

DEPARTMENT OF TRADE AND INDUSTRY - ISMS SPECIFICATION

PREPARED BY : Steyn De Lange

DATE : 04 September 2025

TABLE OF CONTENTS

1.	GENERAL	3
2.	RESPONSE FORMAT	3
3.	PRODUCT ACCEPTANCE.....	4
4.	FUNCTIONAL OVERVIEW.....	4
5.	LICENSING	7
6.	SYSTEM REQUIREMENTS.....	7
7.	SYSTEM SERVERS AND WORKSTATION INSTALLATION.....	8
8.	CENTRAL CONTROL AND SYTEM MANAGEMENT SOFTWARE.....	9
9.	COMMUNICATIONS AND DIAGNOSTICS	12
10.	CYBERSECURITY	13
11.	MULTIPLE SERVER CONNECTIVITY	13
12.	GRAPHICAL OPERATOR INTERFACE	14
13.	SYTEM OPERATOR MANAGEMENT	17
14.	CARDHOLDER MANAGEMENT	18
15.	PHOTO BAGDING AND IMAGE MANAGEMENT	21
16.	INTRUDER ALARM SYSTEM.....	23
17.	ALARM MANAGEMENT	25
18.	CLASS 5 ALARM SYSTEM	29
19.	ACCESS CONTROL.....	30
20.	PERSONNEL IDENTIFICATION VERIFICATION	34
21.	SITE PLANS.....	35
22.	GUARD TOURS.....	37
23.	REPORTS.....	39
24.	NOTIFICATIONS.....	42
25.	BULK NOTIFICATIONS.....	42
26.	AUDIT TRAIL	42
27.	MOBILE DEVICE APPLICATION	43
28.	COMPETENCIES.....	47
29.	RANDOM SELECTION.....	48
30.	ELEVATOR CONTROL AND MANAGEMENT	48
31.	CAR PARKING	50
32.	LOCKER SYSTEM.....	51
33.	PRE-PROGRAMMED OVERRIDE MACROS	51
34.	VISITOR MANAGEMENT KIOSK.....	52
35.	DOOR FUNCTIONALITY – CONNECTED TO CONTROLLER.....	54
36.	DOOR FUNCTIONALITY – DATA ON CARD.....	56
37.	DOOR FUNCTIONALITY – WIRELESS CONNECTIVITY.....	58
38.	FIELD HARDWARE – INTELLIGENT FIELD CONTROLLER (IFC).....	59
39.	ENCRYPTED END OF LINE DEVICE – CLASS 5.....	65
40.	ENCRYPTED END OF LINE DEVICES	66
41.	ACCESS CONTROL READERS – MIFARE TECHNOLOGY.....	67
42.	ACCESS CONTROL READERS – MULTI TECHNOLOGY	71

43.	ACCESS CONTROL READERS – LONG RANGE.....	75
44.	READER – BLUETOOTH AND NFC	75
45.	ACCESS CONTROL READERS – BIOMETRIC (FINGERPRINT).....	77
46.	ACCESS CONTROL READERS – BIOMETRIC (CONTACTLESS).....	78
47.	ALARM MANAGEMENT TERMINAL – ACCESS CONTROL.....	79
48.	ALARM MANAGEMENT TERMINAL – PERIMETER.....	81
49.	ACCESS CARDS AND TOKENS.....	83
50.	TOKEN – MIFARE CLASSIC TECHNOLOGY	84
51.	TOKEN – MIFARE PLUS TECHNOLOGY	85
52.	TOKEN – MIFARE DESFIRE TECHNOLOGY	85
53.	CREDENTIAL – BLUETOOTH AND NFC ON MOBILE DEVICE	86
54.	CREDENTIAL - BIOMETRIC.....	87
55.	RS485 FIBRE TRANSCEIVER REQUIREMENTS.....	88
56.	ENERGISED PERIMETER INTRUDER DETECTION - STRUCTURE.....	89
57.	ENERGISED SECURITY FENCE CONTROLLER – STAND ALONE	93
58.	ENERGISED SECURITY FENCE CONTROLLER - NETWORKED.....	95
59.	SYSTEM INTEGRATION.....	97
60.	VIDEO MANAGEMENT SYSTEM INTEGRATION.....	100
61.	REST API.....	101

1. GENERAL

This specification calls for the supply, installation, and commissioning of a complete ISMS in accordance with appropriate local and international standards and the technical and performance criteria set out in this document.

The system is to be supplied with all equipment, hardware, software, cabling, and ancillary services as required to provide an ISMS complete and functional in all respects. The tenderers are to familiarise themselves with all matters related to such requirements and to account for such in the tendered price.

Other security system components not included in this specification shall be fully integrated with this ISMS.

It is the responsibility of the tenderer to obtain clarification of all matters in which doubt exists as to the exact intent of this document or in which a conflict appears to have arisen. Such information must be obtained prior to the closing and lodging of tenders.

The response shall clearly detail all pricing for components, cabling, installation, training, commissioning, setting to work, and a 24-month comprehensive warranty.

The tenderer must include as part of the tender submission a complete, clause-by-clause response.

2. RESPONSE FORMAT

The tenderer shall respond to each clause with one of the following responses.

Should the tenderer wish to clarify or amplify the response, then the clarification or amplification shall not change the given meaning of the response statement.

