Controlsoft Specification

Section One
Identity Access

Edit as required – this document can be edited and merged where appropriate with additional specifier documents for a complete/customised solution.

Key - **[Square brackets]** – Options. Delete brackets and turn off bold to include.

{Curly brackets} – Comments.

PART 1 GENERAL

1. Summary

A. Section Includes
   a. Electronic Access Control

B. Products
   a. **Access Control Unit (ACU)** – A dedicated access control controller designed to interface with access point peripherals and identity-gathering devices. The ACU shall provide the processing, logic and decision-making required to manage and control individual access points.
   b. **Access Control Reader** – A secure access point device designed to identify and authenticate users by reading authorised credentials, including proximity cards, key fobs, mobile credentials or other supported identification technologies. The reader shall communicate the presented credential information to the access control system for validation and shall provide the appropriate indication to the user regarding the access request.
   c. **Input/Output Controller (IOC)** – An expansion board providing configurable digital inputs and outputs. The IOC can be used for monitoring system states or be used to expand the system to areas such as controlling elevators where there are insufficient inputs or outputs on the ACU.
   d. **Power Supply Unit (PSU)** – A dedicated power supply providing the required regulated power to the access control controllers and associated system components.
   e. **Desktop Reader** – A desktop reader providing a secure and convenient method of enrolling proximity credentials onto the access control system and associating those credentials with individual users.
   f. **Access Control Server Software** – Centralised server software providing system integrators and operators with comprehensive tools for configuring and managing access control hardware, users and permissions. The software shall provide real-time monitoring of access control activity across the system through a single, intuitive management interface. All system configuration, user information and event data shall be securely stored on the server computer running the software.
   g. **Access Control Client Software** – Client software providing operators with the same operational functionality and intuitive interface as the Access Control Server Software. The client shall operate as a workstation-based interface for managing and monitoring the access control system without storing system configuration or event data locally, enabling authorised users to manage the system from multiple workstations.
   h. **Access Control Web Client** – Client Web Interface providing system operators with the same operational functionality as the Access Control Server. The Web Client shall operate using a reverse proxy tunnel directly into the Access Control Server so no data is stored in the Cloud.

C. The products stated above shall form the fundamental part of an Access Control System (ACS), providing complete control and monitoring of access points

D. Overview of System
   a. The system shall provide monitoring and control of facility access through networked electronic access controllers incorporating access control readers. The system shall utilise a TCP/IP-based architecture, with individual electronic door controllers deployed.

b. The system shall be capable of expansion from 1 Door, up to a minimum of 1,000 doors.
c. Each ACU shall be capable to manage and monitor all peripherals related to a single door, this will include inputs for monitoring the door position switches, request to exit button/switches and emergency release monitoring.
d. All ACU's shall maintain a full database of users and events and shall operate independently in cases where they are operating "offline", without a connection to the Access Control Server Software.
e. The ACU shall be capable of operating on DHCP or Static IP network addressing
f. The system shall allow for unlimited Access Control Client software connections. No additional licenses are required for installing and operating the software on additional workstations.
g. The system shall allow for unlimited number of operators using the Access Control Web Client.
h. The system shall support a minimum of a minimum of 100,000 unique card holders and support multiple facility codes.
i. The ACS whilst being highly secure shall be open architecture, utilising a MS SQL Server database. The MS SQL Server should be able to reside either on the Access Control application server or on a third-party database server.

E. The ACS shall provide a minimum of the following features:
a. Access Control
b. CCTV Snapshot
c. Automatic Number Plate Recognition
d. Mobile Phone Wallet Credentials
e. Fingerprint Biometric Enrolment
f. Remote Door Opening
g. Fire Roll Call Reporting
h. Elevator Control
i. Time and Attendance
j. API for 3rd party application Integration
k. Integration with Microsoft EntraID.
l. Graphical Maps
m. 2-Tier Emergency Lockdown
n. Customisable Email Notifications
o. Customisable Events and Actions
p. Photo ID Badge Printing
q. USB enrolment reader
r. Automatic User Image Display at PC on card use
s. Access Control Readers connected on either Wiegand or OSDP
t. Support for Wireless door locks

2. Definitions

A. Access Control System (ACS): The entire system, made up of hardware to control the relevant access points and appliances, readers to identify users, software/hardware to determine access control, and all firmware and additional hardware installed as part of the access control solution.
B. Access Control Unit (ACU): An intelligent control unit that connects the Access Control Management software to access control devices, managing access permissions and monitoring the operational status of the peripheral devices.
C. AWG (American Wire Gauge): A unit of measurement for the diameter of wires.

