CORPORATE EDITION

ENTRAPASS

Access Control and Security Management Software

Architectural and Engineering Specifications

KANTECH

A Tyco International Company

DN2153-1905/Version 8.10

TABLE OF CONTENTS

PART I GENERAL

1.1 GENERAL DESCRIPTION

The security management system (SMS) shall be a modular access management system used to better control employee and visitor movements at various establishments. The SMS shall be designed to maximize all tools offered by the Windows platform. All commands shall be accessible using nothing more than a mouse, and keyboard use shall be limited to documenting fields requiring numeric or alphanumeric data.

The operating program shall be multi-user and multi-tasking and capable of running on a non-proprietary CPU or virtual machines. The application software shall be based on a standard, high level programming language. The SMS shall be modular to facilitate its installation and the development of its capabilities while avoiding major modifications in its operation and in saving all defined system and historical data.

The server shall be a database server using a Sybase embedded SQL database. All database management tools shall be included, such as back-up, indexing, and database cleaning tools. No third party database tools or licensing shall be required. The Multi-Site Gateway shall communicate system information between the server and controllers. The workstations shall be the primary user interface to perform supervisory and programming functions.

The SMS shall enable the selection of at least two user languages. The basic dictionary shall include English, French, Spanish, Italian, Portuguese, Simplified Chinese, Dutch, Turkish, and German, however, the system shall include a vocabulary editor to be used in designing custom language dictionaries. The operator's profile shall permit the selection of one of the two basic languages.

The SMS shall include RS-232 / RS-485 communication link between the various system components as well as TCP/IP network interface capability. Field devices such as card readers, alarm inputs, control points shall be connected to fully distributed intelligent field panels capable of operating without host computer intervention in a non-degraded mode.

The SMS shall be able to design customized ID cards directly from the access management software. No specific program or software other than the access management software and no additional licensing shall be required for this function. Any workstation shall be capable of being used as a badging station. Badging shall be fully integrated with the card database.

1.2 SUBMITTALS

1.2.A Shop Drawings

Prior to assembling or installing the SMS, the contractor shall provide complete shop drawings, which include the following:

1. Architectural floor plans indicating all system device locations.
2. Full schematic wiring information for all devices. Wiring information shall include cable type, cable length, conductor routings, quantities, and point-to-point termination schedules.
3. Complete access control system one-line block diagram.

4. Statement of the system sequence of operation.
5. Riser diagrams showing interconnections.
6. Detail drawings showing installation and mounting.
7. Fabrication drawings for console arrangements and equipment layout.
8. Test and Commission site report.

All drawings shall be fully dimensioned and prepared in DWG file format using AutoCAD.

1.2.B Product Data

Prior to assembling or installing the SMS, the contractor shall provide the following:

1. Complete product data and technical specification data sheets that includes manufacturer's data for all material and equipment, including terminal devices, local processors, computer equipment, access cards, and any other equipment provided as part of the SMS.

2. A system description, including analysis and calculations used in sizing equipment required by the SMS. The description shall show how the equipment operates as a system to meet the performance requirements of the SMS. The following information shall be supplied as a minimum:

    a. Central processor configuration and memory size.
    b. Description of site equipment and its configuration.
    c. Protocol description.
    d. Hard disk system size and configuration.
    e. Backup/archive system size and configuration.
    f. Startup operations.
    g. System expansion capability and method of implementation.
    h. System power requirements and UPS sizing.
    i. A description of the operating system and application software.

1.2.C As-Built Drawings

At the conclusion of the project, the Contractor shall provide "as built" drawings. The "as built" drawings shall be a continuation of the Contractors shop drawings as modified, augmented, and reviewed during the installation, check out and acceptance phases of the project. All drawings shall be fully dimensioned and prepared in DWG file format using AutoCAD.

1.2.D Manuals

At the conclusion of the project, the Contractor shall provide copies of the manuals as described herein. Each manual's contents shall be identified on the cover. The manual shall include names, addresses, and telephone numbers of each security system integrator installing equipment and systems and the nearest service representatives for each item of equipment for each system. The manuals shall have a table of contents and labeled sections. The manuals shall include all modifications made during installation, checkout, and acceptance. Date of project commencement, milestones, CCO's and completion to be included also. The manuals shall contain the following:

1. Functional Design Manual

The functional design manual shall identify the operational requirements for the system and explain the theory of operation, design philosophy, and specific functions. A description of hardware and software functions, interfaces, and requirements shall be included for all system operating modes. All operational changes required by customer are to be documented in writing where they differ from original specification

2. Hardware Manual

   The hardware manual shall describe all equipment furnished including:

   a. General description and specifications.
   b. Installation and test and commission procedures.
   c. Equipment layout and electrical schematics to the component level.
   d. System layout drawings and schematics.
   e. Alignment and calibration procedures.
   f. Manufacturers repair parts list indicating sources of supply.
   g. Load calculations of equipment operating at maximum load.

3. Software Manual

   The software manual shall describe the functions of all software and shall include all other information necessary to enable proper loading, testing, and operation. The manual shall include:

   a. Definition of terms and functions.
   b. Use of system and applications software.
   c. Initialization, startup, and shut down.
   d. Alarm reports
   e. Reports generation
   f. Data base format and data entry requirements.
   g. Directory of all disk files.

4. Operators Manual

   The operator's manual shall fully explain all procedures and instructions for the operation of the system including:

   a. Computers and peripherals
   b. System startup and shut down procedures.
   c. Use of system, command, and applications software.
   d. Recovery and restart procedures.
   e. Graphic alarm presentation
   f. Use of report generator and generation of reports.
   g. Data entry
   h. Operator commands
   i. Alarm messages and reprinting formats.
   j. System access requirements

5. Maintenance Manual

   The maintenance manual shall include descriptions of maintenance for all equipment including inspection, periodic preventive maintenance, fault diagnosis, and repair or replacement of defective components. Maintenance manual shall also include a list

of recommended spares, which are liable to be encountered as part of routine service procedures.

1.3 QUALITY ASSURANCE

1.3.A Manufacturer Qualifications

The manufacturers of all hardware and software components employed in the SMS shall be established vendors to the access control/security monitoring industry for no less than five years and shall have successfully implemented at least five systems of similar size and complexity.

1.3.B Contractor/Integrator Qualifications

1. The security system integrator shall have been regularly engaged in the installation and maintenance of integrated access control systems and have a proven track record with similar systems of the same size, scope, and complexity.

2. The security system integrator shall supply information attesting to the fact that their firm is an authorized Kantech corporate dealer.

3. The security system integrator shall supply information attesting to the fact that their installation and service technicians are competent factory trained and certified personnel capable of maintaining the system and providing reasonable service time.

4. The security system integrator shall provide a minimum of three (3) references whose systems are of similar complexity and have been installed and maintained by the security system integrator in the last five (5) years.

5. There shall be a local representative and factory authorized local service organization that shall carry a complete stock of parts and provide maintenance for these systems.

1.3.C Testing Agencies

1. The following hardware have been tested and listed by Underwriters Laboratories (UL) for UL 294 for access control system units.

    a. KT-300
    b. KT-400
    c. KT-1
    d. IP link
    e. P225W26
    f. P225KPW26
    g. P225XSF
    h. P225KPXSF
    i. P325W26
    j. P325KPW26
    k. P325XSF
    l. P325KPXSF
    m. KT-MOD-REL8
    n. KT-MOD-INP16
    o. KT-MOD-OUT16
    p. KT-3LED-Plate

q. KTES.
r. ioSmart Readers
    1. KT-MUL-MT
    2. KT-MUL-SC
    3. KT-SG-MT
    4. KT-SG-SC
    5. KT-SG-MT-KP
    6. KT-MUL-MT-KP

2. The hardware shall comply with the following regulatory requirements:
    a. FCC Part 15 Class A.
    b. FCC Part 15 Class B.
    c. FCC Part 68 (TIA968).
    d. ICES-003.
    e. CE.
    f. ECCN for AES 128 bit encryption for IP communication.
        i. IP Link, KT-400 or KT-1 only.
    g. Government standards NISPOM 5-313 Automated Access Control Systems, DICD Annex F 2.3 Accept/Reject Threshold Criteria, JAFAN Annex D 2.3 Accept/Reject Threshold Criteria.
    h. The ioSmart readers shall have an IP 55 rating.

3. The SMS shall support Americans with Disabilities Act (ADA) compliance in door and access operation.

1.4 WARRANTY

The security management system (SMS) shall be provided with a 12-month product warranty from date of registration. Software version updates shall be available for no charge during this warranty. The software media warranty shall be 90 days.

PART II PRODUCTS

2.1 MANUFACTURERS

The security management system (SMS) shall be the Kantech EntraPass Corporate Edition.

2.2 DESCRIPTION

The security management system (SMS) shall be an integrated system that utilizes a Sybase embedded SQL database for the storage and manipulation of related data. The SMS shall include a server with applications software, Multi-Site Gateways for communication between the server and controllers, operator and administrator workstations with appropriate software, hard copy printers and backup media. The security field devices (readers, door position switches, REX) shall communicate with the field panels via a dedicated cable network. The field panels shall communicate to the server via a Fast Ethernet 10/100 TCP/IP network, RS-232/RS-485 connection, or dial-up modem.

The SMS shall allow for growth and scalability from a smaller system to a larger, high-end, or enterprise system. The SMS shall be modular in nature, allowing system capacities to be easily expanded without requiring major changes to system operation. All defined system data as well as historical information shall be maintained. Customizable user interfaces shall allow management of system information and activity for administrators and operators. The response time between the moment when a card is presented at the reader and when the door is unlocked shall not exceed one second. The SMS shall include a badging solution with a GUI for badge design. No extra licensing shall be required for the badging solution.

The SMS shall be able to connect to authenticated SSL cloud based or non-SSL or non-authenticated e-mail server for all e-mail features described. The SMS shall be able to connect to an SMTP or POP3 authenticated e-mail server.

The SMS shall support the following devices:

20	Workstations
50	Concurrent Web/mobile applications.
20	Redundant Servers
40	Digital video recorders per type
41	Multi-Site Gateways
2,048	Connections per Multi-Site Gateway (max: 10,000 doors).
10,000	Door controllers per Multi-Site Gateway.
10,000	Readers per Multi-Site Gateway.
100,000	Monitored points per Multi-Site Gateway.
100,000	Control relays per Multi-Site Gateway.
Unlimited	Access cards
Unlimited	Card families or site codes.
2	Simultaneous operator languages.

2.3 PERFORMANCE - MONITORING

2.3.A Monitoring Mode

1. The SMS shall enable every operator to customize their desktop configuration. It shall be possible to modify the desktop appearance and to create up to eight desktops and to associate up to 10 different display screens to each. It shall be possible to modify the size and position of all screens. It shall be possible to determine if these screens shall be floating anywhere on the desktop or fixed on the desktop. If the workstation is equipped with a dual output video card and two or more monitors, it shall be possible to distribute the screen to multiple monitors. However, each screen shall be able to be viewed alone or together depending on operator needs. Once these parameters are saved, the configuration shall automatically take effect whenever the operator logs in.

   For all types of screens, it shall be possible to access the general properties of the screen by simply right clicking at the center of the screen. From there it shall allow for linkage between associated screens without having to exit the current screen or section. It shall be possible to right click events on the desktop for editing which shall bring the user directly to the card, door, or component window and back.

2. Message Screen

   All events that occur shall appear in real time. The text shall include at least the date, time, and a pertinent description of the event as well as its condition. The display of this screen shall be customizable and a different background and message color can be used for every type of event.

   In addition the background color shall be chosen per operator. Events shall appear in their defined color or the operator shall have the option to choose a text color for the events.

   All component modification events shall be tagged with an addition (+), modification (=) or deletion (-) tag.

   Every in-coming event shall be documented by one or more icons representing video images, photos, access card, server, gateway, controller, card reader, and relay or supervision point. It shall be possible to classify the events on the screen by sequence, date and time, type of event, or type of message. In addition, a text filter shall be available to facilitate searching. It shall be possible to access the last up to 100,000 transactions from this window without the need to request a special report.

   It shall be possible to see the origin of the event so that the operator shall be able to see the event's parent. For example door and access events shall show the location (site) of the event.

   It shall be possible to right click on an event and perform edit or other functions linked to the event.

3. Cardholder and Operator Photo Screen

   When a card is presented to a card reader, the software shall automatically display the photograph of the cardholder in this window. From this screen it shall be possible to select the cardholder's name, card number, event text, and comments as well as

specify a door or group of doors for which the operator would like to display a photo. The SMS shall support the display of up to four pictures simultaneously. Furthermore the SMS shall allow that each picture box be assigned to a specific door for additional filtering. In addition the SMS shall support the ability to view the operator's picture when operators generate events.

4. Filtered Message Screen

   This screen shall be a copy of the text messages screen except it shall be possible to select a specific message filter. The SMS shall include a choice of pre-configured filters and the ability to create customized filters. For every new filter it shall be possible to associate a name to it, select the type of event, select door, select workstation, select gateway, select supervision input, and select output.

5. Alarm Screen

   Alarms that require an acknowledgement by an operator shall be displayed on this screen in text form only. The text shall include at least the date, time and description of the alarm, and its condition. It shall be possible to classify events on the screen by sequence, date and time, type of event, or type of message. A text filter shall be available in order to facilitate the search.

   When the SMS pop-up is acknowledged by e-mail, the SMS shall display the operator's name based on the e-mail that acknowledged it.

   If instructions about an alarm are envisaged, they shall automatically appear in a second window on the screen. If a graphic is associated with the alarm, it shall appear automatically on the screen defined to this effect. The icon associated to the control point shall be represented and show the actual state of the point.

   The operator shall be able to access a log book in order to document the alarm that occurred. Once this information is recorded in the log it shall not be erasable or modifiable. Operators shall also be able to see previous comments or system logs added for this event.

   Operators shall be able to run a report of the alarms from this window.

   It shall be possible to associate video call-up with an alarm. When this occurs, the main screen shall become the video screen, not the alarm screen.

6. Video Screen (Video View)

   When the SMS is integrated with American Dynamics, INTEVO Advanced, INTEVO Compact, Exacq or Panasonic DVR/NVR, it shall be possible to view the video images of cameras associated with them. The SMS shall enable the creation of an unlimited number of video views, each one associated with up to 16 different cameras or graphics. It shall be possible for the operator to see at a minimum 48 cameras simultaneously using three video views per screen. It shall be possible for an operator to edit or modify an existing view or create a new one directly from this screen. For each video view it shall be possible to select sequential, mosaic pattern, or preset viewing modes.