Response	Meaning
Complies	The equipment/system offered complies fully in all respects with the specification clause.
Substantially complies	The equipment/system offered does not comply fully but offers most or a substantial part of the requirements of the particular clause. Compliance in excess of 75% of the requirement qualifies for this category. Areas of non-compliance must be clearly identified and explained.
Partially complies	The equipment/system offered provides only a part of the requirements of the clause. Less than 75% compliance with the clause should invoke this response. Areas of non-compliance must be clearly identified and explained.
Does not comply	The equipment/system offered does not provide the requirements of the particular clause.
Accepted	The tenderer understands and accepts the conditions imposed or enunciated by the particular clause and has included provision for such in the tender.
Not accepted	The tenderer does not accept the condition imposed by the particular clause and as such is not included in the tender. Reasons for non-acceptance must be given.

3. PRODUCT ACCEPTANCE

The successful tenderer will be required to demonstrate their competence to supply, install, commission, and maintain the products proposed in the tender submission as follows:

- Provide a letter of reference from the product manufacturers confirming the tenderer's status with the manufacturer, advising:
 - exclusive or non-exclusive agreement to provide the system in the geographical territory for this specific project,
 - the tenderer will be fully supported by the manufacturer in meeting the requirements of this specification.

The tenderer shall provide evidence of competency in carrying out the following areas of work:

- installation management,
- system configuration,
- system commissioning,
- system maintenance.

When working on the installation of the ISMS, each employee of the successful tenderer shall be required to carry an identification card issued by product manufacturers and/or government accredited bodies displaying evidence of current training, the type of products they may install, and indicating the level of training.

4. FUNCTIONAL OVERVIEW

The ISMS shall allow multi-site configuration and be able to be managed by one or more of the connected sites.

The ISMS shall include in the core product code (but not be limited to) the following:

- access control,
- alarm management,
- personnel management,
- CCTV integration,
- visitor management,
- guard tours,
- perimeter deterrent and detection.
- Time and attendance

-
- Fire detection systems
 - PA/EVAC systems
 - Generator and UPS/Invertor monitoring and control

The ISMS 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. All validity criteria shall be stored at the IFC. Access shall be granted or denied dependent on the access privilege. Access privileges shall be programmed in a variety of ways to allow flexibility as defined elsewhere in this specification.

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

The ISMS shall monitor the condition of inputs. The ISMS 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.

The ISMS 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 ISMS 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, AMT, or as required from defined central control locations.

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

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

The ISMS shall have IPv6 address support for all TCP/IP network devices.

IFCs must support peer to peer communications for input and output communications between IFCs. Systems that require a server for communications between panels are unacceptable.

All data communication between the ISMS and IFCs shall use an industry standard asymmetric encryption algorithm for mutual authentication and session key negotiation. This algorithm shall be equivalent to ECC P-384 or stronger. Session keys shall be re-negotiated on a regular basis at intervals no longer than 30 hours.

All data communication between the ISMS and IFCs shall be encrypted using an industry standard symmetric encryption algorithm equivalent to AES-256 or stronger.

All data communication between IFCs shall use an industry standard asymmetric encryption algorithm for mutual authentication and session key negotiation. This algorithm shall

be equivalent to ECC P-384 or stronger. Session keys shall be re-negotiated on a regular basis at intervals no longer than 30 hours.

All data communication between IFCs shall be encrypted using an industry standard symmetric encryption algorithm equivalent to AES-256 or stronger.

All data communication between IFCs and intelligent edge devices such as readers and I/O devices shall use an industry standard asymmetric encryption algorithm for mutual authentication and session key negotiation. This algorithm shall be equivalent to ECC P-256 or stronger. Session keys shall be re-negotiated on a regular basis at intervals no longer than 30 hours.

All data communication between IFCs and intelligent edge devices such as readers and I/O modules shall be encrypted using an industry standard symmetric encryption algorithm equivalent to AES-128 or stronger.

All dry contact type input to field I/O modules must support four state monitoring with the ability to configure the resistance values of the state changes.

The ISMS 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.

The ISMS 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, emailed reports directly from the ISMS itself, screen displays, or exported files.

The ISMS shall provide for a GUI with site plans and interactive icons representing the location and real-time status of all monitored hardware within the ISMS.

The ISMS shall provide emergency evacuation reporting.

The ISMS shall be designed and manufactured by a company who shall be certified under the ISO 9001:2008 (or later) quality procedures.

Where applicable, equipment shall have the following approvals:

- FCC Part 15,
- CE approval BS EN 50130-4 Alarm Systems Electromagnetic Compatibility (Immunity),
- CE approval BS EN 55022 Emissions,
- UL294 Access Control,
- UL1076 Burglar Alarms,
- ULC-ORD-C1076.

Encoders and readers shall also meet:

CE ETS 300 683 Short Range Devices,

C-Tick AS/NZS 4251 Generic Emission Standard,

C-Tick RFS29.

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

Comprehensive backup and archiving facilities shall be incorporated as an integral part of the ISMS.

The ISMS shall include partitioning suitable for multi-tenanted buildings. Users shall only be able to access those parts of the system which fall within their partition.

5. LICENSING

If system licensing is required, the license to use the system shall allow usage in perpetuity.

Details of the license model shall be provided in the tender response.

Licensing shall permit all operational requirements for a specific system. This shall include but not limited to:

- the live (operational) system,
- temporary test installations used for investigating configuration options or new software releases,
- secondary installations required for standby operation.

Updating of license content to make changes to the number of licensed items shall not require a server restart.

It is acceptable to require a restart to allow incorporating additional features to the license.

The license content shall be viewable from within the ISMS GUI.

6. SYSTEM REQUIREMENTS

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 shall be submitted with the tender response.

