



Access Control

Architect & Engineer Specifications

October 2007



Table of Contents

1. OBJECTIVE OF THE PROJECT	5
2. GENERAL	5
DESIGN OF THE INSTALLATION	5
MODULARITY	7
INTEGRATION.....	9
OPERATING PRINCIPLES.....	11
<i>Geographic authorization.....</i>	<i>11</i>
<i>Time related authorization.....</i>	<i>11</i>
<i>Access authorization groups.....</i>	<i>12</i>
<i>Access authorization.....</i>	<i>12</i>
<i>Additional functions.....</i>	<i>13</i>
<i>Multi-card support per person.....</i>	<i>14</i>
3. HARDWARE	15
ACCESS CONTROLLER	15
INPUT/OUTPUT CONTROLLER	20
LIFT CONTROLLER.....	21
NETWORK COMMUNICATION DESCRIPTION	23
<i>Cabling architecture:.....</i>	<i>23</i>
<i>Communication Dispatcher.....</i>	<i>23</i>
READER TECHNOLOGIES	25
INSERTION READERS	25
4. DESCRIPTION OF THE SOFTWARE MODULES	26
ACCESS CONTROL MODULE	26
<i>Environment.....</i>	<i>26</i>
<i>Functions of access control software module.....</i>	<i>26</i>
ADVANCED ACCESS CONTROL FUNCTIONS	32
<i>Logical control of position.....</i>	<i>32</i>
<i>“Confirmation” cards.....</i>	<i>32</i>
<i>Access to sensitive areas using multiple cards (Multi-card access).....</i>	<i>32</i>
<i>Multi-site management.....</i>	<i>33</i>
<i>Graphic monitoring module.....</i>	<i>34</i>
<i>Macro-instructions language.....</i>	<i>34</i>
TECHNICAL MONITORING OF THE SOFTWARE	35
CRISIS MANAGEMENT	35
ADDITIONAL SOFTWARE MODULES.....	36
FILTERS CRITERIA / REPORT GENERATION.....	36
VISITOR MANAGEMENT MODULE	38
<i>Advanced functionality of the visitor management software:.....</i>	<i>39</i>
<i>Pre-visit management via Intranet.....</i>	<i>40</i>
CARD PERSONALIZATION MODULE	40
EXTERNAL DATABASE INTERFACES.....	42



1. Objective of the Project

The purpose of the project is the supply, installation and commissioning of an access and intrusion control, visual graphic monitoring and visitor management system.

2. General

The project consists of installing a system for controlling access by use of Readers and Controllers that activate various access, egress and locking systems: electrical locks, ventilation outlets, parking barriers, turnstiles, etc.

In order to be able to offer the best guarantees with regard to reliability, security and simplicity, the installation shall be designed in accordance with the principle of distributed intelligence.

The principle of distributed intelligence means that under no condition will a Controller have to interrogate any concentrator or central processing unit in order to authorize the opening of the controlled access. Passing an authorized card through the reader results in an immediate command to open the controlled access, regardless of the load on the communication network or on the system's main control unit (computer). A detectable waiting period may only occur when an anti-passback function has been configured, or in a rare case where the administrator of access authorization management has selected this configuration option in the management system for a specific part of the installation.

The Controllers shall be CE Marked.

Design of the Installation

Each monitored access shall be equipped with:

- Electronics Controllers managing up to two entrance/exit doors* or up to four ordinary entrance doors (with distributed intelligence in all cases)
- Entry: a card reader outside the protected area.
- Exit: a pushbutton or request-to exit unit and a reader if exit control is required (option).
- An electrical system for locking and unlocking the door, continuously operating at 12 V and opening when there is a power failure.
- A monitoring switch providing the status of the door.

** NOTE: The Controller shall be able to have a maximum of 4 readers*



Comments:

- All Controllers shall be able to support a reader for exit, in addition to entry (if the Controller manages one or two doors).
- All Controllers shall support a keypad, at the entrance as well as at the exit, in order to enable the use of personal identification numbers (PIN) in addition to the card.
- Should directional obstacles (turnstiles, single-person locks, etc.) be used, the same Controller shall enable a different command relay to be activated, depending upon the direction of passage (one relay for entry and another for exit).
- All the Controllers shall be connected to a main management PC via a reliable communication link (Ethernet, etc.).

