Access Control Configuration, Management and Reporting System

CONTENTS

1) PURPOSE AND SCOPE

a) This specification is a description of the integrated Access Control System (ACS) and its minimum required capability. Equipment specified herein includes the ACS computer and software organisation, the ACS features and functions, and the ACS intelligent controllers and their capability

b) It is recognised that not all of this specification will be deliverable from a basic core system and that some additional system modules may be required. Optional modules required in order to comply with this specification shall be readily available from the manufacturer's standard catalogue of products and options.

2) INTRODUCTION

a) The system shall include all hardware and software, including intelligent controller units, ID tokens and readers, power supplies, enclosures and all other relevant equipment.

b) The ACS shall be feature-rich and scalable for small, medium and large installations and shall be specifically designed to be easy to administer by operators with limited experience of such a system

c) It is a requirement that the ACS shall consist of a Server, operated from one or more Client machines.

d) The ACS whilst being highly secure shall be open architecture, utilising a MS SQL Server database. Only industry standard tools and practices shall be required to create customised management reports

e) The ACS shall support a network of Intelligent Controllers which shall be responsible for managing the real-time status of fixed control points such as doors, turnstiles or airlocks and initiating system-wide logical actions across alarm input groups and relay output groups

f) The Intelligent Controllers shall employ micro-controller units and memory and shall be responsible for authorising card and token presentations at readers and for storing relevant system information.

g) The controllers shall be capable of operating over an IP network. A Master controller connected to the IP network shall be capable of connecting to Slave controllers via an RS485 bus. Each 'Channel' shall comprise of one Master controller with up to 15 Slave controllers.

3) SYSTEM CAPACITY OVERVIEW

a) SYSTEM-WIDE SYSTEM LIMITATIONS

i) Door/Reader capacity – Unlimited for the system but 32 door / reader limit per iNet Controller

ii) Users – Unlimited for the system but 200,000 user limit in each iNet Controller

iii) Access Groups – No system limit

iv) Time Zones – No system limit

v) User Definable data fields for Personnel records – No system limit

vi) Anti-Passback – No system limit

vii) System and Access Logs – Only limited by the restrictions of MS SQL Server software

b) COMMUNICATIONS

i) TCP/IP direct to Controllers for IP connected Controllers – No system limit
ii) 3-wire RS485 Downstream Controllers – Up to 15 per Master controller

c) SYSTEM INPUTS

i) 9 inputs per controller providing 144 inputs per channel

ii) Each input shall be capable of supporting normally open or normally closed devices.

d) SYSTEM OUTPUTS

i) 4 relay outputs per controller providing 64 outputs per channel

ii) Each relay output shall provide voltage free changeover contacts

4) SYSTEM HARDWARE

a) SYSTEM ARCHITECTURE AND BASIC OPERATIONAL OVERVIEW

i) The system shall use intelligent distributed processing controller architecture with access decisions being made locally at each controller.

ii) Where decisions need to be made across controllers (such as a Request to Exit button on one channel releasing a door on a different channel), the communications shall be between Master controllers and NOT via the ACS software.

iii) The ACS main server shall connect to IP based Master controllers

iv) There shall be no limit to the number of channels per system

v) Controllers shall be installed into purpose made steel enclosures and shall be powered by local mains power or POE. Every power supply, including POE shall include battery back-up and battery charging circuits

vi) The ACS main server shall download controller-specific data to each Master Controller, which is then forwarded to each Slave controller. This data shall be stored at each controller and shall be pertinent information relating to the controller's functionality.

vii) Should communication with the ACS main server be lost, the Master controller shall continue to operate, and all event activity and its date and time stamp shall

be stored at the controller. Upon restoration of communications transaction data shall be automatically uploaded to the ACS Server for future historical reporting

viii) Similarly, should communication between the Master controller and the Slave controllers be lost, each Slave controller shall continue to operate, and all event activity and its date and time stamp shall be stored at the controller. Upon restoration of communications, transaction data shall be automatically uploaded to the Master controller and then to the ACS Server for future historical reporting

ix) Under normal system operation, Master Controllers shall send details of events and transactions to the ACS Server to ensure that the latest data is always available in the central logs

x) If communications are lost to a Master Controller, the controller shall enter into fall-back mode. In fall-back mode a Master controller shall:

(1) Carry on normal access control operations using its on-board database

(2) Store up to 100,000 alarms, events and transactions

(3) When the event buffer is full, the oldest, non-important events shall be over-written first

(4) Automatically send stored data to the ACS main server upon return of communications

xi) If transactions are dependant on IP communications between Master controllers, it is recognised that an error with the IP network can adversely affect these operations and result in reduced functionality.

b) IP CONNECTED CONTROLLERS

i) An IP connected Master controller shall be able to connect directly to the ACS Server via an IP network

ii) IP Controllers shall support 10/100 Mbps full duplex communications

iii) IP Controllers shall support DHCP as well as Fixed IP Addresses, the latter being the preferred method of addressing.

iv) A software application shall be provided to allow each IP device to be easily configured on the network

c) INTELLIGENT DOOR CONTROLLERS

i) Master Controllers shall connect to the system via an IP connection directly at the controller. Downstream controllers shall connect to the master via a 3-wire RS485 Bus

ii) To aid installation, servicing and maintenance, every controller shall include plug-in connectors for all wiring

iii) Each controller (Master and Downstream) shall have its own on-board database and shall be capable of carrying out system transactions such as token authorisations without reference to any other controller. Each controller shall allow the on-board database to store up to 63 Time Zones and 200,000 users

with PINs. In addition, there shall be sufficient memory to maintain a local log of up to 250,000 historical events and transactions if the controller if offline from its master controller or from the ACS Server

iv) In the event that the historical memory buffer becomes full at a controller whilst offline, the oldest events shall be over-written by the newest events. These events shall be synchronised with the main historical database once communications are restored

v) The ACS shall allow users to define their own 4-digit PINs. When using PINs, the controller's token holder capacity shall not be reduced

vi) Each controller shall support:

(1) 2 x door lock output relays suitable for switching 30V at 3A each

(2) 2 x outputs to drive optional sounders for providing local alarm signals

(3) 2 x inputs capable of supporting N/O or N/C Request to Exit (REX) buttons

(4) 2 x inputs capable of supporting N/O or N/C door contacts

(5) 1 x input capable of supporting N/O or N/C enclosure tamper switch

(6) 4 x inputs capable of supporting N/O or N/C devices for functions such as:

(a) Fire and emergency monitoring

(b) Intruder detection monitoring

(c) Monitoring for operation of Breakglass

(d) Power supply monitoring for Mains Fail and Battery Fault

vii) Each controller shall support of two card readers or keypad readers which may be used to support two doors with IN reader and REX for egress, or one door with IN and OUT readers.

viii) Each controller shall be capable of supporting two different reader technologies at the same time, whether the combination is on one door or two

ix) Each controller shall be capable of supporting a minimum of 63 different time zones

x) In the event of a power failure, the power supply in each controller shall monitor the voltage at its battery. In the event of the battery voltage dropping below 10.5v the power supply shall disconnect power to prevent damage occurring to the battery.

xi) Each controller shall incorporate a memory which, in the event of total power failure, shall retain its configuration for a minimum of 100 hours. When power is restored the IDC shall continue to operate without having to communicate or reload data from the ACS Server

xii) Diagnostic LEDs shall be included on each controller (Master and Downstream) for:

(1) Activation of each input

(2) Activation of each relay output

(3) Communication activity between the Master and Slave controllers

(4) LAN activity

d) INPUT/OUTPUT CONTROLLERS

i) Input/Output Controllers (IOCs) shall connect to a Master controller via a 3-wire RS485 Bus

ii) To aid installation, servicing and maintenance, each IOC shall support plug-in terminal blocks for all wiring

iii) IOCs shall be support:

(1) 8 x inputs

(2) 8 x relay outputs with voltage free change-over contacts

iv) The IOC shall present activity at the inputs to the master controller, which will then provide instructions to the IOC to activate relevant outputs.

e) CONTROLLER FIRMWARE

i) Controller firmware shall be held in flash memory. Future firmware upgrades shall be downloaded from the ACS Server or from a standalone machine, without the need to change any physical ICs.

f) ENCLOSURES AND POWER SUPPLIES

i) Controllers shall be housed within a steel enclosure and include a tamper input on the controller board

ii) Controllers shall have a mains power supply or a Power over Ethernet (POE) splitter. Each power supply option shall include an integral 4-hour battery back-up

iii) Each PSU shall be incorporated into the Controller enclosure and support the system electronics, two card readers and two lock outputs. The PSU shall have a capacity of 3A at 12Vdc. POE shall support POE++ (PoE 802.3bt @ 60W)

g) READERS AND KEYPADS

i) The system shall support readers with a Wiegand interface, allowing the use of ID card and biometric technologies

ii) In addition, controllers shall be configurable to allow support for Wiegand readers, OSDP readers or Aperio locks.