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

- Configured concurrent workstations 150
- Graphical site plans Unlimited
- Access readers Unlimited
- Elevators 1000 elevators of 256 levels each
- Fully supervised 6 state alarm inputs Unlimited

• Output relays	Unlimited
• Access control zones	Unlimited
• Schedules per day	100
• Schedule categories	50
• Holiday days	30
• Operators	Unlimited
• Concurrent operator sessions	100
• Cardholders	1,500,000
• Cardholder card issue levels	15
• Cardholder configurable data fields	>1000
• IFC	Unlimited

The system architecture shall be a tiered system consisting of:

- one installation of the head-end software application operating on a main server,
- operator workstations as a sub-set of the application installed on the server,
- IFCs managing the system in a distributed intelligence format,
- semi-intelligent sub-units (output modules, input modules, readers, etc) which rely on IFCs to function.

7. **SYSTEM SERVERS AND WORKSTATION INSTALLATION**

The server shall use a Microsoft Windows(64 bit) operating system. Server operating systems such as Linux, Unix, and OS X shall not be acceptable.

The operating system used by the system server shall be Microsoft Windows Server 2022.

The operating system used by the workstations shall be Microsoft Windows 10 Professional (64 bit) or Windows 11 Pro.

The database engine used by the system shall be one of the following:

- Microsoft SQL Server 2022, or
- Microsoft SQL Server 2022 Express.

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

Workstation display resolution shall be a minimum of 1920 x 1080 pixels.

Workstation shall be able to use up to 4Gb of RAM.

8. CENTRAL CONTROL AND SYTEM MANAGEMENT SOFTWARE

The ISMS servers shall use a Microsoft Windows operating system as defined previously.

The system database shall be a version of Microsoft SQL Server appropriate for the system size required. The version of Microsoft SQL Server is among those defined previously.

The connection between ISMS and Microsoft SQL Server shall use Windows Authentication.

The ISMS shall employ a server incorporating current generation design and components. The hardware specification, including processor speed, internal memory and hard disk size shall be specified by the supplier and must be sufficient to meet or exceed the capacity and throughput of the specified system.

The ISMS shall be capable of supporting configured concurrent Workstations. Workstations running terminal emulation software will not be accepted.

The ISMS 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.

The configuration GUI shall make extensive use of menus and windows and require a minimum of operator training to operate the system proficiently. Systems requiring a script/program language approach to configure the system will not be accepted.

A free text notes/memo field shall be available for each logical/physical object to store abstract information relating to that item.

- The notes field shall support 128,000 characters of text.
- The notes field shall support word-wrap, insert, delete, cut, copy and paste functions.

The ISMS must be capable of receiving simultaneous alarm signals from 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.

The ISMS shall be fitted with a real-time clock, the accuracy of which shall be preserved over the period of a mains power supply failure. Time synchronisation between the ISMS and Ethernet connected IFCs shall be automatic and not require operator intervention.

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

As a minimum the following operational and monitoring functions are required:

- program either a group or individual card readers with access control parameters, without affecting other card readers,
- program the access criteria for individual cardholders or groups of cardholders,

-
- store non access control data fields for each cardholder. The names of these data fields shall be user-definable,
 - authorise or de-authorise a cardholder in the system with the result reflected immediately throughout all access points in the system,
 - enable a card trace against selected cardholders so that an alarm is raised each time that cardholder presents their access card or token,
 - pre-program holidays so that different access criteria apply compared to normal scheduled days. The system must have a capacity to set at least 400 holiday days,
 - recognise and manage regional holiday requirements,
 - define as many access zones as there are card readers fitted,
 - allow or disallow individual cardholder access to any single, or group of card readers, in real-time,
 - log all ISMS and operator activity to hard disk as it is received at the ISMS server,
 - program alarm response instructions into the system so that these are presented to the operator when processing an alarm event,
 - enable an operator to enter messages against alarm events. This may be an enforced operator operation based on configuration on a per operator basis,
 - configure user-definable short messages to allow the operator to enter commonly used comments with minimal effort when entering messages related to alarms. For example, false alarm, user error, etc. These messages should also be assigned to keyboard shortcut keys to enable faster commenting on alarms,
 - temporarily override a cardholder, or group of cardholders, pre-programmed access criteria.
 - Update multiple AMTs display messages quickly using the bulk change feature

The operator GUI 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. The event message shall advise:

- the time of event created at the IFC,
- the time the event was received at the ISMS server,
- the source of the event,
- any successful or unsuccessful access attempt,
- if the access attempt is unsuccessful, the reasons for the denial.

This includes but is not restricted to the following items:

-
- all card attempts,
 - all door alarms,
 - all operator activity including logon, logoff, and alarm response messages,
 - all alarm monitoring activations,
 - all communication link failures.

Time schedules for different days shall be configurable.

Regional holidays shall be configurable to allow for regional variations.

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

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

- item characteristics,
- related items,
- times related to events including within properties of a configured item (creation and modification events).

The system shall integrate with Microsoft Active Directory enabling cardholder and user records to be fully synchronised on a real-time, bi-directional basis.

- Integrations that use third party applications to synchronise between Microsoft Active Directory and the system shall not be acceptable.

The system shall allow for a separate biometric operator privilege.

The system shall be able to find unmigrated and duplicate DesFire cardholder keys.

ISMS shall be able to purge pending queued messages from IFCs as required by the user with this privilege.

ISMS shall be able to deploy IFC firmware as follows via an upgrade tool.

On demand.

On a predetermined schedule.