This connection shall serve three objectives:

- Enabling the configuration data to be downloaded into the Controller to allow distributed intelligence (cards, codes, schedules, etc.).
- Enabling PC commands to be sent to the Controller (unlocking, etc.).
- Enabling the information to be retrieved by the PC (events, alerts, etc.).

Should this connection be interrupted, the system's operation shall not be affected and the Controller's response time shall remain the same (due to the principle of distributed intelligence).

- The switching power supply of a Controller shall be sufficient to operate a 12V locking system. The power supply shall be backed up by battery.

Modularity

The principle of distributed intelligence and the type of communication used shall enable the broadest possible modularity.

Controllers shall easily be added or removed from the installation at any time.

There shall be no limit to the number of Controllers that the installation can contain. Nevertheless, a management capacity of 15 Controllers per loop is advised to maintain adequate response times; an unlimited number of loops can be used.



Integration

The system shall be comprised of an integrated solution for managing access, timetables, alerts, card personalization and visitor management, all using a common database and enabling use of different cards technologies.

The system shall enable:

- The integration of a card identification management system with photos (**Maximage – delete references to product names if spec needs to be generic) which makes it possible to capture photographs, store them and print cards. This system uses the same card and the same database, and can use the same management PC.
- The integration of an optimized visitor management system (**MaxVisit – delete product name if spec needs to be generic) thereby making it possible to rapidly enroll and edit the visitor cards. The visitor management system shall be able to generate paper or adhesive cards as well as regular access control tags. These tags will be automatically validated on the company access control system according to the visit needs. Management of visitor's history shall also be possible.
- The integration of a graphic management software (**SynopSYS – Delete product name if spec needs to be generic) for protection and security resources, which shall ensure the synthesis of information from the different asset and people protection systems, displays to the operator the instructions to be applied in case of an alarms and events, and is able to display the sites and action resources available to him.

The graphic management software shall also enable (among other functionality):

- The display of alerts on a map
- The selection of the events and alerts to be displayed
- The programming of an order of precedence of the alerts
- The acknowledgement of the alerts
- The processing of the alerts
- Automatic actions and/or transmissions in the absence of an operator
- The integration of information from other systems by controller contacts and software integration (intrusion alarm systems, fire alarm systems, NVR and DVR systems, Building Managements systems, etc.)
- The display and management of security and safety elements (fire-fighting resources, emergency exits, etc.).

The solution shall be part of a comprehensive and integrated system that enables future development and expansion of the system.



Operating principles

The authorization for card access shall depend upon the following criteria:

- Geographic authorization
- Time-related authorization
- Beginning and end dates and times for the validity of the card for the whole installation
- Beginning and end dates and times for the validity of the card at certain specific doors

Geographic authorization

Accesses shall be sorted by reader groups, which define the authorized access zones for certain categories of people.

There shall be up to 1,500 reader groups.

An access shall be part of several reader groups.

A card shall only be authorized for the access assigned to a specific group and within a specific timeframe.

This principle enables flexible and easy management of access authorizations and does not require individual reprogramming for each card in the event of changes in the organization.

Nonetheless, exception management is anticipated (for one time events, contactors, service people, etc.) and makes it possible to individually program authorized access for each card (reader-by-reader and/or by reader group).

Time related authorization

The access authorizations can be limited to specific times during the day.

Time related constraints shall be based upon the following principle:

- The timetables shall be sorted according to different categories (known as “access types”).
- Each card shall be identified by an Access Authorization Group (AAG) which classifies the reader groups and the types of access.
- 16 types of access shall be available.
- An authorized access schedule shall be assigned to each access type in each Controller, thereby allowing different access authorizations for each door for the defined categories of people.
- There shall be 299 schedules available.
- One schedule shall allow definition of three authorized timeframes per day, for all days of the week including holidays. These timeframes shall be configurable in the software at any time; they shall be definable minute-by-minute.
- 36 holidays shall be programmable.

This principle enables flexible and easy management of access authorizations and does not require individual reprogramming for each card in the event of changes in the organization.



Access authorization groups

Different access authorizations may be grouped into “access authorization groups” to simplify enrollment and management.

An access authorization group may contain an unlimited number of access authorizations.

Each card can be assigned an individual selection of access authorizations or a group of access authorizations.