The SMS shall allow the operator to switch between pre-programmed video and dynamic view. The dynamic view shall allow the operator to select any camera and view it regardless of the need to create a new video view. The dynamic view shall support up to 16 cameras simultaneously.

It shall be possible for an operator to access all the commands of a motion PTZ camera to include rotate on its axis, adjust its focus, and have a larger view of the image. Accessibility to camera images and commands shall be limited by operator security level.

No additional licensing shall be required to perform this function.

The SMS shall allow the operator to select video views based on site linking. Site linking will allow SMS operators to navigate the SMS with ease by site or system wide.

7. Historical Message Screen

This screen shall allow operators to choose from a previously created custom report. Operators shall choose a start and end time, and a start and end date. The report will be populated in this window and have the same characteristics of the message screen including all right click functions.

The historical message screen shall allow operators to add comments to any event to view and edit at a later stage.

2.3.B Graphics Screen

1. There are three options for graphics that appear as background on the screen. The first is a reproduction of the building(s) floor by floor. The graphic module shall be capable of importing files in BMP, EMF, WMF, JPEG, GIF, PCX, PNG, TIF, or PCD formats.

2. The second option is using web pages, or WebViews, as background on the screen. This can be used in the following manners:

    a. Accessing to DVR web servers.
    b. Embedding default web pages into operator desktops.
    c. Adding an IP camera onto a video view.
    d. Embedding Intranet pages or directories into the operator environment.
    e. Adding PDF, Word documents to the desktop.
    f. HTML or PDF pop-up instruction on alarm.
    g. Integrating report folders in the desktop for quick access.

3. The third option is to assign a live video view as background on the screen if video integration is being utilized.

4. For all three options, control points shall be represented by a descriptive icon. Control points include workstations, gateways, controllers, card readers, doors equipped with either card readers or supervision contacts, cameras, relays, cameras, video views, task triggers and input monitoring points such as motion sensors. The icons shall be animated, meaning they shall represent the state of the point to which they are associated in real time. Every graphic shall support at least 100 control points.

4. Right clicking on an icon shall directly access the manual commands of each control point. A door shall be capable of but not limited to temporarily unlocking, manually unlocking or locking, enabling or disabling a reader, viewing the reader's comments, and enabling or disabling the KT-400 or KT-1 door contact. A supervision point shall be capable of being enabled or disabled. A control relay shall be capable of being activated, deactivated, or temporarily activated. Cameras shall be capable of viewing images or live video.

5. No additional licensing shall be required to perform this function.

6. The SMS shall allow the operator to select graphics based on site linking. Site linking will allow SMS operators to navigate the SMS with ease by site or system wide.

2.3.C Communication Methods

1. The SMS shall ensure the communication to remote sites over a LAN or WAN/Internet using a dedicated communication server device, Kantech IP Link, KT-1 Controller or the KT-400 controller. This shall only be applicable with the use of Multi-Site Gateways. It shall communicate using 128-bit AES encryption. It shall reduce bandwidth consumption by managing the communication protocol of Kantech controllers at the remote site. Polling of Kantech controllers shall be done by the Kantech IP Link, KT-1 controller or KT-400 in the field and not over the network. The Kantech IP Link, KT-1 controller or KT-400 shall provide support for up to 32 door controllers. The Kantech IP Link or KT-400 shall be configured from the access software or from a web page which has the security feature of being disabled after successful use.

2. For connections that do not have network links, communication to remote sites shall be ensured by dial-up modems. This shall only be applicable with the use of Multi-Site Gateways. The SMS shall support up to 32 such modems that can simultaneously transmit or receive data from remote connections. No modem shall be dedicated to a specific connection; communication shall be established where the first connection calling shall have access to the first available modem, and so on.

3. Each Multi-Site Gateway shall be able to control 32 local controller loops by using the RS-232/RS-485 protocols via serial or USB port. In addition, each Multi-Site Gateway shall be able to control up to 2048 (10,000 doors maximum Ethernet loops using TCP or UDP protocols, via the use of the Kantech IP Link, KT-1 controller or KT-400 of 32 controllers each.

4. The SMS shall differentiate between sites and connections. A connection shall be a hardware connection of controller over IP, direct, or dial up to the Multi-Site Gateway. A site shall be a collection of any connection from any Multi-Site Gateway.

    a. Operators shall be able to add connections to sites as needed.
    b. Operators shall assign access levels to cardholders via the site. Having to assign an access level to every connection shall be unacceptable as this is time consuming.
    c. Operators shall be able to view, lock and unlock all doors belonging to a site regardless of their connection.
        i. Operators shall have the option to expand the site and see which connection the doors belong to.

d. When programming access levels, operators shall see all doors belonging to one site. From there the operator shall be able to assign a schedule to a door for the user's access.
e. Operators shall be able to take existing connections that are not part of any site and merge them into existing sites.
    i. The SMS shall give them an option to merge identical schedules in order to remove duplication and unwanted schedules.
    ii. The SMS shall give the option to enter a duplicate name as a prefix.
    iii. The SMS shall give the ability to rename the connection's access levels names.
    iv. The ability to reprogram access levels and other items shall not be available.

5. Each site and connection shall have the ability to have 20 user definable fields. The field label names shall be changeable.
    a. Operators shall be able to enter up to 40 characters per field.

6. In all communication methods, the door controller shall retain in their memory all necessary data for controlling doors that they supervise. In case of communication failure, the door controller shall execute all its functions normally.

7. When using a KT-1 it shall be possible to use the auto-enrollment functionality. An operator shall be able to press a button on the KT-1 controller which shall find the EntraPass Multi-Site Gateway. Once found by the SMS, the operator shall quickly and efficiently be able to enroll the KT-1.

    a. The auto-enrolment shall work on a local LAN segment of the network.
    b. The SMS shall display -a dedicated list of all unassigned KT-1s. From the EntraPass workstation or Web. The operator shall simply pick the KT-1 they are interested in.
    c. The SMS shall allow the following functionality using the auto-enrolment wizard:
        i. Assign a KT-1 to a site/connection.
        ii. Name the door
        iii. Activate the exit reader.
        iv. Activate the door contact.
        v. Activate the request to exit.
    d. The SMS shall auto-fill the MAC address and Serial number. Having to manually enter the MAC address or serial number in the auto-enrolment shall not be acceptable.

2.4 PERFORMANCE – PROGRAMMING & CONFIGURATION

2.4.A User Section

1. This section shall include all functions involved in the issuance of an access or ID card as well as database search and importation tools. During the addition or modification of a card, information about the card shall be sent to the door controllers affected by these new parameters as soon as the operator accepts the addition or modification. An additional command requiring a reloading of the cards database in the door controllers shall not be acceptable.

2. The SMS shall allow adding door access exceptions to the cardholder's list of access rights.

    a. The SMS operator shall be able to provide a pre-defined access level and separately add a specific door to be part of the cardholder's access rights.
    b. The door shall have its own schedule.
    c. The SMS operator shall have the option of allowing or disallowing access to that door based on that schedule.
    d. There shall be no limit to the number of doors that can have exceptions.
    e. The KT-400 and KT-1 shall keep in memory the door access exceptions even in standalone mode. This feature shall be available with the KT-400 and KT-1.

3. The SMS shall enable the creation and definition of a user access card. There can be up to five cards per user, and users can be managed by cardholder name or card number. When creating user cards, the operator shall be able to select a card format directly from a Card dialog and enter the card number as it is printed on the card.

4. The following user information shall be able to be saved in the user section:

    a. Five card numbers each with their own expiration date, trace and lost or stolen statuses.
    b. Each card numbers shall have their own expiration date and expiration hour.
        a. The card numbers shall have the option to be mandatory or not mandatory.
    c. First and last name.
    d. Card type.
    e. Additional information (10 fields).
    f. Start date
    g. Expiry date
    h. Personal ID number (PIN).
    i. State of the card
    j. Multi-swipe activation
    k. Comments
    l. User's e-mail address
    m. go Pass configuration:
        1. Notification
        2. Language
    n. HID Mobile credentials management.

    In addition, it shall be possible to associate a photograph, signature, and badge template to a card. The picture of the cardholder shall always be visible when the profile is active on the screen.

5. The SMS shall allow for the creation of an unlimited number of card templates to be used as ID cards. Template parameters include name, number of sides, and size. It shall be possible to directly print a template on an access card. The operator shall be able to design customized badging templates directly from the access management software. No specific badging program or software other than the latter and no additional licensing shall be required for this function. Any workstation shall be capable of creating ID cards based on operator security level. The following items shall be capable of being added to and modified on a badge template:

a. All information fields associated to a cardholder.
b. Bar code
c. Text zone
d. Start date, expiry date, today's date.
e. Saved images and logos
f. Borders
g. Rectangles (including rounded rectangles, ellipse).
h. Lines and arrows
i. Photograph (can be cropped)
j. A background

6. The SMS shall allow for the creation of a day pass to be issued to visitors for a single day. The SMS shall also have the ability to create temporary ID visitor cards.

7. The SMS shall offer the possibility of modifying the parameters of a group of cards simultaneously based on Card Type. The system shall enable the creation of an unlimited number of card types. The following fields shall be modifiable:

    a. Card status (valid, invalid, lost, stolen).
    b. Card monitored (yes, no).
    c. Start date (schedule).
    d. End date (schedule).
    e. Delete after expiration (yes, no).
    f. Wait on keypad (yes, no).
    g. Access group (selection menu).
    h. Template model (selection menu).

8. The operator shall be able to search for a card by last or first name, card creation date, card number, or any of the ten fields of user definable information.

9. The system shall display the last card transactions, namely the latest sixteen denied access events, authorized events, database events, and/or time & attendance events.

10. The SMS shall offer an extended last card transactions window; to get a complete access events report the SMS operators shall simply enter the start date and time, and the end date and time

11. The operator shall be able to quickly search by username directly on the card window. The SMS shall automatically provide the 24 first search results by simply typing the value and then expanding the dropdown list.

12. The operator shall be able to view quickly the cardholder's door list.

    a. Operators shall be able to export the door access list.
    b. A detailed view of the door's schedule shall be show when selecting a door.

13. The operator shall have the option of expanding the comments field in the user section for better viewing.

14. The SMS shall enable the creation of an unlimited number of import/export models, give them a name, select required fields, select their layout, and determine the filed

delimiter. This shall allow for acceleration of the data entry process by importing databases from a spreadsheet.

a. The SMS shall allow the operator to import and export cards using a unique card identifier. If required, the unique identifier can replace the card number for importing and exporting card numbers.

b. The SMS shall allow operators to quickly add a door to a list of access levels.
    i. The SMS operator shall select a door and see a list of access levels.
    ii. The SMS shall return to the access level assigned to the door shown on the schedule. If the door is not assigned to an access level, it shall show none.
    iii. The SMS operator shall be able to change any of the doors assigned access levels by simply changing the schedule.

15. The SMS shall allow for 250 access levels programmed per loop/site of controllers. Every card shall be assigned an access level, which shall determine where and when the access card will be valid. When the system consists of several sites or gateways, it shall be possible to use batch programming of access levels.

16. The SMS shall support up to a total of five access levels for each card user per site/connection when using the Multi-Site Gateway. This feature shall be available with the KT-400 and KT-1. The SMS shall advise the operator if doors are not supported when adding additional access levels (two to five).

17. The SMS shall allow for creation of tenant lists that can be imported in the (Kantech Telephone Entry System) KTES units. The lists shall be easy to fill up and allow for up to 3000 tenants in each list. The SMS shall support the creation of unlimited amounts of tenant lists.

18. The SMS shall allow of importing and exporting of tenant lists. The operator shall have the ability to choose which fields to import and export.

19. The following tenant information shall be able to be saved for each tenant:
    a. Tenant name
    b. Tenant ID (customizable in length per tenant list).
    c. Primary telephone number.
    d. Secondary telephone number
    e. Tenant PIN (customizable in length per tenant list).
    f. Pin access schedule
    g. Tenant level
    h. Tenant language
    i. Card number
    j. Disable card trace
    k. Start/end date
    l. No disturb schedule
    m. Prioritized tenant in the display list.
    n. Call second phone number, option schedule.
        i. Ability to call the second phone number only (does not call primary) during valid schedule.

20. The SMS shall allow for a card number to be assigned to a specific tenant. The KTES unit will be able to send the card number to other controllers of a Wiegand protocol.

21. The SMS shall allow for an unlimited amount of card types. Cards types shall be used to group cards together for ease of management. Card types shall have the option of being assigned a card access group template. Card access groups shall be copied to the cardholder's profile to give the cardholder's access levels.

22. The SMS shall provide the possibility to perform card batch operations. The mass card modifications shall take effect in real time. Each batch operation shall allow for a batch of cards to be changed based on their card type. The batch card modification shall be able to change the following :

    a. Card state
    b. Supervisor level
    c. Card count value
    d. Card tracing
    e. Start date
    f. End date
    g. With deletion on expiration.
    h. Waiting for keypad
    i. Card access group
    j. Replacing access levels
    k. Updating access levels
    l. Adding new access levels.
    m. Updating and adding new access levels.
    n. Card badge layout

2.4.B Video Section

1. The SMS shall be capable of connecting with a maximum of 40 DVRs per product type, without any additional licensing. Products include the following: such as American Dynamics Intellex digital video recorders, American Dynamics Hybrid DVR (HDVR), American Dynamics TVR2, American Dynamics VideoEdge, American Dynamics VideoEdge Hybrid NVR v4.03, INTEVO Advanced, INTEVO Compact, exacqVision A-Series, exacqVision Z-Series, exacqVision EL-Series (EL-S, ELX-S, ELX-IP, ELX-SR), exacqVision LC-Series (LC, LC-IP), IP DVR/NVR.
    a. The SMS shall allow the operator link video servers and cameras to a site. Site linking will allow SMS operators to navigate the SMS with ease by site or system wide.

2. From any of the workstations it shall be possible to do the following:

    a. View one or more camera images from different sources.
    b. Query the history of each recorder and view images saved on disk.
    c. View, modify, or delete programming parameters of a recorder.
    d. Control the movement of all motion cameras directly with the workstation mouse of the SMS (PTZ control).
    e. Export camera images to hard disk and video vault (capable of exporting multiple formats, password protected to protect chain of evidence).

3. The SMS shall ensure the time management and synchronization for all the American Dynamics DVR/NVR. It shall be possible to determine the time refresh frequency on

the network for the American Dynamics DVR/NVR. The SMS shall allow for configuration of each DVR/NVR. For each recorder it shall be possible to:

a. Assign a name
b. Determine the recorder type.
c. Determine the network IP address or domain name.
d. Alternative IP Address or domain name.
e. Manually configure the video, communication and event ports.
f. Determine the number of cameras.
g. Determine the query frequency.
h. Determine the number of failed queries required before a loss of communication message is displayed on the screen.
i. Import camera details from existing video servers.

