E N T R A P A S S™

# Architectural and Engineering Specifications

# Managed Access Control and Integrated Systems

KANTECH

DN1924-1010 / 4.04 Version

## TABLE OF CONTENTS

## HOSTED & MANAGED SECURITY SYSTEM SERVICES A&E SPECIFICATIONS

## PART I GENERAL

### 1.1 GENERAL DESCRIPTION

Hosted and Managed Security System Services are a means of outsourcing a company's security to a qualified Managed Services Provider (MSP). Clients benefit from reliable, cost-effective security without the overhead of a full staff to manage the system nor the necessary computer infrastructure required to run the system. The MSP procures and maintains the system server, manages the applications and database, and provides operational monitoring. Therefore there is no client on-site software or dedicated computer to maintain, minimal training required, and minimal local administration of the system.

While the MSP manages the system, the client can (optionally) still control the system by adding, deleting, or modifying cards and badges, performing manual operations, and requesting reports. This management can be done via a secure web interface (Web Portal), phone call, fax, or email.

There are base services that all MSP's shall provide as well as optional services that can be provided either based on the capabilities of the MSP or the requirements of the client. What services the MSP provides to the client is completely customizable on a client by client basis.

No specialized equipment or software is required for Managed Security System Services. Regularly provided Kantech EntraPass software with the Managed Access Control license activated and Kantech controllers and associated equipment, making up a Security Management System (SMS), are all that is required. The controllers connect to the Managed Service Provider through a domain name or IP address. Database management tools are built into the server for reliability with minimal maintenance and down time. The managed system is a plug and play solution; there is no port forwarding, IT management functions, or static IP addresses required. All system communication is secure 128-bit AES Encrypted communication.

The SMS shall be a WAN-based access control security service providing unlimited system growth and services by employing the option of either Hosted or Managed Security Services. The flexibility of SMS shall enable it to meet world-wide security concerns from foreign governments of having the data within their respective country borders.

### 1.2 SUBMITTALS

Prior to assembling or installing the Security Management System (SMS) as part of the Managed Security System Services, the MSP 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 shall operate 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. Start up 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.

## 1.3 HOSTED SERVICES

A Hosted SMS shall enable the end user to manage their own Account and application. The MSP shall host the database, server applications and hardware infrastructure. The MSP shall provide the initial set-up of the Account and components. The end user shall be able to administer the services from either a secure web client or workstation.

The hosted system shall include services but not limited to;

1. Employee permission administration.
2. Automated alerts monitoring by MSP operators.
3. Automatic or manual email reports.
4. Add/delete/modify cards or other credentials
5. Creation of additional access levels
6. Provide an Account Workstation (thick client) as well as the Webstation (thin client) at client site.

## 1.4 MANAGED SECURITY SERVICES

The MSP shall manage 100% of the end users' needs and requirements as outlined in Section 1.6 of these specifications. In addition, optional services may be provided as outlined in Section 1.7 of these specifications.

The MSP shall host and manage the database, server applications and hardware infrastructure. The MSP shall provide on an ongoing basis all functionality and needs of the Account and components. The end user shall make requests to the MSP for all changes and operation. The end user shall also have the ability to perform day to day operations from the secure web client.

## 1.5 MANAGED SERVICES PROVIDER QUALIFICATIONS

1. The Managed Services Provider (MSP) 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 MSP shall be actively engaged in reselling Managed Services as part of their normal business offerings. The service provider shall sell services only to customers to whom they can provide onsite support, either directly or through a Dealer network.

3. The MSP shall be an authorized Kantech Corporate or Global Dealer.

4. The MSP, prior to responding to any RFP/RFQ, shall be an authorized reseller of Kantech Managed Services having been vetted by Kantech and met prequalification criteria as set out in the Managed Services Reseller contract. Service providers shall not submit application to Kantech solely for one Account / project.

5. The MSP shall at a minimum utilize a server, gateway, workstation, redundant server, and web server. Optionally the service provider shall utilize a video vault and email server.

6. The MSP shall offer at least 1 Redundant Server in case of server failure. The redundant server shall automatically rollover and offer maximum up-time. The platform must be within 6 months of current release.

7. The MSP shall at all times employ competent factory trained and certified installation and service technicians capable of maintaining the system and providing reasonable service time. The certification must be current to the latest software release.