Access authorization

All of the parameters that make it possible to define the programming of a card will be sorted into “access authorization groups”.

An “access authorization” covers the following parameters:

- A Controller group
- One type of access
- The use of a PIN (personal identification number)
- Triggering automatic commands when the card is presented (for instance, triggering an additional relay on the controller)
- The authority to send commands from the keypad
- The validity starting date and time
- The validity expiration date and time
- A selection of access days

Each card can have an unlimited number of access authorizations.

Thus, it shall be possible to schedule different starting and expiration validity dates and times for the card, for different installation areas.

Similarly, different and very specific authorizations and behaviors for different areas of the installation shall be programmable.

This key function in the software enables, among others, provisional planning of the authorizations and provisional management of the irregularities, as well as changes in the allocation of personnel.

Additional functions

A “highly privileged” (VIP) type of access shall make it possible to associated permanent access (24 hours / 7 day a week) to a card for all doors or areas of authorized geographical access.

A Controller can be deactivated thereby restricting access, even for “highly privileged” cards, and deactivating all logical entries and exits.



Multi-card support per person

Each person may receive up to four cards (with or without PIN [personal identification number]) and one unique PIN code. Each of these cards and codes shall have its own access authorizations.

This broadens the range of card technologies that may be assigned to and used by single person (vehicle tag and card, proximity card and barcode card, etc.). It also allows to easily manage cases where people forgot or temporarily lost their cards.

These cards must be able to be verified simultaneously or individually.

(**Delete screen image if spec needs to be generic)

The screenshot shows a software window titled 'Persons' with a menu bar (Window, Edit, Search, Options) and a toolbar. The main content is divided into several sections:

- Personal info:** Fields for Name (Mr, John), First name (Smith), Reference number (46DEA3AE), Language (English), and Badge layout (RISCO). There is a small image of a clown. Identification numbers 1 through 5 are listed, with the first one set to 10.
- Valid from/Valid until:** Date and time selection fields.
- Cards and code:** A table with columns for Card, Code, Access authorization, Status, and Level. It lists four cards, each with a checkbox, a code field, an authorization dropdown (set to '<<<< SELECT >>>>'), an 'and' button, a 'Select' button, a 'Status' dropdown (set to 'Activated'), and a 'Level' dropdown (set to 'Only'). There is also a 'Code only' field and a 'Bypass position antipassback' checkbox.
- Access authorization for a visitor:** A dropdown menu set to '0' and a 'Reception site' dropdown.
- Authorized access time slots:** Fields for 'Presence board' (set to 0), 'Last' (set to 'Other'), 'The' (date dropdown), 'Zone' (set to 0), and an 'Options' button.

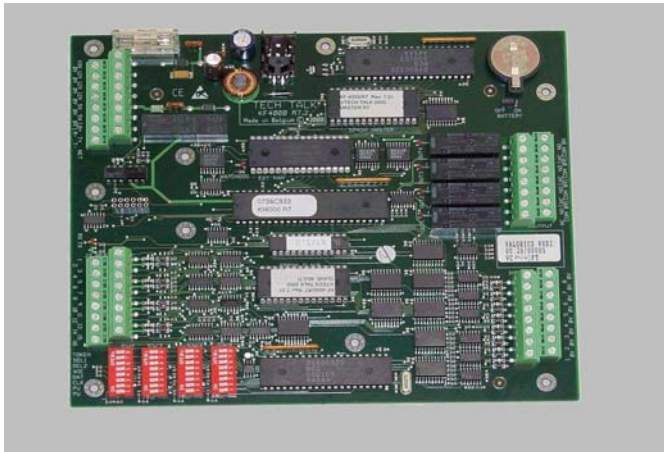
Moreover, it must be possible to refer to recent events linked to a person in the persons screen.



3. Hardware

Access Controller

Access Controller (**KF-R7 – delete product name and photo if spec needs to be generic)



Access Controller - Main Capabilities

Management and control

- ✓ 1 to 4 doors
- ✓ 1 to 2 turnstiles
- ✓ 4 relays, 4 readers and 8 inputs
- ✓ Memory: 22,000 people / 2,500 events
- ✓ Performance monitoring and alert

Communication

- ✓ 4800 & 9600 bauds (Keyfree)
- ✓ TCP/IP (option)
- ✓ RS232 (option)
- ✓ WiFi (option)

Security

- ✓ Detecting when switching to backup battery operation
- ✓ Detecting low backup battery power
- ✓ Detecting low lithium battery power

The Access Controller (**KF-R7 – delete product name if spec needs to be generic) shall ensure control over one or two accesses (reader + keypad at entry or at entry/exit) or four entry accesses. The Controller shall be CE marked.