4. The SMS shall define the programming parameters for every camera connected to a DVR/NVR. For each camera it shall be possible to:

a. Assign a name
b. Determine the type of camera.
c. Assign a representative icon for identification on a graphic screen.
d. Determine if the camera image can be visible on a video view.
e. Determine the type of recording.
f. Determine which events from the recorder shall display an alarm message on the screen.
g. Determine the number of pre-selections desired.
h. Determine the number of patterns desired.
i. Add comments to record in the video vault.

5. The SMS shall allow for the creation of an unlimited number of video views. For each video view it shall be possible to connect up to 16 cameras from various sources.

6. The SMS shall be able to incorporate on the same view on multiple cameras from different American Dynamics Intellex DVRs or graphics. Furthermore on different video views the SMS shall be able to incorporate multiple camera sources from different American Dynamics HDVRs, INTEVO Advanced, INTEVO Compact, Exacq or graphics. In addition, on different video views the SMS shall be able to incorporate multiple cameras source from different American Dynamics TVR2 or graphics. In addition on different video views the SMS shall be able to incorporate multiple cameras source from different American Dynamics Video Edge NVRs or graphics. Also, on different video views shall the SMS shall be able to incorporate multiple camera sources from different Panasonic DVR/NVR of the same model or graphics.

7. The video view programming parameters make it possible to complete the following:

a. Assign a name
b. Determine the view size.
c. Determine the refresh rate of the image.
d. Determine whether to show metrics.
e. Determine whether to show camera controls.
f. Determine whether to show overlays.
g. Determine whether to auto-hide text.
h. Determine whether to activate image zoom.
i. Determine whether to activate video sequence.
j. Determine delay before sequence launch.

k. Determine camera display delay.
l. Determine display pre-selection delay.
m. Determine pattern display delay.
n. Determine graphic display delay.
o. Determine display mode (1 x 1, 2 x 2, 3 x 3 and 4 x 4).
p. Incorporate up to 16 cameras from various sources or 16 graphics.

8. The SMS shall be able to trigger, from one or more specific events, the start of a recording on a recorder with one or more cameras connected to it. The SMS shall allow for the creation of an unlimited number of video triggers. The SMS shall allow for the creation of an unlimited number of recording parameters. For each recording parameter it shall be possible to:

    a. Define a name
    b. Select the DVR/NVR to which this recording parameter refers.
    c. Select the camera to which this recording parameter refers.
    d. Associate a pre-selection or size.
    e. Determine the start recording trigger.
    f. Determine the pre-alarm time.
    g. Determine the total recording time.
    h. Determine the stop recording trigger.

9. It shall be possible for a video event on one DVR/NVR to trigger an action on another DVR/NVR.

10. The SMS shall allow the playback of all recordings stored on the hard drive of any of the DVR/NVR. The operator shall be able to save the video into the video vault.

11. The SMS shall provide the operator access to the complete list of normal and abnormal events that required the activation of video recording. The sequence of images can be saved to a hard drive for subsequent consultation and shall be encrypted. The SMS shall allow the operator to access a complete list of alarm recordings in progress including origin of the alarm. The SMS shall be capable of displaying a list of exported videos.

12. It shall be possible to view recorded video tagged to an access or video event by quick linking from the message desktop.

13. The SMS shall be capable of connecting 40 DVRs per type, such as American Dynamics, INTEVO Advanced, INTEVO Compact, exacqVision A-Series, exacqVision Z- series, exacqVision EL series (EL-S, ELX-S, ELX-IP, ELX-SR) and the exacqVision LC-Series (LC, LC-IP), IP DVR/NVR products with no additional options needed.

2.4.C Definition Section

1. The SMS shall allow the creation of 100 schedules per connection/site of controllers and an unlimited number of system schedules. Each schedule can include up to 20 intervals. By default, each schedule shall support four internals. A schedule can be associated with a supervision point, a relay, an access level, a door, elevator floor, an operator, or an event. The SMS shall allow time zone management.

2. With a Multi-Site Gateway, specific schedules, which include up to 20 intervals shall be available for the KT-400 and KT-1. The KT-400 and KT-1 shall keep all 20 intervals in memory when in stand-alone mode.

3. The SMS shall allow the creation of 366 holidays. It shall be possible to define a name, define a date, and determine the type. The SMS shall allow the operator to view all the holidays defined in holiday type and sites by viewing them all in a yearly calendar.

    a. The SMS shall not require a same date to be created multiple times when affecting certain sites. The SMS shall allow for the same holiday date to be used on certain sites or on the entire system.

4. The SMS graphics shall enable operators to view the exact location of a component installed at the site, or the state of components and peripherals represented in the graphic such as doors, contacts, motion sensors, controllers, video views and cameras. The SMS shall allow for the creation of an unlimited number of graphics. The components on the graphics represented by icons as well as the graphics themselves shall have the ability to be modified. The SMS shall allow for printing of the graphics with their respective components on the graphical floor plan.

5. The SMS shall allow the management of 2,048 elevator cabs of 64 floors each for each gateway. It shall be possible to associate a schedule to the call button. Outside of the schedule, a valid card for a particular floor will have to be presented to the cab reader for it to be activated. The floor selection button group associated with the card's access level will become operational for a predefined duration and all other buttons shall become inactive. The SMS shall allow the creation of groups of floors and access levels.

6. When using KT-400 controllers, each elevator floor shall have the ability to associate to its own unlock schedule. Thus, every elevator floor shall be available without a card read at its respective time.

7. The SMS shall provide the possibility to setup unlimited amount of tasks via the user-friendly task builder. The operator shall be able to create e-mail templates that can incorporate a variable to dynamically populate the e-mails. Using the command GUI menu, the operator can program commands for any component in the SMS. Commands such as but not limited to lock, unlock, temporary unlock, toggle, back to schedule for the doors, relays, inputs and enable and disable readers. The operator can also program commands for specific card count. The commands shall be able to accept specific components or variables that can filled dynamically.

8. The SMS shall provide the possibility to setup unlimited batch card operations via the user-friendly task builder. The batch card modifications shall take effect in real time. Each batch card modifications task shall allow for cards to be changed based on their card type. The batch card modification task shall be able to change:

    a. Card state
    b. Supervisor level
    c. Card count value
    d. Card tracing
    e. Start date
    f. End date
        i. With deletion on expiration
    g. Waiting for keypad

h. Card access group
   i. Replacing access levels
   ii. Updating access levels
   iii. Adding new access levels
   iv. Updating and adding new access levels.
i. Card badge layout.

9. The SMS shall provide the possibility to assign the tasks previously created to be triggered on specific components and specific events.

10. The SmartLink task commander shall process the command from the first available SmartLink application on the SMS.
    a. The use of a specific SmartLink to run the SmartLink task commander shall not be accepted. The SMS shall accept multiple SmartLink to be installed thus providing a redundant SmartLink for all SmartLink task commander tasks.

11. The SMS shall allow for the creation of unlimited instructions. These instructions shall be attributed to one or more events that will be used in documenting the event and guide the operator on duty in performing tasks. It shall be possible to edit the instructions in two different languages.

12. The SMS event trigger shall also serve alarm acknowledgement (pop-ups) configuration. Pop-ups shall be configured to alert SMS operators in real time of specific events on specific components.

13. The SMS shall allow how pop-up's occur by allowing the SMS operator to configure a component (or components) and specific event (or events) are sent to the SMS workstations and/or e-mail.
    a. For each pop up the SMS operator shall be able to choose the following features but will not be limited to them:
       i. Event (or events)
       ii. Component (or components)
       iii. Workstation (or workstations) receptions
       iv. Instructions
       v. Schedule the pop-ups occurs.
       vi. Instructions
       vii. Mandatory operator comments.
       viii. E-mail notification
       ix. Able to acknowledge by e-mail.

14. When the alarm pop-up occurs in real time, the SMS pop-up shall display the following but will not be limited to them:
    a. Date/time
    b. Event
    c. Component name
    d. Instructions
    e. Video playback of associated camera and video clip created.
    f. Automatically opens live video of associated camera.
    g. Able to acknowledge or temporary suspend an alarm.
    h. Audible sound playing wave file to audibly alert SMS operator.

15. When the alarm pop-up occurs in real time, the SMS pop-up if configured accordingly will send an e-mail with the following items but will not be limited to the following:

a. Date/time
b. Event
c. Component name
d. Instructions
e. Event assigned color.
f. Able to acknowledge alarm.

16. The SMS shall support up to 999 action schedulers. These action schedulers shall allow the user to perform actions on the KT-400 and KT-1 on a pre-defined timeframe.
    a. Each action scheduler shall allow up to eight different components to be triggered. These components can be from the same controller or a different controller.
        i. The action scheduler shall be stored in the KT-400 and KT-1. Once programmed by the SMS, the controller shall not need the SMS to trigger the action scheduled.

    b. The action scheduler shall allow but will not be limited to the following:
        i. Toggle door unlock.
        ii. Unlock door.
        iii. Relock door.
        iv. Temporarily unlock door.
        v. Activate Relay.
        vi. Deactivate Relay
        vii. Temporarily activate relay.
        viii. Arm door partition

    c. The action scheduler shall be scheduled to trigger at limited intervals but will not be limited to these intervals:
        i. Once on a specific date and time
        ii. Daily at a specific time until a specific date
        iii. Weekly at a specific time until a specific date

    d. The SMS shall also allow the SMS to trigger a task (task builder) within the action scheduler.
        i. These tasks shall be SMS dependent but can trigger anything configurable in the SMS tasks.

    e. The SMS shall offer overview windows were SMS operators can easily see the upcoming action schedulers.
        i. The SMS operator shall be able to see the upcoming action schedulers in a the following views:
            1. Daily
            2. Weekly
            3. Monthly
            4. Yearly
            5. “Bring me to the next action” button shall bring the SMS operator to the next action scheduled.
        ii. The SMS operator shall be able to see if the action scheduler is a one-time action or a reoccurring action without having to open the action scheduler.

    f. The SMS operator shall be able to add keywords in the action scheduler during programming. This will allow the SMS operator to quickly search

for the actions using the action scheduler name or keywords programmed.

g. The SMS shall give the option to delete the action scheduler once it is completed.

2.4.D Devices Section

1. The physical components of the SMS including workstations, Multi-Site Gateways, gateway, site, controllers, Kantech Telephone Entry System (KTES), doors, relays, ioSmart Readers, ioSmart reader templates, and monitored inputs shall be individually configured and defined. Individual sites shall also be defined. The software shall allow the use of a controller express setup feature in order to minimize the time needed for controller definition.

2. Each component in the devices section shall allow for a comment section per component. The SMS shall allow for unlimited amount of characters in the comment section.

3. The SMS shall allow to migrate from the SMS legacy controllers to KT-400 and KT-1 without having to reprogram the controllers, access levels, doors and their respective associations.
    a. The SMS controller in the database shall only take a second.

    b. The SMS shall not in the background erase or reprogram the controller. By migrating and not erasing/reprogramming, the SMS will allow any custom integration and SMS associations to continue to work as the controllers are the same.

    c. The SMS shall allow to migrate from a KT-100, KT-200, KT-300, KT-1 to a KT-400.

    d. The SMS shall allow to migrate from a KT-100 to a KT-1.

    e. The SMS expansion modules shall be reprogrammed manually.

    f. The following values at the minimum shall remain the same after the migration:
        i. Reader and keypad types
        ii. Anti-passback settings
        iii. Input EOL (end of line) resistor settings.
        iv. Door name
        v. Unlock times
        vi. Door unlock schedules
        vii. Door contact settings
        viii. Rex contact settings
        ix. Intrusion integration settings
        x. Access level programming
        xi. Reporting filters
        xii. Workspace division settings

4. The SMS shall support the programming of the ioSmart readers and ioModules with the KT-400 and KT-1 controllers over 128-bit AES encrypted RS-485 communication.

    a. The SMS shall offer an reader template where the SMS operators can customize the ioSmart behavior of the following items but not limited to:
        i. HID Prox 125 kHz support.
        ii. ioSmart native support
        iii. Mifare Plus, Mifare classic card serial number support.
        iv. ISO 14443b card serial number support.
        v. BLE Active/Inactive
        vi. Keypad illumination intensity:
            1. Keypad always on.
            2. Keypad dim
            3. Keypad off but wake up on touch.
        vii. LED color management for the following but not limited:
            1. Tamper in alarm.
            2. Standby
            3. Key press
            4. Communication failure alarm.
            5. Low power
            6. Lock power trouble.
            7. Access result, can have different LED patters of the same color for the following results such as a but not limited to:
                a. Access Granted
                b. Access Denied—Bad access level
                c. Access Denied—Card expired
                d. Access Denied—Lost or stolen
                e. Access Denied—Card unknown
                f. Door armed/disarmed
                g. Wait for keypad
                h. Valid floor selection (when doing elevators).
                i. Invalid floor selection (when doing elevators).
                j. Request to exit
                k. Time out on request to exit.
                l. Time out on access granted.
                m. Door open to long
                n. Pre-alarm door open too long.
                o. Wait for second card
                p. Multi-swipe denied

    b. The SMS shall offer a default reader template and allow for custom reader templates to be created by the SMS operators.

    c. The reader templates shall be configured once and be available for all controllers.
        i. Changing the reader template shall automatically change the configuration to all the controllers.

    d. The SMS operator shall be able to:
        i. Assign an ioSmart reader using serial number to a controller door.
        ii. Configure input and outputs settings on ioSmart readers.
        iii. Configure keypad settings.

e. When an ioSmart reader is configured in RS-485 mode, and the BLE is activated on the reader template, the EntraPass go Pass shall require that the EntraPass go Pass phone be within range of the reader for the EntraPass go pass to work.

f. When an ioSmart reader is configured in RS-485 mode, the reader shall offer a multi-factor authentication to enter the door. Each door shall offer the following options but is not limited to them:

    i. Two-factor authentication not available; uses standard supported smart cards or prox cards.
    ii. go Pass biometric; to unlock the door, the cardholder uses the go Pass app totap the door and enter their biometric phone login. The reader still accepts smart cards.
    iii. go Pass & disable card reader; to unlock the door, the cardholder uses the go Pass app to tap the door and enter their biometric phone login.The reader does NOT accept any cards.

g. From the SMS operations screen, the SMS operator shall be able to request the non-programmed ioSmart Serial number and the SMS operator shall automatically assign them to the doors.

h. From the SMS operation screen, the SMS operator shall be able to perform firmware updates on the ioSmart readers.

    i. During the firmware updates the ioSmart shall continue to work.

i. From the SMS operation screen, the SMS operator shall be able to see the ioSmart Reader status such as but not limited to :
    i. Firmware
    ii. Tamper state
    iii. Memory availability

j. The Legacy KT-200 and KT-300 shall also support the ioSmart over standard Wiegand protocol using dedicated cables for LED and BUZ.

k. The operator shall configure the ioModules for the KT-400 or the KT-1 as additional expansion modules.
    i. The ioModules shall communicate with the controllers using encrypted RS-485.
    ii. The ioModules shall have a serial number that the SMS shall use to supervise activity.
    iii. When required the SMS shall upgrade the ioModule firmware.
    iv. Each module shall be configurable as 16 inputs or 16 outputs.
    v. The ioModule shall have the following usage options: inputs, outputs, or elevator floors.