ISMS shall allow the user to track IFC firmware deployments status via the upgrade tool.

ISMS shall allow users additional options to manage ISMS functions via a web-based client safely and securely. Options shall provide an alternative to using the client-based application for the following:

- View Cardholder's History and activities.
- Manage cards (excluding printing and encoding) and credentials.
- Add cardholders and assign to Access Group.
- Remove cardholders.

The ISMS shall incorporate utilities that:

-
- Allow the health and security of the system to be checked with exportable reports.
 - Provide functionality to run pre-upgrade checks that identify any compatibility issues prior to a software upgrade.

ISMS shall allow bulk site configuration to:

- Enable importing and exporting as .csv files, all configuration items currently supported including system devices and Access Groups.
- These shall be able to be modified and re-imported to the existing system or used to import to a new system.

ISMS shall allow for configuration and setup of a read-only replica SQL database in a highly available environment in order to reduce the load on the primary SQL database.

ISMS shall support the redaction of the following Personal Identifiable Information in order to meet GDPR requirements:

- Cardholder Events
- Cardholder Information
- System software installation shall support command-line silent installation.

ISMS shall support cardholder case and accent sensitive searches.

9. COMMUNICATIONS AND DIAGNOSTICS

The ISMS shall automatically restart full and complete processing after a power failure.

The ISMS shall provide a full diagnostic log to enable system engineers to monitor system operations in the event of a system malfunction.

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

The diagnostic log must be available without shutting down or pausing the ISMS.

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

ISMS shall be able to send the IFC its IP address

ISMS shall be able to accept requests from anywhere on the internet and connect these requests securely and easily to REST APIs hosted on an on-premise system using a web-socket tunnel between the ISMS and the API gateway.

API gateway shall have multiple redundant services internally allowing for zero-downtime upgrades, hardware and software fault tolerance and scalability.

API gateway shall use TLS client certificates for Rest API requests.

ISMS real-time data feeds shall integrate with Windows OS performance monitor

10. **CYBERSECURITY**

The ISMS manufacturer shall supply documentation detailing the cryptography used in the supplied products including:

- included digital certificates,
- database encryption,
- server to workstation connections,
- server to IFC connections,
- data at rest on IFC.

The ISMS manufacturer must provide proof of independent penetration testing for the release of software to be installed.

Vulnerabilities found in the ISMS software must be notified to customers via a CVE Entry for a minimum of two years after software release.

The ISMS manufacturer shall supply a software tool external to the ISMS server to test the installed server for vulnerabilities.

The system SMTP library shall support Microsoft office 365.

The system shall support a SQL Database monitor service which logs SQL Database login attempts.

Logins into the ISMS from the web-based client is secured with 2-factor authentication

The web-based client shall not store any sensitive data, data remains hosted on the customer's ISMS server.

11. **MULTIPLE SERVER CONNECTIVITY**

ISMS based on multiple servers shall be supported.

Each server shall communicate directly with its local IFCs.

Should a network failure occur between servers, each shall continue to communicate with their local IFCs.

Should a network failure occur between servers, operators shall be able to continue to manage the local system connected to their respective servers. This includes (but is not limited to) the following functions:

- manage alarms,
- override and manage doors,
- arm and disarm alarms,
- edit cardholders,

-
- run reports.

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

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

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

Communication between servers shall be peer to peer.

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.

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

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

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

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.

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

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 after reconnection to peer servers.

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.

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.

There must be a native tool within the operator GUI to remove redundant servers from a multiple server configuration. The use of scripts applications is not allowed.

12. GRAPHICAL OPERATOR INTERFACE

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

There shall be a user configurable view, designed specifically for the task and the information needs of the operator.

Default operator views shall be provided covering the primary site management functions of:

- events,
- alarm management,
- cardholder management,
- access management,
- site monitoring,
- calendars and scheduling,
- macros,
- operator management,
- mobile device management,
- site wide system changes,
- reports.

The ISMS shall allow the creation of customised views to enable operators to access information relevant to a specific business workflow within one screen.

The operator GUI shall be fully configurable by an operator with authorisation to configure the GUI.

The operator GUI may be dynamically separated into multiple windows to allow for multi-monitor operation, closing the secondary GUI will automatically return navigation items to the primary GUI.

The primary operator GUI will always display an alarm count differentiated by alarm priority.

Each view shall consist of a navigation menu area and a dynamic viewing area as detailed below.

The navigation area shall provide a list of relevant data related to a specific workflow as defined by the task at hand.

It shall be possible to select and order the columns of data in the navigation area associated with alarm and cardholder views.

Dynamically updated search results shall be provided when typing into the search field for a cardholder view.

Selection of a line item in the navigation area shall cause the associated dynamic information viewing area to be populated with data relevant to the selected item.

Within the dynamic viewing area one or more data tiles shall be provided to display detailed data associated with the navigation area item selected.

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

Each data tile shall be configurable with the required data fields as determined by the function of the tile.

Data tiles shall be maximised to enlarge the display area for that data by single click operation. Another single click operation on this tile will return all tiles to original size and location.

When a data tile has been maximised, other tiles shall remain visible in thumbnail format, allowing a single click to make them the selected maximised data tile.

Where applicable, minimised tile icons shall display dynamic content.

There shall be provision for displaying data tiles within the dynamic viewing area that link to external sources.

The linked data tile shall allow either a URL address, PDF, or TXT file to be selected.

Navigation from a URL shall be configured either as:

- navigation enabled,
- restricted navigation allowing navigation to hyperlinks on the site but not to enter a URL,
- navigation disabled.