The Controller's main operational features shall be:

- The capacity to handle and process 22,000 cards*
- A buffer memory which can retain the last 2,500 transactions: authorized accesses, denied accesses, alerts, etc.
- Stand-alone logical operation (the Controller does not interrogate any concentrator or PC for access authorization, except in specific cases).
- The possibility to function in a centralized mode (a specific mode in which management software generates an exception to the access authorization, for doubtful situations, etc.)
- The possibility to connect different reader technologies to the same Controller (proximity and barcode, for example).

** NOTE: the number of people retained by the Controller may be reduced when very specific software functions are used. (**Please contact RISCO Group for more information).*



- Scheduling capacity according to the following breakdown:
 - 14 access profiles (access types)
 - One reader schedule
 - One schedule for free access
 - One schedule for free exit
 - One schedule for conditional contact
 - One schedule for the use of PIN (personal identification number)
 - One schedule for the use of the logical position (anti-passback)
 - One schedule for activation per entry
 - Three timeframes per day
 - 36 holidays
- Configurable inputs:
 - For free access, subject to an individual activation schedule
 - For free exit, subject to an individual activation schedule
 - For controlling the status of the door (open, closed, open too long, etc.)
 - For managing locks or barriers (conditional sensors or inputs allowing, for instance, opening of a gate only if a car is present) subject to an individual activation schedule
 - Additional entrances whose use is subject to an individual activation schedule (one schedule per entry)
- Option to display of the status of the entries on an intelligent synoptic chart
- Configurable outputs:
 - Door activation relay
 - Specific alarm relay
 - Ancillary command relay (configured as an exit relay in the case of reader module for a directional barrier)
 - Individual relay configuration
 - LED status display of the relays
- Remote-controlled operation of the relay via software
- Managing a door alarm: door open too long, door not opened following presentation of a valid card, door forced open
- The possibility of connecting a keypad to use PIN codes
 - The use of PIN codes can be imposed individually (on a card-by-card basis)
 - The use of PIN codes can be imposed on a reader by reader basis
 - The use of PIN codes can be subject to an individual usage schedule (on a reader by reader basis)
 - The use of the PIN code can be imposed for single direction monitored access only (entry or exit)
 - The card can be invalidated for after the introduction of three wrong PIN numbers (card + code)



- The possibility of triggering automatic functions by activating the relay with the use of PIN code and card
- The possibility of activating a logical control of geographical position (anti-passback) for 199 area zones, subject to an individual activation schedule (on a reader by reader basis)
- The possibility of activating an anti-timeback functionality (on a reader by reader basis). This prevents a badge to be re-presented within a specified time on the reader.
- The possibility of using a coerced code without changing the number of keypad keystrokes used.
- The possibility of activating the Controller's command relay from an optional keypad to which it is connected
 - An individual authorization for using these commands can be selected (per card and per reader)
- The possibility of disabling an access (halt / resume free access)
- Possibility of selecting the types of events to be stored, per door
- Saving events in case of power failure
- Real-time clock
- LED watchdog for the electronic components
- A network loop bypass relay making it possible to isolate the Controller from the communication loop in the case of power failure, etc.
- TTL inputs configured as NO/NC
- Detecting 220VAC power failure and switching to backup battery operation
- Detecting low backup battery power
- Detecting low lithium battery power (RAM protection)



Input/Output Controller

The Input/Output Controller (**KF-24/24 Input/Output – Delete product name if spec needs to be generic) shall be an electronic remote control and acquisition unit with 24 inputs / 24 relay outputs, operating in accordance with the principle of distributed intelligence. The Controller shall be CE marked.