5. The SMS shall allow to import KT-400 Standalone and KT-1 Standalone backup into the SMS as a new connection.
    a. The SMS shall allow to import the following but will not be limited to:
        i. Controller name, programming, networking and MAC settings.
        ii. Door names and programming.
        iii. Schedule names and programming.
        iv. Holiday names and programming.
        v. Action scheduler name and programming.

vi. Cardholder lists and programming.
vii. Cardholder door access rights shall also be imported as door exceptions.

2.4.E Alarm Interface

1. The SMS shall interface with any external alarm system thereby arming or disarming the system by presenting a valid card to an entry/exit door. It also shall be possible to associate a keypad with a reader forcing the cardholder to enter a number in the keypad after presenting a card. This integration shall only be possible with the use of a Multi-Site Gateway. It shall be possible at a minimum to complete the following:

    a. Set a monitored input as an arming button.
    b. Associate a usage schedule with an arming button.
    c. Set the exit and entry delay.
    d. Determine whether the system must wait for a valid access to arm.
    e. Determine whether the system must wait for a valid access card swipe and appropriate pin number to disarm. Determine whether the door must relock on arming request.
    f. Associate a monitored input with an alarm panel condition.
    g. Lock a door unlocked by a schedule when armed.

2.4 F Integrations

1. LDAP- Operator synchronization (Active directory).
   The SMS shall interface with the Active Directory (LDAP) for operator management. The SMS shall receive operators from the LDAP system these operators shall be modified and deleted as required.

    a. The SMS shall sync from the Active Directory (LDAP) on a configurable time. Operator changes will flow from LDAP into the SMS. The SMS shall allow operators force a sync manually instead of waiting for the next sync cycle.

    b. The LDAP shall be the authority manager for all operators synced with the SMS.

    c. The SMS shall allow the creation of SMS operators that shall not be synced with LDAP.

    d. The SMS shall be able to sync but not limited to following LDAP fields:
        i. Display name
        ii. User principal name
        iii. User account control (active or inactive).
        iv. Password last set
        v. Bad password time
        vi. Bad password count
        vii. Maximum passwords before change.
        viii. Account expiration date
        ix. Picture
        x. E-mail

    e. The SMS shall allow for as many security level/workstation configurations as needed. The Active Directory shall send down via profiles the proper rights.
    f. The SMS shall give the option for operators to log into the SMS manually if active directory credentials do not match.

g. Certain operators shall be separate from the LDAP sync and shall be managed manually.
h. The SMS shall manage the LDAP integration from the SMS SmartLink and will require a license per LDAP.
i. The SMS shall support up to ten different LDAP connections.

2. Single Sign On (SSO)
   a. The SMS shall allow the SMS workstation to offer single sign on when using the LDAP integration.
   b. Operators shall simply need to login to Windows using their Windows domain login and open the workstation.
   c. The SMS shall also allow a manual login to the client software.
   d. The need to enter a username and password is not required with single sign on.

3. LDAP – Cardholder Synchronization
   The SMS shall interface with the Active Directory (LDAP) for cardholder management. The SMS shall receive LDAP users from the LDAP system, these users shall be modified and deleted as required.

   a. The SMS shall sync from the Active Directory (LDAP) on a configurable time. Cardholder changes will flow from LDAP into the SMS. The SMS shall allow SMS operators to force a sync manually instead of waiting for the next sync cycle.

   b. The LDAP shall be the authority manager for all operators synced with the SMS.

   c. The SMS shall allow the creation of SMS cardholders that shall not be synced with LDAP.

   d. The SMS administrator shall be able to pair the SMS field below to the LDAP Attributes. SMS values such as but not limited to the following):
      i. Display name
      ii. E-mail
      iii. Card state
         1. The Card state shall be automatically linked to the LDAP “User is Disabled” value and disable/enable the SMS cardholder accordingly.
         2. The SMS administrator shall be able to overwrite the default assignment and provide a custom LDAP numerical attribute instead. This configuration shall ignore the LDAP “User is Disabled” value.
      iv. Card numbers one to five.
      v. Card number’s variables such as expiration date and hour.
      vi. Card type
      vii. Access levels via the card access groups.
      viii. Start/end date
      ix. Picture
      x. E-mail
      xi. User definable fields one to 40.

   e. When an SMS field is paired with an LDAP attribute, this such field shall be modifiable only from the LDAP. All other SMS fields shall be modifiable from the SMS client.

   f. The SMS shall be allowed to pair any or all fields with the LDAP Attributes.

g. Certain SMS cardholders shall be separate from the LDAP sync and shall be managed manually.

h. The SMS shall manage the LDAP integration from the SMS SmartLink and require a license per LDAP.

i. The SMS shall import as SMS Cardholders the LDAP users that are part of a LDAP group and its children groups.

i. The SMS shall support up to 10 different LDAP connections.

4. Intrusion
   a. The SMS shall allow interface with the DSC PowerSeries PC1616, PC1832, PC1864, the MaxSys 4020, DSC PowerSeries Neo HS2016, HS2032, HS2064, HS2128, and the DSC PowerSeries Pro HS3032, HS2128 intrusion alarm panels. This interface eliminates the requirement for hardwire integration between the SMS controllers and the DSC PowerSeries® intrusion panel.

   b. When integrating with the DSC PowerSeries Neo and PowerSeries Pro; the SMS operator shall have the ability to offer type 2 encryption or type 3 encryption

   c. With the DSC Power Series Neo and the appropriate communication module the SMS shall connect up to four sessions withKantech controllers. With the appropriate communication, the SMS shall support 1 x RS-232 session and 3 x IP sessions, or 4 x IP sessions.

   d. With the DSC PowerSeries Pro and the appropriate communication module, the SMS shall connect up to four IP sessions with Kantech controllers.

   e. The DSC PowerSeries Pro intrusion panels shall communicate with the Multi-Site Gateway using one of the following methods: TCP-IP or UDP-IP connection, orDirectly to a KT-400/KT-1-PCB controller.
   The SMS shall allow up to four controller sessions back to one PowerSeries Pro.
      i. The SMS shall allow for virtual zones integration with the DSC PowerSeries Neo or PowerSeries Pro.
      ii. The SMS shall trigger the DSC zone status based on the access controller event without the need for hardwiring relays or inputs. Zone statuses include alarm, in trouble, or tamper.
         1. The SMS has the capacity to assign up to 32 virtual zones.
         2. The SMS shall have the capacity to assign up to 32 access controllers from the same Multi-Site Gateway to one DSC PowerSeries Neo, or DSC PowerSeries Pro (for a virtual zone).
         3. The 32 controllers shall be from any type of controller. (KT-300, KT-400, KT-1). The main controller communicating with the DSC PowerSeries Neo or DSC PowerSeries Pro shall be either a KT-400 or KT-1.
         4. The SMS shall be able to assign one door to one virtual zone.
         5. The SMS shall be able to assign one input (access control) to one virtual zone.
         6. The SMS shall be able to assign access control events to one virtual zone, including but not limited to:

a. Access denied - Card expired
b. Access denied - Card lost or stolen
c. Access denied - Bad access level
d. Controller tamper
e. Controller AC failure
f. Controller low battery
g. Door forced open
h. Door open too long.
i. Input in alarm

f. The DSC PowerSeries, PowerSeries Neo, and MaxSys series intrusion panels using the appropriate communicator shall communicate with the Multi-Site Gateway using RS-232 connection to a KT-400/KT-1-PCB controller.

g. The DSC PowerSeries Pro intrusion panels shall communicate with the Multi-Site Gateway or to a KT-400/KT-1-PCB controller over IP connections.

h. The SMS shall allow the DSC Maxsys, PowerSeries, PowerSeries Neo, and PowerSeries Pro to perform the following functions:

i. Single and multiple partitions arming and disarming using a reader.
i. Disarm using a card only or forced valid card and pin.
ii. Single and multiple partitions arming and disarming using operator commands.
iii. Receive events from intrusion panel.
iv. Receive partition names, user codes and zone names programming.
v. Update user codes.
vi. Assign user codes to cardholders.
vii. View a fully functional virtual keypad to perform all functions available on the DSC PowerSeries® 1616, 1832, 1864 or the MaxSys 4020 intrusion panel keypad.
viii. Control the PGM outputs from a graphic screen with the MaxSys 4020 integration.
ix. Bypass zones with the Maxsys 4020, DSC PowerSeries NEO, and PowerSeries Pro integration.

5. Simplex fire event viewing
   a. The SMS shall allow an interface with the Simplex 4100ES fire panel thereby eliminating hardwired integration between the SMS controllers and the Simplex 4100ES fire panel. The Simplex 4100ES fire panel shall communicate using one of the following methods: a Multi-Site Gateway using a RS-232 connection or directly to a KT-400/KT-1PCB controller. The SMS shall allow the following actions:

      i. View the events coming from the Simplex 4100ES fire panel.
      ii. The events shall be able to be used for but not limited to: reporting, video triggers, and e-mail notifications.
      iii. View the virtual keypad.

6. Assa Abloy Aperio wireless locks

a. The SMS shall integrate with Assa Abloy Aperio wireless locks. The integration shall be managed and maintained by the KT-400/KT-1PCB controllers.

b. Up to eight Assa Abloy AH30 hubs shall be able to be put on the KT-400 /KT-1PCB over the RS-232 port using a VC-485.

c. The KT-400 shall support four wired doors and eight additional wireless doors. The wireless doors shall not take a slot of the wired doors in the controller memory.

d. The Assa Abloy Aperio Wireless locks supported shall be firmware version 2.xx.

e. The KT-1PCB shall support one wired door and eight additional wireless doors. The wireless doors shall not take a slot of the wired doors in the controller memory.

f. The SMS shall unlock these wireless doors via licenses. The SMS shall accept licenses in various increments. The licenses shall be distributed to any controller the customer wishes. For example 96 license package can be divided to the customer's needs between controllers.

g. The wireless licenses shall be transferable and re-usable within the same SMS. If the customer wishes they may remove the wireless lock from one controller and attach it to another controller without losing licenses.

h. The SMS shall support one token for every 1 to 16 wireless locks. The tokens shall only be needed for updating the software. Enforcing tokens to maintain the integration within the same version shall not be accepted.

i. The day-to-day operations such as but not limited to access granted, access denied, door forced open, door open too long, shall be managed locally by the KT-400 and KT-1PCB. The need for the SMS software to generate the access granted shall not be accepted. The KT-400 and KT-1PCB shall be the authorities' state for the cards and locks.

j. The wireless locks shall still work with 100,000 cards even if the SMS is not communicating with the access controller.

k. To converse battery on the Assa Abloy Aperio locks the lock shall only wake up when a wireless door action/event is generated. The wireless door shall transmit the event to the controller and SMS within one second.

l. The wireless locks shall be shown as standard doors/readers in the SMS. From the SMS clients the customer shall be able to assign the wireless locks in access levels for the users, door access exceptions, groups, Smartlink task and others. The customer shall be able to see real time status of his doors and run reports similar to the wired doors.

m. The SMS shall allow wireless lock integration with KT-400 and KT-1PCB with the Multi-Site Gateway.

n. The wireless locks shall allow triggering KT-400 and KT-1PCB relays on specific access or door events. The wireless locks shall support at a minimum:

    a. HID proximity cards and HID iCLASS smartcards.
    b. The IN100 v3 locks shall also support ioProx XSF cards.

c. PIN numbers
d. Relay activation on the following events:
    i. Door forced
    ii. Door open too long.
    iii. Door alarm relock.
    iv. Invalid card status.
    v. Bad access level.
    vi. Other access denied.
    vii. Access granted
    viii. Card trace
    ix. Extended door access delay.
e. Unlock Schedule with first man in.
    i. Must be woken up to schedule to start and end.
f. Secondary REX
    i. Must be woken up for the secondary REX to take effect.

o. The SMS shall allow manual operations on the wireless doors. The action on the door shall only take effect when the wireless door wakes up and transmits to the KT-400 or KT-1PCB based on local access or door event. A local door event shall also need to lock or restore the door to its normal state. Manual operations allowed shall be but not limited to:
    a. Unlock/lock door.
    b. Door back to schedule.
    c. Temporary unlock
    d. One time access.
    e. Enable/disable reader.

p. With the IN100 v3 locks the SMS shall allow for the lock to report periodically and update its status based on the KT-400 or KT-1PCB door programming.

q. In addition to the standard access and door events, the SMS shall receive specific events and status from the AH30 hub and the wireless locks. The following specific events shall be available but will not be limited to:
    a. Communication failure
    b. Device online/offline
    c. Radio disturbance
    d. Battery flat/low/ok
    e. Device tamper
    f. Door state
    g. Lock state: Unlocked/locked/secured/jammed
    h. Handle state: Used/not used
    i. Key cylinder state

2.4.G System Section

1. The SMS shall define the profile of a system operator based on name, password, language, privileges, login schedule, security level, workspaces, and password expiry date. The SMS shall provide the possibility to force the operators to assign a mandatory card type to the users. The operator shall be able to provide a default card type for every card.
    a. The SMS shall allow to send a welcome e-mail to the SMS operator.
        i. The SMS shall allow the SMS operator to re-send the welcome e-mail as needed.

ii. This welcome e-mail shall include links to automatically pair the SMS operator with the following SMS applications:
    1. Link to download the WebEntraPass web.
    2. Link to download and pair the SMS operator automatically to EntraPass Go for Apple® and Android® devices.
    3. Link to download and pair the SMS operator automatically to EntraPass Go Install for Apple® and Android® devices.

b. If required, the operator can customize the SMS welcome message with different e-mail headers and footers.

