INTEGRATED
ACCESS CONTROL and INTRUDER ALARM SYSTEM SPECIFICATION

Agriculture and Agri-Food Canada

107 Science Place
Saskatoon, Saskatchewan
S7N 0X2

Contents

1 Functional Overview

1.1 The system shall provide comprehensive access control and intruder alarm functionality; allowing multi-site configuration able to be managed by one or more of the connected sites.

1.2 The system shall provide a means to control access through nominated doors having electric locking door status monitoring and token or biometric access control readers. Access rights associated with a presented access token or biometric identifier shall be checked for validity based on token or identifier, access area, access time and any other access management function defined in this specification; as stored in intelligent field controllers. Access shall be granted or denied, dependant on the access privilege. Access rights shall be programmed in a variety of ways to allow flexibility as defined elsewhere in this specification.

1.3 The system shall provide access control in elevators enabling access to any combination of floors over specified time periods. The interface to the elevator manufacturer's equipment shall be by either low level interface (relay outputs) or by a high level (data) interface.

1.4 The system shall monitor the condition of inputs. The system shall be able to be programmed to apply a variety of conditions to the way in which these inputs are monitored and shall enunciate the condition of such inputs in accordance with such programming.

1.5 The system shall provide a fully functional intruder alarm system including entry and exit delays where intruder detection sensors are connected to system inputs. The Intruder Alarm Systems component shall be fully integrated with the Access Control aspects of the system. It shall be possible to set (secure) or unset (unsecure) areas from any access control reader associated with an area, access control reader with keypad, Remote Arming Terminal, or as required from defined central control locations.

1.6 The system shall provide an integrated software facility for the design and production of photo ID cards.

1.7 The system shall be OPC (Alarms and Events) and OPC (Data Access) enabled using Microsoft COM and DCOM enabling integration of event data with other third party OPC enabled automation and business systems.

1.8 4.8 The system shall allow data exchange with other applications using XML protocols for schedule changes, and card record changes.

1.9 All system communications must be totally integrated with either existing or new LAN/WAN networks. Tenderers must make themselves familiar with the specific requirements for this project.

1.10 Connection to Intelligent Field Controllers (IFCs) shall be achieved using cabling supporting Ethernet and TCP/IP protocols. The network connection must be on-board the IFC. Interface transceiver units (Ethernet to RS485, RS232 etc) are not acceptable.

1.11 Remote IFCs not permanently connected to the network can be connected via a PSTN service, using TCP/IP protocols.

(a) Connection from the remote IFC to the server shall be either via dialup to an Internet Service Provider (ISP) using encrypted TCP/IP; and then via an approved firewall through into the IT environment or via dialup directly to a RAS connection on the Server.

1.12 All system software upgrades shall be downloadable through the network to the IFC.

1.13 All data communication internal to the system on the TCP/IP network between IFC?s and between IFC?s and the Server shall be encrypted using symmetrical session keys and an industry-standard encryption algorithm to a minimum of 128 bit AES. Session keys shall be changed on a regular basis at intervals no longer than 24 hours.

1.14 Communication authentication shall use 1024 bit RSA keys.

1.15 The system shall report all events to the operator(s) as configured and shall produce and maintain a log of all system events, alarms and operator actions.

1.16 The system shall provide a means for an operator to extract information relative to the event log and system configuration and produce this information in the form of printed reports, screen displays or ASCII files.

1.17 The system shall provide for a Windows based User Interface with Site Plans and interactive icons representing the location and real-time status of Access Control, and Alarm Monitoring equipment.

1.18 The system shall provide emergency evacuation reporting.

1.19 The system shall be designed and manufactured by a reputable company who shall be certified under the ISO 9001:2000 quality procedures.

1.20 All equipment shall have the following approvals:

(a) FCC Part 15

(b) CE approval BS EN 50130-4 Alarm Systems Electromagnetic Compatibility (Immunity)

(c) CE approval BS EN 55022 Emissions

(d) UL294 Access control

(e) UL1076 Burglar Alarms

(f) CSA C22.2 No. 205

(g) ULC-ORD-C1076

1.21 Encoders and readers shall also meet:

(a) CE ETS 300 683 Short Range Devices

(b) C-Tick AS/NZS 4251 Generic Emission Standard

(c) C-Tick RFS29

1.22 The system software shall be written in a fully structured, fully validated and commercially available language that provides a strictly controlled development environment.

1.23 The user interface for operational management of site security shall be developed using Microsoft .net and Windows Presentation Foundation (WPF) development tools.

1.24 Comprehensive backup and archiving facilities shall be incorporated as an integral part of the system software.

1.25 The system shall include system divisioning suitable for multi-tenanted buildings. Operators shall only be able to access those parts of the system which fall within their division and operator privileges.

1.26 IFC's must support peer to peer communications for input and output communications between IFC's. Systems that require the main server for communications between panels are unacceptable.

2 System Servers and Workstation Hardware

2.1 The server and workstation equipment will be supplied by the facility to the following requirements.

2.2 The server installation shall support 64 bit operating system.

2.3 The operating system used by the system server shall be either:

(a) Microsoft Windows 2008 Server.

(b) Microsoft Windows 2008 Server R2 (64 bit only)

(c) Microsoft Windows 7 Professional/Ultimate

2.4 The operating system used by workstations shall be Microsoft Windows 7 Professional/Ultimate

2.5 A Microsoft SQL Server shall be used as the database engine for the system. The system server shall be either:

(a) Microsoft SQL2005, 2008,2008R2 or 2012 Server.

(b) Microsoft SQL 2005,2008 or 2012 Express Edition

2.6 Workstations shall support multi-monitor operation, allowing an operator to set up one or more monitors for each workstation.

2.7 Where a workstation is configured for a lower resolution, dragging the view onto a higher resolution monitor shall cause the view to resize, taking advantage of the higher resolution.

2.8 Manual Deployment using installation media shall also be supported.

2.9 It shall be possible for an operator to run a workstation solely from files stored on and run from a USB memory device and without requiring any pre-installation of software on the PC.

3 System requirements

3.1 The system shall be in commercial operation with the same or similar configuration as detailed in this specification and shall be available for inspection. A reference list of such similarly configured systems and details of contact persons shall be submitted with the tender response.

3.2 The system described in this specification must have the following capacity as a minimum:

(a)	Graphical Site Plans	Unlimited
(b)	Access Readers	Unlimited
(c)	Elevators	100 elevators each with up to 75 levels
(d)	Fully Supervised 4 state Alarm Inputs	Unlimited
(e)	Output relays	Unlimited
(f)	Access Control Zones	Unlimited
(g)	Schedules per day	100
(h)	Schedule categories	50
(i)	Holiday days	30
(j)	Operators	Unlimited
(k)	Concurrent Operator Sessions	Unlimited
(l)	Cardholders	Unlimited
(m)	Cardholder Issue Levels	15
(n)	Cardholder Personal Data Fields	64

3.3 The system architecture shall be a tiered system consisting of:

(a) One or more installations of the head-end software application operating on computer servers and operator workstations;

(b) Intelligent Field Controllers (IFC's) managing the system in a distributed intelligence format;

(c) Semi-intelligent subunits (outputs, inputs, readers, etc) which rely on IFC's to function.

4 Central Control and System Management Software

4.1 The system shall use the Microsoft Windows© operating system as defined previously. The version of Microsoft Windows shall be a currently supported version.

4.2 The system database shall be a version of Microsoft SQL Server appropriate for the system size required. The version of Microsoft SQL Server shall be a currently supported version as defined previously.

4.3 The system shall be OPC enabled in accordance with the current OPC specification for OPC (Alarms and Events) and OPC (Data Access).

4.4 The central server shall employ a high quality personal or server computer incorporating current generation design and components. It shall be of a Microsoft approved model for operation with current versions of Microsoft Windows operating systems. The PC specifications, including processor speed, internal memory and hard disk size shall be specified by the supplier and must be sufficient to meet or exceed the specified system requirements.

4.5 The system shall be capable of supporting a minimum of 20 PC based operator workstations simultaneously running. Operator workstations running terminal emulation software will not be accepted.

4.6 The system shall automatically log and time/date-stamp all events within the system including intruder alarm set/unset events, access control events, operator actions and activity.

4.7 The central control software shall be easy to use, make extensive use of menus and windows and require a minimum of operator training to operate the system proficiently. Systems requiring a program language approach to configure the system will not be accepted.

4.8 The central control must be capable of receiving simultaneous alarm signals from a number of remote locations, without loss or excessive delay in their presentation to the operator. Any authorised operator should be allowed to acknowledge, view and/or process an alarm from any screen.

4.9 The central control shall be fitted with a real time clock, the accuracy of which shall be preserved over the period of main power supply failure. Synchronisation between the central control and Ethernet connected IFCs shall be automatic, not requiring operator intervention.

4.10 Operator selection of processing tasks shall be via menu selections. Authorised Operators shall be able to process alarms, produce reports and modify database records without degrading system performance.

4.11 The following is the minimum operational and monitoring facilities required. The ability to:

(a) Program either a group or individual card readers with access control parameters, without affecting other card readers.

(b) Program the access criteria for individual Cardholders or groups of Cardholders.

(c) Store at least 64 non-access control data fields for each cardholder. The names of these “Personal Data” fields shall be user definable.

(d) Authorise or de-authorise a Cardholder in the system with the result reflected immediately throughout all readers in the system.

(e) Enable a “Card Trace” against selected Cardholders so that an alarm is raised each and every time that cardholder presents their access card or token.

(f) Pre-program holidays so that different access criteria apply compared to normal working days. The system must have a capacity to set at least 30 holiday days.

(g) Recognise and manage regional holiday requirements

(h) Define as many access zones as there are card readers fitted.

(i) Allow or disallow individual Cardholder access to any one, or group of card readers, in real time.

(j) Log all system and operator activity to hard disk as they occur.

(k) Program alarm response instructions into the system so that these are presented to the Operator when processing an alarm event.

(l) Enable an Operator to enter messages against alarm events.

(m) Override (temporarily) a Cardholder’s, or group of Cardholder’s, pre-programmed access criteria.