The Controller's main operational features shall be:

- 24 configured inputs:
 - Protected TTL inputs configured as NO/NC
 - Subject to an individually activated schedule (on an input by input)
 - Able to launch one or several of the Controller's 24 output relays.
 - Alarm point groups can be configured to activate / disconnect automatically or manually
 - The groups may trigger relays on specific Controllers (sounder, transmitter, etc.) even when not communicating with the server
 - The groups may be controlled via key contacts
- 24 configured outputs (relays with 250V 8A power):
 - Individual configuration of the relays
 - LED status display of the relays
 - Buffer memory retaining the last 1,500 events
 - Remote-controlled operation of the relay via software
 - Relays configured as NO/NC

The connection blocks of the Input/Output Controller shall be "unpluggable" in order to simplify maintenance.



Lift Controller

The access control system shall also make it possible to manage lifts (elevators), and shall operate in accordance with the principle of distributed intelligence.

The Lift Controller (**KF-Lift - delete product name if spec needs to be generic) shall be capable of managing a minimum of 12 floors.

A larger number of floors shall be manageable by installing additional Lift Controllers in series.

The Controllers shall be CE marked.

Following are the main operational features:

- Stand-alone operation (the Controller does not interrogate a concentrator or a PC for access authorization, except in specific cases).
- Floor-by-floor control
 - Each floor is considered as a door
 - A name is assigned to each floor in the software
- Ability to adapt to different types of lifts by using four operating modes
- 16 available schedules:
 - One schedule per floor for free access
 - One reader schedule
 - 14 types of access schedules per floor
- The possibility to track floors selected by a person (modes 1, 2 and 3 only)
- Automatic bypass function (mode 1 only)
 - In case a breakdown is detected
 - In case of a power failure
 - In case a specific input is closed
- Each floor appears in the software by name
- Priority mode
- A technical failure output (absence of 12V or current failure)

Note:

In order to be able to install the Controller in the equipment room, and the reader in the lift cubicle, reader distance extension modules shall be used (**KF Far – HD Far - delete product names if spec needs to be generic)



Network communication description

Cabling architecture:

All of the following solutions shall be possible within a single installation.

- Cabled link (bus with RS-232 or USB link)
- Ethernet link addressing TCP/IP 10/100 Mbits
- Optical fiber link
- Specialized lines
- WiFi
- PSTN link

Communication of the Controllers with each other and with the PC shall be accomplished by a double current loop. This method is highly protected against external interference and enables, for example, proper operation of the system in lifts or in zones with strong electrical or electromagnetic interferences.

The cable between the various Controllers shall be a two-pair cable. Should a Controller network be created, it is recommended to use a 9/10th notched cable. The communication network is opto-coupled.

The distance between two Controllers shall be up to 600m on a 9/10th copper cable, where each Controller restores the signal. This distance may be increased to +/- 5 km by adding modem line drivers

Should any Controllers fail or encounter a power failure, an automatic bypass system in each Controller shall remove this Controller from the loop and allows the communication loop to remain operational.

Once such a Controller returns to normal operation, the same system shall automatically enable re-integration of the Controller into the communication loop.

To ensure a high level of security when managing communication with the Controllers connected to an Ethernet TCP/IP network, it shall possible to encrypt this communication (3-DES encryption).

Communication Dispatcher

The solution shall include communication dispatchers for providing the following functionality:

- Enabling Star cabling architecture
- Providing LED display of the communication status with each Controller connected
- Enabling quick identification of any defective Controller in case of failure and allowing to manually isolate (via a simple switch on the dispatcher) one or several Controllers from the network
- Enabling gradual setting up of the installation should this be necessary



Reader technologies

The access control system shall enable use of the following different means for identification:

- Identification by card:
 - Magnetic readers
 - Contact-less readers (Wiegand)
 - Read/write readers (Mifare, i-Class, Legic)
 - Infrared (barcode) readers
 - Hyper frequency readers
 - Remote radio control readers
- Biometric Identification
 - Hand
 - Fingerprint (integration of the Sagem biometric module within the access control software: enrollment in a single software)
 - Eye (iris)

All these identification means may be combined in the same installation.

Insertion readers

Insertion readers may also be integrated into the system.

The following functions shall be configurable with regard to an insertion reader, taking the parking exit as an example:

- After insertion of an “employee” card, returning the card and opening the barrier
- After insertion of a “visitor” card, keeping the card and opening the barrier



4. Description of the Software Modules

Access control module

Environment

The access control software module (**MaxiTalk – delete name if spec needs to be generic) shall be flexible and user-friendly, written in an advanced language (C and C++).