2. The SMS shall allow configuration of their Web/mobile rights to each operator:
    a. Allow to login to Web/mobile.
    b. Default message list filter.
    c. Default message filter buffer upon login.
    d. Concurrent login option.
    e. Session timeout on idle timer.

3. The SMS shall offer the option for the SMS administrators to force strong passwords for operators. The strong password settings shall be configurable by the SMS administrators.

4. The SMS shall determine access rights granted to an operator based on security levels. There shall be three predefined access levels called installer, administrator, and guard. The SMS shall have the ability to create an unlimited number of security levels that can be assigned to one or more operators. It shall be possible to determine from which system components the operator shall be authorized to receive events and take action. It shall be possible to specify for each programming window if the operator can (any combination):

    a. View the component in read only.
    b. Add new components
    c. Modify existing components (cannot add new).
    d. Delete components
    e. Save as
    f. Print components
    g. View links

5. The SMS shall allow system administrators to grant or deny operators access to all system physical components such as gateways, sites, controllers, doors, relays, inputs, access levels, reports, schedules, tenant lists, video servers, card types using workspaces. This allows greater ease for larger sites to locate and assign components that pertain to specific gateways and sites. System administrators shall be able to tailor specific system applications and workstations Workspaces, therefore restricting access to information to all levels of operators. Operators shall be able to use temporary workspaces to narrow their fields of view when accomplishing specific tasks, and then easily revert back to their main workspace.

6. The SMS shall allow the configuration of a system wide feature that will automatically disable an operator who has not logged in at least once in X days.

a. The SMS administrator shall have the option to customize the inactivity timer from 30 days to 365. The SMS feature can also be turned off by the SMS administrators
b. The SMS shall automatically notify the operator via e-mail 10 days prior to the deactivation.

2.4.H Report Section

1. The SMS shall include templates for various types of reports to include the following:

    a. Card use reports.
    b. Manual operations reports.
    c. Alarm reports.
    d. Historical reports.
    e. Time & attendance reports.
    f. Detailed reports.
    g. Summary reports.
    h. Statistical reports.
    i. Roll call reports.

2. The SMS shall allow for the creation of custom reports based on any event or component in the system. The SMS shall support an unlimited amount of customized reports.

3. All reports shall be able to be displayed on screen, printed, or sent by e-mail on a daily, weekly, or monthly basis. All event reports can be automated to be generated and sent at a specific time for a specific time period.

4. The SMS shall support at a minimum the following report formats: Sybase, Dbase IV, CSV, XLS, PDF, RTF, and TXT.

5. The SMS shall be able to generate an access report in CSV with all the card information associated to that access event.

6. All component modification events shall be tagged with addition (+), modification (=) or deletion (-) tag. In all event driven reports the operator shall have the choice to specify a tag or all tags in order to further filter report.

7. The system shall support for the creation of custom time and attendance reports. Each time and attendance report shall support up to 32 rules for masking the entry and exit times of each card. Also each report shall support a “First entry and last exit” feature.

8. Time and attendance reports shall have the possibility to compile the report in using fractions base (percentage) or actual hours and minute base.

9. The SMS shall allow the creation of custom roll call reports, which can without operator intervention be e-mailed to multiple people and/or printed on multiple printers. The roll call report shall be a system wide feature.

10. Each report, quick report, historical report and time attendance report shall have a priority number assigned to it. When multiple reports are requested. The SMS shall prioritize the creation of the report based on their priority number. From the report queue management window the operator shall have the possibility to promote the

report to a higher priority. The operator shall also have the ability to request more processing power form the computer in order to expedite the report creation.

11. Reports shall be prioritized from queue of 1 to 99. When the report is requested as priority one it shall be processed first. The default value for all new reports shall be set to 50. Operators shall be able to change it as needed.

12. The SMS shall have a statistical window showing all reports executed, the time of execution, the time lapse, the number of events, the requestor, and the application request. The report shall be exportable in CSV format.

2.4.I Help Section

1. The SMS shall have a contextual help button in every window. The operators shall also have the option of pressing F1 on their keyboard and the help window will appear with the correct section of the item they were looking at in the SMS.

2. The SMS shall include an about window which shall include basic information about the SMS. It shall also include the KAP start/end date and tokens needed. The operator shall be able to send KAP details via e-mail to a pre-defined e-mail list by the click of one button.

3. In addition the about window shall include contact information for the SMS manufacturer and contact information for the installation company/dealer. In addition the SMS shall support to identify the SMS to the customer with his contact information The dealer information shall at a minimum but not limited to:

    a. Company name.
    b. Address.
    c. Website link.
    d. E-mail link.

2.4.J Audit Trail Reporting

1. The SMS shall include the ability to track all specific field changes made by the operators. The following events are the minimum the SMS shall track:
    a. The operator that made the change.
    b. The time the change occurred.
    c. The component that was changed.
    d. The field that was changed.
    e. The value of the field prior to the save.
    f. The value of the field after the save.

2. If required, the SMS administrator shall track specific components or even the entire database. The following list of components are trackable, but the SMS is not limited to the them:
    a. Access level groups.
    b. Access levels
    c. Cards
    d. Card types
    e. Badges
    f. Action scheduler
    g. Schedule and holidays.
    h. Tasks and SmartLink triggers.
    i. Hardware programming (devices)

j. Graphics
k. Areas
l. Virtual alarm panels
m. Report templates
n. Operator, security level, and workspaces.

3. To view the exact details of the modification transactions the SMS operator shall click the audit trail button and select the needed transaction. The following is a list of the transactions but the SMS is not limited to this list:
    a. Data type (text, numerical, date, boolean).
    b. Modification date
    c. Operator name (that did the modification).
    d. Reference type
    e. Field name (column name in database).
    f. Field description (GUI label name).
    g. Old value
    h. New value

4. To view all changes performed by an operator, the SMS shall provide a filter to generate a transaction report. Choose from the following options:
    a. Date range
    b. Component type
    c. Operator

5. To export all the changes of a specific component, the SMS shall provide a transaction report in a CSV format. . Each row shall represent one transaction and shall include all required information.

6. In a CSV format report, it shall be possible to export one modification or all modifications from that component.

7. The SMS shall be capable of storing up to five years of transactions. It shall be configurable by the SMS administrator

2.4.K Options Section

1. The SMS shall allow operators to access basic server and display functions and allow the operator to determine default settings for the server hard drive. The operator shall also be able to determine the time to perform a server backup, programmable on monthly, weekly, or daily basis. It shall be possible to schedule and plan mass automatic KT-400 and KT-1 firmware updates.

2. The SMS shall allow for the servicing company to enter their contact information for the SMS operator's disposal.

3. The SMS shall allow system administrators to put the SMS in a read-only mode. When the SMS administrator puts the SMS in read-only mode, the SMS operators are visually notified. In addition SMS operators can no longer perform changes or add components in the SMS. The SMS operators are allowed to receive events, perform door operations such as, but not limited to unlocking, locking, and temporary unlocking.

4. The SMS shall allow system administrators to put the SMS in a maintenance mode. When the SMS administrator puts the SMS in maintenance mode, the SMS operators

shall be able to perform their regular actions based on their rights but will not receive pop-ups and real-time e-mail notifications.

5. The SMS shall allow system administrators to easily migrate ioProx Extended Security Format (XSF) cards from a seven character HH:DDDDD to a HHHH:DDDDD format without downtime.
   a. The SMS shall allow the system administrator to convert automatically all ioProx XSF cards to an Extended Security Format of their choosing. The SMS shall change all the card programming instantly.

   b. The SMS shall allow the system administrator to run a conversion tool that will convert ioProx XSF and ioSmart cards in real time into their proper Extended Security Format without having any down time.

      i. This process shall have the option to be turned on or off as the system administrator wishes.
      ii. The cardholder would need to swipe the card twice, the first time the process is started.
      iii. The conversion shall be in real time, and take less than one second per card to occur.

   c. The SMS Extended Security Format conversion is optional, as the SMS shall support standard HH:DDDDD or other formats supported.

2.4.K System Status Section

1. The SMS shall allow operators to view the state of various access system components in text or numerical form. A specific controller's state shall also be able to be viewed in graphic form via the picture of the controller with the status of each terminal. Workstation and database status shall also be able to be displayed.

      a. The SMS shall offer an active status count of all operators in the SMS.

2. The SMS shall offer the ability to run reports on login counts so that operators can run trends on operator peak usage.

3. The SMS shall offer the ability to have a window displaying all the current logins in the SMS. The SMS logins shall be filterable and sortable by type of application such as Web, mobile workstation or database applications.
      a. The SMS all allow the operator to force logout operators thus ending immediately their sessions in the workstation, web and mobile clients.
      b. The SMS all allow the operator to force logout and permanently disable the operator thus ending immediately their sessions in the workstation, web and mobile clients. The operator won't be able to login until reactivated manually.
      c. The list shall be exportable in CSV file format.

2.4.L Various Tools

1. The SMS shall employ an express setup to configure system components such as sites and controllers, as well as peripherals associated to these components such as ports and inputs. This utility will reduce the programming time to a minimum.

2. The SMS shall employ a database utility to allow the re-indexation and verification of archived files and verify the integrity of indexes, links, and database arborescence.

3. The KT-Finder tool shall help troubleshoot the Kantech IP Link, KT-1 and KT-400 on site or remotely. It can also be used as an alternate method of configuration for both.

4. The SMS shall include a vocabulary editor to be used in designing custom language dictionaries.

2.4.M Video Vault

1. Video vault is an optional remote networked application used to automate recovery of video data from the DVR/NVR and save it on a disk for long term video storage and retrieval. The information can be stored on an independent system or within the server. The footage that shall be tagged and recoverable from the DVR/NVR shall include SMS triggers, manual triggers, and saved video server footage.

2. For the archived video files it shall be possible to complete the following:

    a. Assign a folder name to index the archived files.
    b. Create sub folders based on day of the week, day, week, month of the year, month, video server name, camera name and/or event description name.
    c. Determine the hard drive to store the recovered videos.
    d. Determine the composition of the name of the saved file.
    e. Determine the format of the saved video.
    f. Assign a frame from the saved video to represent as a saved file.
    g. Determine the number of simultaneous downloads.
    h. Determine a size limit for recoverable videos.
    i. Assign a password to videos stored.
    j. Determine a delay between requests to the server.

3. There shall be scheduled transfers for archiving thereby reducing video network traffic during peak times.

4. Create a sub folder to divide the stored videos in logical folders. The sub folders shall be based on day of the week, day, week, month of the year

5. The operator shall have the ability to configure the SMS to send an e-mail with four thumbnail images of the alarm.
    b. The e-mail contains four thumbnail images that capture the following time stamps:
        - Five seconds before the alarm.
        - The alarm.
        - Two seconds after the alarm.
        - Five seconds after the alarm.

2.5 PERFORMANCE – WEB/MOBILE APP

2.5.A WebEntraPass web

1. WebEntraPass web shall be an optional tool that will allow for performing certain functions from a remote location to be used with the regular SMS system via a web browser.

2. EntraPass shall be based on Microsoft, Windows Presentation Foundation (WPF) and be a download application from the main web server. The operator shall run the EntraPass web from their desktop.

3. WebEntraPass web shall be updated automatically when the main web server is updated.
    a. Manual updating of WebEntraPass web shall not be supported.

4. EntraPass web interface shall allow the operator to have a favorite list of connections. The operator shall be able to select from the favorite list of servers and logins. A username and password shall be required for each one.

5. EntraPass web operator transactions such as modifications and operations shall be sent to the SMS in the local time zone of the operator.

6. EntraPass web shall offer the following operations:

    a. Operator specific security rights. The SMS workstation shall allow configuring operators to be able to access EntraPass web. It shall also allow the operator's security rights and workspaces to be used on EntraPass web. An operator who cannot add cards on the SMS workstation shall not be able to do the same on EntraPass web.

    b. Automatically adjust the operator's language selection. The language selection shall be done at the creation of the operation in the SMS workstation. The languages supported shall be English, French, Spanish, Italian, Portuguese, Simplified Chinese, Dutch, Turkish and German.

    c. There shall be no limits to the amount of EntraPass web applications that can be installed.

    d. Shall not require any kind of refreshing to receive any new data
        i. Refreshing the "page" shall not be supported.

    e. EntraPass web licenses shall be managed by concurrent active logged on sessions.
        i. The need to have dedicated licenses per computer shall not be supported.

    f. Shall support a right-click action to allow additional functions.

7. EntraPass web shall have a complete, easy to use, intuitive, look and feel.

8. EntraPass web shall allow the following for door, relay and input menus:

    a. The operator is allowed to select multiple components using the SHIFT/CTRL buttons on the keyboard and the mouse.

b. The operator is allowed to view real-time status of the components. Systems righting a manual refresh shall not be acceptable.

c. The operator is allowed to search for a particular component within the site. The search filter shall update the results as the operator types.

d. Retrieve the last site visited and load the same site when revisiting the menu.

e. On doors the operator shall be able to:
   i. Unlock/lock a door.
   ii. Use the one time access functionality (pulse door).
   iii. Temporarily unlock a door.
   iv. Return to schedule.
   v. Enable/disable exit/entry readers separately using the same door icon.
   vi. Arm/disarm doors when using the KT-400, KT-1 and alarm panel.
   vii. View full text status.
   viii. Enable/disable floors when programmed as elevator.
   ix. Change unlock schedule for the door.
   x. Clear unlock schedule for the door.

f. On relays the operator shall be able to:
   i. Activate relays
   ii. Deactivate relays
   iii. Temporarily activate relays.
   iv. Retrieve the initial door schedule.

g. On inputs the operators shall be able to access the following features:
   i. Normal supervision
   ii. Continuous supervision
   iii. No supervision
   iv. Temporary no supervision

9. EntraPass web shall provide complete card management.

   a. EntraPass web shall learn and remember the operator's screen settings.
      i. It shall be possible to see all settings of the cardholder at once without the need to use tabs.
      ii. Its fields shall be grouped in a logical order to allow operator to completely accomplish their tasks without moving around the window.

   b. EntraPass web shall support up to a total of five access levels for each card user per site/connection when using the Multi-Site Gateway. This feature shall be available with the KT-400 and KT-1. The SMS shall advise the operator if doors are not supported when adding additional access levels (2-5).

   c. EntraPass web shall allow adding door access exceptions to the cardholder's list of access rights.

   d. EntraPass web shall allow configuring every aspect of the card that the EntraPass Workstation offers.

   e. EntraPass web shall allow for operators to manage the user's go Pass.

f. EntraPass web shall allow for operators to manage the user's HID Mobile Credentials.

g. EntraPass web shall allow the operator to print badges using dye-sublimation printers (badge printers).
    i. The operator shall be:
        1. Able to assign a badge template to a user.
        2. Able to preview both sides of the card printing.
        3. Assign a badge printer to print on.
        4. Able to print both sides, back side only or front side only.

h. EntraPass web shall include additional operations for the cardholder:
    i. Link a cardholder to a tenant list for the KTES.
    ii. Import and take a picture of the cardholder using a webcam.
    iii. View a list of cardholders.
    iv. The cardholder list shall be configurable to include cardholder information. It shall also allow to sort by columns.
    v. The cardholder list shall allow a right-click function to modify or delete the cardholder.
    vi. Search by card number and username.
    vii. Import and export cardholders using CSV.
    viii. View all doors assigned to a cardholder regardless of an access level.
        5. The door list shall be printable and exportable in an Adobe PDF file or Microsoft Excel file.