8. The MSP 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.

9. 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.

## 1.6 MANAGED SERVICES PROVIDER BASE SERVICES

At a minimum, the Managed Service Provider (MSP) shall provide the following services:

1. Real time building access control and management of the controllers.
2. System redundancy that will allow the system to continue to work in the event of a main server failure. The redundant server shall communicate and function with the primary server without the need of operation intervention. The redundant server shall take complete control of the system without the need of operation intervention
3. System growth management to system capacity of section 2.2 states 2.8 million readers.
4. The MSP shall be capable of updating to the newest version of the software when it is released by the manufacturer.

5. The MSP shall purchase, administer, update, and maintain servers and software licenses to offer Managed Services.
6. True server Account segregation and sub-Account segregation. The MSP shall require only 1 SMS to manage an unlimited amount of accounts. MSP's that use one computer/SMS server per Account shall not be permitted.
    a. Each Account's segregation shall be completely independent of the other accounts.
    b. MSP operators shall be able to see all accounts and login to a specific Account to perform any actions allowed on that account.
    c. Account operators shall only be able to manage their respective account(s).
7. The controllers shall communicate with the MSP via Internet, GSM, or dial PTSN communications.
    a. When communicating via Internet or GSM connection the communication shall be a secured 128-bit AES Encrypted Ethernet communication.
    b. The communication via Internet connection shall be extremely low bandwidth, no more than 5Kb/second when sending 10 messages and less than 1Kb/minute during standby. The controllers shall be able to communicate to the MSP via DNS (domain name).
    c. The customer shall not be required to have a static public IP address for their Internet connection
8. One year of online data archiving.
9. The component management and manual operations shall be in real time.
    a. All modifications or manual operations from the MSP or by the customer via the WebStation shall be in real time and shall take less 1 second at all times to perform.
10. Acknowledgement of modifications made.
11. WebStation Self-Serve Features
    a. Card management
    b. Access level management
    c. Real time Report request (report to be sent via email)
    d. Schedule management
    e. Operator password management
    f. Operations – doors, inputs, outputs, elevator doors
    g. Web Views
13. Data import of cards (in blocks of 100 cards)
14. Customized operator control through Web Portal for each client.
12. Trained technicians to professionally install hardware.
13. A factory trained and certified system administrator.
14. A consistent set of business rules to manage the system.
15. Professional system administration including data backups and system redundancy.

## 1.7 MANAGED SERVICES PROVIDER OPTIONAL SERVICES

The Managed Services Provider (MSP) shall have the option of providing the following services (modify A&E specifications based on desired services):

1. Monitoring of access control system 24 x 7 x 365.
2. Employee permissions administration.
3. Automated alerts monitoring by MSP operators.
4. Automatic or manual emailed reports.

5. Additional years of online data archiving.
6. Automated daily reports
7. Automated weekly reports.
8. Automated monthly reports.
9. On demand reporting through Web interface.
10. Add/Delete/Modify single card by MSP or WebStation.
11. Creation of additional access levels by MSP or WebStation.
12. Credential services such as Badge printing.
13. Video integration.
14. Viewing live video and monitoring of video 24 x 7 x 365.
15. Real time concierge services such as door locking and unlocking.
16. Web Portal customized by client.
17. Provide an Account Workstation (thick client) as well as the WebStation (thin client) at client site

## PART II PRODUCTS

### 2.1 MANUFACTURERS

The Security Management System (SMS) shall be the Kantech EntraPass Corporate or Global Edition.

### 2.2 DESCRIPTION

The security filed devices (readers, door position switches, REX, etc) shall communicate with the field panels via a dedicated cable network. The field panels shall communicate to the SMS via a Fast Ethernet 10/100, TCP/IP network, cable modem, DSL, or other high speed Internet connection, or dial up modem. The SMS shall allow for growth and scalability from a two reader system to over 2.8 million on 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 platform shall support up to:

| | |
|---|---|
| 128 | Redundant servers |
| 300 | Digital video recorders |
| 41 | Corporate gateways |
| 17,408 | Controllers per gateway |
| 69,632 | Card readers and/or keypads and/or elevator cabs of 64 floors each per Corporate gateway |
| Unlimited | Access cards |
| Unlimited | Card families or site codes |
| 4,456,448 | Alarm points monitored per Corporate gateway |
| 4,456,448 | Control relays per Corporate gateway |

Not all the performance parameters of the SMS described herein may apply to all systems using Managed Services (modify A&E specifications based on desired services).