D. Client: A PC that can monitor and change the access control databases but does not house the databases.
E. DHCP: Dynamic Host Configuration Protocol
F. EMC: Electromagnetic Compatibility.
G. I/O: Input / Output, relating to peripherals where an input is used to monitor the high/low state of a signal, and an output consists of a relay capable of switching a device on/off.
H. IP: Internet Protocol incorporated into Microsoft Windows.
I. LAN: Local area network.
J. Mbps: Megabits per second
K. Mobile Phone Credential: A digital access control token which resides on the user's mobile phone, either within a dedicated mobile app or within the phones digital wallet.
L. Monitor: A piece of hardware that allows an occupant to validate entry to an unknown user via a location on the network.
M. Multicast: Communication where information is addressed to multiple recipients simultaneously.
N. Open air: Without obstruction or interference.
O. Operator: A user of the ACS that performs administrative tasks to the system such as enrolling users and running reports.
P. PC: Personal computer, used as the Central Station, workstations, and file servers.
Q. PoE: Power over Ethernet.
R. Reader: A proximity credential, mobile phone, or biometric reader that captures credential information.
S. RS-485: A TIA/EIA standard for multipoint communications.
T. Server: A PC that contains the database of users and access control settings, which runs the access control software.
U. TCP: Transport Control Protocol incorporated into Microsoft Windows.
V. Token: The credential issued to a person. This can be a PIN or a device containing an encoded number, used to determine if access will be granted or denied.
W. Triggers and Actions: A software component which provides the ability to create rules to perform custom/bespoke functionality.
X. UDP: User Datagram Protocol incorporated into Microsoft Windows.
Y. UPS: Uninterruptible power supply.
Z. User: A person who is enrolled to the access control system and actively uses the system to gain entry to a building.
AA. USB: Universal Serial Bus.
BB. WAN: Wide area network.
CC. Wiegand: Patented magnetic principle that uses specially treated wires embedded in the credential card. Also known as reader data output format and Wiegand signal.
DD. Windows: Operating system by Microsoft Corporation.
EE. Workstation: A PC with software that is configured for specific limited security system functions.

3. System Description

A. General
    a. The ACS shall control the movement of authorized and non-authorized users through access points.
    b. Users shall be identified by one of the following means:
        i. Presenting a physical token or digital mobile phone credential to a reader.
        ii. Entering a unique PIN number to a keypad reader.
        iii. Scanning a unique physical property at a biometric reader.
        iv. A combination of all/some of the above.

c. The system shall facilitate the use of customer provided facility codes for card credentials, allowing the user to work with manageable token numbers.
d. The ACS shall reside on a PC.
    i. The ACS shall be capable of a Client/Server structure to allow multiple operators to manage the system at any time.
    ii. A password shall be required to login and shall limit the activities an operator is able to perform. All activities are to be logged against the operator and be reportable.
    iii. The ACS shall provide the ability to be remotely managed via a Web Client. The Web Client shall be operatable by any with a Web Browser and should not require any additional software to be installed other than the Web Browser.
e. The ACS Web Client shall have a responsive web design, for use of mobile devices, such as mobile phones and tablet.

B. Hardware
    a. Hardware shall consist of:
        i. Access Control Units (ACU's)
        ii. Input / Output Controllers (IOC's)
        iii. Access Control Readers
        iv. Desktop Enrolment Readers
        v. Power Supply Units

C. Software
    a. The software shall feature:
        i. Multi-user and multi-tasking capabilities to allow for independent activities and monitoring simultaneously from different workstations.
        ii. A graphical user interface with a tabular menu structure to allow the operator to easily navigate their day-to-day activities.
        iii. A Web Browser interface for user administration, event reporting, remote door opening and roll calling.
    b. Software licensing shall be for the entire system.
    c. Access shall be restricted using password-protected operator logins. No default passwords should exist within the system.

4. General Software Requirements

A. The software version shall come in 3 tiers:
    a. A 'Lite' version of the software shall contain all the standard access control features to manage privileges and report on users. The 'Lite' version shall be limited to a maximum of at least 6 access-controlled doors.
    b. A 'Pro' version of the software shall contain all the features within the 'Lite' version, with the addition of the professional features pack, these will include non-standard access control functions, such as Web Client, System Lockdowns, Fire Alarm Roll Calling, CCTV Snapshots. The 'Pro' version shall be limited to a maximum of at least 32 access-controlled doors.
    c. An 'Enterprise' version of the software shall contain all of the features within the 'Pro' version, but be unlimited on the number of access-controlled doors.

B. Overall Software capacity
    a. The software shall allow the configuration and control of all hardware components that make up the ACS. Hardware configuration shall not only be permissible on the access control server and should be possible from any client workstation.
    b. The software shall monitor and report access control events of the entire ACS. It shall be possible to view these events from any workstation if operator permissions allow.

c. The software shall allow for mobile credentials and biometrics directly from its own graphical user interface and not require any third-party software to run.
d. The software shall be capable of supporting at minimum 100,000 unique credentials and be able to manage and report on at minimum 1,000 access points.

C. The software shall provide the following feature set as a minimum:
a. Access Control
b. Mobile Phone Wallet Credential Integration
c. Web Browser Client Interface
d. Integration with Microsoft Entra ID
e. Biometric Integration
f. Time and Attendance
g. Intruder Alarm Inhibit Points
h. Fire Alarm Roll Call Reporting
i. Graphical Maps
j. Elevator Control
k. Email Notifications
l. 2-Tier Emergency Lockdown
m. Evacuation Roll Call
n. Card Designer
o. Reader Monitoring Points
p. Customisable Events and Actions
q. Timesheet reporting
r. Anti-passback
s. Support for multiple facility codes and HID card formats
t. Support for a credential enrolment reader

D. The Server and Client Graphical User Interface (GUI) shall be identical.
a. The client interface should allow the ability to maintain and extend the access control system without the need for accessing the Server.