The database used shall be a standard one, and not exclusively that of the software's creator.

The availability of an ODBC access to the database shall expose it to external databases and tools via ODBC links. These links open up potential opportunities for dynamic compatibility between the integrated Keyfree system software and the client's internal databases and tools, without going through the process of exporting the data.

Several languages shall be available (multilingual software):

- French, English, Dutch, German, Italian (**For additional languages: please contact RISCO Group for further information).

The software shall be available for Windows 2000, 2003 and XP for single-user, multi-user and client/server configurations.

(**Please consult RISCO Group regarding for PC requirements, as they depend on the size and functionality of the installation).

Functions of access control software module

The basic function of the software shall be to offer a user-friendly interface in order to be able to program the system, as well as to manage the events.

The access control software shall enable:

- Loading the data into the Controller intelligent synoptic and presence charts or panels.
- Sending PC commands to the Controller (unlocking, etc.).
- Managing the different types of communication.
- Retrieving data from the Controller using the PC (events, alerts, etc.).
- Optimizing the rate of communication for the start-up phase
- Setting the date and time of the installation and automatic changing of summer and winter time.
- Managing card status:
 - Active
 - Inactive
 - Lost
 - Stolen
 - Returned
 - Out of service
 - Not returned



- Managing access:
 - Per Controller
 - Per reader groups
 - Per person
 - Per groups of people
 - Using cards and/or PIN codes
 - Etc.
- Programming up to 4 access cards and one access code for each person
 - Each of these cards or codes has its own access authorization
 - Each card or code may be verified simultaneously or individually.
 - Each card can be for different identification technologies
- The definition of access authorization consists of the following parameters:
 - One reader group
 - One access type
 - The use of a PIN code
 - Launching automatic commands
 - The authorization to execute commands from the keypads
 - Date and time for the beginning of the validity
 - Date and time for the expiration of the validity
 - A selection of access days
- The definition of access authorization groups to simplify card management
- The definition of zones enabling logical control of geographical position.
- Managing schedules (up to 3 cycles per day) in which the following are selected:
 - The schedules used for the configuration
 - The schedules used for the deferred and the automatic processes (for instance, printing the list of people on-site every Monday morning at 9:00 AM)
 - Each reader's individual schedule:
 - Access schedules for the access types
 - Free access schedule
 - Free exit schedule
 - Schedule for using the PIN codes
 - Schedule for activating anti-passback
 - Schedules for activating the sensors
 - Etc.
- Up to 36 holidays
- Event management and monitoring:
 - Intrusion alarms
 - Open door alarms
 - Technical alarms
 - Etc.



- Selecting events to be stored
- Relay commands
- Defining the connection between card presentation and commands
- The authorization to activate/deactivate other systems (authorization on a card-by-card basis) by using the auxiliary command relay
- Direct enrollment by card reader (option)
- Storing and retrieving encoded data
- Generating lists :
 - Lists of events (by type, by timeframe, by person, etc.)
 - In alphabetic order
 - In chronological order
 - For a period freely determined by the user
 - Lists of people
 - In alphabetic order
 - By card number
 - By reader group
 - By access type
 - Etc.
 - All the printed reports can use filters that make it possible to select the components to be printed, based upon a variety of selection criteria
 - The possibility to export reports in Microsoft Word and Microsoft Excel format as well as in HTML format.
- Managing user and passwords
 - Accessing the session by user name + case sensitive password
 - Five password levels
 - An unlimited number of passwords
 - Display the previous use of the software (user log file)
 - Display the list of users currently using the software
 - LDAP (Lightweight Directory Access Protocol) authentication
- Administrative breakdown of the database
 - Five personalized levels (departments, services, etc.)
 - An unlimited number of categories for each level
- The configuration of a description of the personnel in 50 customized fields

The principle of distributed intelligence makes it possible to use this software on a non-dedicated PC (A PC that is used for other tasks and not always on site).



Advanced access control functions

Logical control of position

The system shall enable an anti-passback (logical control of position) function to be initiated:

- For certain accesses
- For a section of the user population (for example, the option to deactivate anti-passback for security personnel or the General Manager).