5) SYSTEM SOFTWARE – OVERVIEW

a) GENERAL SYSTEM OPERATION

i) System software shall be installed on the ACS Server and shall be accessed via one or more Client machines

ii) The ACS Graphical User Interface (GUI) shall be easy to understand and intuitive to use

iii) A single log-on page shall open all of the administrative privileges for any given operator. ACS management including configuration, administration, real-time system monitoring and system reporting shall all be accessed from a common interface. Systems that require an operator to log-on more than once in the same session or requires a separate log-on instance for different parts of the system will not be acceptable

iv) The features and options that are available within the ACS shall be controlled by licensing. The software shall operate without a licence in its basic form, with trial licences being available for a 30 day period.

v) The ACS software shall include a multi-lingual capability that is readily available within the ACS application. It shall be possible to link an operator to a specific language so that the required language is invoked automatically as that operator logs on.

vi) The ACS shall be easily navigated via a system of menus.

vii) Every device and operating parameter within the system, for example Readers, Time Zones, Access Levels, etc. shall be described with a name

viii) System transactions and system status shall be transmitted from each controller to the ACS Server in real time. This information shall be used to generate on-screen incidents and historical reports

ix) The ACS shall support pre-defined emails upon the occurrence of nominated incidents or events

x) The system shall interface with third-party systems for example Fire and Intruder systems.

xi) Background operations shall be implemented via Windows Services, configured to prevent unauthorised access.

b) OPERATOR ACCESS

i) The ACS shall support multiple operators with 2 levels of administrative access: “Administrators” who have full access to all software menus and “Operators” whose permissions may be defined by an Administrator

ii) Each operator shall have a log-on username and password

iii) An operator shall belong to an operator group which shall determine the system functions the operator is permitted to use. The system shall support an unlimited number of operator groups

iv) It shall be possible for an Administrator to edit the permitted system functions and options associated with each Manager operator group.

v) It shall be possible to set up and edit system policies for the use and management of passwords. The password policy shall specify the minimum

length of the password and whether upper case, lower case, numeric and special characters are mandatory.

vi) The system shall support Operator Profiles, an option to allow each individual operator to configure the size and location of screens. If this option is selected, these changes will not affect the size and location of the screen for other operators.

c) PC REQUIREMENTS

i) The Server software shall be capable of running on a PC with the following specifications:

(1) Intel i5 processor @ 3GHz

(2) 8GB RAM

(3) 100GB Free Disk Space

(4) 10/100 Network Card

(5) USB Port

(6) Screen Resolution = 1280 x 800 or higher

ii) The Client software shall be capable of running on a PC with the following specifications:

(1) Intel i3 processor @ 3GHz

(2) 4GB RAM

(3) 100GB Free Disk Space

(4) 10/100 Network Card

(5) USB Port

(6) Screen Resolution = 1280 x 800 or higher

iii) The software shall support the following operating systems:

(1) Windows 10 Home or Pro (x64)

(2) Windows Server 2012 R2

(3) Windows Server 2016

(4) Windows Server 2019

6) SYSTEM SOFTWARE – HARDWARE CONFIGURATION

a) GENERAL

i) The ACS system shall allow hardware configuration to be implemented via the Server or any Client.

b) CONTROLLER CONFIGURATION

i) There shall be no practical limit to the number of controllers on the system

ii) The following connection attributes shall also be specified for each Master controller:

(1) Name

(2) IP address

(3) Operation port

iii) The following minimum attributes shall also be specified for each Downstream controller on the system:

(1) Master controller connected to the downstream controller

(2) Unique address on the RS485 Bus

c) DOOR CONFIGURATION

i) There shall be no limit to the number of doors on the system

ii) The following minimum attributes shall be specified for each door on the system:

(1) Name

(2) Associated controller

(3) Input and Output configuration for devices such as Request to Exit Buttons, Locks etc.