10. EntraPass web shall support up to 999 action schedulers. These action schedulers shall allow the user to perform actions on the SMS controllers within a pre-defined timeframe.
    i. Each action scheduler shall allow up to eight different component triggers. These components can be from the same controller or a different controller.
    ii. The action scheduler shall be stored in the KT-400 and the KT-1. When EntraPass web programs the action scheduler, the controller shall not need the SMS to trigger the action scheduled.

        1. The action scheduler shall allow but will not be limited to the following features:
            a. Toggle door unlock.
            b. Unlock door
            c. Relock door
            d. Temporarily unlock door.
            e. Activate relay
            f. Deactivate relay
            g. Temporarily activate relay.
            h. Arm door partition.

        2. The action scheduler shall be scheduled to trigger at limited intervals but will not be limited to these intervals:
            a. Once on a specific date and time.
            b. Daily at a specific time until a specific date.
            c. Weekly at a specific time until a specific date.

3. EntraPass web shall also allow the EntraPass web to trigger a task (task builder) within the action scheduler.
    a. These tasks shall be SMS dependent but can trigger anything configurable in the SMS tasks.

    b. The SMS shall offer overview windows where SMS operators can easily see the upcoming action schedulers.

    c. The SMS operator shall be able to see if the action scheduler is a one-time action or a reoccurring action without having to open the action scheduler.

11. EntraPass web shall provide complete access level management.
    a. EntraPass web shall allow the operator to customize their access level list to show more access levels in columns in order to provide a better view of the access levels.

    b. EntraPass web shall provide a preview on how the access level is programmed:
        i. It shall be possible to zoom in on the access level preview and see down to the hour how the access level is programmed.

    c. EntraPass web shall allow operators to add quickly a door to a list of access levels.
        i. The operator shall select a door and see a list of access levels.
        ii. EntraPass web shall return to the assigned door shown on the schedule. If the door is not assigned to an access level, it shall show none.
        iii. The operator shall be able to change any of the doors assigned access levels by simply changing the schedule.

12. EntraPass web shall provide complete schedule management.
    a. EntraPass web shall allow the operator to customize their schedule list to show more schedules in columns in order to provide a better view of schedule.
    b. EntraPass web shall provide a preview on how the schedule is programmed.
        i. It shall be possible to program quickly the schedule by either entering the times or using a scroll bar.
        ii. It shall also be possible to quickly program the days by choosing them manually or selecting pre-defined day templates.

13. EntraPass web shall provide complete holiday management.
    a. EntraPass web shall allow the operator to customize their holiday list to show more holidays in columns in order to provide a better view of holiday.
    b. EntraPass web shall provide a preview on how the holiday is programmed.
        i. It shall be possible to program the holiday date and using the drag and drop function to select the appropriate sites affected.

14. WebEntraPass web shall provide complete tenant and tenant list management.
    a. EntraPass web shall allow the operator to customize their tenant list to show more tenant lists in columns in order to provide a better view of tenant lists.
    b. EntraPass web shall allow for complete tenant programming in an easy to use GUI interface.
    c. It shall be possible to see all tenant settings at once without the need to use tabs.

15. EntraPass web shall allow for map management.
    a. The operator shall be able to use easily and intuitively the map creation tool to import floor plans or maps in EntraPass web. The image formats support shall be JPEG and GIF.

    b. The operator shall have the ability to place components on specific parts of the map and assign double click actions.

    c. The operator shall be able to view maps from their screen.

    d. The operator shall be able to:
        i. See real time visual status of a component. At a minimum the following components shall be available:
            1. Doors and elevators
            2. Inputs
            3. Relays
            4. Map links
            5. Virtual keypad
            6. Controller
            7. Video Cameras
        ii. Double click on the component to perform actions.
        iii. Right click on the component and choose a different action.
        iv. Quickly move to different maps by using links.
        v. Maximize the map. EntraPass web shall be able to keep the visual aspect ratio.

    e. EntraPass web shall remember the last map used and load it so that operators do not need to choose a map to start every time.

    f. The operator shall be able to modify the assigned door schedule from the map.
        i. The operator shall not need to have access to entire door to be able to change the assigned door schedule.
        ii. Changing the door schedule shall be a privilege that can be turned on or off by the SMS administrator per operator.

16. EntraPass web shall allow for operator programming and management.

    a. EntraPass web shall allow to create, modify, delete and view operators.

    b. EntraPass web shall allow the following but is limited to operator management:
        i. Operator display name
        ii. Operator login name

iii. Operator password following the SMS password complexity rules.
iv. Language
v. Security level
vi. Workspace
vii. Password reset
viii. Password last set every X days.
ix. Disable operator X consecutive bad logins.
x. Maximum passwords before change.
xi. Account expiration date
xii. Picture
xiii. E-mail
xiv. Disable operator
xv. Welcome e-mail settings

c. EntraPass web shall allow to send a welcome e-mail to the SMS operator.

d. EntraPass web shall allow the SMS operator to re-send the welcome e-mail as needed.

i. This welcome e-mail shall include links to pair automatically the SMS operator with the following SMS applications: link to download the EntraPass web.
ii. Link to download and pair the SMS operator automatically to EntraPass go for Apple® and Android® devices.
iii. Link to download and pair the SMS operator automatically to EntraPass go Install for Apple® and Android® devices.

17. EntraPass web shall provide video integration with the American Dynamics HDVR and VideoEdge (NVR), INTEVO Advanced, INTEVO Compact and exacqVision A-Series, exacqVision Z-Series, exacqVision EL-Series (EL-S, ELX-S, ELX-IP, ELX-SR) and the exacqVision LC-Series (LC, LC-IP) IP DVR/NVR products.

a. EntraPass web shall allow the operator to complete the following:
i. To create and manage video views.
ii. To select a single camera and drag it into the viewing screen to view live video.
iii. To select a predefined video view and drag it into the viewing screen to view live video.
iv. To view video cameras without the need to create video views.
v. To select nine different video camera layouts.
vi. To support up to 16 cameras at once per view.
vii. To video search for up to one hour.
viii. To video search exporting in watermarked or AVI format.
1. The watermarked format shall include a video player embedded in the clip.
ix. To video search using metadata to only show alarm clips based on camera motion alarms or access event video recording clips, thus speeding up finding video alarms for the customer.
x. To PTZ control cameras using the mouse or computer keyboard (arrows for pan/tilt and +/- for zoom in/out).
1. The PTZ shall offer three speeds based on mouse movement.

18. EntraPass web shall allow the operator to generate reports:

    a. All reports shall be sent using e-mail to multiple e-mail addresses in PDF or EXCEL (XLS) format.

    b. Reports shall also be viewable on the EntraPass web screen. The operator shall still be able to use EntraPass web while a report is generating.

    c. Reports viewed on screen shall allow the operator save the report in an Adobe PDF file or Microsoft Excel (XSL) file.

    d. Reports shall allow additional filtering within the report values to better accommodate report filtering.

    e. EntraPass web shall allow generating quick reports.

        i. Quick reports are pre-defined event templates among which operators can choose. The operator shall be able to select multiple event templates.

        ii. Quick reports shall offer the following pre-configured event templates:

            1. All events
            2. Access events
            3. Alarm system events
            4. Area events
            5. Camera events
            6. Controller events
            7. Database events
            8. Door events
            9. Guard Tour events
            10. Input events
            11. KTES Events
            12. Operator events
            13. Relay events
            14. Server based events
            15. Time and attendance based events
            16. Video server based events

        iii. The operator shall have the ability to choose a specific timeframe based on date and time.

    f. EntraPass web shall allow the creation of custom reports:
        i. Custom reports shall be built in the SMS workstation and can be used in EntraPass web
        ii. The operator shall have the ability to choose a specific timeframe based on date and time.
        iii. Custom reports shall be of limitless availability to the operator.

    g. EntraPass web shall allow the creation of reports based on user lists
        i. The operator shall be able to quickly filter the user list based on:
            1. The entire card database

2. Door access
3. Assigned card type
4. Assigned access level

ii. The operator shall also be able to filter the report based on:
1. One user definable field with a search value
2. Card status
a. Enabled/disabled
b. Lost/stolen
c. Postdated
d. Expired
e. Suspended
3. Comments
4. Card traced
5. To be deleted when expired
6. Wait for PIN
7. PIN search

iii. Allow the operator to choose which values to include to the report. These values should include but not be limited to:
1. Username
2. Card number
3. Card type
4. Card filter
5. Picture
6. Access level
7. Card information fields (selectable)
8. Card state
9. Start/end date
10. Count values
11. Card parameters

h. EntraPass web shall allow the creation of a doors “assigned to” report:
i. The operator shall be able to quickly filter the report based on:
1. The access level
2. The card type
ii. The operator shall be able to select the component (access levels or card types) to include to the report.
iii. The report output shall include the access level or card type name and the doors associated with the schedule.

19. EntraPass web shall allow the operator to view events in real time.
a. EntraPass web shall allow the operator:
i. To view events in real time. Each event at a minimum shall include:
1. Date and time
2. Event name
3. Description of the component.
b. The event viewer shall support natively a swipe and show feature. The picture of the cardholder shall appear on access related events.
c. On predefined video alarm recordings, a video button shall appear on the event screen for each event that has video alarm.
i. The operator shall be able to click the button to view the alarm video clip.
d. From the event viewer the operator shall be able at a minimum to:
i. Search for any event, date, time, description using the filter field

ii. Sort by date/time, event and description.

20. EntraPass web shall allow for the DSC PowerSeries, Maxsys and Simplex Fire 4100ES Virtual keypad to be used. From the maps or dedicated menu the operator shall easily be able to bring up a fully functional DSC Virtual keypad and perform all actions allowed by the DSC PowerSeries 1616, 1832, 1864 keypad and Maxsys keypad.

21. EntraPass web shall allow for the DSC PowerSeries, Maxsys, PowerSeriesNeo, and PowerSeries Pro operators to complete the following actions:

    a. View partition status.
    b. Arm and disarm partitions.
    c. View zones status.
    d. View and control the virtual keypad from the DSC PowerSeries 1616, 1832, 1864, and Maxsys.

22. EntraPass web shall allow for the programming of Kantech hardware.
    a. EntraPass web shall support but not be limited to programming the following:
        i. Sites
            1. Naming a site
            2. Adding user definable fields, to best describe the sites.
            3. View linked connections
        ii. IP connections
            1. IP Link
            2. KT-400 IP
            3. KT-1 IP
            4. KTES IP
        iii. Direct connections
            1. USB or Serial
        iv. Controllers:
            1. KTES
            2. KT-100
            3. KT-200
            4. KT-300
            5. KT-400
            6. KT-1
        v. ioSmart readers configuration in the controller menu
            1. Configuring ioSmart Readers to the KT-400 and KT-1 controllers.
                a. Assigning an ioSmart reader via serial number to a door.
                b. Configuring input and outputs settings on ioSmart readers.
                c. Configuring keypad settings
        vi. ASSA ABLOY Aperio wireless locks configuration in the controller menu.
            1. Associate the Aperio wireless lockset to a door for the KT-400 and KT-1.
        vii. Component
            1. Door programming including but not limited to:
                a. Multi-swipe settings
                b. Intrusion arming/disarming

c. Unlock/open settings
d. Door contact and REX settings
e. Schedule assigned
f. Door naming
g. First Person in with grace period.
h. Exit/entry readers per door with KT-400.

2. Relay programming including but not limited to:
   a. Activation schedule
   b. Disable relay schedule
   c. Temporary activation timer
   d. Relay naming
3. Input programming including but not limited to:
   a. Monitoring schedule
   b. NC/NO status
   c. Relay activation settings
   d. Input Name
4. Firmware updates request to the controllers so that the SMS shall update them to the latest firmware provided.

b. When using the KT-1 with the auto-enrolment feature
   i. The auto-enrolment shall work on a local LAN segment of the network.
   ii. EntraPass web shall display a dedicated list of all unassigned KT-1s. Using EntraPass web the operator shall pick the KT-1 they are interested in.
   iii. The WebEntraPass web shall allow using the auto-enrolment wizard:
      1. Assign a KT-1 to a site.
      2. Name the door
      3. Activate the exit reader.
      4. Activate the door contact.
      5. Activate the request to exit.

c. EntraPass web shall support a quick, intuitive, and easy to use express setup to configure controllers and their doors, relays and inputs.
d. The operator shall be able to modify, delete or add components manually after the express setup.
e. The operator shall be able, at a glance, to see in a visual and easy to understand the site communication time, communication status and the number of controllers communicating.
   i. The operator shall also be able to see the communication status per controller.

23. EntraPass web shall provide e-mail notification and alarm management with the watchlist.
    a. EntraPass web shall have the ability to select manually which door, relay, input and elevator will be watched for abnormal events.
    b. A watched component shall generate an alarm on EntraPass web. The operator shall have a column (watchlist) where all the alarms will appear as bubble-color-coded events with text.
       i. Each event shall be categorized with the appropriate color by the SMS.

c. The operator shall be able to see watchlist events regardless of the time zone difference between the event and the EntraPass web instance.

d. The operator shall be able to complete the following actions:
   i. Right click the event and go to associated:
      1. Component
      2. Video recording
      3. Map
   ii. Scroll back to the first alarm since he logged in to an EntraPass web session.
   iii. Shall be able to tag a watchlist with e-mail notification as well.

24. EntraPass web shall provide tabs similar to a web browser.
   a. The operator shall be able to create unlimited tabs.
   b. Each tab shall be customizable to the operator's specifications. A tab can be customized to have any of two the following features configured, but will not be limited to the following items:
      i. Schedule management
      ii. Access level management.
      iii. Holiday management
      iv. User management
      v. Tenant management
      vi. Door/elevator operations.
      vii. Relay operations
      viii. Input operations
      ix. Events
      x. Maps
      xi. Video viewing
      xii. Reports
      xiii. Action schedule
      xiv. Hardware setup

   c. Each tab shall perform the following functions:
      i. Become a floating tab to use on multiple screens or embed in EntraPass web.
      ii. Retrieve the last map used so that operators do not need to reselect the map.
      iii. Option to split each tab into two to display two features in a horizontal or vertical layout.

   d. The operator shall have the ability to open an unlimited tabs at the same time.