4.12 The central control shall display a one-line plain language event message for every activity event (alarm or otherwise) occurring in the system. All activity logged shall be time and date stamped to the nearest second (hh:mm:ss). On having the appropriate operator authorisation it shall be possible to drill down into the properties of each component that makes up that event for future details. The event message shall advise:

i. Time of event

ii. Action

iii. Successful or unsuccessful

iv. If the transaction is unsuccessful, the reasons for the denial.

(a) This includes but is not restricted to the following items:

i. All card attempts

ii. All door alarms

iii. All operator activity including log on, log off, alarm response messages and any alteration of system data files

iv. All alarm monitoring activations

v. All communications link failures.

4.13 Time schedules for different “day types” shall be configurable.

4.14 Regional holidays shall be configurable to allow for regional variations.

4.15 The system shall provide a detailed operator help file. This help file shall provide operators with text, audio and video help instructions and tutorials.

4.16 The system shall allow for searching of items configured within the system based on the following:

(a) Item characteristics

(b) Related items

(c) Times related to events including the item

5 Multiple Server Connectivity

5.1 Systems based on multiple servers installed at several locations shall be supported.

5.2 Alarms and events from all servers shall be able to be displayed on any or all of the system workstations.

5.3 The cardholder database shall be automatically replicated to all servers as a “global” entity.

5.4 Replication of cardholder changes shall occur as changes are made and not batch processed.

5.5 Communication between servers shall be peer to peer.

5.6 The multiple server environment shall allow for evacuation reports for each site on the multiple server system to be generated on one server, for one or more remote servers.

5.7 Operator views and access privileges shall follow the same rules across multiple servers as apply within a single server.

5.8 Security system items configured on existing servers shall automatically be recognised by any servers added to the multiple server group. Likewise system items configured on the server(s) being added shall be automatically recognised by the existing multiple server group.

5.9 Use of software interface modules, custom written, to connect servers into a multiple server configuration shall not be permitted.

5.10 Manual or script re-entry of data for existing servers into any new servers being added to the multiple server group shall not be permitted.

5.11 Synchronisation of data across all servers shall be automatic, real-time function not requiring operator intervention or initialising.

5.12 Should communication be lost between two or more servers, the individual servers shall continue to function independently and shall resynchronise all changes made whilst off line automatically.

5.13 Should a conflict occur resulting from two items being created in two or more servers whilst servers are off line then an alarm shall be raised when the servers are re-joined advising of the conflict.

5.14 Should an existing record be modified in two or more servers whilst the servers are off line then on reconnection, the modifications shall be carried out in time order of the modifications.

6 Graphical User Interface

6.1 Configuration Graphical User Interface

6.1.1 The system access shall be via a Graphical User Interface (GUI)

6.1.2 All functionality shall be managed via the GUI

6.1.3 Drop-down menus shall be provided to select all configuration functions.

6.1.4 System items (hardware items and software items) shall all have an associated properties menu to allow item configuration.

6.1.5 Configuration or operation using scripting or other forms of text-based programming will not be accepted.

6.2 Operator User Interface

6.2.1 In addition to the User Interface defined in 9.1above, the Operator User Interface shall be provided as follows:

(a) Full screen, user configurable Viewers, designed specifically for the task and the information needs of the operator.

(b) Default viewers shall be provided covering the primary site management functions of:

i. Alarm management

ii. Cardholder management

iii. Monitor Site

(c) The system shall allow customised viewers to be created.

(d) The Operator User Interface shall be fully configurable by an operator with authorisation to configure Viewers.

6.2.2 Each Viewer shall consist of a Navigation Area and a Panel Area, as detailed below.

(a) The navigation area shall provide a list of system information associated with the specific viewer.

i. It shall be possible to select and order the columns of data associated with alarm and cardholder viewers.

ii. Incremental searching shall be provided based on preselected data columns for cardholder viewers.

iii. Selection of a line item in the navigation area shall cause the associated tile data to be populated.

iv. Alarm Viewer headers shall display the number of unprocessed alarms for each alarm.

(b) One or more data Tiles shall be provided to display detailed data associated with the navigation area item selected.

i. Tiles shall be able to be created based on a range of default Tiles provided for this purpose.

ii. Each tile shall be configurable with the required data fields as determined by the tile's function.

iii. Tiles shall be maximised by single click operation.

iv. When a Tile has been maximised, other Tiles shall remain visible in a film-strip format, allowing single click to restore them.

v. Where applicable, minimised tile icons shall display dynamic content.

7 Site Plans and Site Plan Icons

7.1 It shall be possible to manage and monitor alarms, overrides, the general status of site items and open doors through the Graphical User Interface with the use of interactive real time dynamic site plans and icons.

7.2 Site plan usage shall support touch-screen technology.

7.3 All site plans stored on the server PC shall be automatically updated if amended at any of the networked workstations.

7.4 External drawings shall be imported into the system from external drawing software.

7.4.1 The ability to import at least the following drawing formats shall be supported:

(a) BMP

(b) WMF, EMF

(c) JPG

(d) GIF

7.5 It shall be possible to assign icons to system functions and place these at any position on a site plan.

7.6 Provision for drawing lines and areas to form “objects” shall be available. These objects shall be able to be associated with system items allowing system item status to be visually indicated by the object.

7.7 It shall be possible to place free text onto a site plan.

7.8 Site plans shall be “nested” allowing a single action (mouse click on a current site plan icon) to move from one site plan to another.

7.9 The following functions should, as a minimum, be able to be executed by clicking on Site Plan icons:

(a) View the current status of a Door, Input or Output.

(b) Monitor and acknowledge an Alarm

(c) Open an access controlled door

(d) Move from one plan to another plan

(e) Activate an Intercom on a reader

(f) Override an alarm, access or perimeter fence zone state.

(g) Display the properties of the item.

7.10 Icon names shall user the item name by default but a short name shall be selectable if available.

7.11 The size of the Icons shall be scalable.

7.12 A pre-designed set of icons covering basic access control functions shall be provided.

7.13 It shall be possible to design and load icons from external software for use in the system.

7.14 It shall be possible to design macro buttons to reside on siteplans. On activation, macro buttons must be capable of performing multiple overrides for any site items simultaneously.

7.15 It shall be possible to click and drag over an area within a site plan or individually select items on a site plan in order to override their state in one action.

7.16 It shall be possible to search for, select and navigate through available site plans within a single window (tile) and to view, move backward or forward through the list of recently visited site plans.

8 Field Hardware

8.1 The IFC shall be the main controller in the field. The head-end application shall communicate directly with all IFC's in the system.

8.2 Each IFC shall be intelligent in that in the event of failure of power or communications to the central control, for whatever reason, the system shall continue to allow or deny access based on full security criteria.

8.3 The IFC shall store on-board all the security and access parameters to operate completely independently from the central control server. Systems that rely on the central control PC for access decisions will not be considered.

8.4 The IFC shall "concentrate" activity data and immediately transmit it to the central control server computer.

8.5 Should communications fail with the central control, each IFC shall be capable of buffering up to 80,000 events.

8.6 All events shall be time-stamped at the IFC at the time of occurrence.

8.7 The IFC shall transfer buffered events to the central control automatically when the communications link is re-established.

8.8 The IFC shall be capable of storing up to 500,000 card records with associated access criteria.

8.9 The ratio between stored events and stored cardholders shall be configurable for each IFC to allow site requirements to be configured in accordance with specific site needs (more cardholders or more events per IFC).

8.10 The system shall monitor input circuits and enunciate whether the circuit is in Normal, Alarm, Open Circuit Tampered or Short Circuit Tampered as separate conditions.

8.11 A configurable range of end of line resistor values shall be supported as a software function to support pre-existing input circuits when required.

8.12 The use of any circuits using other than dual 4k7 end-of-line resistors must be approved by the consultant.

8.13 The IFC shall include tamper protection for the front and the back of the panel. The front panel shall be tamper protected for door open, and the rear of the panel to detect if the panel has been removed from the wall. These shall use optical tamper detection. Mechanical tamper devices are not acceptable.

8.14 The IFC shall incorporate an ARM 9 processor with at least 256 Megabytes of non-volatile FLASH EEPROM. The IFC shall incorporate boot code in a protected sector of the flash memory. For software upgrades, all system software shall be downloaded from the central server over the network

8.15 The IFC shall support direct download via USB to allow local upgrade of the IFC.

8.15.1 The upgrade process shall only accept authenticated downloads via the USB port.

8.16 The IFC shall operate from a separate battery backed 13.6V DC supply.

8.17 The IFC shall continue to operate for at least 24 hours in the event of a mains supply failure.

8.18 The system shall be capable of automatically detecting and reporting a power failure, low battery and battery not connected.

8.19 IFCs shall automatically restart and resume processing following a power failure.

8.20 IFCs shall be fitted with "watchdog" hardware and software to provide automatic detection and restart should the processor lock up.

8.21 The IFC shall contain its own real time clock. The clock shall be synchronised with the central control's clock at least once per hour. The accuracy shall be such that the time difference between IFC's shall not vary more than 0.5 second at any time.

8.22 The IFC shall be allocated to a time zone appropriate to the IFC location.

8.23 The IFC shall have an on board Ethernet (TCP/IP) connection and driver for communications with the central control supporting 10BaseT and 100BaseT operation.

8.24 When specified, the IFC shall support 100/1000BaseT

8.25 When specified, the IFC shall be fitted with 2 Ethernet ports providing alternate communication capability.

8.26 The IFC shall be provided with a pre-configured IP address to allow off-line initial configuration via a web browser application.

8.27 The IFC shall support DNS (Domain Name Server) operation to obtain an IP address.

8.27.1 Should the primary DNS not be available, the IFC shall be able to automatically establish contact with a secondary or tertiary DNS.

8.28 Should excessive network broadcast traffic occur (resulting from a ping attack or similar), an alarm shall be generated.

8.29 All communications between the IFC and the system PC shall be encrypted TCP/IP using 256 bit AES. Communications shall be on-line and monitored for interruption.

8.30 The IFC shall include one RS 232 multi-communications port.

8.31 The IFC shall include one USB2.0 port.

8.32 The IFC shall support remote site dial-up.

8.33 Remote communication between the IFCs and the remote devices shall use the switched telephone network circuits.

8.33.1 Incoming connection shall be via an ISP service.

8.33.2 Outgoing connections via modems connected to the customer LAN are not permitted, however dial-out directly from the Server is allowed provided the modem is fixed to "non-answer" mode.