The anti-passback function shall verify the logical position of a card for all those zones in which it is activated, and shall prevent use of a card to enter or exit a zone where logically it should not be, or use of the same card by two people to enter or exit.

The anti-passback function shall be programmable by the access control software which defines the different zones (up to 199 configurable zones per user) as well as the Controllers which are not taken into account for this function. It shall be possible to define a usage schedule to determine, Controller by Controller, the periods during which the anti-passback function will be active.

A timed anti-passback function (enabled on each reader independently) shall also be available (enabling to deny access to a card presented twice within a configurable period of time).

“Confirmation” cards

This function shall enable verifying and authorizing the passage of a person "requiring confirmation" by presenting a "confirmation" card.

For example, this function is used to authorize visitor access to sensitive areas in the building, ensuring that someone accompanies them.

Access to sensitive areas using multiple cards (Multi-card access)

Multi-card access shall consist of defining that the passage through an access requires presentation of up to 10 cards, and by defining the maximum time between presentation of each card.

This function is used, for example, to ensure the presence of two people when accessing a sensitive room.

Multi-site management

The system shall include an advanced Multi-site management function regarding the user passwords, that enables multi-site management of access control systems, alarms and visitor management and includes:

- User rights based upon a password
- A multi-criteria filter can be attributed to each user
- Filtering criteria using any combination of:
 - The password levels
 - The people
 - The readers
 - The reader and access authorization groups.
 - Geographical zones



Graphic monitoring module

A Graphic monitoring module (**MaxiMon – delete name if spec is generic) shall enable display of all or selected events with customized graphic monitoring:

- By color (Windows Palette)
- The possibility to affix a photo to an event card
- The possibility to configure the maximum number of events to avoid displaying too much detail, and to place the monitoring option in “pause” mode.

Access to the software shall be by customized password, with the option of defining multiple environments (filtering events, selecting colors, the origin of the alarm points, monitoring a selected population, etc.)

Macro-instructions language

The system shall include a macro-instructions language, intended for advanced users to enable creating a macro-instructions library to program actions and reactions in different components of the integrated system.

Macro-instructions shall enable to adapt the system to installation specifications and to adapt and simplify the user interface of the operators, without software engineering intervention.

It shall be possible to trigger the macro-instructions automatically upon receipt of an event, or manually from a management PC.



Technical monitoring of the software

When the installation consists of several management PC's, the system administrator must be kept informed of any technical problems throughout the installation.

It shall be possible to monitor the proper operation of each software program and generate error messages in case of failures (hardware and software monitoring).

The error messages shall be displayed on the management PC's, if required.

It shall also be possible to program the automatic sending of an email message when an internal technical problem is detected in the system.

An application that makes it possible to monitor all communications from a remote station shall also be available with the possibility, for example, to monitor and manage the communications between the controllers and the server remotely from a PC located in the IT department.

Managing event logs in the database

The software shall include the possibility to manage event logs; to decide which events will be logged and where they will be located in a "syslog" database.

The types of logs shall be: urgent, alarm, critical, error, warning, notification, information and debug. The first seven log types are standard and used by the syslog protocol on all the larger servers (AIX, UNIX, Linux, Windows). The latter type, bug, shall be used internally by the access control manufacturer.

Crisis Management

In order to be able to rapidly modify the access authorizations in the event of a crisis (strike, demonstration, terror attack, etc.) crisis level management will be integrated into the access control software, thereby allowing the authorized person on site to change personnel access parameters.

The five-level crisis management shall meet requirements of DEFCON, ISPS, Vigipirate standards.



Additional software modules

The following additional software modules shall be integrated to simplify project implementation:

- ASCII import/export module
- Management of people present in areas (people count)
- Deferred processing module (automation of reports, purges, backups, etc.)
 - Possibility to define a number of alerts and a number of events online
 - Possibility to define the number of days online
- Interactive access control module used when video verification for doubtful situations is required. It can be directly interfaced with the PC or using the output of a Video matrix. The operator may view a live video of a person presenting his card, together with a database image and the personal information linked to the card presented.
- Internet/Intranet server module. This module enables Web access for visit planning and macro-trigger (using Maxiweb) and card and person management using Maxi.Net

Filters criteria / Report generation

The software shall enable creating filters and generating reports according to the following specific criteria:

- Name
- Card
- Controller
- Controller group
- Access type
- Type of events
- Date or period
- Five additional criteria that are opened in a multi-criteria selection process

These different criteria may be combined, or processing libraries created and carried out automatically (using the deferred processing module) or manually by the operator.

