to the elevator cab control module.

#### **2.2.2.15 Input Supervision**

Supervision of system input points shall be provided by the control panel. User definable EOL resistances values shall be configurable for every input in the system including reader door contacts and request to exit inputs. Failure or fault of power supply to panels(s) or data connections between the panel(s) and server(s) shall be indicated on the system display on a User Interface PC.

### **2.3 Field Hardware**

#### **2.3.1 Controller Panels**

##### **2.3.1.1 Eclipse™ 700 System Processor Module (SPM)**

The SPM shall provide access control, alarm monitoring and time zone control for both access to and egress from selected areas. The panel shall provide two-way communications via TCP/IP, RS-485 or RS-232 to the host computer. The panel will provide RS-485 communications protocol between panels. The panel shall accommodate system expansion and shall support up to sixty-four (64) readers when door modules are added via RS-485.

The System Processor Module shall be Model DHS-EP-1502 provided by Keri Systems Inc.

#### **2.3.1.2 Eclipse™ 700 Dual Door Module (DDM)**

The Dual Door Module (DDM) shall provide access control, alarm monitoring and time zone control for both access to and egress from selected areas. The DDM shall provide two-way communications via RS-485 protocol between panels. The DDM shall accommodate system expansion and support up to two (2) readers.

The module shall be Model DHS-SCP-DDM, or DHS-AP-DDM provided by Keri Systems Inc..

#### **2.3.1.3 Eclipse™ 700 Input Control Module (ICM)**

The Input Control Module (ICM) shall provide 8 or 16 general-purpose four-state supervised inputs when connected to the SPM. Each input point shall have an LED indicating the state of the point. Input shall be defined as Normally Open (NO), Normally Closed (NC), Supervised, Non-Supervised and shall have user definable end of line supervision values.

The Input Control Module shall be Model DHS-SCP-ICM, or DHS-AP-ICM provided by Keri Systems Inc..

#### **2.3.1.4 Eclipse™ 700 Output Control Module (OCM)**

The Output Control Module (OCM) shall provide 8 or 16 general-purpose form 'C' relays when connected to the SPM.

The Output Control Module shall be Model DHS-SCP-OCM, or DHS-AP-OCM provided by Keri Systems Inc..

#### **2.3.2.3 Ethernet LAN Adapter**

The LAN Adapter will allow connection of the SPM to the host PC via TCP/IP communications.

The LAN Adapter shall be Model DHS-DP-LAN provided by Keri Systems Inc..