8.34 It shall be possible to view the IFC status and configuration for commissioning and diagnostic purposes without the use of the central server software or other proprietary software. This may be achieved by the use of conventional WEB based browser. In high security applications, it must be possible to disable this feature at the IFC.

8.35 The IFC shall support logic functionality by way of configurable Logic Blocks.

8.35.1 The IFC logic functionality shall be able to be run independent of the central control system being online.

8.35.2 The following items shall be useable as inputs to Logic Blocks:

(a) Physical Input states

(b) Output states (both physical and logical)

(c) Door states

(d) Other Logic Block states

8.35.3 Up to 10 Logic Block input items shall be configurable in "AND" or "OR" combinations to cause an output to operate. Up to 10 "AND" or "OR" rules shall be configurable for each item.

8.35.4 The Logic Block output shall be able to be configured as an internal (virtual) output.

8.35.5 The Logic Block output shall be able to be assigned to an external output.

8.35.6 The Logic Block output shall be able to be assigned as an input on one or more other logic blocks.

8.35.7 The Logic Block output timing shall be configurable to at least the following:

(a) Delay on

(b) Delay off

(c) Latched

(d) Pulse time

(e) Maximum on time

(f) Explicit

8.35.8 The IFC Logic Block output shall be able to trigger actions across multiple IFCs, independent of the central control system being online

8.36 A separate alarm message shall be transmitted to the central control for at least the following alarm conditions. The alarm message shall be displayed in plain language text.

(a) Tamper

(b) Tamper Return to Normal

(c) Unit Stopped Responding

(d) Card error

(e) Maintenance Warning

(f) Alarm Sector State Change

(g) User Set

(h) User Unset

(i) Card Trace

(j) Wrong PIN

(k) Access Denied

(l) Duress

(m) Zone Count Maximum

(n) Zone Count Minimum

(o) Door Open Too Long

(p) Forced Door

(q) Door Not locked

(r) Power Failure

(s) System Reboot.

(t) Intercom

8.37 The IFCs shall communicate with and control the following equipment:

(a) Token or biometric access readers

(b) Card access readers with PIN keypads

(c) Elevator access equipment

(d) Alarm monitoring Input/Output panels and equipment

(e) Alarm response equipment

8.38 Any failure of a token or biometric reader unit and its communications with the IFC shall be raised immediately as a high priority alarm and shall not cause the IFC or other associated hardware to stop working correctly.

8.39 The IFC shall communicate with remote devices (token and biometric readers, alarm equipment, elevator readers) using a fully encrypted data communications protocol. Unencrypted ASCII text or similar data transmissions are not acceptable.

8.40 All communications between the IFCs and the remote devices must be check-digit coded to protect data from manipulation during transmission.

8.41 All communications links between the IFCs and the remote devices shall be monitored such that an alarm is raised at the central control if the data being transmitted is corrupted or tampered with in any way.

8.42 Communication between IFC's and readers and other "downstream" devices shall support Generic Wiegand connections protocol, supporting up to 9999 bit Wiegand format:

8.42.1 Wiegand formats shall be configurable, allowing for:

(a) Number of bits

(b) Facility/site code bits

(c) Card number bits

(d) Parity bit configuration

8.43 Communication between IFC's and downstream devices shall support a high speed protocol of at least 1Mbit/second

8.43.1 The data Communication sessions between IFC's and devices shall use certificate exchange protocols using keys have a minimum strength of 256 bit elliptical encryption.

8.43.2 Data communication between IFC's and devices shall use a minimum of 128 bit AES encryption.

8.44 The high speed communication circuit shall support at least 20 individual devices on each circuit.

8.45 Each device connected to the circuit shall report its serial number to the IFC, for identification and assignment for a specific function.

8.46 Each IFC shall support up to 10 high speed communication protocol electrical circuits.

9 Access Control, Security Alarm And I/O Programming

9.1 The system shall provide complete flexibility and be capable of programming an unlimited combination of access control, security alarm and I/O parameters subject only to performance and memory limitations within the IFC.

9.2 For ease of programming Cardholders shall be grouped into access groups sharing the same access criteria.

9.3 Cardholders may be assigned with an extended door unlock time, as may be required by cardholders with a disability.

9.4 It shall be possible to assign an individual cardholder to an access group on a temporary basis with predetermined start and finish times.

9.4.1 During the period of temporary access, the cardholder shall have the rights of the group to which they have been assigned in addition to any permanent access rights they may have been assigned.

9.4.2 The access group property page shall display both permanent and temporary access members with the status of temporary members shown as:

(a) Pending (with the start and finish times)

(b) Active

(c) Expired

9.5 Any cardholder or access group in the system shall be able to be programmed to have access to any combination of controlled doors in the system with each period of access for each door controlled to within the nearest minute.

9.6 The IFC shall check entry based on ALL of the following criteria:

(a) Correct facility code

(b) Authorised card in database

(c) Correct issue number

(d) Authorised door / access zone

(e) Authorised time of day

(f) Valid card holder competencies (refer to Section 13)

(g) Correct PIN (If PIN entry is required)

(h) Double entry (anti-passback, anti-tailgating or escort modes).

9.7 Anti-passback mode shall be able to be configured in any of the following modes:

(a) Disallow second access to an area if a valid exit has not previously been registered and generate an alarm (hard anti-passback).

(b) Allow second access to an area if a valid exit has not previously been registered but generate an alarm (soft anti-passback).

(c) Exclude specific Access Groups from the rules defined in (a) and (b) above.

(d) Anti-passback rules shall be able to be reset by either:

i. Automatically after a preset period after valid entry.

ii. Automatically at a standard time each day

iii. Automatically on exit from site

iv. Manually as an over-ride.

(e) Must support Global Anti-passback allowing multiple access zones to be linked for the purpose of anti-passback, across multiple IFC devices utilising encrypted peer-to-peer communications.

(f) The IFC's shall not rely on the server for anti-passback operation. Global anti-passback shall work across multiple IFC?s, even should the server be off line.

9.8 Anti-tailgate mode shall be able to be configured in any of the following modes:

(a) Disallow exit from an area if a valid access has not previously been registered and generate an alarm (hard anti-tailgate).

(b) Allow exit from an area if a valid access has not previously been registered but generate an alarm (soft anti-tailgate).

(c) Exclude specific Access Groups from the rules defined in x.7(a) and x.(b).

(d) Anti-tailgate rules shall be able to be reset by either:

i. Automatically after a preset period after valid entry.

ii. Automatically at a standard time each day

iii. Manually as an over-ride.

(e) The IFC's shall not rely on the server for anti-tailgate operation. Global anti-anti-tailgate shall work across multiple IFC?s, even should the server be off line.

9.9 Every incorrect PIN attempt shall be notified at the central control as an alarm condition.

9.10 Each reader shall be capable of automatically switching the access mode at a door at different times of the day, based on control parameters received from the central control. The following access criteria modes are required:

(a) Free access Door is unlocked, no card entry required.

(b) Secure access Door is locked, a successful card attempt is required for valid entry. Door re-secures after access attempt.

(c) Secure + PIN access Door is locked, a successful card and correct PIN number attempt is required for valid entry. Door re-secures after access attempt.

(d) Override from reader Members of certain access groups shall be able to change the access and PINs mode of the door at certain times.

(e) Dual Authorisation Access is granted when two different but legitimate cards are presented within a given time frame.

(f) Escort A second card is required to be presented from a cardholder who is nominated in the "Escort Access Group".

(g) Shared PIN Number The system Operator determines what the PIN number will be and programs this into the system. Access is allowed through the door when the correct 4 digit PIN is pressed followed by the "Enter" key.

9.11 Cardholder access reporting to the central control and logging in the audit trail shall be configurable in two modes:

(a) Only when there has been a successful presentation of a valid access card or token AND the door open sensor has detected that the door has actually been opened.

(b) Whenever there has been a successful presentation of a valid access card irrespective of if the door has been opened.

9.12 Readers with integrated PIN pads, or fingerprint readers using identification, shall provide an "Entry under Duress" facility.

9.12.1 Duress shall be initiated by the cardholder either by the addition of a unique number to their PIN number, or by incrementing the last digit of their PIN number by one. Duress on fingerprint readers shall be initiated by the cardholder presenting their pre-enrolled duress finger.

9.12.2 There must be NO indication of a Duress entry at the reader.

9.12.3 A high priority "Duress Alarm" shall be displayed at the central operator station.

9.12.4 It must be possible to configure the system such that duress or other selected critical alarms pop to the front of the display, ensuring immediate operator attention. The existence of other incoming alarms shall be visible to the operator but must not interrupt their current task.

9.13 Zone counting shall be available to provide real-time counting of cardholders in access zones.

9.13.1 The result of the number of cardholders in the zone being outside of the specified range(s) shall generate an event or an alarm.

9.13.2 The minimum and maximum numbers of cardholders in a zone before an event is generated shall be configurable.

9.13.3 It shall be possible to set up a “grace time” in seconds to allow the zone count to be outside the minimum within the mid-range or outside the maximum number of cardholders, without generating an event.

9.13.4 It shall be possible to assign a specific message for each of the below minimum, mid-range or above maximum conditions.

9.13.5 It shall be possible to set up the system to prohibit one cardholder being allowed in a zone by:

(a) Requiring two valid but different cards to access a zone should the zone count reports zero cardholders in the zone;

(b) Requiring one card to access a zone should the zone count report two or more cards in the zone;

(c) Requiring one card to exit from a zone should the zone count report three or more cards in the zone;

(d) Requiring two valid but different cards to exit from a zone should the zone count report two people present;

(e) Prohibiting exit from a zone and generate an alarm if the zone count reports one person present.

9.13.6 It shall be possible to increment and decrement zone counting based on logical inputs not related to access events.

10 Identity Analytics - Competencies

10.1 Competencies shall be cardholder-based assignable attributes, used to determine if the cardholder is allowed access to specified areas based on factors relevant to the cardholder. The factors may be based on authority or skill levels or similar.

10.2 Multiple competency attributes may be assigned to one or more cardholder records.

10.3 Each competency will assume one of 4 different states:

(a) Active - The competency is currently valid for the cardholder.