Auto refresh of a URL shall be configurable down to 1-minute resolution.

An event view shall be available with the following capabilities:

- allow the operator to view events in real-time,
- the displayed data columns shall be configurable,
- the columns shall be sortable,
- auto scroll capability.

The event view shall also allow the operator to search for and select historic events, even when they have been cleared from the real-time view window. This shall include:

- search based on time/date,
- search based on the source of the event,
- the selected historic event shall appear in the event window with the same relevant data as if it were a real-time event,
- display a count of the number of events which were found.

When a single event has been selected the following information shall be possible to be displayed:

-
- instructions for the operator,
 - details of the event,
 - site plan,
 - cardholder image (where appropriate to the event),
 - video camera feed (where appropriate to the event),
 - recent event history for the door (where appropriate to the event),
 - recent event history for the cardholder (where appropriate to the event).

The system shall support Microsoft Edge as the default browser if Webview 2 Runtime is installed on workstations.

Calls from supported intercoms shall be managed from a central location from within the GUI using a unified intercom viewer.

13. SYTEM OPERATOR MANAGEMENT

Operator establishment and maintenance shall be a restricted privilege.

It shall be possible to define specific ISMS privileges for a group of operators and an individual operator can be added or removed to this group without changing any other properties of that group or the operator than this relationship.

Operators (non-Admin) inactive for a specified time period can be configured to have the user account disabled.

Operator access to the operator GUI is to be restricted by means of a unique operator identifier and password.

It shall be possible to apply password restrictions that consist of (but are not limited to) the following:

- minimum password length,
- mixed case,
- mixed alpha and numeric characters,
- mandatory change of password after a defined period,
- remembering and rejecting at least 999 previously used passwords.

There shall be default password restrictions that cannot be disabled as follows:

- Passwords must not contain the login name, first name, or last name of the operator
- There shall be a file containing common passwords that will not be allowed, this file will be editable by the customer to strengthen or relax the disallowed passwords.

The system shall support an Active Directory Single Sign-On feature to allow access to the operator GUI without password if they are already logged into an authenticated Windows session.

Each operator shall have the authority to alter their own password.

Automatic logoff may occur after a preset time of up to 1440 minutes of operator inactivity.

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

It must be possible to allow or deny operators access to various menu functions.

It shall be possible to blend the right to view groups of system objects for different operators; i.e. an operator in building 1 can see alarms for building 2 but is not able to perform any function on them. An operator in building 2 has the inverse relationship and can only action alarms for building 2 but still view alarms in building 1.

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

It shall be possible for a suitably authorised operator to view all connected data sessions on the ISMS, and the following minimum information shall be displayed:

- device name,
- login credential,
- session type, i.e. operator GUI, mobile application, data connection OPC/XML etc,
- session status,
- it shall be possible for a suitably authorised operator to terminate any data session.

14. CARDHOLDER MANAGEMENT

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.

The system must allow at least 15 issue levels per card or token. This must deny access and raise an alarm to the operator when a wrong issue level is presented to a reader.

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

Where a PIN is assigned to a card three consecutive or repeating digits shall not be allowed.

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

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

The options for encoding and printing shall be:

- print card,
- encode card,
- print and encode card in a single operation.

It shall be possible to prevent the duplication and/or re-printing of cards on a per operator basis.

Where a PIN is assigned to a card it should be stored in the database of the ISMS not as part of card data.

There must be an option to save a copy of the PIN for later retrieval for forgotten PINs, if this option is not selected then a cardholder's PIN will be saved in a one-way hash to the database.

Card numbers shall be enrolled against a cardholder by manually entering the card number or in the case of any Mifare technologies, a reading device connected directly to a workstation.

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

At least 64 user-definable data fields shall be provided which may be selectively reported on.

Cardholder data fields shall be able to be configured as:

- text; user data may be entered,
- text list; operator selects text from a pre-prepared list of text strings,
- numeric; operator must enter numeric data,
- date; calendar dates may be entered based on the workstation date format,
- default value; the field has a default value assigned,
- no default value; default value disabled,
- image; the field may only contain an image,
- email/mobile; the field contains an email address or mobile number to be used for communication by the ISMS,
- required field; the value may not be null,
- unique values; data must be unique from all other cardholder records.

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

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

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

- the date when a cardholder record was created,
- the date when the record was last modified,
- access groups that a cardholder is a member of,
- for ease of programming, cardholders shall be grouped into access groups sharing the same access criteria and default cardholder data fields,
- it shall be possible to allocate start and end dates and times for an access groups membership,
- cardholder additional data fields,
- images which may include photos, signatures etc,
- allocated cards,
- it shall be possible to enter an expiry date/time for the card,
- cardholder qualification information relating to fields such as “Security Clearance”, “Safety Induction” etc,
- a URL link to additional information which may be located on the customer intranet, or the internet.

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

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.

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

- delete selected cardholder records,
- change custom cardholder data fields
- change cardholder card details,
- change cardholder access options.

The system shall support the ability to bulk change the system division that database objects are assigned to.

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

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

A personal user code (4 to 8 digits) shall be a property of the cardholder record to allow access via readers with a keypad and to arm and disarm alarms.

Operator management shall be a property of the cardholder record.

A change history record associated with each cardholder record shall list all changes made to a cardholder record, including details of which operator or API login made the changes.

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.

The cardholder record screen shall display a real-time event trail of cardholder activity.

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.

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 cardholder administration tasks.

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. custom data fields, cards, access groups, biometric information etc). Different operators shall be able to view different sub-sections of the cardholder information.