(4) Unlock period (in seconds, variable between 1 and 60)

(5) Extended unlock period for DDA compliance (in seconds, variable between 1 and 60)

(6) Max. open period before the door is deemed to be held open

iii) The controller shall support Turnstile and Airlock options (where one door can be interlocked with another door on the same controller such that both doors cannot be opened at the same time)

iv) The system shall allow a lock to immediately re-lock once a door has been opened

d) READER CONFIGURATION

i) There shall be no limit to the number of token readers on the system

ii) The following minimum attributes shall be specified for each reader on the system:

(1) Name

(2) Whether the reader has an associated keypad

(3) Associated controller

(4) Associated door

e) ELEVATOR CONTROL

i) The system shall allow access to elevators and elevator floors to be restricted according to access management rules including time, day and system mode

ii) The ACS shall be capable of operating system outputs that can be used to restrict access to specific floor buttons in an elevator cab. Subsequent to a successful token read, and subject to access groups associated with the token, Input/Output (IOC) relay outputs shall be operated to invoke nominated floor buttons

iii) The ACS shall support a maximum of 64 floors per elevator

7) SYSTEM SOFTWARE – ACCESS CONTROL ELEMENTS

a) TIME ZONES AND PUBLIC HOLIDAYS

i) The ACS shall support the definition of time zones

ii) The system shall use time zones for:

(1) Defining when access is permitted at certain doors

(2) Defining when system actions such as the automatic locking and unlocking of doors are in operation

(3) When keypad readers are used in two factor authentication mode

iii) There shall be no practical limit to the number of time zones defined on the system although each controller shall support a maximum of 63 time zones.

iv) Each time zone shall consist of up to 3 time periods, where each time period will define one or more specific periods of time

v) Relevant time zones shall be stored at the controllers and continue to operate in the event of a communications failure or failure of the ACS Server

vi) It shall be possible to disable a time zone, for example public holidays. Public Holidays shall be created and shall be definable as recurring.

b) ID CARD/TOKEN PRINTING

i) The ACS shall support the printing of cards/tokens for cardholders

ii) The card/token designs shall enable personal data from the ACS database to be incorporated, including photos. The designs shall also enable the inclusion of standard text and graphics such as company names and logos

iii) ID card printing shall be managed via a Client PC connected to ID card/token printers

c) UNUSED TOKEN

i) The ACS shall include a facility to report on tokens that have not been used for a number of days / weeks / months

ii) This period of inactivity shall be configurable per report

d) ANTIPASSBACK CONTROL

i) It shall be possible to define entry and exit readers which shall allow the system to monitor people to enforce AntiPassBack rules

ii) When a user enters an enforced AntiPassBack area, all of their tokens shall be deemed to be in the same area. This shall prevent the user from passing back any of their tokens for use a second time into the area and shall also prevent other tokens held by the user being distributed for use by others into the same area

iii) In the event of loss of IP communications, controllers shall maintain AntiPassBack rules at doors on the same channel.

e) TIME & ATTENDANCE

i) It shall be possible to define entry and exit readers which shall allow the system to monitor people to record date and time that they entered and exited the site.

ii) This information shall then be used to generate a ‘Time & Attendance’ report, a simple timesheet report listing the duration that selected users spent on-site.

f) Lockdown

i) The system will support multilevel lockdown.

ii) It shall be possible to instigate lockdown by clicking a button the Dashboard, or by operating an allocated key switch or pushbutton.

iii) Resetting Lockdown shall only be possible by clicking a button the Dashboard.

iv) 2 levels of lockdown shall be functional:

(1) Level 1 – users are prevented from access doors, other than users in a group configured as priority users.

(2) Level 2 – ALL users are prevented from access doors.

v) Furthermore, individual doors shall be configurable to remain active in either lockdown condition.

g) DURESS ALARMS

i) The system shall support Duress Alarms via any combination of the following methods:

ii) Duress Fingerprint – this will require the user to enrol an additional finger as a duress finger.

iii) Duress Token – this will require the user to carry an additional token to generate the duress alarm.

iv) Duress PIN - this will require the user to remember an additional PIN which, when used in conjunction with their normal token, will generate the duress alarm.

v) When a duress alarm is generated, the relevant door will open as normal, and the duress information will be displayed in the Alarms screen on the Dashboard.

vi) It must be possible to allow further actions to be instigated when a duress alarm is generated, using “Events and Actions”.