25. EntraPass web shall at a minimum be supported by any web browser and Windows® OS.

26. The SMS administrator shall be able to change the splash screen title and image of the login page, and the highlight color of EntraPass web.

2.5.B Mobile app - EntraPass go

1. The mobile app is an optional tool that will allow performing certain functions from a remote location to be used with the regular SMS system via iPad, iPhone, Android phones and Android tablets. The mobile app provides card management to guards, secretaries, or managers without the need to deploy a full workstation. A concurrent connection option shall provide access to a predetermined number of simultaneous users.

2. The concurrent connections are shared with EntraPass web connections.

3. EntraPass go operator transactions involving modifications and operations shall be sent to the SMS in the local time zone of the operator.

4. The mobile app shall have the ability to be viewed in multiple languages. The mobile app shall be available in English, French, Spanish, Italian, Portuguese, Simplified Chinese, Dutch Turkish and German. The languages shall be preselected based on the device language.

5. The following functions are available using mobile app:

    a. Card management (including five cards per username) including but not limited to.
        1. Card names.
        2. Card numbers.
        3. Card expiry hour.
        4. Go Pass management.
        5. Access levels.
        6. User pictures.
        7. Access levels.
            a. Additional access level when using a Multi-Site Gateway
            b. Access door exceptions.
        8. Forty card fields to best describe the user.
        9. Start/end date.
        10. PIN.

    b. Live cardholder picture capture using a camera.
    c. Create, modify and delete access levels.
    d. Create, modify and delete schedules.
    e. Assign access levels.
    f. Perform door operations.
    g. Change the unlock schedule of the door.
    h. Perform relay operations.
    i. Perform input operations.
    j. Perform elevator operations.
    k. Request historical or quick reports via e-mail.
    l. View live events using the menu or the quick launch viewer.
    m. Search for events using text filters.
    n. Arm and disarm DSC partitions.
    o. View DSC zone status.
    p. For VideoEdge, Exacq, or INTEVO video management systems:
        1. Live video view in portrait and landscape mode.
        2. Video search.
        3. Video alarm clip view on access events. When video is available on the access or DSC event, a camera icon shall appear and

operators shall be able to click on this icon and view the video alarm.

6. The mobile app shall offer the ability to perform quick actions for efficiency; this will include the ability to expand the menu to perform all associated actions.

7. The mobile app shall have a home screen that can perform door, DSC actions and view video without having to change menus.

8. For Apple® devices that allow thumbprint login, the mobile app shall allow login using this thumbprint. No extra information is required.

9. The mobile app shall support multiple SMS logins and servers stored in memory.

10. The SMS shall support gesture logins in order to login quickly to the Mobile App.

11. The mobile app shall be downloadable at no-charge from the App Store® and Google Play®.

12. The Mobile App shall be supported but will not be limited to the following:

    a. Apple:
        i. iOS: 12.x
    b. Android:
        i. OS:
            1. Kitkat
            2. Lollipop
            3. Marshmallow
            4. Nougat
            5. Oreo

2.5.C Mobile app - EntraPass go Pass

1. EntraPass go Pass is an optional tool that will allow cardholders with this privilege to use their smartphone Apple® or Android® devices as their credentials.

2. EntraPass go Pass simulates a card swipe by sending the request over WI-FI or mobile data to the SMS SmartLink. The SMS sends the request to the controller; the controller devices then generate access or not to the door based on the real time door status.
    a. The SMS controller shall have the final say to unlock the door and the EntraPass go Pass request shall follow every rule of the door.
    b. EntraPass go Pass shall work on any Kantech controller.
    c. EntraPass go Pass shall not be tied to work on specific readers.

3. The EntraPass go Pass is paired to a SMS cardholder using encrypted one time use e-mail. The encrypted e-mail can only pair one smartphone at a time. A second smartphone trying to pair itself with the SMS cardholder shall be automatically rejected.
    a. The SMS operator can issue a new encrypted e-mail. Once this is done the first smartphone is unpaired automatically and EntraPass go Pass stops working. The new smartphone can be paired.
    b. The SMS operator can completely revoke the EntraPass go Pass credential if needed.

4. The EntraPass go Pass shall display all the doors assigned to the cardholder (using the access level).
    a. The doors shall be listed by site where the EntraPass go user shall be able to expand the list and see the doors within the site.

5. The first time an EntraPass go Pass user goes to the door, the EntraPass go Pass shall ask if they are onsite so that the EntraPass go Pass can tag the location of the site.

6. Site lists shall be ordered by location distance and not alphabetical.

7. EntraPass go Pass shall be able to place their popular doors in the Favorite window for quick access.

8. EntraPass go Pass can be extended to be used with Apple® Watch.
    a. The EntraPass go Pass user shall be able to open their app and request their favorite doors to be unlocked.

    b. The user's EntraPass go Pass favorite doors can be placed as widgets on Apple® and Android® smartphones for quick access.

9. The concurrent connections are shared with the EntraPass web connections.

10. EntraPass go Pass shall support BLE geo fencing.
    a. When an ioSmart reader is wired over RS-485 to a KT-400 or KT-1 controller the reader shall emit a BLE signal. The door shall only be available to tap when the EntraPass go Pass is near the BLE signal of that reader.
    b. If the reader is not an ioSmart reader the go Pass shall work without geo fencing for that reader.

11. EntraPass go Pass shall support two-factor authentication.
    a. When an ioSmart reader is configured in RS-485 mode the reader shall offer a multi-factor authentication to enter the door. Each door shall offer the following options but is not limited to them:
        i. Two-factor authentication not available; uses standard supported smart cards or prox cards.
        ii. go Pass Biometric; to unlock the door, the cardholder uses the go Pass mobile app to tap the door and enter their biometric. The reader still accepts smart cards
        iii. go Pass & disable card reader; to unlock the door, the go Pass cardholder uses the go Pass mobile app to tap the door and enter their biometric phone login. The reader does NOT accept any cards.

2.6 INTEGRATION

2.6.A SmartLink

1. The SmartLink application offers the ability to send messages to pagers and cell phones by e-mail. SmartLink provides instant e-mail notification of alarm events and the ability to e-mail reports.

2. Integration with other systems can also be done through the SmartLink API. This tool is used for advanced integration with third party applications like visitor management software, human resources systems, time and attendance systems, video systems, and HVAC.

2.6.B Card Gateway

1. The card gateway is an optional external interface that shall allow the client to make modifications to the system card database through an Oracle or MS-SQL database. The application can be installed and run on the server's CPU. It shall allow for HR software integration and enable operators to modify, add, or obtain information on cards in real time.

2.7 REDUNDANCY & MIRRORING

2.7.A Redundant Server

1. The SMS shall be able to support an optional Redundant Server whose main function shall be to monitor the primary server and ensure automatic (hot standby) take over if necessary. The Redundant Server shall have all the same characteristics and functions as the primary server.

2. The transition between these servers shall be completely transparent. When the primary server is operational once more, it shall be capable of synchronizing its database automatically with the Redundant Server and then resume absolute control of the access management system. No human intervention shall be required in this operation.

3. The operator shall be able to perform any and all operations during a fail-over synchronization between the primary server and Redundant Server.

4. The system shall support the use of multiple simultaneous Redundant Servers. The need to install third party (not EntraPass) licensing shall not be acceptable.

5. The SMS shall no longer allow the primary server to run and manage quick and custom event based reports. The quick and custom reports shall be managed by the active Redundant Server. This gives power to the primary server to manage the database and day-to-day operations.

6. The SMS shall allow the Redundant Server to perform backups.

7. The SMS shall allow for asynchronous and synchronous mirror database of archives, time-attendance and video events. This allows for slower networks where the Redundant Server is in a different building or city to only sync events every X minutes. The timer shall be configurable:
    a. In case of primary server failure the Redundant Server shall start and take over. The database (data) is synchronized in real time at all times.
    b. Once the primary server restarts, the missing event shall be fully synchronized.

8. The SMS shall synchronize all Redundant Servers instances at the same time and not in sequence.

2.8 HSPD-12 COMPLIANCE AND INTEGRATION

1. The SMS shall be HSPD-12 compliant when integrating with PIVCheck Plus and Certificate Manager Solution. The SMS and PIVCheck integration shall be seamless and the operator shall not need to enter the cardholder's information twice.

2. The integration shall support up to three-factor authentication, extraction and verification of the cardholder's data on the FIPS 201 smart card and shall perform a biometric match against the template stored on the card. Digital certificates shall verify against the issuer's validation authority, SCVP or OCSP Responders. All cards shall be validated using the FIPS 201 challenge-response (CAK or PAK) in order to identify forged or cloned cards. The SMS integration shall work with all PIV, TWIC, CAC and FRAC cards.

3. The PIVCheck solution shall verify the following items to ensure that the cardholder is the card owner, the card is authentic, and the card has not been revoked by the agency that issued it:

    a. Smart card expiration date.
    b. Non-duplicated card (forged/cloned).
    c. Biometric.
    d. Certification status.
    e. PIN verification.

4. The SMS shall natively support the FIPS 201 driver when using the KT-400 and KT-1 controllers and shall display the FIPS 201 card number correctly.

5. The SMS integration shall allow associating SMS card fields with the PIVCheck card field in order to have a seamless cardholder entry. The SMS integration shall allow but not limited to associating with the following fields:

    a. User definable fields (ten).
    b. Cardholder pin.
    c. Card number.
    d. Card user name.
    e. Card type.
    f. Card status.

6. The SMS integration with PIVCheck shall require option codes to activate all integration functions.

2.9 OPERATION

The SMS shall perform the following tasks:

1. Allow card access management for one or more buildings.

2. Control access to various doors equipped with a card reader. Allow the ability to set card use count options to limit the number of times a card can be used.

3. Monitor all defined alarm points as well as all doors controlled by card readers based on programmed schedules.
4. Send transactions for which printing is required to one or more printers, based on a set schedule.
5. Access the system using the main and secondary menus (to which access is limited by a password) to make additions and required changes to various data files so that they can be updated by the user without the manufacturer's assistance.
6. Enable the entry of access code data for every card or group of cards.
7. Seamlessly connect to onsite alarm systems.
8. Fully functional virtual keypad with DSC® PowerSeries PC1616, PC1832 and PC1864 alarm system in addition with the DSC MAXSYS 4020 alarm panel. The operator shall perform all functions available on a standard keypad with the PowerSeries or MAXSYS 4020 series alarm systems. The operator shall be able to use the computer keyboard or the mouse to perform actions on the virtual keypad.
9. Interface with the Simplex 4100ES Fire Panel, thereby eliminating hardwired integration between the SMS controllers and the Simplex 4100ES fire panel to receive events from the Simplex 4100ES panel and view the virtual keypad.
10. Associate to each event a recording schedule for each destination (hard drive, monitor).
11. Automatically display all alarms on screen in text with optional graphic or picture and trigger a sound requiring an acknowledgement on the keyboard to stop the alarm.
12. Alarm pop-ups can be sent to many workstations. An alarm pop-up shall be acknowledged once by one operator.
13. Mandatory comments can be added by the operator when acknowledging the alarm pop-up.
14. In the case of an unacknowledged alarm within a customizable time; the alarm shall be sent to all active operators with additional log information.

15. Each event shall print on a log printer. For security reasons, each event shall be incremented with a print number. Numbering shall start from zero every day.

16. Generate reports and view them on the screen, output them to a printer, or send them to an e-mail address.

17. Supervise based on programmed schedules of specific points such as door contacts, volumetric detectors, mechanical points, high and low temperature sensors, or any other equipment necessary for good building management.

18. View and/or save video images.

19. When integrated into a DVR/NVR system (American Dynamics, INTEVO, or Exacq), allow the management of the recordings of all the cameras via access system workstations.

20. When connected to a DVR/NVR system (American Dynamics, INTEVO, or Exacq), allow the orientation of all PTZ cameras directly using the workstation mouse of the access system.

21. The SMS shall offer the option to create four digit, five digit or six digit PIN for the cardholders.

22. The PIN length shall be defined SMS wide.

23. When connected to a digital video recording system (American Dynamics), allow the recovery and storage of selected videos to an independent server.

24. Save the database manually or automatically backup following a schedule.

25. Uninterrupted backups. The operator shall be able to perform any task during a SMS backup.

26. The operator shall be able to perform any and all operations during a fail-over synchronization between the primary server and Redundant Server.

27. The SMS shall remind SMS operators via e-mail and messages (pop-ups) of the SMS KAP status. The SMS shall have pre-defined reminders set to:

    a. Sixty days before KAP expiration.
    b. Thirty days before KAP expiration.

c. Day of KAP expiration.
d. Thirty days after KAP expiration.

28. The SMS KAP reminder shall include but not be limited to SMS serial number tokens needed and SMS Edition.

29. The SMS shall offer administrators to post a message upon operator login. The message shall be customizable to be per operator and system wide.

30. The login message shall be configurable in both SMS languages and appear on the SMS workstation or SMS web in the operator's respective languages.

31. The login message shall be configurable to specific timeframe (per operator):
    a. Never.
    b. Always requires acknowledgement.
    c. Only one acknowledgement.
    d. Always requires acknowledgement until a specific date.
    e. Only one acknowledgement until a specific date.

32. The SME administrator shall be able to force strong password rules. The SMS shall allow the SME administrators to select the password settings. Password settings shall be configurable with the following rules:
    a. Password length between 8 and 20 characters.
    b. Upper case characters between 0 and 20.
    c. Numeric characters between 0 and 20.
    d. Special characters between 0 and 20

33. When the access control system manages parking lot entry and exit, it shall be possible to set a maximum number of vehicles authorized to simultaneously access the parking area. Once the parking lot is full, the system shall prevent access to any cardholder for as long as a parking space has not become available.

34. Save events on a hard drive according to required criteria.

35. The SMS shall allow storing the live transactions (events) portion of the system on a different local drive. This shall speed up performance of the SMS.

36. Once activated the SMS shall allow that the each door's request-to-exit events shall be ignored and not stored.
    a. The events shall not be stored or viewed on the screen
    b. Operators shall be able to ignore request-to-exit events on a per door basis by schedule.

37. It shall be possible to program on a KT-400 or KT-1 controller reader to bypass a door contact on a schedule. The bypass shall be at the controller level and at the software level.