The SMS shall ensure the communication to remote sites over a LAN or WAN/Internet using a dedicated communication server device, Kantech IP Link or the KT-400 controller. This shall only be applicable with the use of Corporate Gateways. It shall ensure secure communications by the use of 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 IP Link or KT-400 in the field and not over the network. The Kantech IP Link 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.

For sites 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 Corporate Gateways. No modem shall be dedicated to specific sites; communication shall be established such that the first site calling shall have access to the first available modem, and so on.

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.

## 2.3 ACCOUNT WORKSTATION

2.3.A Account Workstation

1. It shall be possible for the client to have a permanent fully functional workstation installed on their computer. The client shall have the possibility to perform various functions to manage their own components without the need to host the server computers at their location.

2. The Account Workstation shall have VPN connection to the MSP. The Account Workstation shall be programmed to work only with its corresponding account.

3. Only logins belonging to the Account shall have the option to login to the Account Workstation.

4. Once logged in, the operator shall only see events, and components that belong to their Account to perform operations.

5. The Account Workstation shall have at a minimum the functions listed in Section 2.3 of these specifications. Depending on the operator's security level and workspace; certain functions may not be available to the operator.

2.3.B Monitoring Mode

1. The account workstation shall enable every operator to customize his/her desktop configuration. It shall be possible to modify the desktop appearance and to create up to eight desktops and to associate up to ten 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.

1. 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.

   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.

3. Card Holder 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 Account Workstation shall support the display of up to 4 pictures simultaneously.

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 Account Workstation 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.

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.

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 Account Workstation is integrated with American Dynamics Intellex digital video recorders, it shall be possible to view the video images of cameras associated with them. The Account Workstation 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 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.

   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.

2.3.C 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 WebView, 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, etc. to the desktop
   f. Accessing to network cameras from the Webstation
   g. HTML or PDF pop-up instruction on alarm
   h. 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, 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.

   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, and enabling or disabling a reader. 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.

   No additional licensing shall be required to perform this function.

2.3.D 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 Account Workstation 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.

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

   a. Card number
   b. First and last name
   c. Card type
   d. Additional information (10 fields)
   e. Start date
   f. Expiry date
   g. Personal ID number (PIN)
   h. State of the card
   i. Comments

   In addition, it shall be possible to associate a photograph, signature, and badge template to a card.

4. The Account Workstation 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

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

6. The Account Workstation 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)

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

8. The Account Workstation 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 field delimiter. This shall allow for acceleration of the data entry process by importing databases from a spreadsheet.

9. The Account Workstation shall allow for 250 access levels programmed per loop of controllers. Every card shall be assigned an access level which shall determine where and when the access card will be valid.

10. The Account Workstation 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 Account Workstation shall support the creation of unlimited amounts of tenant lists.

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

12. 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

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

2.3.E Video Section

1. The Account Workstation shall be capable of being combined with up to 128 American Dynamics Intellex digital video recorders. 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 Account Workstation(PTZ control)
    e. Export camera images to hard disk and video vault (capable of exporting multiple formats, password protected to protect chain of evidence)

2. The Account Workstation shall ensure the time management and synchronization for all digital video recorders. It shall be possible to determine the time refresh frequency on the network. The Account Workstation shall allow for configuration of each digital video recorder. For each recorder it shall be possible to:

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

3. The Account Workstation shall define the programming parameters for every camera connected to a digital video recorder. 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 should 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

4. The Account Workstation 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. The video view programming parameters make it possible to:

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
p. Incorporate up to 16 cameras from various sources or 16 graphics

5. The Account Workstation shall be able to trigger, from one or more specific events, the start of recording on a recorder with one or more cameras connected to it. The Account Workstation shall allow for the creation of an unlimited number of video triggers. The Account Workstation 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 digital video recorder 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

6. It shall be possible for a video event on one digital video recorder to trigger an action on another digital video recorder.

7. The Account Workstation shall allow the playback of all recordings stored on the hard drive of any of the digital video recorders. The operator shall be able to save the video into the video vault.