E. Operating System
a. The Server software at a minimum shall be supported on the following operating systems:
i. Windows 11
ii. Windows Server 2022
iii. Windows Server 2025

F. PC Specifications
a. The PC running the Server software shall be able to be operated with the following, or grater, performance specifications:
i. Memory Size: 8GB
ii. Hard Disk Free Space: 100GB
iii. Display: 1024 x 800
iv. 10/100 Network Card
v. Processor: Intel i5 or equivalent
b. One PC running the server software shall be required per system.
c. There shall be no limit on the number of PC that can run the Client software.
d. There shall be no limit on the number of devices connecting using the Web Client interface.

5. Performance Requirements

A. The Server software shall create and maintain a single set of databases for access-control, credential creation and logging of all access and system events.

B. Any changes made to the database shall be automatically communicated to the access control hardware:
    a. When hardware is online, updates shall be communicated with appropriate changes to take effect in a timely manner.
    b. When hardware is offline, updates will be polled and communicated when the hardware is next online.
C. Distributed Intelligence
    a. The system shall be a fully distributed processing system so that all information is downloaded to the ACU's in such a manner that the ACU makes the decision for its location.
    b. The intelligence must be distributed to each ACU allowing ACU's to make access control decisions for one another across the whole system, and never reliant on the access control server to make decisions.
    c. ACU's must be capable of a peer-to-peer communication approach allowing for Events and Actions to be performed without the need of the Access Control Server.
    d. If communication with the Access Control Server is lost, all ACU's shall automatically buffer transactions until communications are restored, at which time the events will be uploaded automatically to the Access Control Server.
D. System Capacity:
    a. The system shall support at a minimum:
        i. 1,000 controlled access points
        ii. 100,000 unique credentials
        iii. 10,000 individual access levels
        iv. 64 Time Schedules with 3 individual time segments each
E. System Network Requirements
    a. Client PCs shall communicate with the Server PC via TCP/IP on either a LAN or WAN.
        i. System events recorded at the Server shall be communicated to the Client PC's
        ii. Changes made by the Client PC's shall be communicated to the Server and logged to the individual Client PC and Operator.
    b. The system shall utilise standard networking protocols to allow installation on corporate infrastructure.
    c. The ACU's are recommended to have an unique Static IP Address on the network, however DHCP shall also be supported.

6. Quality Assurance

A. All equipment shall be covered by a manufacturer's warranty period for a minimum of 2 years. The following aspects shall be covered:
    a. Electrical
    b. Electronic
    c. Component
    d. Mechanical
B. All components shall receive firmware updates from the manufacturer free of charge.

7. General Requirements for Communications

A. ACU to Server
    a. The "master" ACU shall communicate with the Server using TCP/IP
    b. The ACU shall be addressable using:

i. Static IP
ii. DHCP with MAC Address binding

c. At minimum, 100 Mbps Ethernet network speed shall be supported
d. The network connection between the ACU and the Server shall be encrypted.

B. ACU to ACU
a. System expansion between ACU's shall be supported using RS-485 to daisy chain downstream ACU's to a Master ACU. The following cable shall be used:
i. Belden 8723
ii. 2 x Twisted Pair with individual paired screens
iii. Maximum length 1000m (3000')
iv. CAT5, CAT5e, or CAT6 shall not be used.
b. Each RS-485 data bus shall support a minimum of 16 ACU's

C. ACU to Reader
a. Communication between the reader and the ACU shall support Wiegand or OSDP
b. Readers shall be wired for Wiegand communication over the following or technical equivalent cable:
i. Belden 9538
1. 8 Core Screened Cable
2. 24 AWG
3. Maximum Length: 80m (270')
c. Readers shall be wired for OSDP communication over the following or technical equivalent cable:
i. Belden 8723
1. 2 x Twisted Pair with individual paired screens
2. Maximum length 1000m (3000') from start to end of the data bus.

Part 2 Products

1. Manufacturers

A. **{Delete if necessary}** Acceptable manufacturer: Controlsoft
a. Email Address:
i. [support@controlsoft.com]
b. Telephone Number:
i. {UK} [01451 844896]
ii. {US} [800-340-1407]
iii. {SA} [010 595 1266]

B. **{Delete if necessary}** Substitutions: Not permitted
C. All components of the ACS shall be supported by a single source manufacturer to assure compatibility of the system.
D. Components shall consist of:
a. Access Control Software.
b. Access Control Units.
c. Readers
d. Physical Tokens/credentials.
e. Mobile Phone credentials.
f. Power Supply Units

E. Substitution Limitations.
a. No Substitutions.

2. Specific Requirements for Tokens

A. The manufacturer of the ACS shall be able to supply and support encoded smart cards which are equal to industry standard DesFIRE EV3 or HID SEOS.
   a. The supplied tokens shall contain authentication methods to deter from copying and unauthorised use of tokens.

B. The manufacturer of the ACS shall be able to supply and support Mobile Phone credentials which are stored within the Mobile Phones Wallet and use NFC to communicate with the reader. The Mobile Phone Credential shall use encryption keys to allow for the use of multiple credentials from the same Mobile Phone device.