It shall be possible to locate a cardholder record by presenting their card to a reading device connected directly to an operator's workstation.

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

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

The system shall be able to display up to 30 historical cardholder activity items instantly in a viewer.

15. PHOTO BAGGING AND IMAGE MANAGEMENT

The ISMS 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.

The ISMS shall provide a means to:

- electronically capture images,

-
- store the images in the server database,
 - integrate those images into a pre-designed ID card from within the system,
 - produce an integrated and finished identification card.

The ISMS must be capable of storing at least three images per cardholder.

The ISMS offered shall capture images in 24-bit colour and at least 800 x 600 pixel resolution, using standard video capture hardware offering a TWAIN, Direct Draw standard interface, or a USB digital camera.

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

The image capture editing controls must be integrated into the system software.

The ISMS shall store images in the JPEG compression format. User definable compression rates shall be easily selectable by the operator, a minimum of three levels of JPEG compression are required.

The facility to import background images from other sources into the card designer must be available.

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

- JPEG,
- Windows BMP,

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

- EAN 13,
- EAN 128,
- UPC A,
- UPC E,
- Code 39,
- Code 128,
- Interleaved 2 of 5,
- Codabar,
- Telepen,
- PDF417.

The card design must be capable of user-selecting up to 16.7 million colours with a custom colour palette available.

Card design must be accomplished using drag and drop options via a mouse.

Card design must support both sides of the card.

The system shall be capable of linking data relating to the cardholder and printing it the card. This data shall include (but not be limited to):

- first name,
- last name,
- card number (displayed as text and/or barcode),
- card issue level,
- expiry date,
- personal data as defined in the cardholder database.

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

The image files that are selected to incorporate into the card design must be scalable on the card. When scaling the image, the card designer must offer automatic aspect ratio adjustment throughout the size range.

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

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

16. INTRUDER ALARM SYSTEM

The ISMS will incorporate a fully functional intruder alarm system.

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.

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

Arming and disarming the intrusion detection system shall be either by using card readers, alarm management terminals, key-switches or schedules.

It shall be possible for the system to cause readers to beep during entry and exit delays.

It shall be possible for the system to active outputs during entry and exit delays.

It shall be possible to configure the system to isolate faulty external devices so as not to trigger false alarms.

It shall be possible to configure the system to fail to arm if an input point is active.

It shall be possible to configure the system to fail to arm if an input point has unacknowledged alarms.

It shall be possible for the system to cause readers to beep when alarms are present in the system.

It shall be possible to set the system to a test mode to allow for testing and maintenance.

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

The intruder alarm system shall provide a dependency feature whereby an alarm zone does not go into the set state until all dependent alarm zones are in the set state.

- If the alarm zone is set (armed) and the access door is secure:
 - A cardholder shall require authorisation to both unset (disarm) the intruder alarm zone, and to access the access zone to be allowed access.
 - If the cardholder is not authorised to unset the alarm zone or not allowed to access the access zone, then access shall be denied.
- If the alarm zone is unset (disarmed) and the access door is secure:
 - A cardholder shall require access to the access zone only for access to be allowed.
 - If the cardholder is not authorised to access the access zone, then access shall be denied.
- For normal operation, after an authorised token is presented, and access is granted, then the alarm zone shall remain unset after the door relocks.
- As an optional function, the alarm zone may auto-set after a predetermined time period.

When specified, alarm monitoring may use a connection with central alarm monitoring stations via digital communicators using Contact ID format, connected directly to the IFC panels.

Connection with central alarm monitoring stations may be by TCP/IP or cellular networks.

- It shall be possible for alarms from one IFC to be transmitted via a second IFC where the digital communicator is installed. (Peer-to-peer communications).
- Digital communicators are to be able to communicate alarms from all system IFCs, independent of system server.
- The system shall report and log all digital communicator activity and the reason for any failure to communicate.
- The system shall provide for up to two back up communicators on different IFCs to provide automatic backup capability should the designated digital communicator fail to operate on the appropriate alarm condition.

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:

- unset intruder alarm zones,
- set intruder alarms zones,
- status of alarms and inputs on AMT,
- acknowledge alarms,
- shunt inputs,
- force-arm alarm zones,
- auto-isolate alarm zones.

17. ALARM MANAGEMENT

The ISMS shall provide entry and exit delays for the setting (arming) and unsetting (disarming) of alarms.

The entry delay shall be configurable from 0 to 999 seconds in increments of one second.

An optional audible warning must sound during the entry delay (from the time the alarm occurs to the time that the zone state is changed). It must be possible to designate specific card readers and Alarm Management Terminals (AMTs) 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.

The exit delay shall be configurable from 0 to 999 seconds in increments of one second.

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 AMTs 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.

The system shall include an alarm escalation as a feature. The new event shall correspond to the original alarm but will have a higher priority and may include a different set of alarm relays to operate.

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

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

- Escalate if the alarm is not acknowledged for a period of time. This must be configurable from 0 to 9999 seconds in increments of one second.

-
- Escalate if the alarm point remains in an active state for a period of time. This must be configurable from 0 to 9999 seconds in increments of one second.
 - Escalate if a user defined zone contains a specified number of unacknowledged alarms from any number of alarm points. This must be configurable from 0 to 99.
 - Escalate if there are two events from the same alarm point within a user-defined period of time. This must be configurable from 0 to 9999 seconds in increments of one second.
 - Escalate if there are two events from different alarm points in a defined group within a user-defined period of time. This must be configurable from 0 to 9999 seconds in increments of one second.