(b) Expiry due - The competency is currently valid for the cardholder but will expire in a specified period.

i. A configurable message shall be displayed advising the cardholder that the competency is about to expire.

(c) Expired - The competency has been assigned to the cardholder but has expired.

(d) Disabled - The competency, is temporarily disabled (or overridden) for the cardholder.

i. A field shall be provided to store the reason for disabling a competency.

10.4 The competency states shall be configurable as “soft” allowing access but generating an alarm; or “hard” denying access, should a competency requirement not be met.

10.5 Each competency shall be individually set per cardholder

10.6 A field shall be provided to store the reason for disabling a competency.

10.7 Competencies shall be configured as required per access zone.

10.8 It shall be possible to exempt specific access groups from the requirement to meet specific competencies.

10.9 Denied access due to an invalid or missing competency shall be displayed to the user at the door reader.

10.10 Access permission based on competency criteria must be determined at the IFS, independent of the Server being on line.

10.11 The reason for denied access due to an invalid competency shall be displayed on the door reader or keypad.

10.12 Advanced warning of a cardholder’s competency about to expire shall be sent to the individual and/or other nominated persons.

10.13 Notice of a cardholder's competency expiry shall be sent to the individual and/or other nominated persons.

10.14 A consolidated report detailing competency expiry warnings for cardholders shall be sent via email to the associated manager.

11 Pre-programmed Override Macros

11.1 To allow for making changes to the system configuration on demand, it shall be possible to pre-configure the required changes and assign them to a macro command.

11.2 An operator shall be able to initiate the macro (to carry out the changes) via either a menu item or by a site plan icon.

11.3 Macro assembly must be by the use of GUI features such as drop down lists and drag-and-drop techniques. The use of script language to write macro?s is not acceptable.

11.4 Macro’s shall be able to be initiated on a time schedule.

11.5 Macro’s shall be able to execute command line actions

11.6 Up to 300 character variables shall be able to be specified for each command line

11.7 Each Macro shall be able to contain multiple command line entries

11.8 The configuration and execution of command line Macros shall be user account name and password protected. These user names and passwords shall be obscured on entry, and transmitted and stored at the central command system server in an encrypted format.

12 On-Line Door control

12.1 Access control for a door shall allow for the following features where specified:

(a) Access reader

(b) Emergency release switch input

(c) Reception control switch input

12.2 Egress control for a door shall allow for the following features where specified:

(a) Exit reader

(b) Push button request to exit

(c) Emergency exit break-glass

12.3 Push button request to exit as referred to in 15.2(b) shall record the exit in the event database.

12.4 When requested by a valid means of access or egress, the door shall unlock for a preset period, after which the door shall relock.

12.4.1 If access or egress is completed prior to the preset time expiring, then the door shall relock immediately the door has closed.

12.4.2 The period of unlock shall be extended should a cardholder be a member of an access group where extended entry time is required. Refer to 12.3 above.

12.5 Entry and exit methods referred to in clauses 15.1(b),15.1(c) and 15.2(c) shall each record the event in the event database.

12.6 The door shall be monitored for both door open/closed and door unlocked/locked using concealed monitor switches appropriate for the door installation.

12.7 Where the door is a double door, the inactive door leaf shall also be monitored for door open/closed and door unlocked/locked. The inactive leaf door monitor switches may be connected as part of the active door leaf monitoring.

12.8 It shall be possible to configure the door in a way that generates a forced door alarm should the door be unlocked and/or opened without reference to the system.

12.9 Should a door be left unlocked or open after a preset time, an alarm shall be generated reporting the condition.

12.10 The door open/unlocked warnings shall provide an audible warning at the door.

12.11 It shall be possible to disable the reader audible warning.

12.12 It shall be possible to generate the audible warning via a relay connected elsewhere in the system.

12.13 Should a valid request to access a door be generated and access not taken, it shall be possible to ignore the request (not record it as an entry event) and automatically re-secure the door after a preset time.

12.14 When a valid access through a door is undertaken, the door shall immediately re-secure on re-closing.

12.15 It shall be possible to "lock-down" an Access Zone by assigning an input condition to the access zone. When the input is operated, all doors in the access zone shall go to secure mode

12.15.1 It shall be possible to assign specific cardholders the right to access a zone when the access zone is locked, whilst refusing access to all other cardholders.

12.16 It shall be possible to create an interlock relationship between a group of doors. Up to 20 doors shall be included in any interlock group.

12.16.1 It must be possible to configure interlock groups via GUI "drag and drop" functionality, without the requirement to write scripted logic.

12.17 The system shall support a challenge or video verification mode as specified below:

12.17.1 When a card is presented at a reader, images from the cardholder database (as many as required) shall be displayed in the challenge window.

12.17.2 Associated with the images, it shall be possible to display a video image from one or more assigned cameras. .

12.17.3 In challenge mode it shall be possible to view a site plan showing the location and status of the controlled entry point and nearby items.

12.17.4 In challenge mode it shall be possible for the operator to view the status of the cardholder's cards and competencies for the purpose of informing the cardholder, at the time of entry, if any expiries are imminent.

12.17.5 Specific personal data shall also be able to be displayed, associated with the cardholder (name details, department etc).

12.17.6 Associated with a challenge entry, the selection and layout on screen of cardholder images, cardholder personal data, cardholder card or competency status, site plans or video images must be configurable using simple drag and drop, or click and drag techniques to resize or reposition information.

12.17.7 The challenge made shall be configurable to either:

(a) Automatically grant access to a valid card. In this case the system shall be able to display the current access decision (granted or denied) to the challenge operator.

(b) Require operator intervention to grant access to a valid cardholder.

12.17.8 Should a second challenge be requested while an unanswered challenge remains in the system, the second and subsequent challenges shall queue automatically awaiting response.

12.17.9 It shall be possible for an operator to view waiting challenge events and to select and process challenge events within the queue in any order they choose.

12.17.10 The system shall allow challenge events to be managed from a single full-screen view per operator or multiple filtered views, as dictated by the customer.

13 Off-Line Door control

13.1 Where specified, doors shall be managed using an off-line door locking system.

13.2 A single interface shall be provided that allows for administration and reporting including both the online and offline (or standalone) locking systems.

13.3 The off-line doors shall be fully integrated into the Access Control and Intruder Alarm System as described below:

13.3.1 Card technology shall be contactless 4k Mifare standard, as required for all on-line doors.

13.3.2 Card encoding shall be carried out as a single encode operation for both on-line and off-line door readers.

13.3.3 Operational data shall be transferred between the integrated security system and off-line doors automatically, without the need for specific operator actions. This data shall include:

(a) Multiple levels of door low battery voltage alarms.

(b) Access activity from all doors.

(c) Disabled card information

(d) Changes to cardholder access privileges.

13.3.4 Assignment of access privileges for use in both online and offline doors shall be available through a single interface.

13.3.5 Access privileges based on the time of day shall be available (e.g. office hours versus after hours) or type of day (e.g. weekdays versus weekends) with full flexibility in specifying the time intervals or day types for any user.

13.3.6 It shall be possible to configure the system to ensure access updates for off-line doors are enforced within a given period of time, configurable as a minimum from 1 to 7 days.

13.3.7 Access privileges must not be stored at the door escutcheon (eliminating the need to update each door escutcheon when a user is added or removed).

13.3.8 For disabled access, the ability to specify an extended door opening time for specific users shall also be available for off-line doors.

13.3.9 Off-line doors shall support partitioning to allow specific administrators to control and assign access privileges within their own environment/facility.

13.4 The range of hardware shall include an option for an internal privacy lock which, when activated, prevents entry except for privileged users.

13.5 Hardware shall not use proprietary batteries. Batteries must be commonly available types.

13.6 Battery life shall support a minimum of 35,000 operations before replacement is required.

13.7 The escutcheon hardware shall be compatible with the lock hardware specified for this project.

13.8 Electronic escutcheon hardware shall be simple to fit to existing mechanical door lock hardware.

13.8.1 Escutcheon hardware must be compatible with the mechanical door lock hardware, noting:

(a) Spindle size; and

(b) door handle rotation angle.

13.9 Basic maintenance (changing batteries, changing basic configuration) shall be able to be carried out by customer maintenance staff with minimal instruction.

13.10 The off-line escutcheons should be able to hold an audit trail of at minimum the last 1000 events.

13.11 The off-line escutcheons shall be able to function in a variety of modes such as but not limited to, free (unlocked), secure (locked) by schedule or as controlled by a user with privilege to change the escutcheon mode.

13.12 It shall be possible to change a door state between the free and secure states using an authorised card.

13.13 It shall be possible to specify on a user by user basis what modes they can place the lock in (e.g. free or secure) and override functions the user can perform (i.e. entry allowed when privacy lock is on).

13.14 A handheld programming device shall be available for the purposes of:

(a) Diagnosing problems

(b) Performing an emergency opening of an offline escutcheon.

(c) Updating software from time to time.

(d) Provide power to the escutcheon to allow resolving a no battery voltage situation.

(e) Initialising future doors that may be added from time to time.

13.15 Multiple levels of warning for low battery indication including audible, visual and physical warnings (i.e. initially a visual signal progressing to an audible and visual indicator and then finally progressing to an audible, visual and delayed opening of the door to indicate/prompt someone to report the occurrence).

13.16 Environmental protection shall be provided for the door installation.

13.16.1 The environmental rating for the escutcheon shall be at least ip46

13.16.2 The environmental rating for the cylinders shall be at least IP66

13.17 The hardware range shall include the ability to upgrade off-line doors to wireless through a wireless gateway.

14 Wireless Door control

14.1 Where specified, doors shall be managed using an escutcheon based, wireless door locking system.

14.2 A single, seamless user interface shall be provided within the head end to ensure integrity of access decisions are maintained within the primary access control system.

14.3 The flow of information from the RFID card shall be transmitted instantaneously to the wireless card reader/lock, (escutcheon or cylinder type) which shall in turn send the card credentials to the hub and access control system.

14.4 The primary Access Control and Intruder Alarm system shall provide immediate access decisions as described elsewhere in this specification.

14.5 Assignment of access privileges for use in both wired online and wireless doors shall be available through a single interface.