8) SYSTEM SOFTWARE – USERS

a) USER GROUPS

i) There shall be no practical limit to the number of Groups on the system

ii) There shall be no practical limit to the number of users that can be allocated to each group

iii) The following information shall be required for each group:

(1) Name

(2) Users allocated / not allocated to the group

(3) Whether the users in the group are to be monitored for Time & Attendance

(4) Whether the users in the group are to be subject to AntiPassBack

(5) To assist users that have mobility difficulties, an extended unlock feature shall allow selected users to have longer unlock periods at nominated doors. This feature when selected, shall only apply at pre-defined readers/doors and shall not be a global setting

(6) Whether the users in the group require extra time at selected doors

(7) Whether the users in the group are granted access during Lockdown Level 1

(8) Card readers allocated to the group

(9) Fingerprint readers allocated to the group

(10) AntiPassback doors allocated to the group

(11) Elevator floors allocated to the group

(12) Time zones allocated to the group

(13) A comment ‘free text’ field (256 characters minimum)

b) USERS

i) There shall be no practical limit to the number of users on the system

ii) The system shall support 3 type of user, Employees, Visitors and Contractors

iii) There shall be no practical limit to the number of users that can be allocated to a group

iv) The following information shall be required as a minimum for users:

(1) Title

(2) First name

(3) Surname

(4) Personnel number

(5) Company and Department name

(6) A ‘Valid from’ date and a ‘Valid for’ period for each user. Visitor’s tokens shall be configured to expire at the end of the day and a facility shall be provided to quickly and easily re-activate individual tokens at the start of the day.

(7) Custom defined ‘Extra Data’ fields with no practical system limit to the number of fields definable

(8) Token management for up to 6 tokens allocated to the user, including the issuance of Mobile Access tokens

(9) Fingerprint management for the user

(10) Access management for the user by allocating to user to one or more groups

(11) Photo management for the user

(12) A comment ‘free text’ field

c) USER TOKEN MANAGEMENT

i) The ACS shall permit token management tasks to be directly available from the user record. These shall include

(1) Creating and issuing tokens (including Mobile Access tokens) for the user

(2) Printing a card with a selectable design at a selectable ID card printer

(3) Revoking individual tokens from the user

(4) Suspending and resetting individual tokens from the user

ii) The system shall support intelligent issue of temporary tokens, such that when a temporary token is assigned to a person, the Primary token assigned to that user will be temporarily suspended.

d) USER PHOTO MANAGEMENT

i) The ACS shall allow personnel ID images to be associated with individual users.

ii) The system shall permit images to be captured directly from a webcam feed or imported from previously acquired .jpg or .png images.

iii) The system shall allow images to be cropped to any desired aspect ratio.

iv) The system shall also allow other documents such as passport and driving licence images to be saved with the user's 'Extra Field' records

9) SYSTEM SOFTWARE – DASHBOARD

a) GENERAL

i) The ACS shall incorporate a Dashboard that allows operators to monitor and interact with the system in real-time.

ii) The ACS shall display alarms and normal events (non-alarms).

iii) Normal events shall be for information only and shall not have a workflow.

iv) The ACS shall be capable of displaying a list of doors on the system with the capability of selecting an individual door and remotely Granting Access, Unlocking and Re-locking the door.

v) The system shall support interactive controls on a floorplan that an operator can control directly. For example, it shall be possible to:

(1) Monitor status of the door as well as Grant Access, Unlock or Lock the door.

(2) Grant access Inhibit Reader, Restore Reader

(3) Monitor the status of a controller for functions such as tamper, mains fail etc

b) ALARM REPORTING

i) The ACS shall display alarms on the Dashboard.

ii) Alarms shall be displayed such that repeat alarms overwrite previous alarm from the same source. This will minimise the number of alarms on the screen at any given time.

iii) Alarms shall have three states and shall require a basic workflow:

(1) Raised – This shall be the initial state when an Alarm is generated

(2) Acknowledged – This state shall be caused by the operator by selecting an alarm and choosing to acknowledge it

(3) Cleared – This shall be the final state of an alarm when the alarm is removed from the list and no further action is required

iv) The system shall optionally allow an operator to include notes when acknowledging or closing specific types of alarm.