An additional option of advanced Alarm management will allow:

- Escalation to supervisors when alarms are not processed within a set timeframe.
- Operators to manually escalate alarms to a higher level operator.
- Operators to start and stop receiving alarms whereby alarms are automatically re-distributed to other active operators.

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

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

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

- code access at an AMT,
- operation of the card plus PIN reader at an AMT,
- presenting a valid access card to a card reader associated with the alarm zone, twice within a nominated time period (double card badging).

It shall be possible to set and unset multiple alarm zones from an AMT.

All alarm occurrences shall be presented at the ISMS within 5 seconds of their occurrence at the remote field device.

All alarm events shall be viewable from an alarm stack.

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.

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 ISMS.

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

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.

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

It shall be possible to assign a system definable colour to each alarm priority.

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.

The ISMS must be able to control the priority assigned to any alarm activation according to a schedule. This means an alarm activation may be programmed as “Low Priority” during office hours and “High Priority” at other times.

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 change immediately to free access.

The ISMS shall support two-stage alarm processing as:

- Acknowledge alarm:
 - An acknowledged alarm shall remain in the alarm stack and be easily identified as having been acknowledged but not yet processed.
 - The ISMS shall record in the hard disk activity log that the operator has acknowledged the alarm.
 - A second alarm from the same source as the acknowledged alarm shall be indicated as a new alarm.
- Process alarm:
 - A processed alarm shall clear from the alarm stack.
 - The ISMS shall record in the hard disk activity log that the operator has processed the alarm.

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

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

the ISMS 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:

- full alarm message,
- related cardholder name,
- acknowledging operator name,
- alarm Zone,
- alarm source,

-
- related access zone,
 - event type,
 - event group,
 - division of the alarm source,
 - count (occurrences of alarm).

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

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

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

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

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

“Door Open Too Long” alarms must display selected and configurable information. Including, as an example, the photo and contact details for the cardholder who left the door open, i.e. last successful access.

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

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.

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

- Alarm instructions shall have the following features:
 - 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.
 - Individual alarm instructions shall be able to be programmed and applied to individual alarm events.
 - A repository of configurable data fields of volatile information shall be available when programming alarm instructions, and applied to alarm instructions via text tags or drag and drop.
 - When the data fields in the repository are updated, the linked alarm instructions shall automatically update with the current value when displayed to an operator.

-
- The alarm instruction text shall be able to be formatted using common text formatting features including but not limited to:
 - bold, italic, underline,
 - text colours,
 - left, centre, and right justified,
 - bulleted text,
 - standard Microsoft Windows font types and sizes.
 - It shall be possible to copy and paste alarm instructions between alarm events.

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

- 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.

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

ISMS shall allow the user with the appropriate privilege to mute alarms in the alarm stack.

18. CLASS 5 ALARM SYSTEM

The system shall be capable of being installed and configured up to Class 5 level of the AS/NZS 2201 Intruder Alarm System standard.

The Class 5 system shall include provision of Class 5 compliant end-of-line modules for alarm sensor communications protection.

The Class 5 system shall include provision of Class 5 compliant cabinetry, including Class 5 compliant locking mechanism, tamper sensor, and vibration sensor.

The Class 5 system shall include provision of Class 5 compliant power supplies, capable of:

- recharging up to 100Ah of battery backup,
- recharging all batteries within 48 hours of power being restored.

The Class 5 system shall include support for a battery backup system which meets the following:

- a minimum of 16 hours of battery backup for a monitored system,
- a minimum 24 hours of battery backup for a non-monitored system.

The Class 5 system shall include provision of Class 5 compliant AMT, supporting the following:

-
- user authentication with card + 6-digit minimum PIN length,
 - alarm arming,
 - alarm disarming,
 - manual alarm condition isolation,
 - automatic alarm condition isolation.

The Class 5 system shall include provision of Class 5 compliant controllers, supporting the following:

- data communications authenticated utilizing a minimum of ECC P-256 to the following;
 - AMT
 - end-of-line modules
- data communications protected utilizing a minimum of AES-128 to the following;
 - AMT
 - end-of-line modules
 - dedicated hardware cryptographic key storage, compliant to the FIPS 140-2 specification.

19. ACCESS CONTROL

The ISMS 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 each IFC.

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

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

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

- 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.
- The access group details page shall display both permanent and temporary access members with the status of temporary members shown as:
 - pending (with the start and finish times),
 - active,

-
- expired.

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

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

- correct site code,
- authorised card in database,
- correct issue number,
- authorised door / access zone,
- authorised time of day,
- valid card holder analytics,
- correct PIN (If PIN entry is required),
- double entry (anti-passback, anti-tailgating, or escort modes).

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

- disallow second access to an area if a valid exit has not previously been registered and generate an alarm (hard anti-passback),
- allow second access to an area if a valid exit has not previously been registered but generate an alarm (soft anti-passback),
- exclude specific access groups from the rules defined in (a) and (b) above.

Anti-passback rules shall be able to be reset by:

- automatically after a preset period after valid entry,
- automatically at a standard time each day,
- automatically on exit from site,
- manually as an override.

The ISMS must support global anti-passback allowing multiple access zones to be linked for anti-passback, across multiple IFCs utilising encrypted peer-to-peer communications.

The IFCs shall not rely on the server for anti-passback operation. Global anti-passback shall work across multiple IFCs, even if the server is offline.

The anti-passback capability of the ISMS shall enforce anti-passback on a single cardholder for the use of multiple credential types (e.g. mobile phone, keyfob, Mifare card).