3. Specific Requirements for Access Control Units

A. Features
   a. The ACU shall store its database locally and work independently from the Access Control Server.
   b. The ACU shall be capable of making all access control decisions locally.
   c. ACU's shall be capable of communicating with other ACU's on the network using peer-to-peer communication to allow for Events and Actions across the network and independent from the Access Control Server.
   d. The ACU shall allow for monitoring of all door components, including Door Position and Emergency Break Glass monitoring.
   e. The ACU shall be capable of supporting a combination of at least the following:
      i. Proximity readers
      ii. Keypads
      iii. Fingerprint Readers
      iv. Facial Recognition Readers
      v. Dual / Triple Authentication readers.
   f. The ACU shall support up to 100,000 unique card holders.
   g. The ACU shall retain all events data when there is no connection to the Access Control Server. Upon reinstatement the ACU must automatically upload the retained logs to the Access Control Server.
   h. The ACU shall be able to automatically unlock doors on a specified time periods.
   i. The ACU must support a 2-Tier Lockdown system.
   j. The ACU must employ non-volatile memory to retain memory on power loss.
   k. The ACU must employ AES-256 Bit encryption from Server to ACU.
   l. The ACU shall include removable connectors to provide ease of installation and board exchange if required. The connection points should not require any special tools to terminate.

B. Ease of Installation and Fault Finding
   a. The ACU shall show clear representations for where to terminate the reader, exit devices, communications, power connections and monitoring inputs.
   b. The ACU shall include LED indications showing, output relay status', input status', TCP/IP communication status, RS-485 connection status and power status.

C. Communications
   a. The ACU shall include direct TCP/IP connection to the processor board. Add-on modules are not approved.
   b. In addition to TCP/IP, the ACU shall include RS-485 communications for system expansion.
      i. The following data cable shall be supported:
         1. Belden 8723

ii. The maximum data cable length shall not exceed 1,000m (3,280') from first to last controller
iii. A single ACU, shall support at least 15 ACU's connected on RS-485.

c. The ACU shall support the connection of readers using either:
i. Wiegand
ii. OSDP

d. The following cable types shall be supported:
i. Wiegand: Belden 9538
ii. OSDP: Belden 8723

D. Peripherals
a. The ACU shall provide minimum support for 2 readers, either for readers in and out on 1 door, or reader in and reader out for 2 doors.
b. The reader peripheral shall output current states relevant to the appliance to control for supplying feedback to the token holder in the form of an LED and speaker.
c. The reader peripheral shall provide a voltage of 12V DC to power the reader.

E. Outputs
a. The ACU shall provide independent changeover relay channels.
b. The ACU shall provide a minimum of 2 relays.
c. Each relay shall be provided with normally open and normally closed channels to support both fail safe and fail secure locking mechanisms.
d. Relay contacts shall be voltage free.
e. Each relay shall be capable of switching a resistive load of at least 2A at 30V DC.
f. The ACU shall house a powered output for controlling locks.
i. The lock output should provide a minimum 1A at 12V DC.
g. The ACU shall be capable contain a Tamper monitoring input.
i. The tamper input shall be used to alert operators of unknown/impermissible access to the ACU.
h. The ACU shall contain a power supply unit failure input.
i. The power supply failure input shall be used to alert operators of an unplanned power failure.
i. The ACU shall contain a door monitoring / contact input.
i. The door monitoring input shall be used to alerts operators when a door is forced open.
ii. The door monitoring input shall be used to alert operators when a door is left open after a set time period.
j. The ACU shall contain a emergency break glass / release input.
i. The emergency break glass / release input shall be used to alert operators when an emergency release has been used to unlock a door.
k. The ACU shall contain an exit button input.
i. The exit button input shall switch the relay for a set time.

F. Power Supply
a. It shall be possible to power the ACU with a 12V DC Power Supply source.
b. The ACU shall have a maximum power usage of 200mA at 12V.

G. Temperature
a. The ACU shall meet the required temperature standards for an internal product.
i. The ACU shall operate reliably within the temperature range of 0°C to 55°C (32°F to 131°F)

H. Housing
a. The ACU shall be available in a metal housing for the ACU and power supply unit.

b. The housing shall be:
    i. Wall mountable
    ii. Lockable
    iii. White

I. Dimensions
a. The dimensions of the ACU shall not exceed:
    i. Width x Height: 175mm (6.9”) x 138mm (5.4 inches)
    ii. Depth: 25mm (1 Inch)

4. Specific Requirements for Power Supply Unit (PSU)

A. Features
a. PSU voltage shall be correct for all ACS hardware requiring an external DC power source.
    i. Output voltage shall be 12V DC (+/- 10&)
    ii. Output current ripple shall not exceed 100mV
b. The PSU shall be capable of providing a minimum of 2A.
c. The PSU shall be capable of powering at least the ACU, 2 x Readers, 1 x Lock.
d. The PSU shall allow connection to a 12V / 7Ah backup battery.
    i. The PSU shall trickle charge the connected battery to keep it continuously charge at its maximum capacity.

B. Power Supply
a. The PSU shall operate from either Main Supply or POE.
    i. Mains Supply:
        1. 100-240V ac
        2. 50-60Hz
    ii. POE:
        1. PoE++ (PoE 802.3bt) 60W

C. Display
a. An LED shall indicate when the PSU’s supply voltage is applied.
b. An LED shall indicate when the PSU is in a fault status

D. Peripherals
a. The PSU shall provide a supply voltage fault output.
b. The PSU shall provide a battery fault output.

E. Temperature
a. The PSU shall operate at -10 to +40°C at 75% RH non-condensing

5. Specific Requirements for IOC

A. Features
a. The ACS shall include support for input/output boards designed to monitor auxiliary inputs and provide relay outputs for control of external control devices.
b. The IOC shall support a minimum of 8 inputs and 8 outputs.
c. It shall be possible to use the input status from the I/O board to trigger actions in the ACS via Events and Actions.
d. It shall be possible to the trigger the IOC’s relays via Events and Actions within the ACS.
e. The ACU shall include removable connectors to provide ease of installation and board exchange if required. The connection points should not require any special tools to terminate.