14.6 Card encoding shall be carried out as a single encode operation for both wired on-line and wireless door readers

14.7 A wireless RS485 communication hub shall support up to 8 wireless escutcheons or cylinders and have reliable communication to each reader within a distance of 15 metres.

14.7.1 Wireless hubs shall be able to be wired in series with RS485 compatible cable.

14.7.2 The wireless hub shall conform to the radio standard applicable to the region of installation and conform to IEEE802.15.4 (2400 – 2483.5 MHz).

14.7.3 AES 128bit encryption shall apply for communication between the hub and each wireless reader.

14.7.4 Up to 16 (installer selectable) channels per hub shall be available to ensure each wireless escutcheon or cylinder is configured with reliable communication.

14.7.5 The hardware shall use non propriety batteries commonly available and provide for up to 40000 operations before replacement.

14.8 The wireless doors shall be fully integrated into the Access Control and Intruder Alarm System as described below:

14.8.1 Card technology shall be contactless Mifare standard, as required for all on-line doors.

14.8.2 Operational data shall be transferred between the integrated security system and wireless doors automatically, without the need for specific operator actions. This data shall include:

(a) Multiple levels of door low battery voltage alarms.

(b) Access activity from all doors.

(c) Disabled card information

(d) Changes to cardholder access privileges.

14.8.3 Escutcheon hardware must be compatible with the mechanical door lock hardware, noting:

(a) Spindle size; and

(b) door handle rotation angle.

14.9 Basic maintenance (changing batteries, changing basic configuration) shall be able to be carried out by customer maintenance staff with minimal instruction.

14.10 The installer service tool shall communicate with each wireless hub and enable configuration, management and override of each door independent of the access control system.

15 System Integration

15.1 The system shall support OPC (OLE for Process Control) Alarms and Events protocol to provide an open interface to allow integration with Building and Facilities Management, and Management Information Systems.

15.2 17.2 The OPC (Alarms and Events) interface shall allow third party OPC clients to register to receive the security system's alarms and events.

15.2.1 17.2.1 When an alarm is processed, the OPC Alarms & Events client shall send an event processed message back to the security system to process the alarm on the security system.

15.3 The system shall support OPC (OLE for Process Control) Data Access protocol to provide an open interface to allow the status of system components to be reported to an external OPC (Data Access) client.

15.4 The OPC Interface shall allow third party OPC (Data Access) clients to generate system component overrides including but not limited to alarm zone and access zone overrides.

15.5 The system shall provide an XML interface to allow for the import, export, and synchronisation of data in an ongoing basis from other applications directly into the Cardholder database both an on-line real time manner or in a batch oriented approach. A developer's kit shall be readily available to allow for easy implementation.

15.6 The system shall provide an XML interface to allow for updating access control schedules from other applications directly into the system configuration database both an on-line real time manner or in a batch oriented approach. A developer's kit shall be readily available to allow for easy implementation.

15.7 An Application Programming Interface (API) shall be available to allow 3rd party systems to be integrated into the system.

15.7.1 The API shall be managed at the IFC level, to allow inputs from the 3rd party system to be managed as system inputs, and to allow the IFC to directly trigger actions in 3rd Party systems.

15.8 Access via OPC or XML shall be managed as "operator events" and logged accordingly.

15.9 A facility shall be provided in the system to allow for the real-time export of any alarm or event information to 3rd party systems via customisable strings for the purposes of controlling the 3rd party application.

15.10 The system shall support accepting events from one or more 3rd party applications and displaying these and their status' in the event and/or alarm windows.

15.11 Events from 3rd party systems shall be managed in the same way as inputs connected directly to the IFC's.

16 Access Control Readers

The technology for the Access Control Readers will be specified in accompanying sections. When required, these readers shall meet the following specification:

16.1 The following features shall apply to both 125 kHz and Mifare technologies:

16.1.1 The Card only reader option shall include an audible beeper and red/green LEDs, to provide feedback to users.

16.1.2 The beeper shall give different beeps to indicate:

(a) Access granted

(b) Access denied.

(c) 2nd card required when dual card authorisation or escort mode is programmed.

16.1.3 A steady red LED shall indicate door secure.

16.1.4 A flashing red LED shall indicate access denied.

16.1.5 A steady green LED shall indicate door free access.

16.1.6 A flashing green LED shall indicate access granted.

16.1.7 Readers must comply with at least IP68 environmental protection rating.

16.1.8 Readers must comply with an impact rating of at least IK07

16.1.9 A vandal resistant enclosure having an impact rating of at least IK08 rating shall be provided where.

(a) Vandal covers shall be fixed to the wall surface using tamper-resistant screws.

(b) Vandal covers shall have bevelled edges to limit the ability for persons use the reader as an aid to climbing the building.

(c) All external surfaces shall be bevelled and without protruding parts to meet anti-ligature requirements.

16.1.10 Readers shall generate a heartbeat signal to enable the IFC to identify lost communications and thereby generate an alarm.

16.1.11 The reader must accept a message from the IFC to advise that the data from reader to IFC has been received and to consequently stop sending the card data.

16.1.12 Each reader shall be identified independently at the central control by means of a unique plain language descriptor. The central control plain language descriptor shall be at least 60 characters in length.

16.1.13 Where a PIN pad is specified, the reader shall include:

(a) A PIN pad fully integrated with the reader.

(b) Backlit PIN pad

(c) An backlit LCD display indicating:

i. Card required

ii. PIN required

iii. Access denied

iv. Intruder alarm set

v. Intruder alarm unset

vi. Free access

vii. 2nd card required

16.1.14 The PIN pad shall include:

(a) Standard 0 to 9 digit keys

(b) CE (clear entry)

(c) IN (enter key)

(d) Three function keys (F1, F2 and F3)

16.2 Mifare technology is specified:

16.2.1 Card Serial Numbers (CSN's) shall only be used as the access card identifier when approved by the consultant.

16.2.2 The reader shall read the card identifier from any of Sectors 1 to 15 as programmed, using the MAD address to identify the specific sector

16.2.3 Readers shall support enhanced encryption as described later in this specification.

19.3 Supply readers that have the ability to read multiple technology's this includes 125 Khz Wiegand, Mifare, Bluetooth and NFC Communication

17 Access Reader Self-discovery and Communication

17.1 Readers shall be individually serialized.

17.2 When connected to an IFC, the serial number of the reader shall be reported at the system server.

17.3 Once assigned to a function within an IFC, if any attempt is made to substitute readers in the field without authorization, an alarm shall be generated.

17.4 Data communication rate between IFC's and readers shall be at least 1Mbit/second.

17.5 Communication sessions between IFC's and readers shall use certificate exchange protocols using keys have a minimum strength of 256 bit elliptical encryption.

17.6 Data communication between IFC's and readers shall use a minimum of 128 bit AES encryption.

18 Long Range Access Control Readers

18.1 The requirement for Long Range Access Control Readers will be specified in accompanying documents. When required, these readers shall meet the following specification.

18.2 The reader shall be provided in a vandal resistant enclosure, having an environmental rating of at least IP65.

18.3 The reader shall have a read range up to 10m (33ft).

18.4 The reader shall successfully read a tag/booster passing through the reader field up to 200km/hr (125mph).

18.5 Multiple channel support shall allow at least 32 readers to operate within close vicinity of each other.

18.6 Access cards and tokens as defined in Section 0 below shall be read by the reader using an associated tag/booster.

18.7 The access card or token shall be temporarily associated with the tag/booster to allow the data from the card or token to be transmitted to the long range reader.

18.8 The transfer of data from the access card or token, through the tag/booster, via the reader to the system; shall be seamless to the end user.

18.9 A unique identifier for the tag/booster shall be sent to the reader.

18.10 The access control decision shall be able to be based on a combination of valid access card associated with a valid tag/booster. For example, an access decision based on a driver (cardholder ID) permitted access only with an approved vehicle (booster ID).

19 Access Cards and Tokens

19.1 The access token technology for this project shall match the reader technology as specified separately but in association with this specification.

19.2 Access cards shall be of standard credit card size, being no larger than CR-80 and shall be direct printable using a dye-sublimation print process or be capable of accepting an adhesive label printed through such a process.

19.3 All cards shall meet ISO standards.

19.4 As well as CR80 sized cards, vehicle tokens and key-ring transponders should also be proposed as an alternative, where available.

19.4.1 The access token data shall include:

(a) Support for up to 2008bit card numbers

(b) Where a proprietary card number format is offered, the card format shall include:

i. A unique facility (site) code not used for any other system worldwide.

ii. A unique cardholder identification number at least 7 digits long.

iii. An issue level for each card number to allow for replacing lost cards without reducing the card database size. Up to 15 levels of issue levels shall be supported.

19.4.2 The access control token shall uniquely identify the cardholder to the access control system.

19.4.3 Access control information shall be stored on or in the access token in a secure format, as described in Sections 22, 23 and 24 below.

19.4.4 Transmission of data between the proximity access token and the proximity reader shall be in a secure format as described in Sections 22, 23 and 24 below.

19.4.5 Access control encoding data shall not be displayed on the access card or token.

19.4.6 There shall be barriers employed to prevent the deciphering of access control data stored on the card using any readily available equipment.

19.4.7 There shall be barriers employed to prevent the copying or altering of access control data stored on the card using any readily available equipment. The Tenderer shall document the barriers used.

19.4.8 Cards and access tokens shall be able to be encoded by the supplier according to the client's specifications, made known at the time of order. Cards and tokens supplied with manufacturer determined card numbers will not be acceptable.

19.4.9 It shall be possible to encode cards and tokens to allow operation of a user defined Personal Identification Number (PIN) in association with the card requirement specified in 21.4.8, with the card still supplied ex stock as defined above.

19.4.10 Allowance shall be made for the supply of encoding software and hardware to the Client to enable encoding of their own cards and/or tokens on site.

19.5 The system shall provide facility to encode cards or tokens in batches of user definable quantity.

20 Mifare Plus Technology

20.1 The cards shall incorporate Mifare Plus technology.

20.2 The card number must be a number specifically coded onto the card. It shall not be the card serial number (CSN).

20.3 The card data encoded shall use a secure sector authentication level of security to protect against card cloning. 128bit AES encryption shall be used.

20.4 The Mifare Plus "S" variant shall be provided.

20.5 The encoded card data shall incorporate data consisting of:

(a) The assigned card number.