Printing may be performed continuously, with or without sorting criteria, on any printer (networked on local) as long as a Windows printer driver is available.



Visitor management module

Visitor management software (**MaxVisit – delete name if spec needs to be generic) that uses same database as the access control module shall be available.

This visitor management software shall make it possible to assign access authorizations (using predefined profiles) to visitors. It also enables to assign authorization based on a predefined access profile associated to the host being visited.

Each visitor can be assigned a card with access authorizations based upon:

- A reader or group of readers
- An access type
- A start and/or expiration date and time

(**delete screen if spec needs to be generic)

Advanced functionality of the visitor management software:

- Multi-site management of visitors (visitors are received at the reception center at X or Y location)
- Unwanted visitors: the screen shall become red if the designated visitor appears on the list of excluded persons (unwanted visitors).
- Printing cards sequentially and automatically in alphabetical order (for printing cards for a meeting, a conference, etc.)
- The visitor management module shall be able to list all scheduled visits in chronological order, in which visitor names are in random order or in chronological order to select a visitor.
- Possibility to detect who added or modified a scheduled visit and when was this done
- Possibility to automatically or manually send an email with the visit details to the host person alerting him/her of the visit.



Pre-visit management via Intranet

A pre-visit management module, available via Intranet at all the office PC terminals, shall make it possible to introduce a future visit into the visitor management database. It shall also allow to query the database for ongoing and future visits.

The module shall enable inserting scheduled visits via an HTML page that can be accessed from a browser.

The inserted data are, on the one hand, shall be the host's name and password which has to be verified on the Intranet, and on the other hand, the information regarding the visitor (name, surname, company, scheduled arrival and departure dates and times).

This will enable the receptionist to permanently access the list of expected visitors and prepare their cards, if needed.

The data will be verified and automatically transferred to the Access Control visitor database by the Access Control HTTP server.

Standard HTML pages shall be included in the module. It shall also be possible to customize the pages to include, for instance, company logo or other customer specific data if needed.

Card personalization module

The solution shall include a card-personalization module (**MaxImage – delete name if spec needs to be generic) that enables:

- Video camera capture
- Digital storage of photos
- Printing of cards

The database shall be shared with the Access Control module (**MaxiTalk – delete name if spec needs to be generic) ; the data shall be entered only once.

The package shall enable to use existing photo files in BMP or JPG format and re-using the current photo material if compatible. (This shall be confirmed after analysis of the technical documentation, drivers, etc.)

A 160*200 pixel format shall be used for the personnel file (conversion to this format is not included, in case current photos need to be used).

The system can also acquire a signature (in addition to a photo) to be printed on the card.



External database interfaces

The system shall provide an integrated solution for managing access, timetables, alerts, card personalization and visitors, by using a single central database and allowing use of many different card technologies.

Several standard interfaces in the application shall make it possible to add, change and delete records in the system's database, using external applications:

1- *ASCII files interface*

This interface shall enable the access control applications to import and export data in ASCII format (one line per record), one file shall contain all records to import.

This interface allows importing personal information (name, title, department, etc.) but does not enable real-time validation of cards on the Controllers.

2- *ACC interface: ASCII files interface*

ACC is an ASCII file, one file per person, describing the identity of the person and his/her access authorizations. The ACC interface specification is available upon request.

This interface shall function in real time.

Once the file(s) have been placed in the specified directory (the directory location can be configured), the information will be dealt with in real-time, import will be performed and card validation on the Controllers will also be done automatically.

This interface shall enable to verify information by using the access control parameters (i.e., start and expiration dates for the verification, Controller groups, time periods, etc.)

Note: It shall be possible to generate the ACC files directly in the specified directory, or to generate them elsewhere and transfer them to the specified directory using FTP.

3- *General interface*

A general interface shall enable communication with the software application using TCP/IP or RS232 interface. It shall enable to output Access Control events to external customer applications in real-time using a predefined protocol. The General Interface protocol definition is available upon request.

4 - *ODBC link*

The software application shall be accessible via an ODBC link, which shall enable, for example, to display the table content in Excel or adding a record from an external application