B. Ease of Installation and Fault Finding

a. The IOC shall include LED indications showing, output relay status', input status', status, RS-485 connection status and power status.

C. Power supply
   a. The IOC shall be powered from a 12V, 2A Power Supply Unit (PSU)
   b. Power usage shall not exceed 400mA when all relays are energised.

D. Display
   a. Peripherals shall be labelled clearly and intuitively.
   b. The item shall house LEDs for fault finding.

E. Communications
   a. The IOC shall communicate using RS-485 to the Master ACU.

F. Peripherals
   a. The I/O board shall house 8 digital inputs.
   b. The IOC shall house 8 independently controllable relays.
   c. Each relay shall be provided with COM, N.O. and N.C. contacts.
   d. Relay contacts shall be voltage free.
   e. Each relay shall be capable of switching a resistive load of at least:
      i. 2A @ 30V DC
      ii. The relay functionality shall be configurable in the access control software provided with the ACS.

G. Temperature.
   a. The item shall operate reliably within the temperature range of 0°C to 55°C (32°F to 131°F)

H. Housing
   a. The ACU shall be available in a metal housing for the ACU and power supply unit.
   b. The housing shall be:
      i. Wall mountable
      ii. Lockable
      iii. White

I. Dimensions
   a. The dimensions of the IOC shall not exceed:
      i. Width x Height: 175mm (6.9") x 138mm (5.4 inches)
      ii. Depth: 25mm (1 Inch)

6. General Requirements for Software

A. The software shall use familiar style user interface, enabling intuitive use.
B. The software should utilise Microsoft SQL Server for its database engine.
   a. The software shall include a copy of Microsoft SQL Server Express
   b. It should be possible to utilise a centralised Microsoft SQL Server on a centralised database server.
C. The software shall be capable of importing end exporting user data in .csv and .txt formats.
D. The software shall allow for support on multiple workstations at no extra cost.
E. Access Permissions
   a. Access Groups shall be used to administer who is permitted through what access points and at what time they are permitted on a minute by minute basis.
   b. It shall be possible to allow users to be provided multiple Acces Groups to allow for easier system expansion.
   c. Access Groups shall be permitted extra time at the door if required to aid less abled individuals.
F. Mobile Phone Credentials

a. The software must natively support mobile phone credentials without the need of any third-party applications
b. The software must support issuing Mobile Phone credentials into the users mobile phone wallet not requiring a third-party application to run.

G. Reporting
   a. Access and system events shall be viewable in real time.
   b. System events and access events shall be segregated for quicker reporting purposes.
   c. Reports shall be configured within the access control user software and not a third-party application. A simple wizard shall be used to make configuring and saving reports as simple as possible for the user.
   d. Reports shall be customisable. They shall allow for selection of date, time, users or user groups and access points.

H. Users
   a. The system shall be capable of supporting 100,000 unique token holders.
   b. The system shall be capable of supporting at least 6 tokens per user.
   c. Users License Plates, Fingerprints and Mobile Phone Credentials shall be stored and managed within the Users Profile.
   d. The system shall allow for customisable extra data fields of, Text, Photo, Number and Colour.

I. Companies and Departments
   a. The system shall allow for users to be groups into their Companies and Departments.
   b. Individual companies and/or departments shall be selectable when reporting.

J. Operators
   a. Any user may be given operator rights that allow them to log onto the software and administer the system.
   b. A minimum of 50 operators shall be supported.
   c. The system shall provide operator groups, allowing for restrictions of operator privileges to certain areas on a group basis.
   d. The system shall allow for operators to be permitted or restricted from using the Web Client on an Operator Group basis.

K. Card Design & Printing
   a. The software shall include an optional integrated card designer application for the customisation and printing of ID Cards via the software user interface.
   b. The card designer program shall allow for unlimited card designs.
   c. The designer shall support static text, shapes, and colours.
   d. The designer shall support automatically generated text based on information entered into the user record.
   e. The card designer shall support bar code and QR codes for printing onto the ID card.
   f. The card designer shall support CR80 size ID cards.
   g. The card designer shall support single- and double-sided card prints.
   h. The card designer shall have the ability to print cards use a standard Windows card printer and not be manufacturer specific.

L. Access Control Alarms
   a. The software shall be capable of reporting alarms within an Alarm viewer and within the systems log, the following alarms shall be supported as a minimum:
      i. Door forced open
      ii. Door left open
      iii. Break Glass Operated
      iv. Power Supply Failure

v. Battery Fault
vi. Mains Failure
vii. Hardware Tamper

b. Each alarm event shall be reported in the systems log.
c. The Alarm Viewer should allow for operator to acknowledge and clear the alarm, also allowing the operator to add a message to when acknowledging.
d. The system shall support email notification of alarms.
e. Alarms shall be permitted to operate a local door sounder to notify nearby users of the alarm.
f. Data protection
    i. The system shall comply with the General Data Protection Regulation (GDPR) 2018.
    ii. It shall be possible to permanently delete:
    iii. A user, their events and activity.
    iv. A user but retain anonymised user events.
g. Events shall be automatically deleted after a user defined period of time.