(b) A site-specific key consisting of 32 hexadecimal characters.

(c) The 32 hexadecimal key shall optionally be sourced from a customer specified key-safe.

20.6 Card encoding shall be an integral part of card production. Refer to Section 28 below.

20.7 It shall be possible to specify the card sector where the card number is stored.

20.8 The sector unlock key and the Mifare MAD unlock key shall be user definable.

20.9 Where multiple reader technologies are deployed, as defined in sections covering other technologies, single pass card encoding shall be used.

21 Cardholder Management

21.1 The cardholder database shall be structured so that the name field is the master field for each record. A background unique identifier may be used as the key field for each record but this must not be required by an operator to identify a cardholder. Use of the card number as the key field is not acceptable.

21.2 Each IFC shall cater for the number of cardholders as defined in 11.8 and 11.9 above.

21.3 The system must allow at least 15 Issue Levels per card or token to match that specified in 21.4.1(b)(iii) above. This must deny access and raise an alarm to the operator when a wrong issue level is presented to a reader.

21.4 Cardholders must be able to be issued with more than one access token of different description and different number (i.e. access card, biometric identification and vehicle token) whilst maintaining only one cardholder record in the database.

21.5 Where biometric identification is required, the fingerprint data shall be a property of the cardholder record.

21.6 Encoding and printing cards shall be properties of the cardholder record.

21.6.1 The options for encoding and printing shall be:

(a) Print card

(b) Encode print

(c) Print and encode card

21.7 Access groups shall be linked to cardholders by both assigning access groups to cardholders or cardholders to access groups.

21.8 At least 64 user-definable “Personal Data” fields shall be provided which may be selectively reported on.

21.8.1 Personal Data Fields shall be able to be set up as either:

(a) Text User data may be entered.

(b) Text List User selects text from a pre-prepared list of text strings.

(c) Numeric User must enter numeric data.

(d) Date Calendar dates may be entered based on the workstation date format.

(e) Default Value The field has a default value assigned.

(f) Image The field may only contain an image to the field.

(g) Email/Mobile The field contains an email address or mobile number to be used for notifications.

21.8.2 Personal data Fields shall also be able to be configured as:

(a) Required field Data must be entered.

(b) Unique Values Data must be unique from all other card records.

(c) No default Value Default value disabled.

21.8.3 Personal data fields shall support rules to ensure data accuracy. Examples: @ in email addresses; employee codes are in the correct format.

21.9 A notes/memo field shall be available, associated with each card record.

21.9.1 The notes field shall support word-wrap, insert, delete, cut, copy and paste functions.

21.10 It shall be possible to “group” or “filter” cardholders for the purposes of editing access, generating reports and assigning operator privileges.

21.11 The following information fields shall optionally be displayed on the Cardholder editing window:

(a) The date when a cardholder record was created.

(b) The date when the record was last modified.

21.11.2 For ease of programming Cardholders shall be grouped into access groups sharing the same access criteria and default personal data fields.

21.11.3 It shall be possible to enter an automatic expiry date/time for the card.

21.11.4 It shall be possible to automatically expire cards that have not been used for a predetermined period of inactivity of up to 999 days.

21.11.5 It shall be possible to allocate start and end dates and times for an Access Groups access to a particular access zone.

21.12 Access shall have start and end dates and time to within one minute.

21.13 The system shall be capable of importing database information, on selected cardholders, from other systems and be capable of exporting that cardholder’s data, either with or without controlled alteration or amendment, to other databases.

21.14 The system shall support the capability to allow bulk changes to card records. It shall be possible to carry out the following changes as a bulk change:

(a) Delete selected cardholder records.

(b) Change personal data fields

(c) Change card details.

(d) Change access options

(e) Change the system division the records are assigned to.

21.15 A bulk change shall be able to be saved and scheduled to run at a later time.

21.16 A window shall be provided to show details of created, saved, edited, pending, successful and failed bulk changes.

21.17 A personal user code (4 or 6 digit) shall be a property of the cardholder record to allow alarm setting and unsetting.

21.18 System operator management shall be a property of the cardholder record.

21.19 A change history record associated with each cardholder record shall list all changes made to a cardholder record, including details of who made the changes.

21.20 The system shall support an event trail for the cardholder which details recent card usage events for the cardholder as well as operator events which have modified the cardholder record. The number of prior events to be shown or prior length of time to be covered shall be configurable. The system shall allow different prior length of time / number of prior events to be displayed for different operators.

21.21 The system shall allow an operator to search for a cardholder by entering any part of their first and/or last name, in any order and separated by a space if using both. After three characters have been entered the system shall automatically return matching results and filter these dynamically as the operator continues to type.

21.22 The system shall allow the cardholder search fields and search results to be configurable. The system shall allow different operators to use and see different search fields and search results for the purpose of cardholder administration tasks.

21.23 The system shall allow the information returned for a cardholder and visible to the operator to be configurable and include any sub-section of the total information stored in the cardholder record (e.g. personal data, cards, access groups, competencies, biometric information etc). Different operators shall be able to view different sub-sections of the cardholder information.

21.24 The system shall allow design of different screen layouts for the purpose of cardholder administration, for use by different operators.

21.25 The system shall allow cardholder information to be viewed and updated in one screen.

21.26 Configuring operators shall, subject to the required privileges, be able to design single screen cardholder management viewers adapted for the specific screen resolution of the operator(s) who will use the viewer, to ensure best use of available screen real-estate.

21.27 The system shall provide tools to maximise, on screen, specific cardholder details when required. Maximising an area and returning to standard layout must both be single-click actions.

21.28 The system shall allow all cardholder administration functions to be managed solely via keyboard.

22 Visitor Management

22.1 The system shall provide visitor management functionality as described in this section.

22.2 Visitor details shall be able to be pre-registered into the system.

22.3 Visitor details for several visitors associated with a single visit shall be able to be pre-registered into the system.

22.4 A visitor escort shall be able to be assigned to each visitor.

22.4.1 The escort functionality is defined in sections 12.10(f) and 30.7.1(e) of this specification

22.5 Attributes associated with the visitor(s) shall be configurable and set as mandatory or option fields. These shall include:

(a) The reception where the visitor(s) will be expected to arrive.

(b) The visitor category.

(c) The person the visitor(s) will be meeting.

(d) Visitor arrival time.

(e) Visitor departure time.

(f) Building access rights to be given to the visitor(s).

(g) Visitor photo-ID image.

22.6 Visitor badges shall be able to be printed on a reception label printer.

22.7 Visitor personal details shall be stored if required, to be reused for future visits.

22.8 Visit details shall be recorded in the system event database.

22.9 The system shall raise an alarm should a visitor not sign out by the due time.

22.10 Multiple visitor management (reception) workstations shall be allowed.

22.11 A visitor management screen shall provide a visitor "snapshot" showing the following parameters:

(a) Expected to arrive during the day.

(b) Location status - currently on site, due to leave or temporarily off site.

(c) Cards associated with visitors remaining after the expected departure time plus a predefined grace period, shall be automatically disabled.

22.12 Groups of visitors shall be selectable as a group and their status processed as a single action.

22.13 The visitor management (reception) workstations shall support configurable macro actions. The macros shall be preconfigured system macros.

22.14 Visitor reporting requirements are defined in section 39.13 of this specification.

23 Photo ID Badging and Image Management

23.1 The system shall provide a means to:

(a) Electronically capture images.

(b) Store the images in the server database,

(c) Integrate those images into a pre-designed ID card from within the system

(d) Produce an integrated and completely finished identification card within the nominated time frame.

23.2 Images are defined as being one or more of the following:

(a) Photographic image of the cardholder

(b) Signature of the cardholder and/or authorising person

(c) A fingerprint of the Cardholder

23.3 The system shall have an integrated method of card design within the system software without the requirement of having to import background files from other software programs. The facility to import background images from other sources must also be available. This must include scanned logos and other graphical imagery if desired.

23.4 The system offered shall capture images in 24 bit colour and at least 640 x 480 pixel resolution using standard video capture hardware offering a TWAIN or Direct Draw standard interface, or a USB digital camera.

23.5 Images must be able to be “cropped” after capture to optimise the image size within the desirable image area. This movable “cropping” box must be user-definable as to size.

23.5.1 The controls must be easy to use from within the system software and once set, they must be capable of applying the same setting on subsequent image captures for future cardholder records.

23.6 Up to three images per cardholder must be capable of being captured and stored within the system. Images may be defined as per section x.2 above.

23.7 The system shall store images in the JPEG compression format. User definable compression rates shall be easily selectable by the operator permitting, as a minimum; at least three levels of JPEG compression are required.

23.8 The system offered shall be capable of importing image files, for use in either card layout or cardholder images, from at least the following formats:

(a) JPEG

(b) Windows BMP

(c) LEAD Compression

23.9 The card design must be capable of incorporating, storing, printing and displaying bar-code information and must support the following bar-code formats:

(a) EAN 13 & 128

(b) UPC A & E

(c) Code 39 & 128

(d) Interleave 2 of 5

(e) Codabar

(f) Telepen

23.10 The system must have an integrated card design program. Systems offering a separate card design program where card designs must be created in alternate drawing programs and imported are not acceptable however the system offered must also be capable of using imported images as per clause 28.8.

23.11 The card layout section of the system must be capable of user-selecting up to 16.7 million colours with a custom colour palette available.

23.12 Card design must be accomplished by the use of “drag and drop” options using a mouse.

23.13 The system must be capable of using all of the common word processing fonts and must also be capable of normal text manipulation including, text sizing, left and right justification, centring, bolding, underlining & italicising.

23.14 The variable cardholder image files that are selected to incorporate into the card design must be user-definable as to size. Full size being defined as 30mm x 40mm. The sizing must be fully user-configurable from 25% of full size up to 200% of full size, as a minimum, and must offer automatic aspect ratio adjustment throughout the size range.

23.15 The system shall be capable of producing hard copy output of images and data using any standard MS-Windows printer.

23.16 The system shall produce photo ID cards using a single step hard-card colour MS-Windows compatible printer. Systems offering multi-stage production, heat lamination or heat & pressure card production are not acceptable.

23.17 The system shall be capable of printing directly onto Hi-Co magnetic stripe cards, Wiegand effect cards and proximity cards without damaging the card technology.