38. It shall be possible to bypass the door contact for door forced events, and door open too long events. It shall be possible to have the door open too long event be an optional bypass on a door basis.

39. Operators shall be able at any time to bypass the door contact manually from the SMS workstation.

40. It shall be possible to program on KT-400 controller readers a double and triple switch function.

41. It shall be possible to have the multi-swipe function activating a predetermined schedule.

42. The double and triple swipes shall be able to be activated on reader simultaneously each with their respective actions.

43. The multi-swipe function shall be able to but not limited to:
    a. Toggle door unlock.
    b. Unlock door.
    c. Relock door.
    d. Temporarily unlock door.
    e. Activate Relay.
    f. Temporarily activate relay.
    g. Arm door partition request when using a Multi-Site Gateway.

44. Each cardholder shall have the option of having the multi-swipe function active.

45. A specific event shall be generated for any valid or invalid, double or triple swipes.

46. When using ioProx/ioSmart XSF/SSF format readers and the KT-400 controllers the SMS shall support eight readers for four doors.
    a. Each door shall have two readers on the same reader port. The installation shall be simple and not require any extra modules to be added.
    b. The exit reader of the door shall be wired on the same terminals as the entry reader by simply reversing D0/D1.
        1. The ioSmart readers shall communicate to the KT-400 over RS-485 on COM2 or standard Wiegand.
    c. Power, LED/piezo outputs shall be shared with the entry/exit reader.
    d. The SMS shall offer specific exit reader functionalities but not limited to:
        i. Assigning a specific access level schedule to each reader independently.
        ii. Enabling/disabling the entry/exit reader separately.
        iii. Running reports on the readers separately or together.
        iv. Follow the entry reader door name with a suffix of “-exit”.

v. Share the same locking output.
vi. Share the same door contact.
vii. Share the same unlock schedule.
viii. Share the same unlock time and open time.

e. All eight readers shall be used if needed in a controller based anti-passback.

47. First person in, shall unlock the door on a schedule:
    a. With the KT-400 and the KT-1 a one hour grace period shall be configurable. The cardholder shall be able to enter within that grace period time and keep the door locked. When the door schedule activates the door shall go on a schedule.
    b. If no cardholder has presented their card within the grace period or within the schedule the door shall remain locked.
    c. The “first person in” shall be configurable on a per door basis.
48. Save events on a hard drive according to required criteria.
49. Perform the following operations from all workstations:
    a. Lock or unlock, one time unlock, return to schedule one door or a group of doors.
    b. View the last access event on the door.
    c. Bypass the door contact and keep door locked.
    d. Temporarily unlock a door using a custom timer for additional door unlocking on KT-400 and KT-1 controller doors.
    e. Disable and enable readers.
    f. View custom programmed comments in the component’s Operation section.
    g. Activate or deactivate a relay or a group of relays.
    h. Activate or deactivate the recording of one camera or a group of cameras.
    i. Activate or deactivate a point or a group of points.
    j. Program or modify one card or a group of cards.
    k. Assign single door access exception to the card.
    l. Validate or invalidate one card or a group of cards.
    m. Change time and date.
    n. Demand the system state in text or graphic mode.
    o. Query, create and/or modify data on: access levels, schedules and holidays, access card, instructions, reports and log, doors, supervision points and relays, operator levels, and graphics.
    p. Ability to use an easy to use system tree view to select the components.
    q. View, which cards are in the roll call sectors.
    r. View the card’s last known access in the roll call sector.
50. The operator shall be able to double click on components on the operation screen to automatically view the status in detailed text values.
51. Perform the following operations from the SmartLink task commander:
    a. Alarm.
    b. Disable and enable any reader.

c. Lock, unlock, temporary unlock return to schedule, disable enable any elevator and elevator floor.
d. Activate, deactivate, temporary activate, toggle and return to schedule of any relay.
e. Shunt, unshunt, temporary shunt, toggle, return to schedule and continuous supervision of any input.
f. Set count usage, manually overwrite the count, disable count usage, decrement count usage, and increment count usage for all the cards.
g. Send alarm e-mails.
h. The use of variables in the SmartLink task commander can be used instead of hard coded values.
i. Mass card modifications on without operator intervention.
j. Ability to use generically created commands to perform task on different components.
k. Each specific card shall have the ability to activate a specific component in the above mentioned states without the need to create hard coded the commands.
l. The SmartLink task commander shall process the commands on the first available SmartLink on the SMS.
m. The use of a specific SmartLink to run a specific SmartLink task commander shall not be accepted.
n. The SMS all allow for many SmartLink to be installed without the need to purchase additional option codes.
o. The SmartLink task commander shall be run from any of the available SmartLink.
p. The SmartLink task commander shall allow for single or grouping of components of the same type to trigger the same task. The need to have a specific trigger programmed per component to trigger the same task shall not be accepted.

2.10 EQUIPMENT

2.10.Server and Redundant Server requirements.

The SMS server and Redundant Server shall meet the following minimum requirements:

1. The server shall have a dual core processor or better.
    a. If doing video the server shall have an Intel quad core processor or better.

2. The server shall have a 500-watt power unit.

3. The server shall have 4 GB RAM.
    a. If doing video, the server shall have 8 GB RAM or more.

4. The server shall have 100 GB hard disk drive space at minimum.

5. The server operating system shall be Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows 7, Windows 8.1, or Windows 10. All operating systems shall be 32-bit or 64-bit.
    a. The integration platform requirements shall possibly change the EntraPass requirements depending on integration products.

6. The server shall have a 100/1000 Base-T network adapter.

7. The server shall have a high quality multilingual keyboard.
8. The server shall have a two button ergonomic mouse.
9. The server shall have an on-off switch.
10. The server shall have an appropriate UPS.

2.10.B Multi-Site Gateway, SmartLink and videovault requirements.

The SMS Multi-Site Gateway shall meet the following minimum requirements:

1. The Multi-Site Gateway shall have a dual core processor or better.
2. The Multi-Site Gateway shall have a 500 watt power unit.
3. The Multi-Site Gateway shall have 4 GB RAM.
4. The Multi-Site Gateway shall have 100 GB hard disk drive space.
5. The server operating system shall be Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows 7, Windows 8.1, or Windows 10. All operating systems shall be 32-bit or 64-bit.
6. The Multi-Site Gateway shall have a 100/1000 Base-T network adapter.
7. The Multi-Site Gateway shall have a high quality multilingual keyboard.
8. The Multi-Site Gateway shall have a two button ergonomic mouse.
9. The Multi-Site Gateway shall have an on-off switch.
10. The Multi-Site Gateway shall have an appropriate UPS.

2.10.C Workstation Requirements

The SMS workstations shall meet the following minimum requirements:

1. The workstation shall have a dual core processor or better.
    a. If doing video, the workstation shall have an Intel quad core processor or better.
2. The workstation shall have a 500 watt power unit.
3. The workstation shall have 4 GB RAM.
    a. If doing video, the workstation shall have an 8 GB of RAM or more.
4. The workstation shall have 100 GB hard disk drive space.
5. The workstation shall have a 48 x CD-ROM drive.

6. The server operating system shall be Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows 7, Windows 8.1, or Windows 10. All operating systems shall be 32-bit or 64-bit.

    a. The integration platform requirements shall possibly change the EntraPass requirements depending on integration products.

7. The workstation shall have a 100/1000 Base-T network adapter.

8. The workstation shall have a high quality multilingual keyboard.

9. The workstation shall have a two button ergonomic mouse.

10. The workstation shall have an on-off switch.

11. The workstation shall have an appropriate UPS.

2.10.D Controllers

The SMS shall support the following door controllers:

1. Kantech KT-400:

    The KT-400 is an Ethernet-ready four-door controller with sixteen monitored points, on-board door strike power, sixteen reader outputs, four relay outputs, and auxiliary power output. It shall accept Wiegand, proximity, ABA clock and data, bar code, magnetic, integrated keypad, and smart card reader types. It shall also support FIPS 201 cards, with and without checking the expiration date. It supports RS-232, RS-485 and 128-bit AES encrypted Ethernet 10/100Base-T communication. It supports expansion modules to provide 256 inputs and 256 outputs. It shall support 256 double end of line inputs with ioModules. It shall support up to support eight card formats (nine with DUAL ioProx driver). The KT-400 shall support 20 native intervals per schedule. The KT-400 shall support the following native features but will not be limited to them:

    a. Twenty intervals per schedule.
    b. Five access levels per card when connected to a Multi-Site Gateway.
    c. Multi-swipe capabilities.
    d. 100,000 cards in standalone mode.
    e. 20,000 events in standalone mode.
    f. First person in with one hour grace period.
    g. Elevator unlock schedule per floor.
    h. Eight readers, four doors with ioProx XSF readers or ioSmart readers.
    i. Eight Assa Abloy wireless locks (licenses required).
    j. ioSmart readers support over Wiegand or RS-485.
    k. ioModules input/output expansion module communicate over RS-485.

2. Kantech KT-1:

    The KT-1 is an Ethernet-ready one-door controller PoE/PoE+ with four monitored (single, double, or no end-of-line) points, on-board door strike power, two reader outputs, two relay outputs, and auxiliary power output. It shall support a lock output of

750mA when powered by 12dvc or PoE+. It shall accept Wiegand, proximity, ABA clock and data, bar code, magnetic, integrated keypad, and smart card reader types. It shall also support FIPS 201 cards, with and without checking the expiration date. It supports RS-232, RS-485 and 128-bit AES encrypted Ethernet 10/100Base-T communication. It shall support up to eight card formats. It supports expansion modules to provide 256 inputs and 256 outputs. It shall support 256 double end of line inputs.

a. The KT-1 shall support the following native features but will not be limited to them:
   i. Twenty intervals per schedule.
   ii. Five access levels per card when connected to a Multi-Site Gateway.
   iii. Multi-swipe capabilities.
   iv. 100,000 cards in stand-alone mode.
   v. 20,000 events in stand-alone mode.
   vi. First person in, with one hour grace period.
   vii. Eight Assa Abloy wireless locks, licenses required.
   viii. ioSmart readers support over Wiegand or RS-485.
   ix. ioModules input/output expansion module communicate over RS-485.
b. The multi-purpose single button shall be used for:
   i. Auto-enrolling a new KT-1 to the SMS over a local LAN segment
   ii. Enrolling a new KT-1 to a primary KT-1 over IP (over local LAN segment).
   iii. Status of the controller's communication, locks and relays.
   iv. Used as a request-to-exit.
c. The multi-purpose button shall be LED configurable.
d. The KT-1 shall be installed in two ways:
   i. Mountable quickly and efficiently on a single gang installation on the internal side of the door.
   ii. In a cabinet on a PCB board. This configuration shall support a DSC integration.

3. Kantech KT-300:

   The KT-300 is a two-door controller with eight monitored points on board expandable to sixteen, door strike power, auxiliary power output, and two auxiliary outputs. It shall accept Wiegand, proximity, bar code, magnetic and integrated keypad reader types. It supports RS-232, RS-485, and Combus communication. It supports relay, input, and output expansion modules. The KT-300 is available in 128k and 512k memory versions.

4. Kantech KT-100:

   The KT-100 is a one-door controller with four monitored points, door strike power, and four auxiliary outputs. It shall accept Wiegand, proximity, bar code, magnetic and integrated keypad reader types. It supports RS-485 communication.

5. Kantech KT-200 (Legacy).

2.10.E Kantech Telephone Entry System (KTES)

1. The KTES enables tenants to grant access to the building, to their visitors, via their own telephone line or cellular telephone. The KTES supports 250 tenants with the option of supporting up to 3,000 tenants. The KTES also includes:

- Four lines x 20 characters LCD module with controllable LED backlighting.
- Programming menus available in three (3) languages (English, French and Spanish).
- Built-in RS-485
- 128-bit AES encrypted Ethernet.
- Internal modem
- Three (3) relays
- Microphone
- Speaker
- Backup battery

2. Optional KTES accessories are:
   - Heater kit
   - Postal lock
   - Color camera
   - Goose neck mounting
   - Paper index (flush mounted).

3. The KTES shall be programmed using the keypad and LCD for standalone mode or via the SMS.

4. The unit shall support a Wiegand reader that will allow tenants to swipe their cards and enter the building.

5. The KTES shall employ flashable firmware with auto update.

2.10.F Card and Reader Support

1. The SMS shall support configuration of unlimited card formats.
2. The SMS shall support up to two card formats per KT-100 and KT-300 controller.
3. The SMS shall support up to eight card formats per KT-400 controller or KT-1 controllers
4. The SMS shall support readers that provide Wiegand signaling and magnetic ABA signaling to include:

   a. Kantech ioProx family of readers.
   b. Kantech ioSmart family of readers.
   c. Wiegand swipe readers.
   d. Proximity readers.
   e. Biometric readers.
   f. Smart card readers.
   g. Wireless readers.
   h. Magnetic readers.

PART III EXECUTION

3.1 TESTING

1. The software shall be entered into the SMS computer systems and debugged. The contractor shall be responsible for documenting and entering the initial database into the system. The contractor shall provide the necessary blank forms with instructions to fill-in all the required data information that will make up the database. The database shall then be reviewed by the contractor and entered into the system. Prior to full operation, a complete demonstration of the computer real-time functions shall be performed. A printed validation log shall be provided as proof of operation for each software application package. In addition, a point utilization report shall be furnished listing each point, the associated programs utilizing that point as an input or output and the programs which that point initiates.

2. Upon satisfactory on-line operation of the system software, the entire installation including all subsystems shall be inspected. The contractor shall perform all tests, furnish all test equipment and consumable supplies necessary and perform any work as required to establish performance levels for the system in accordance with the specifications. Each device shall be tested as a working component of the completed system. All system controls shall be inspected for proper operation and response.

3. Tests shall demonstrate the response time and display format of each different type of input sensor and output control device. Response time shall be measured with the system functioning at full capacity. Computer operation shall be tested with the complete data file.

4. The contractor shall maintain a complete log of all inspections and tests. Upon final completion of system tests, a copy of the log records shall be submitted as part of the as-built documentation.

3.2 TRAINING

The contractor shall provide a competent trainer who has extensive experience on the installed systems and in delivering training to provide the instruction. As an alternate, the contractor may propose the use of factory training personnel and coordinate the number of personnel to be trained.

3.3 MAINTENANCE

1. The contractor shall offer a Kantech Advantage Program (KAP) to provide twelve additional months of free software updates and online training for the end user.

2. Technical support is available at no charge to all Kantech dealers whether or not they have a KAP activated for the systems they are supporting.

END OF SPECIFICATIONS

D29010754R001