7. Specific Requirements for basic 'Lite' Software

A. The manufacturer shall provide a 'Lite' version of software.
B. The software shall be free of charge.
C. The manufacturer shall provide updates free of charge.
D. The software shall offer all features required to manage a basic access control system.
E. As a minimum, the 'Lite' software shall provide the following features:
    a. Access Control
        i. The system shall manage a minimum of 100,000 unique token holders.
        ii. The software shall manage a minimum of 6 doors with 12 access readers or 12 doors with 12 access readers.
    b. Access Levels
        i. The software shall provide support for up to 256 access groups.
        ii. Each access group shall include a combination of access points.
        iii. Each access group can be defined a time zone to only permit users within the group access during specific time periods.
    c. Time Zones
        i. The software shall provide a minimum of 64 separate time schedules (zones) with each schedule allowing for 3 separate time segments.
        ii. Time Zones can be applied to:
            1. Doors: Allowing for Door Open Schedules
            2. Groups: Restricting users access permissions at certain times
            3. Readers: Restricting the use of readers at certain times.
    d. Users
        i. Disabling a user without the need to delete the user altogether.
        ii. Integrated photo to provide user verification.
        iii. Customizable Extra Data Fields
        iv. Selectable Facility Codes
        v. Valid From, Valid for and Valid To fields to allow for automatic user expiry.
        vi. Assignment of 6 unique tokens per user.
        vii. Automatic Employee Number Field
        viii. Manual Employee Number Field
        ix. Capacity to run a individual user report with a single command.

x. Emergency information including:
    1. Address
    2. Town
    3. County
    4. Postal Code
    5. Home telephone number
    6. Home fax number
    7. Cell phone number
    8. Email address

xi. Last known location including location, date, time and event.

xii. Identify token button to allow for token search.

e. Component Configuration
    i. It shall be possible to view the ACU's:
        1. IP Address
        2. RS-485 Status
        3. Firmware Version
        4. MAC Address
        5. Status (online/offline)
        6. Controller Type
    ii. Doors
        1. Lock unlock time selectable from 1 to at least 1800 Seconds
        2. Lock should be configurable as pulsed (defined time period) or latched (badge to unlock, badge to lock)
        3. Allow a lock to immediately re-activate once a door has been physically opened.
        4. Automatic Door Open Schedule (Time Zone)
        5. Sound local alarm under the following conditions:
            a. Door is forced open
            b. Door is held open after a set time period
            c. Breakglass is activated
    iii. Readers
        1. Allow readers to operate in Token Only or Token + PIN mode.
        2. Allow for Token + PIN to be required at set times.
        3. Shall allow for intruder alarm inhibiting points to disable the reader when the intruder alarm is set and enable when set.

f. Remote Door Management
    i. The system shall allow for doors to be remotely unlocked for their set time period (grant access)
    ii. The system shall allow for doors to be remotely unlocked indefinitely (remote release)
    iii. The system shall allow for doors to be remotely reset to relock the doors.

g. Photographic Identification
    i. Any reader can be selected to monitor the users' photos when activated.
    ii. A minimum of 2 readers can be monitored at any time.
    iii. The event message shall be displayed within the User Image window.

h. Bulk Enrolment
    i. The system shall allow for bulk enrolment of user's token numbers for easier commissioning and system handover.

8. Specific requirements for advanced 'Pro' and 'Enterprise' Software

A. The manufacturer shall provide a 'Pro' and 'Enterprise' version of software with an advanced feature set.
B. The software shall be field upgradable from the 'Lite' version using a License Key.
C. The software shall offer all the features of the 'Lite' Software.
D. At minimum the 'Pro' software shall provide the following features:
    a. Anti-Passback
        i. The software shall provide the functionality of denying a user repeat access into or out of the defined site.
        ii. Anti-Passback will be global for the defined 'site', any readers marked as an on-site or off-site reader for anti-passback will deploy the global anti-passback rule.
        iii. Readers shall be required on both sides of the access point that is expected to employ anti-passback.
        iv. It shall be possible to mark certain access groups to override the anti-passback rule.
    b. Time and attendance
        i. Any access point can monitor time and attendance of staff; the readers are defined as an on-site T&A reader or an off-site T&A reader.
        ii. The software shall produce reports showing the total number of hours on site, and shift reports.
        iii. It shall be possible to ignore certain time periods on the Time and Attendance report where people may be temporally leaving site.
    c. Lockdown
        i. The software shall provide the functionality of a two-tier lockdown. Designed but customisable for the following:
            1. Tier 1:
                a. All doors within the Lockdown lock.
                b. Override users can still access locked down doors however it is noted in the log that this is an exception. This is to aid reviewing the threat.
            2. Tier 2:
                a. Override users now are unable to access locked down doors.
                b. Request to Exit Buttons stop operating
        ii. The Lockdown procedure shall allow for doors to be omitted from either Level 1 or Level 2 lockdown.
        iii. Lockdown should only be reset by an operator in the software or web client.
        iv. To activate lockdown there should be no requirement for the access control server to be online, controller must communicate the lockdown status via a peer-to-peer communication approach.
    d. Roll Call
        i. The software shall be able to generate a roll call report. The roll call report shall be generated manually via the software or automatically via a direct input from a fire alarm panel.
        ii. The roll call report shall document, users name, department, last known location, users contact number.
        iii. If automatically ran, the roll call report will have the option to be:
            1. Printed to a defined printer.
            2. Emailed to designated email addresses.
    e. Web Client