8. The Account Workstation 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 Account Workstation shall allow the operator to access a complete list of alarm recordings in progress including origin of the alarm. The Account Workstation shall be capable of displaying a list of exported videos.

9. It shall be possible to view recorded video tagged to an Access or Video event by quick linking from the Message desktop.

2.3.F Definition Section

1. The Account Workstation shall allow the creation of 100 schedules per loop of controllers or account.. Each schedule can include up to 4 intervals. A schedule can be associated with a supervision point, a relay, an access level, a door, elevator floor, an operator, or an event. The Account Workstation shall allow time zone management.

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

3. The Account Workstation 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, and cameras. The Account Workstation 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 Account Workstation shall allow for printing of the graphics with their respective components on the graphical floor plan.

4. The Account Workstation shall allow the management of 34,816 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 Account Workstation shall allow the creation of groups of floors and access levels.

5. The Account Workstation shall provide the possibility of setting up guard tours with existing components of the system. Card readers, magnetic contacts and motion sensors can be used as control stations for the guard tour. Key switches can also be located at strategic points for the guard to activate.

6. The Account Workstation shall provide the possibility to setup unlimited amount of tasks via the user friendly task builder. The operator shall be able to create emails templates that can incorporate variable to dynamically populate the emails. Using

the command GUI menu, the operator can program commands for any component in the Account Workstation. 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 should be able to accept specific components or variables that can filled dynamically.

7. The Account Workstation shall provide the possibility to setup unlimited batch card operations via the user friendly task builder. The mass card modifications shall take effect in real time. Each mass card modifications task shall allow for mass cards to be changed based on their card type. The mass 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

8. The Account Workstation shall provide the possibility to assign the tasks previously created to be triggered on specific components and specific events.

9. The SmartLink Task Commander shall process the command from the first available SmartLink application on the Account Workstation.

    a. The use of a specific SmartLink to run the SmartLink Task Commander shall not be accepted. The Account Workstation shall accept many SmartLinks to be installed thus providing a redundant SmartLink for all SmartLink Task Commander tasks.

2.3.G Devices Section

1. The physical components of the Account Workstation site, controllers (KT-400, KT-300, KT-200 Legacy, KT-100), Kantech Telephone Entry System (KTES), doors, relays, 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. The Account Workstation shall employ an Express Setup to configure system components for sites and controllers, as well as peripherals associated to these components such as ports and inputs. The Express Setup utility will reduce the programming time.

2.3.H Alarm Interface

1. The Account Workstation shall allow 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 Corporate gateway. It shall be possible at a minimum to:

    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 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

2.3.I Intrusion Integration

1. The Account Workstation shall allow interface with the DSC PowerSeries 1616, 1832, and 1864 intrusion panels thereby eliminating hardwired integration between the Account Workstation controllers and the DSC PowerSeries intrusion panel. The DSC PowerSeries intrusion panel shall communicate with the Corporate gateway via RS-232 or directly to a KT-400 controller. The Account Workstation shall allow for:
    a. Single / multiple partition arming and disarming via reader
    b. Single / multiple partition arming and disarming via operator commands
    c. Receive events from intrusion panel
    d. Receive partition names, user codes and zone names programming.
    e. Update user codes
    f. Assign user codes to cardholders

2.3.J System Section

1. The Account Workstation shall define the profile of a system operator based on name, password, language, privileges, login schedule, security level, workspaces, and password expiry date. The Account Workstation 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.

2. The Account Workstation 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 Account Workstation 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

3. The Account Workstation shall allow System Administrators to grant or deny operators access to system physical components such as gateways, sites, relays, etc. 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 tasks, then easily revert back to their main workspace.

4. The Account Workstation 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.

5. The Account Workstation shall make it possible to customize system events. All events shall be pre-defined to display on all system workstations. For each event it shall be possible to:

a. Determine a display schedule
b. Determine a color
c. Assign a printer
d. Associate one or more workstations
e. Associate an instruction
f. Associate a schedule for an acknowledgement request
g. Determine the priority level

2.3.K Report Section

1. The Account Workstation 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 Account Workstation shall allow for the creation of custom reports based on any event or component in the system. The Account Workstation 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 Account Workstation shall support at a minimum the following report formats: Paradox, Dbase IV, CSV, XLS, PDF, RTF, and TXT.

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

6. 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.