23.18 Cards must be capable of either landscape or portrait printing and Bar-codes must be capable of either vertical or horizontal orientation on the card when printed.

24 System Operator Management

24.1 Operators shall be members of operator groups.

24.2 Operator establishment and maintenance shall be limited to assigned Senior Operators.

24.3 It must be easy to define operator privileges for a group of operators and it must be easy to add an operator to the group.

24.4 Operator access to the system is to be restricted by means of an operator identifier and individual password.

24.5 Passwords shall be managed by using either non-restrictive or force password changes. Forced changes shall include options for:

(a) Minimum password length greater than 8 characters.

(b) Mixed case characters

(c) Mixed alpha and numeric characters

(d) Change password after a defined period of up to at least 365 days.

(e) Remembering and rejecting at least 8 previously used passwords.

24.6 The system shall also support Mifare card logon.

24.7 Each operator shall have the authority to alter his own password, but not that of other operators

24.8 Automatic logoff shall occur after a preset time of up to at least 60 minutes of operator inactivity.

24.9 It shall be possible to configure the system to only allow one logon per operator.

24.10 It must be possible to allow or deny Operators access to system menu functions, including viewing of Cardholder Personal Data fields, Personal Notes and Images.

24.11 It must be possible to restrict Operator access to Cardholders based on system division.

24.12 It shall be possible to assign different access rights for each division an operator is required to access. For example, “advanced user” for division 1; “view only” for division 2; and “no access” for division 3.

24.13 Any menu option not available to an Operator should be either greyed out or not visible.

25 Elevator Control and Management

25.1 The system must provide fully integrated elevator control facilities. The elevator control access equipment must communicate with the same central control as the door card readers.

25.2 The elevator control architecture shall comprise a card reader in each elevator car, reporting to elevator control interface equipment mounted in or near the elevator motor room. Reader type shall be as specified for use on access control doors.

25.3 The elevator control system shall be capable of controlling access independently in a number of elevator shafts simultaneously.

25.4 The elevator control system shall incorporate dedicated intelligence and a local database of authorised cardholders.

25.5 Each elevator reader shall be identified independently at the central control by means of a unique plain language descriptor. The central control plain language descriptor shall be at least 60 characters in length.

25.6 Each reader head shall be capable of raising an alarm if it stops communicating with its elevator controller or is removed from the elevator.

25.7 The elevator control shall check entry based on ALL of the following criteria:

(a) Correct facility code

(b) Authorised card in database

(c) Correct issue number

(d) Authorised level

(e) Authorised time of day

(f) Correct PIN (If PIN entry is required).

25.7.2 The access mode for each elevator shall be capable of automatically changing according to the programmed time schedules, as received from the central control. The following access criteria modes are required:

(a)	Free access	Elevator level select button for that level is unlocked, no card entry required.
(b)	Secure access	Elevator level is locked. A successful card attempt is required for valid entry. Elevator level re-secures after access attempt.

(c)	Secure + PIN access	Elevator level is locked, a successful card and correct PIN number attempt is required for valid entry. Elevator level re-secures after access attempt.
(d)	Dual Authorisation	Access is granted when two different but legitimate cards are presented within a given time frame.
(e)	Escort	A second card is required to be presented from nominated cardholder(s).
(f)	Shared PIN Number	The system Operator determines what the PIN number will be and programs this into the system. Access is allowed at the elevator level when the correct 4 digit PIN is pressed followed by the “Enter” key.

25.7.3 The elevator control system shall be capable of individually setting the access modes for each level as described above.

25.7.4 Levels must be securable on a level-by-level basis, using command instructions transmitted from the central control.

25.7.5 The central control must provide operator override facilities to enable temporary override capability on a level by level basis.

25.7.6 The elevator control system shall continue to operate without performance degradation in the event of a communications link failure with the central control.

25.8 Where a low level interface is specified:

25.8.1 The interface between the access system elevator control equipment and the actual elevator switching control equipment shall be via dry relay contacts.

25.8.2 The voltage from the elevator system connected to the relays shall not exceed 24 volts DC/AC

25.8.3 The elevator control system shall provide one relay contact per elevator shaft per level for the system. This relay contact shall be used to interface with the elevator switching control equipment.

25.8.4 An input shall be provided for each level per elevator to indicate what level the user selected. On activation of this input all relays return to secure state.

25.9 Where a high level interface is specified:

25.9.1 The interface between the access system elevator control equipment and the actual elevator switching control equipment shall be via RS-232 connection.

25.9.2 The elevator control equipment will provide feedback as to which level was selected by the cardholder.

26 Intruder Alarm System

26.1 The system will incorporate a fully functional intruder alarm system.

26.2 All Inputs globally within the system must be able to be utilised as intrusion alarm inputs to allow intruder detection sensors to be connected to the system.

26.3 All outputs anywhere within the system shall be available for intruder alarm purposes such as sounding remote sirens etc.

26.4 Arming and disarming the intrusion detection system shall be either by using card readers, remote arming terminals or key-switches.

26.5 The intruder alarm zone and the access zone for an area shall be treated as separate conditions.

26.6 The intruder alarm system shall provide a dependency feature where by an alarm zone does not go into the set state until the “Dependent” alarm zones are all in the set state.

26.6.1 If the alarm zone is set (armed) and the access door is secure:

(a) A cardholder shall require authorisation to both unset (disarm) the intruder alarm zone and to access the access zone, to be allowed access.

(b) If the card is not authorised to unset the alarm zone or not allowed to access the access zone, then access shall be denied.

26.6.2 If the alarm zone is unset (disarmed) and the access door is secure:

(a) A cardholder shall require access to the access zone only for access to be allowed.

(b) If the card is not authorised to access the access zone, then access shall be denied.

26.6.3 For normal operation, after an authorised token is presented, and access is granted, then the alarm zone shall remain unset after the door relocks.

26.6.4 As an optional function, the alarm zone must auto-set after a predetermined time period.

26.7 When specified, alarm monitoring shall use a connection with Central Alarm Monitoring stations via digital communicators using Contact ID format, connected directly to the IFC panels.

26.7.1 It must be possible for alarms from one IFC to be managed on a second IFC where the digital communicator is installed. (Peer to Peer communications).

26.7.2 Digital communicators are to be able to communicate alarms from the complete system, independent of system server.

26.7.3 The system shall report and log the all Digital Communicator activity and reason for any failure to communicate.

26.7.4 The system shall provide for up to two back up diallers on different controllers to provide automatic backup capability should the designated digital communicator fail to operate on the appropriate alarm condition.

26.8 Cardholders shall be assigned to groups, to which any combination of the following intruder alarm privileges relating to the operation of the system may be assigned:

(a) Unset intruder alarm zones

(b) Set Intruder alarms zones

(c) status of alarms and inputs on Remote Arming Terminal.

(d) Acknowledge Alarms

(e) Shunt Inputs

(f) Force-arm alarm zones

(g) Auto-isolate alarm zones

27 Guard Tours

27.1 The system shall support multiple guard tours.

27.2 Check points shall be card readers at doors, inputs, outputs, logic blocks or external systems.

28 Input and output circuit functionality

28.1 Input circuits shall be connected to the IFC as described in “Field Hardware”.

28.2 Inputs from detection devices covering the same region for control purposes are to be grouped into alarm zones. Alarm zones can be in any one of four states and shall handle alarms differently depending of the state. The first two shall be defined as set (armed) and unset (disarmed). The names of the other states shall be able to be defined at the central control for other purposes such as maintenance testing.

28.3 Alarm priorities can be assigned to any of the four input states.

28.4 The system shall provide entry and exit delays for the setting and unsetting of alarms.

28.5 The entry delay shall be configurable from 0 to 5 minutes in steps of one second.

28.6 An optional audible warning must sound during the entry delay (from the time that the alarm occurs to the time that the Zone state is changed). It must be possible to designate specific card readers and remote arming terminals to sound entry delay warning beeps. Selected output relays should also be able to be operated during the entry delay period allowing suitable sounders to be connected at required locations.

28.7 An exit delay is to be provided to groups of inputs so that a change of state of an exit delayed zone is delayed by the exit delay period, which can be adjusted, from 5 seconds to 5 minutes in steps of one second.

28.8 An optional audible warning must sound during the exit delay (from the time that the alarm occurs to the time that the zone state is changed). It must be possible to designate specific card readers and Remote Arming Terminals to sound exit delay-warning beeps. Selected output relays should also be able to be operated during the exit delay period allowing suitable sounders to be connected at required locations. This applies to both manually and automatically changing the state of a zone ? in the case of automatically changing the state of a zone the exit delay and audible warning gives people working late in the building time to unset the alarms or leave the building.

28.9 The system shall include Alarm Escalation as an event. The new event shall correspond to the original alarm, but may have a different (usually higher) priority, and may require a different set of alarm relays to operate.

28.10 Escalated alarms shall be able to be displayed in a Window specifically provided for this purpose.

28.11 Alarms shall be able to be escalated under the following conditions:

(a) Escalate if alarm not acknowledged after (X) seconds

(b) Escalate if in inactive state for (X) seconds

(c) Escalate if zone contains (X) alarms

(d) Escalate if two event from same point within (X) seconds.

(e) Escalate if two events from different points in same zone within (X) seconds

28.12 It shall be possible to have automatic time based setting and unsetting of alarms.

28.13 It shall be possible to configure the system such that events (such as a card swipe or operation of a key switch connected to an input) can change the state of a zone.

28.14 Authorised cardholders shall be allowed to set and unset alarm zones by:

(a) Operation of the Card plus PIN reader as an alarm panel.

(b) Presenting a valid access card to a card reader associated with the alarm zone, twice within a nominated time period (double card badging).

28.15 It shall be possible to set and unset multiple alarm zones from a Remote Arming Terminal.

28.16 All alarm occurrences shall be presented at the central control within 4 seconds of their occurrence at the remote field device.

28.17 All Alarm events shall be viewable from an Alarm Stack.

28.18 It shall be possible to view all alarm events by clicking on interactive Site Plan icons that, because of their changing audible and visual states, indicate the presence of alarms.

28.19 All alarm events arriving at the central control shall be "time stamped" with the time they occurred and the time they were logged at the central control.