i. The system shall be able to be remotely accessed using a Web Browser Client at no extra cost.
ii. The Web Client should provide the following features as a minimum:
    1. Provide the ability for Multi-Factor Authentication (MFA) for operator login.
    2. Remote administration of users.
        a. It shall be possible to add a new system user, including capturing their photo and issuing mobile phone credentials.
        b. It shall be possible to disable / bar a user from access.
        c. It shall be possible to edit a current user, including increasing their access group permissions.
    3. Remotely open and close doors.
        a. It shall be possible to perform a one-time grant access command to a door.
        b. It shall be possible to perform a remote open and close command to permanently open or reset the door.
    4. Live Event Reporting with filtering.
        a. It shall be possible to see all live events from the ACS. These events will automatically refresh at a configurable rate.
        b. It shall be possible to filter the events down by:
            i. User Details
            ii. Event Result
            iii. Event Reasons
            iv. Date/Time
        c. All access control events should be available for reporting via the Web Client.
    5. Live Roll Call report showing all users that are currently on site.
    6. Remote initiation and reset of system Lockdown status.
iii. The Web Client should be available to all Operators of the ACS but is defined by the operators' permissions to deny access remotely for certain operators.

f. Events & Actions
    i. An event (a system event that can cause an action within the ACS) can be actioned by a minimum of the following:
        1. A certain user is granted access at a door
        2. A certain user is denied access at a door
        3. A member of a specific group has access or denied access at any / a certain door.
        4. Exit button is pressed
        5. Door is Forced Open
        6. Door is Left Open
        7. Door is opened.
        8. A defined digital input is triggered or reset.
        9. A controller goes online or offline
        10. Fire alarm input is activated
        11. When a time zone becomes active or inactive
        12. When a lockdown is activated or deactivated
        13. A battery, mains fail or PSU failure is detected.
        14. A tamper input is detected.
    ii. An action can be any of the following:

1. Send an defined email notification.
2. Activate a WAV sound file.
3. Control system lockdown
4. Enable / Disable Pushbutton Inputs
5. Enable / Disable Readers
6. Open / Close a Door
7. Enable / Disable a Time Zone.
8. Increase / Decrease a system counter.
9. Start / Stop / Reset a Timer.

iii. Camera Integration

1. It shall be possible to connect a CCTV camera into the software.
2. The CCTV camera can be viewable within the software's user interface.
3. The CCTV camera can be used to snapshot certain system events to aid investigation

iv. Graphic floor plans / site graphics

1. The ACS Dashboard shall include the option of including a visual representation of the managed site, and the status of various elements of the ACS.
2. The software shall allow for multiple interactive site graphics to be imported by .jpg, .png, .bmp format.
3. There shall be no practical limit to the number of maps/plans on the system.
4. The objects that can appear shall include, but not be limited to:
    a. Controllers.
    b. Doors.
    c. Readers.
    d. Inputs.
    e. Outputs.
    f. Custom Objects, including Images, Rectangles, Ellipses, Lines and text Boxes.
5. The site graphics shall show the live status of doors including door open/closed, door left open and door forced open.
6. The site graphics shall show the live status of the readers, including access denied, access granted.
7. It shall be possible to interact with the site graphics, to open/close doors.

v. Elevator Control

1. An access control reader shall be able to call an elevator, and if necessary, provide the user with access to only certain floors.
2. Integration shall be achieved with the use of IOCs due to the number of relays required.
3. Floor access is to be provided against the user's access group permissions.
4. It shall be possible to incorporate elevators with Time zones, so at certain times of the day the elevator is on free access.

9. Specific Requirements for Mobile Phone Wallet Credentials

A. Features

a. The Access Control System (ACS) shall natively support mobile phone credentials stored within the user's digital wallet, without requiring a separate third-party application to be running.
b. Mobile phone credentials shall provide a secure digital alternative to physical access control cards and key fobs.
c. Mobile phone credentials shall utilise Near Field Communication (NFC) to communicate with compatible access control readers.
d. Each mobile phone credential shall be uniquely associated with an authorised user within the ACS.
e. Mobile phone credentials shall be managed directly through the ACS software, allowing operators to issue, assign and revoke credentials against individual user profiles.
f. The system shall support the assignment of a mobile phone credential and a wearable credential to a single user, where required.

B. Security
a. Mobile phone credentials shall utilise encrypted authentication mechanisms to protect against credential copying and unauthorised use.
b. The credential technology shall support the use of multiple credentials on the same mobile phone device, using appropriate encryption keys to maintain credential security and separation.
c. Mobile phone credentials shall be subject to the same access permissions, access groups and time schedules configured within the ACS as other supported credentials.
d. Revocation or disabling of a mobile phone credential within the ACS shall prevent subsequent access using that credential, in accordance with the system's credential update and communication procedures.
e. Revocation or disabling of the credential from the users mobile phone shall be updates within the ACS software.