7. The Account Workstation shall allow the creation of custom Roll Call reports, which can without operator intervention be emailed to multiple people and/or printed on multiple printers. The Roll Call report shall be a system wide feature.

## 2.4 ACCOUNT WORKSTATION OPERATION

The Account Workstation shall perform the following tasks:

1. Manage an unlimited amount of accounts per system. The need for the MSP to have separate software per Account shall not be permitted.

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

3. 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.

4. Allow automatic transfer of cards to an unknown area by a push of a button for emergency exit purposes.

5. Monitor all defined alarm points as well as all doors controlled by card readers based on programmed schedules.

6. Send transactions for which printing is required to one or more printers, based on a set schedule.

7. 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.

8. Enable the entry of access code data for every card or group of cards.

9. Seamlessly connect to onsite alarm systems.

10. A fully functioning virtual keypad with DSC PowerSeries alarm system. The operator shall perform all functions available on a standard keypad with the PowerSeries alarm. The operator shall be able to use the computer keyboard or the mouse to perform actions on the virtual keypad.

11. The Account Workstation shall allow interface with the DSC PowerSeries intrusion panel thereby eliminating hardwired integration between KT-400 and the DSC PowerSeries intrusion panel. The Account Workstation shall allow for:

    a. Single / multiple partition arming and disarming via reader
    b. Single / multiple partition arming and disarming via operator commands
    c. Receive events from intrusion panel
    d. Receive partition names, user codes and zone names programming.
    e. Update user codes
    f. Assign user codes to cardholders

12. Associate to each event a recording schedule for each destination (hard drive, monitor).

13. 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.

14. Each event should print on a log printer. For security reasons, each event shall be incremented with a print number. Numbering shall start from 0 every day.

15. Generate reports and view them on the screen, output them to a printer, or send them to an email address.

16. 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.

17. View and/or save video images.

18. When integrated into a digital video recording system (American Dynamics), allow the management of the recordings of all the cameras via access system workstations.

19. When connected to a digital video recording system (American Dynamics), allow the orientation of all PTZ cameras directly using the workstation mouse of the access system.

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

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

22. 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.

23. Allow for a Dual Custody option to add extra security to a door by requesting that two card holders must access the door together.

24. Perform the following operations from all workstations:

    a. Lock or unlock one door or a group of doors.
    b. Activate or deactivate a relay or a group of relays.
    c. Activate or deactivate the recording of one camera or a group of cameras.
    d. Activate or deactivate a point or a group of points.
    e. Program or modify one card or a group of cards.
    f. Validate or invalidate one card or a group of cards.
    g. Change time and date.
    h. Demand the system state in text or graphic mode.
    i. 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.
    j. Ability to use an easy to use system tree view to select the components.
    k. View which cards are in the roll call sectors.
    l. View the card's last known access in the roll call sector.

25. Perform the following operations from the SmartLink Task Commander:

    a. Lock, unlock toggle, return to schedule, temporary unlock, arm and disarm any door.
    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, increment count usage for all the cards.
    g. The use of variables in the SmartLink Task Commander can be used instead of hard coded values.
    h. Mass card modifications on without operator intervention.
    i. Ability to use generically created commands to perform task on different components.
    j. 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.

## 2.5 PERFORMANCE – WEBSTATION

1. The WebStation shall be mandatory for Managed Security Services clients. It is the tool that allows for performing functions from a remote location via Web Browser. The WebStation provides card management to guards, secretaries, managers and others without the need to deploy a full client workstation

2. The WebStation shall have the ability to be viewed in multiple languages. Each WebStation shall come at a minimum in English and French. The MSP may offer the Webstation in any other language they prefer. The WebStation shall automatically detect the Web Browser's preferred language.

3. The following functions are available using WebStation:

    a. Search for cards and deleting cards
    b. Card management: create and modify cards. The following fields at a minimum shall be saved :
        i. Five card numbers each with their expiration date
        ii. First and last name
        iii. Card type
        iv. Card filter
        v. Additional information (10 fields)
        vi. Start date
        vii. Expiry date
        viii. Personal ID number (PIN)
        ix. State of the card
        x. Card holder's picture
        xi. Card holder's signature
        xii. Comments
    c. Viewing the card's last transactions
    d. Forgot Password & Reset password
    e. Create, modify and delete access levels
    f. Create, modify and delete schedules
    g. Assigning access levels
    h. Performing door operation
    i. Performing relay operation
    j. Performing input operation
    k. Performing elevator operations
    l. Requesting historical reports
    m. Using WebViews

4. All operations, modifications and statuses shall happen in less than 1 second.

5. The WebStation shall follow the operator's security level and workspace to provide them with the functionally allowed to them.