c) FLOORPLANS

i) The ACS Dashboard shall include the option of including a visual representation of the managed site, and the status of various elements of the access control system.

ii) The system shall support the import of maps/plans in .jpg or .png format and shall support multiple maps which may provide different levels of detail. There shall be no practical limit to the number of maps/plans on the system.

iii) Objects within the access control system shall be represented by icons appearing on the maps/plans. The system shall distinguish between objects in a normal state and objects in an insecure state.

iv) The objects that can appear shall include, but not be limited to:

(1) Controllers

(2) Doors

(3) Readers

(4) Inputs

(5) Outputs

(6) Custom Objects, including Images, Rectangles, Ellipses, Lines and text Boxes.

d) PHOTOGRAPHIC IDENTIFICATION

i) The Dashboard shall enable the display of user photographs in real-time, in order to check the identity of users as tokens are read at selected readers

ii) The Dashboard shall permit up to 2 readers to be selected for monitoring and shall display the user's photograph with details about the user, time/date and access attempt.

10) SYSTEM SOFTWARE – EVENT CONFIGURATION

a) EVENT NOTIFICATION

i) The system shall support the sending of messages via email for selected Events

ii) Emails shall be configurable by selecting one or more email templates

iii) It shall support the inclusion of strings that shall be substituted by appropriate information about the event at the point the message is sent. For example, the name of the specific object.

b) EVENTS AND ACTIONS

i) The ACS shall include a method of detecting when a specific Event occurs and triggering an Action accordingly.

ii) This would allow, for example, an output on one channel to be activated when an input on a different channel is activated, or a counter to be incremented when someone is granted access at a door.

iii) Objects that shall create Events and subsequent Actions shall be:

(1) Counters

(2) Timers

(3) Inputs

(4) Outputs

(5) Controllers

(6) Doors

(7) Readers

11) SYSTEM SOFTWARE – SYSTEM REPORTS

a) GENERAL SYSTEM REPORTS

i) The system shall offer a variety of management reports that shall be generated from the system database, the access events database and the Time & Attendance database

ii) The ACS shall offer options for tailoring reports by setting filters. Time/date filters will allow a report to be run relative to a specific date, such as yesterday or the start of last month. It shall also be possible to enter absolute time/date for a report such as 11th February 2019 at 10:02

iii) The system shall allow reports to be printed to any system printer

iv) The system shall permit reports to be exported in various formats, including PDF, CSV, RTF, TIFF, HTML and MS Excel formats.

v) The system shall support the saving of report queries so that the same user can run the same report again

b) ACCESS LOG REPORT

i) The Access Log report shall be capable of generating reports based on the following filters:

(1) Start and end date/time

(2) Inclusion of access allowed and/or access denied events

(3) Inclusion of access denied events to be included per event type, such as ‘The user has no access to the reader’ or ‘Time zone violation’

(4) User/s

(5) Company / department

(6) Reader

c) SYSTEM LOG REPORT

i) The System Log report shall be capable of generating reports based on the following filters:

(1) Start and end date/time

(2) Software startup / shutdown

(3) Audit trail for all changes to any of the configuration parameters such as Groups, Employees, Controllers, Readers

(4) Controller events

d) TIME & ATTENDANCE REPORT

i) The Time & Attendance Log report shall be capable of generating reports based on the following filters:

(1) Start and end date/time

(2) User/s

(3) Options shall be provided to use first and last transaction of the day, ignore transactions less than one minute apart and round time to nearest 5 minutes

12) SYSTEM MANAGEMENT OPTIONS

a) USER MANAGEMENT

i) The ACS shall include the facility to allow a system administrator to change an operator's password

b) ADDITIONAL DATA FIELDS

i) The ACS shall allow 'Extra Data' fields to be added to a user's profile

ii) The system shall support extra data fields of different data types, including text, numeric, list, check, date/time, picture or colour

iii) The additional data fields shall be visible within the user interface

13) INTEGRATION OPTIONS

a) ELEVATORS

i) The ACS system shall support specific interfaces in order to integrate with elevator systems

ii) This support shall be provided by IOC hardware, each with 8 relay outputs, each output controlling a specific floor via the lift manufacturer's controller hardware.

iii) Access rights for floors shall be defined in the Groups programming

b) FIRE PANEL

i) The ACS system shall support integration with third party fire panels

ii) The Fire Panel Alarm relay shall connect to an input on a Master controller. It shall then be possible to trigger other Master controllers into Fire Alarm via Events and Actions.