C. Credential Management
a. Mobile phone credentials shall be assignable to users through the ACS user management interface.
b. The ACS shall maintain mobile phone credential information within the relevant user profile.
c. It shall be possible for authorised operators to manage mobile phone credentials without requiring separate third-party credential management software.
d. The system shall support the administration of mobile phone credentials through the Access Control Web Client, where this functionality is available.

10. Specific Requirements for Access Control Readers

A. Features
a. The reader shall support the identification and authentication of users at controlled access points using compatible physical or mobile phone credential.
b. The reader shall support multiple credential technologies, including smart cards and mobile phone credentials.
c. The reader shall provide visual and audible feedback to users following the presentation of a credential.

B. Communications

a. The reader shall communicate with the Access Control Unit (ACU) using Wiegand or Open Supervised Device Protocol (OSDP).
b. Where OSDP is utilised, the reader shall support bidirectional communication with the ACU.
c. The reader shall integrate with the Access Control System (ACS) to enable the validation of presented credentials against the access permissions assigned to the relevant user.
d. The reader shall operate as part of the ACS without requiring separate access control management software.

C. Security
   a. The reader shall support secure credential technologies incorporating cryptographic authentication, where supported by the credential type.
   b. The reader shall support secure reader-to-controller communication where compatible with the reader and ACU.
   c. The reader shall support appropriate configuration of credential technologies to meet the security requirements of the installation.

D. At a minimum, the following token technologies shall be supported:
   a. Mobile Credentials via NFC.
   b. HID® SEOS®
   c. HID® iClass SE®
   d. HID® iClass
   e. Mifare® Classic and DESFire® encoded with HID Secure Identity Object

E. Power Supply
   a. The reader shall be powered by 12V DC.

F. Temperature and Moisture
   a. The reader shall meet the required temperature standards for an internal use product
   b. The reader shall operate reliably within temperature range of -30°C to 66°C (-31°F to 150°F).
   c. The reader shall have a moisture rating of at least IP65 and be rated for Outdoor and Indoor use.

11. Specific Requirements for Wireless Devices

A. Features
   a. The ACS shall support wireless access control devices for the electronic locking and management of doors without requiring a traditional wired connection to each locking device.
   b. Wireless access devices shall be suitable for installation on compatible doors where conventional wired access control is impractical or cost prohibitive.
   c. The system shall support compatible wireless locking devices, including electronic cylinders, escutcheons, electronic handles and complete electronic locks, as appropriate to the installation.
   d. Wireless access devices shall be battery-powered where specified by the selected device.

B. At a minimum, the following token technologies shall be supported:
   a. Mobile Credentials via NFC.
   b. HID® SEOS®
   c. HID® iClass SE®
   d. HID® iClass
   e. Mifare® Classic and DESFire® encoded with HID Secure Identity Object

C. Access Control and Monitoring
    a. Wireless access devices shall operate in accordance with the access permissions assigned to users within the ACS.
    b. The Wireless devices shall support the assignment of access groups and time schedules to users accessing doors fitted with compatible wireless devices.
    c. The ACS shall record access granted and access denied events for reporting and audit purposes.
    d. The ACS shall provide visibility of device status and relevant access events through the ACS interface.
    e. The ACS shall provide notification of low battery conditions to allow maintenance to be scheduled.

D. Installation and Maintenance
    a. Wireless access devices shall be installed in accordance with the manufacturer's published installation requirements and the door manufacturer's recommendations.
    b. The system shall support the addition of wireless access devices to an existing ACS without requiring all existing wired access control hardware to be replaced.
    c. Wireless access devices shall provide access to battery replacement and routine maintenance in accordance with the manufacturer's recommendations.
    d. The selected devices shall be suitable for the intended door type, locking application, security requirements and operating environment.

12. Specific Requirements for Desktop Reader

A. Features
    a. The desktop reader shall read multiple types and formats of proximity tokens.
    b. The desktop reader shall facilitate assigning tokens to users.
    c. The desktop reader shall identify tokens within the ACS that have already been assigned.
    d. The desktop reader should be compatible on any PC and act as a keyboard extension (keyboard wedge mode) and should not require any additional drivers to operate.
    e. The desktop reader shall have the ability to output token data in a variety of formats and lengths.
    f. Proximity reader
        i. The item shall contain a proximity reader:
            1. At a minimum, the following token technologies shall be supported:
                a. HID® SEOS®
                b. HID® iClass SE®
                c. HID® iClass®
                d. Mifare® Classic
                e. Mifare® DESFire® EV1 / EV2 / EV3
                f. Mifare® Classic and DESFire® encoded with HID Secure Identity Object
            2. All the above technologies shall be supported concurrently.
        ii. Power Supply
            1. The desktop reader shall be powered via USB
            2. Maximum current consumption while in use shall not exceed 100mA.
        iii. Communication
            1. The desktop reader shall connect to a PC running the Server, Client or Web Client software via a USB port.
        iv. Display
            1. The desktop reader shall house a LED indication.

2. The LED shall indicate the following states:
    a. Device is powered on.
    b. Credential is read.

v. Temperature
    1. The item shall meet the required temperature standards for an internal use product
        a. The item shall operate reliably within temperature range of 0°C to 55°C (32°F to 131°F).