6. For further security, operators shall not have to choose which Account they are logging in. The operators shall be automatically linked to their respective account.

7. Reports shall be emailed without MSP operator interaction to the client in real time.

8. The WebStation shall be two steps removed from the database (WebStation – SmartLink – Server – Database).

9. The WebStation shall be accessible at a minimum by the following web browsers:

    a. Internet Explorer 6,7,8
    b. Firefox,
    c. Chrome
    d. Safari.

10. The WebStation shall be accessible via secure SSL connection,

11. The need for the client to install client software to run the WebStation on their computer shall not be permitted.

12. The WebStation shall have an optional skin customized to the client specific look.

13. There shall be no ActiveX requirements for the WebStation.

## 2.6 REDUNDANCY & MIRRORING

2.6.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 (up to 128). The need to install third party (not EntraPass) licensing shall not be acceptable.

## 2.7 VIDEO VAULT

1. Video Vault is an optional remote networked application used to automate recovery of video data from the digital video recorders 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 digital video recorders shall include triggers, manual triggers, and saved video server footage.

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

    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 from the client's DVR to the MSP's location thereby reducing video network traffic during peak times.

## 2.8 EQUIPMENT

2.8.A Account Workstation Requirements

The Account Workstation workstations shall meet the following minimum requirements:

1. The workstation shall have an Pentium IV processor, 1.8 GHz or better
2. The workstation shall have a 500-watt power unit
3. The workstation shall have 1 GB RAM.
4. The workstation shall have 20 GB hard disk drive space
5. The workstation shall have a 48xCD / DVD ROM drive
6. The workstation operating system shall be Windows 2000/XP/2003 Standard and Enterprise Server Edition/ Vista Home, Home Premium, Enterprise, Business and Ultimate / Windows 2008 Server / Windows 7 Pro. All OS's must be 32 bit.
7. The workstation shall have a 10/100/1000 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 32 MB graphic adapter card
11. The workstation shall have a 24-bit (16 million colors) color depth monitor with a screen resolution of 1024 x 768
12. The workstation shall have an On-Off switch
13. The workstation shall have an appropriate UPS

2.8.B Kantech KT-400 Controller

1. The KT-400 is an Ethernet-ready four door controller that works with any EntraPass system. It shall also be capable on integrating with the KT-100 and KT-300 controllers.
2. The controller shall provide onboard Ethernet 128-bit AES-encrypted communication with the EntraPass system.
3. The controller shall have 16 onboard inputs expandable to 256, and 4 onboard outputs expandable to 256.

4. The controller shall have supervised door lock outputs and 12 to 24 VDC up to 3 amps of lock power with an internal or external power supply.
5. The controller 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.
6. The controller shall have a 100,000 card capacity and provide up to 20,000 concurrent events in standalone mode.
7. The controller shall support multiple controller configurations including IP (Ethernet), RS-485 (COM1) for communication between EntraPass Gateway and controller, and RS-232 (COM3) for direct connection to the EntraPass Gateway.
8. The controller shall control the occupancy level in a defined area with the anti-passback feature.
9. The controller shall communicate with the EntraPass Gateway only when an event has occurred, reducing the amount of bandwidth consumption. Communication integrity shall be ensured through a heartbeat signal sent at regular intervals to the EntraPass system. Communication failure shall trigger an alarm in the EntraPass system.
10. The controller shall employ LED's to provide controller status and diagnostic information and color coded removable terminal blocks.
11. The configuration of the IP settings for the controller shall be accomplished with a built in Web configuration page accessible through any Internet browser.
12. The controller shall interface with the DSC PowerSeries intrusion panels, eliminating hardwired integration. Functions shall include arming and disarming, assigning and updating user codes, and receiving events.