iii) Each door on the system shall be definable as to whether it releases when Fire is activated.

iv) Each Master controller shall release each programmed door on the same channel.

v) All doors will automatically relock when the signal from the Fire Alarm panel is reset.

vi) The Alarm screen in the Dashboard will display the date and time when the Fire Alarm was activated and deactivated.

c) INTRUDER ALARM PANEL

i) The ACS system shall support integration with third party intruder alarm panels

ii) A relay on the intruder panel indicating its Set status shall be connected to an input on the ACS. It shall be possible to disable a reader depending on the state of this input to ensure that access is denied when the intruder panel is armed.

iii) The reader will be automatically enabled when the state of the input changes.

d) DATABASE IMPORT

i) The ACS system shall provide a method of importing data from external databases, via a .csv file

ii) The interface shall support the linking of columns in the csv file to fields in the ACS database.

e) WIRELESS LOCKS

i) The ACS system shall integrate with Aperio wireless lock systems using the Wiegand and the RS485 hubs. The implementation of the RS485 integration shall be certified by Assa Abloy.

ii) The interface shall support the synchronisation of data between the lock system and the ACS

iii) The interface shall support the representation of wireless locks and associated hardware in the ACS

iv) The interface shall support the issue and updating of tokens from within the ACS

v) The system shall support events and state changes from the lock system being displayed in the ACS

f) FINGERPRINT READERS

i) The system shall be compatible with the Idemia Sigma Series of Fingerprint readers:

(1) Sigma Lite

(2) Sigma Lite Plus

(3) Sigma

(4) Sigma Extreme

ii) The system shall be compatible with variants of the each of the above readers supporting the option of 2 factor authentication with the following card technologies:

(1) HID Prox

(2) iCLASS

(3) MIFARE / DESFire

iii) The system shall integrate directly with the Idemia Sigma Series Fingerprint readers without the need for additional “middleware” software

iv) Fingerprint enrolment shall be integrated into the ACS software and shall provide a simple to understand “enrolment score” to indicate the quality of the enrolment. If the score falls below a minimum level, the fingerprint shall be rejected.

v) The system shall support the Sigma Series fingerprint reader in two operating modes:

(1) “ACU Mode” where the fingerprint reader is connected to the controller

(2) “Direct Integration Mode” where the reader operates in ‘standalone’ mode, but the ACS software periodically uploads the reader’s internal event log via the TCP/IP network and includes all activity in the SQL database.

g) ANPR

i) The system will be compatible with the HIKVision range of ANPR cameras.

14) WARRANTIES, MAINTENANCE AND SERVICE

a) WARRANTY

i) The contractor shall warrant the ACS according to the manufacturers Terms and Conditions of Sale

ii) Support contracts to extend the warranty coverage shall be available from the installing system integrator

iii) The system integrator shall be the focal point for all service issues and questions (with the manufacturer’s support). The system integrator shall be approved by the ACS manufacturer to install and support the system

b) MAINTENANCE AND SERVICE

i) The integrator shall provide all services required and equipment necessary to maintain the entire ACS in an operational state as specified for a period of one (1) year after acceptance of the system, and shall provide all necessary material required for performing scheduled adjustments or other non-scheduled work

ii) The adjustment and repair of the ACS shall include computer equipment, software updates, and signal transmission equipment, access control equipment, facility interfaces, and support equipment. Responsibility shall be limited to integrator supplied and/or installed equipment. The integrator shall provide the manufacturer's required periodic maintenance and other work as necessary

c) QUALITY ASSURANCE

i) The manufacturer of all hardware and software components shall be established vendors to the access control/security industry for no less than five (5) years

ii) All hardware equipment shall conform to the applicable international standards for EMC compliance. The manufacturer shall be certified to ISO9001 or similar

iii) The integrator shall have been regularly engaged in the installation and maintenance of integrated access control systems similar in size and scope to that outlined herein for a period of no less than five (5) years

iv) The integrator shall supply certification that they are an authorised dealer for the proposed system

v) The integrator shall supply certification that the installation and service personnel have been factory trained in the installation and maintenance of the ACS

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

vii) The integrator shall be a factory-authorised service organisation which stocks a complete inventory of spare parts, and which can provide maintenance for the system