28.20 All alarm events shall have a user definable alarm priority assigned. A minimum of 8 alarm priority levels plus non-alarm event and ignored shall be provided.

28.21 It shall be possible to assign a different audio warning sound to each alarm priority.

28.22 Incoming Alarms shall be presented in the Alarm stack according to their assigned priority with the highest level at the top. Alarms with the same priority shall be presented in time order.

28.23 The priority of Alarms in the alarm stack shall be identifiable by a user definable colour.

28.24 Identical consecutive alarms that occur within a predefined time span shall be report as a single alarm with the number of occurrences reporting as a flood alarm quantity.

28.25 The Central control must be able to control the actual priority assigned to any alarm activation throughout the day. This means any alarm activation may be programmed as "Low Priority" during office hours and "High priority" at all other times.

28.26 It shall be possible to nominate an Input (e.g. Smoke, Fire or Gas detection) as an “Evacuation Input” in which case certain doors within the Site will revert immediately to Free Access.

28.27 Operators shall be required to complete 2-stage alarm processing as:

28.27.1 Acknowledge Alarm.

(a) An Acknowledged alarm shall remain in the alarm stack and be easily identified as having been acknowledged but not yet processed.

(b) The central control shall record in the hard disk activity log that the operator has acknowledged the alarm. An alarm is “acknowledged” by the operator selecting the “Acknowledge” button in the alarm-viewing window.

(c) A second alarm from the same source as the acknowledged alarm shall be indicated as a new alarm.

28.27.2 Process Alarm.

(a) A Processed alarm shall clear from the Alarm Stack.

(b) The central control shall record in the hard disk activity log that the operator has processed the alarm. An alarm is ?processed? by the operator selecting the ?Process? button that is displayed in the alarm viewing window.

28.28 The system shall allow an operator to multi-select contiguous or non-contiguous alarms in the list in order to add a note, acknowledge or process all selected alarms in one action.

28.29 The alarm list shall support mandatory fields of alarm time, alarm priority and alarm state.

28.30 The system shall allow a suitably privileged operator to configure any of the following additional fields to be visible in the alarm list and to configure their order:

(a) full alarm message

(b) related cardholder name

(c) acknowledging operator?s name

(d) alarm zone

(e) alarm source

(f) related access zone

(g) event type

(h) event group

(i) division of the alarm source

(j) count (occurrences of alarm)

28.31 It must be possible for an operator to sort the alarm list by any of the available fields.

28.32 The system shall display a summary of alarms, by priority, which is visible to the monitoring operator at all times and updated dynamically as new alarms occur or existing alarms are actioned.

28.33 The alarm summary shall indicate if there are any unacknowledged alarms for a given priority.

28.34 The system shall allow configuration of filtered alarm lists. Alarm lists shall be filterable based on any combination of selected divisions, escalation status or alarm priority.

28.35 The system shall allow different information to be configured and displayed to a monitoring operator based on the type of alarm.

28.36 Door Open Too Long alarms must display selected and configurable information (including, as an example, the photo and contact details) for the person who left the door open (last successful access).

28.37 Cardholder related alarms shall automatically display recent events and selected information (name, photo, personal details etc) for the person causing the alarm.

28.38 An active alarm shall not be able to be finally processed and cleared from the Alarm Window until the cause of the alarm has been removed and the alarm condition has returned to the normal state.

28.39 Pre-programmed alarm instructions shall be available for the operator to provide instructions for acknowledging and processing each alarm.

28.39.1 Alarm Instructions shall have the following features:

(a) Default Alarm Instructions shall be able to be programmed and automatically applied to all events of a common type e.g. all wrong PIN events applicable to all readers.

(b) Individual Alarm Instructions shall be able to be programmed and applied to individual alarm events.

(c) A table of contact names, phone numbers or other frequently used volatile information shall be available when programming Alarm Instructions, and applied to Alarm Instructions from a pick list.

(d) When items in the pick-list are updated, the linked Alarm Instructions shall automatically update.

28.39.2 The alarm instruction text shall be able to be formatted using common text formatting features including but not limited to:

(a) Bold, italic and underline

(b) Text colours

(c) Left, centre and right justified.

(d) Bulleted text

(e) Standard Microsoft Windows font types and sizes.

28.39.3 It shall be possible to copy and paste Alarm Instructions between alarm events.

28.40 The Alarm window shall allow the operator to enter a comment. Such comment will be date/time stamped by the system, and recorded against that alarm event in the audit trail.

28.40.1 When required, a pre-defined list of alarm responses shall be available for operators to select the appropriate response to an alarm. The alarm responses shall be user configurable to suit site requirements.

28.40.2 Keyboard function keys (F1 to F8) shall be mapped to the first 8 alarm response messages to automatically insert the associated message as required.

28.41 The system shall provide relay output facilities that are system activated in response to alarm activations. Relay functions required are:

(a) Activate and latch a relay in response to an alarm. Relay to remain latched until alarm processed.

(b) Activate a relay for pre-set "pulse" time. The relay to release after the "pulse" time lapses.

(c) Relay activation to "mirror" or “follow” the alarm input activation.

28.42 The system shall incorporate relay outputs that can be activated according to time schedules, rather than alarm event. These outputs may be used to control lighting, heating, or to electronically lock or unlock non-monitored doors.

29 Remote Arming Terminals

29.1 Remote Arming Terminals (RATs) shall be provided to allow keypad functionality as described in this section.

29.2 Logging on to the RAT functionality shall be by:

(a) A User Code (PIN) assigned to each cardholder.

(b) Presenting a card to a reader associated with the Remote Arming Terminal.

(c) Presenting a valid card to a reader associated with the Remote Arming Terminal plus entering a 4 or 6 digit PIN on the Remote Arming Terminal.

29.3 Authorised cardholders shall be able to:

(a) Set and unset all or selected intruder alarms zones that have been assigned to a Remote Arming Terminal.

(b) Acknowledge alarms.

(c) Shunt inputs for alarm zones.

(d) View a summary of status of all devices associated with the RAT.

(e) See and operate on the appropriate alarm zone information they have access to.

29.4 Cardholder and groups of Cardholders shall be able to be assigned to operate any number of Remote Arming Terminals across a system.

29.5 Communications between the Remote Arming Terminals and the controllers shall be encrypted to a minimum strength equivalent to 40 bit AES.

29.6 Remote Arming Terminals shall be capable of being programmed to handle combination of up to any 30 alarm zones and up to 100 of their associated Inputs across a complete system.

29.7 Multiple remote arming terminals can be used anywhere in the system to remotely manage assigned Intruder alarm zones.

29.8 Remote Arming Terminals shall be capable of arming and disarming perimeter fence zones.

30 Notifications

30.1 Specific event and alarm messages shall be able to be configured to be sent to nominated users via either email or SMS message.

30.2 It shall be possible for persons receiving alarm messages to be able to acknowledge the alarms via email or SMS message.

30.3 It shall be possible to send notification of imminent card or competency expiry to an individual, their manager or other nominated person. Refer also to Sections 13 and 39.

30.4 A comprehensive filtering feature shall be provided to manage notification information transmission.

31 Audit Trail

31.1 The Server hard disk shall be used to record all system activity for archiving purposes. It shall not be possible to alter archived data.

31.2 Every system activity event along with all details, including but not limited to the following list, shall be time stamped with the time of occurrence to the nearest second and shall be recorded in the system activity log for archiving.

(a) All access attempts (allowed and disallowed).

(b) Alarm events.

(c) System events.

(d) Operator activity.

31.3 The central control shall provide an on-line facility to archive system data and event records to an archive file to free hard disk space for further activity logging.

31.4 The archive process shall be initiated by either manual operation or automatically by time.

31.5 It shall be possible to nominate the number of days of data that shall remain on the server subsequent to an archive process.

31.6 It shall be possible for an operator to view filtered event trails, e.g. for filtered for selected site items.

32 Reports

32.1 The central control shall provide historical reporting capabilities from the following sources of information:

(a) System activity data

(b) Cardholder access data

(c) Cardholder Personal Data fields

(d) Site configuration and setup data.

32.2 The report generation feature shall be easy to use and based on a “wizard” style of parameter selection and preparation. The wizards shall provide features to simplify report generation by incorporating selections such as report for “yesterday”, “last week”, “last month” etc. This is for the purpose of quickly generating recurring, standard format, reports.

32.3 The parameters for producing the report must be fully user definable and must be capable of searching on any cardholder or access event criteria.

32.4 It shall be possible to automatically produce the reports listed in this clause. The methods available to generate the report(s) are defined in previously.

(a) Activity Any site activity.

(b) Evacuation Last known location of all cardholders on site.

(c) Exception Unprocessed alarms, un-acknowledged alarms and doors temporarily overridden from secure to free

32.5 The report shall be generated by any of the following means, as may be required by the operator:

(a) Operator running a macro.

(b) An alarm event trigger.

(c) On a recurring schedule.

32.6 The central control shall generate and format reports in "background". This means the operator must be able to process alarms, alter database parameters and perform other system changes while the report is being generated. Report generation must continue if the operator decides to perform any other task.

32.7 The central control shall have a screen preview function, so that reports can be previewed on-screen before they are printed.

32.8 It shall be possible to email reports to nominated people or groups of people.

32.9 Report formats shall be able to be saved for future use.

32.10 The central control shall have a "printer spooler" so that reports can be printed at any network-supported printers connected to the system.

32.11 The central control shall have a printer queue facility to enable reports to be queued if the target printer is off-line, busy, not connected or faulty.

32.12 The central control shall be able to produce voltage reports for electrified fencing perimeter security voltage monitoring.

32.13 Visitor management reporting shall provide reports as follows:

(a) Visitor status (expected, on site, departed).

(b) Planned visits.

(c) Past visits (who visited who, who escorted a visitor).

33 Communications & Diagnostics

33.1 The central control shall automatically restart full and complete processing after a power failure.

33.2 The central control shall provide a full diagnostic performance log to enable system engineers to monitor system performance in the event of a system malfunction.

33.3 The diagnostic performance log shall be stored in a separate file on hard disk from all other data files.

33.4 The diagnostic performance must be available without shutting down or "freezing the system".

33.5 The central control shall provide on-line system diagnostic facilities which enable authorised operators or systems engineers to monitor and then tune the system performance (communications network performance tuning, for example).