2.8.C Kantech IP Link Controller

1. The IP Link shall interface Kantech KT-100, KT-200 and KT-300 control panels using 128-bit AES encrypted static or dynamic internet protocols.
2. Up to 512 IP links shall be supported per EntraPass gateway.
3. The IP Link shall be able to operate up to 115,200 baud for serial communication.
4. The IP Link shall be compliant to; FCC Part 15, EN55022, EN55024, CE, C-Tick and UL294.

2.8.D Kantech KT-300 Controller

1. The KT-300 is a two door controller available in 128k and 512k memory versions and shall be capable of linking to a network.
2. The controller shall communicate at up to 115,200 baud.
3. The controller shall have 8 onboard inputs expandable to 16, 4 onboard outputs expandable to 16, and 2 control relay outputs.
4. The controller shall accept Wiegand, proximity, bar code, magnetic, and integrated keypad reader types.
5. The controller shall provide both 5V and 12V reader power and 12VDC door strike power.
6. The controller shall support RS-232, RS-485, and Combus communication.
7. The controller firmware shall update directly from a system workstation using 128K flash memory.
8. The controller shall be capable of interfacing with an external alarm system.

2.8.E Kantech KT-100 Controller

1. The KT-100 is a one door controller with a two reader capacity.
2. The controller shall communicate at up to 115,200 baud.
3. The controller shall have 4 onboard inputs, 2 onboard outputs, and 2 control relay outputs.
4. The controller shall accept Wiegand, proximity, bar code, magnetic, and integrated keypad reader types.
5. The controller shall provide 5 VDC reader power and 12VDC door strike power.
6. The controller shall support RS-485 communication.
7. The controller firmware shall update directly from a system workstation using 64K flash memory.
8. The controller shall be capable of interfacing with an external alarm system.

2.8.F Kantech KT-200 (Legacy) Controller

1. The KT-200 is a two door controller with a Z80-6MHz processor.
2. The controller shall communicate from 1200 to 19,200 baud.
3. The controller shall have 16 onboard inputs and 2 control relay outputs.
4. The controller shall accept Wiegand, proximity, bar code, mag stripe, and biometric reader types.
5. The controller shall provide 27 VDC door strike power.
6. The controller shall support RS232 and RS485 communication.
7. The controller shall keep the access control database in memory.

2.8.G KTES (Kantech Telephone Entry System)

1. The KTES is a stand alone or integrated one door telephone entry system. It shall enable tenants to grant building access to their visitors via their own telephone line or cellular telephone.
2. The KTES shall include a vandal and weather resistant metal enclosure with a keypad, speaker, microphone, and a 4-line, 20 characters LCD module with controllable LED backlighting. Three contextual function buttons shall be used to navigate through the interface.
3. The KTES shall include an electronic directory with a capacity of 125 to 3,000 tenants. Menus shall be available in three (3) languages (English, French and Spanish).
4. Programming shall be done either directly from the keypad or through remote programming with EntraPass software. Communication shall be via built-in RS-485, 128-bit AES encrypted Ethernet, or internal modem. Importing of tenant information from the EntraPass workstation shall be in CSV format.
5. The KTES shall include 4 monitored inputs, 3 auxiliary relays, and supervised battery backup.
6. Optional KTES accessories shall include a heater kit, postal lock, color camera, goose neck mounting, and paper index (flush mounted).
7. The unit shall include Wiegand inputs and outputs so a Wiegand reader can also be utilized for tenant access.
8. The KTES shall employ flashable firmware with auto update.
9. The telephone line utilized shall be standard touch tone or rotary. One telephone line shall support up to five units.
10. The KTES shall allow for alarm and trouble reporting directly to the EntraPass system and shall also maintain a local event log which can be viewed from the LCD.

11. The call length shall be programmable from 10 seconds to 1 hour.

2.8.H Card and Reader Support

1. The Account Workstation shall support configuration of unlimited card formats.
2. The KT-400, KT-300 and KT-100 controllers shall support up to 2 card formats per controller (3 with DUAL ioProx driver).
3. The controllers shall support readers that provide Wiegand signaling and magnetic ABA signaling to include:
    a. Kantech ioProx family of readers
    b. Wiegand swipe readers
    c. Proximity readers
    d. Biometric readers
    e. Smart card readers (if reading CSN, then KT-400 only)
    f. Wireless readers
    g. Magnetic readers

## PART III EXECUTION

### 3.1 TESTING

1. The software shall be entered into the Account Workstation 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.

END OF SPECIFICATIONS