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

-
- disallow exit from an area if a valid access has not previously been registered and generate an alarm (hard anti-tailgate),
 - allow exit from an area if a valid access has not previously been registered but generate an alarm (soft anti-tailgate),
 - exclude specific access groups from the anti-tailgate rules.

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

- Automatically after a preset period after valid entry.
- Automatically at a standard time each day.
- Manually as an over-ride.

The IFCs shall not rely on the server for anti-tailgate operation. Global anti-tailgate shall work across multiple IFCs, even if the server is offline.

The anti-tailgate capability of the ISMS shall enforce anti-tailgate on a single cardholder for the use of multiple credential types (e.g. mobile phone, keyfob, Mifare card).

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

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

- free access (no credential required),
- secure access (credential required),
- secure and PIN access (credential and PIN required),
- specific users exempt from requiring secure and PIN for accessibility purposes,
- override from reader - members of certain access groups shall be able to change the access and PINs mode of the door at certain times,
- dual authorisation - access is granted when two different but legitimate cards are presented within a given time frame,
- escort - a second card is required to be presented from a cardholder who is nominated in a specified access group,
- shared code - The ISMS operator determines what the code will be and programs this into the ISMS. Access is allowed through the door when the correct 4-digit code is entered.

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

- only when there has been a successful presentation of a valid access card or token and the door open sensor has detected the door has opened,

-
- whenever there has been a successful presentation of a valid access card irrespective of whether the door has been opened.

Readers with integrated PIN pads, or biometric readers using identification shall provide an “Entry under Duress” facility.

- Duress shall be initiated by the cardholder either by incrementing the last digit of their PIN number by one. Duress on biometric readers shall be initiated by the cardholder presenting their pre-enrolled “Duress finger”.
- There must be no indication of a duress entry at the reader.
- When a duress alarm is raised at a reader a critical priority “Duress Alarm” shall be displayed at the ISMS.
- It must be possible to configure the ISMS such that duress or other selected critical alarms pop to the front of the display, ensuring immediate operator attention. The existence of lower priority incoming alarms shall be visible to the operator but must not interrupt their current task.

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

- The zone count shall be viewable on the Site Plan Access Zone object.
- The result of the number of cardholders in the zone being outside of the specified range(s) shall generate an event or an alarm, depending on ISMS configuration.
- The minimum and maximum numbers of cardholders in a zone before an event is generated shall be configurable.
- It shall be possible to set 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.
- It shall be possible to assign a specific message for each of the minimum, mid-range, or above maximum conditions.
- It shall be possible to set up the ISMS to prohibit one cardholder being alone in a zone by:
 - requiring two valid but different cards to access a zone should the zone count reports zero cardholders in the zone,
 - requiring one card to access a zone should the zone count report two or more cards in the zone,
 - requiring one card to exit from a zone should the zone count report three or more cards in the zone,
 - requiring two valid but different cards to exit from a zone should the zone count report two people present,

-
- prohibiting exit from a zone and generate an alarm if the zone count reports one cardholder present.
 - It shall be possible to increment and decrement zone counting based on physical inputs not related to access events.
 - It shall be possible to increment and decrement zone counting based on logical inputs not related to access events.
 - It shall be possible to schedule an access zone for a “First Card Unlock” mode, whereby the access zone is scheduled to go to free access, but only when a suitably privileged card is badged at the reader. All other cards will be granted access, but will not be able to set the door to free access unless they have the “First Card Unlock” privilege.
 - It shall be possible for suitably privileged cardholders to toggle the access mode of a reader between free and secure by badging their card at the reader twice in quick succession.
 - It shall be possible for suitably privileged cardholders to log on to a reader with a keypad either by a credential or credential and PIN and change the access mode of the reader to either free or secure.
 - In addition to unlocking a door when granting access, it shall be possible to activate an additional output or macro which is uniquely related to the cardholder or access group to which they belong.
 - It shall be possible to “lock down” specific areas of a site such that cardholders who would usually have access, are denied access. cardholders with suitable privileges such as security personnel will still have access. The “lock down” should be activated and/or cancelled by the following methods:
 - clicking an icon on a site plan,
 - triggered based upon an event within the ISMS,
 - triggered from an input.

20. PERSONNEL IDENTIFICATION VERIFICATION

The ISMS shall be certified as complying with the requirements of FIPS 201-2 on the GSA FIPS 201-2 Approved Products List (APL)

The ISMS must provide a fully integrated solution that will harvest the information from the PIV card, validate it with the online certification authorities and store that information on the server database, this must include as a minimum:

- the PIV certificate,
- the CAK certificate,
- the biometric template,
- the cards “printed Information”,

-
- the full FASC-N for a PIV card or the GUID for the PIV-I card.

The ISMS shall provide an interface to allow integration to Enterprise Identity Management systems. This interface shall allow certificates and images to be imported into the ISMS database.

At all times the ISMS shall use the full FASC-N or GUID as the credential number in the ISMS and it shall not be allowable to use a truncated or non-unique representation for access control.

All access validation shall be done at the IFC. This shall include:

- CAK signature check,
- CAK expiry or notBefore Check,
- CAK and PIV certificate revocation – based on cached data,
- The challenge of the PIV card's CAK private key.

The ISMS must implement the CAK Authentication single factor access mode authentication.

Contactless CAK Access decisions, card presented to door released, shall take no longer than the following times:

- RSA 2048-bit keyed CAK Certificate: 3 Seconds,
- ECC P256 bit keyed CAK Certificate: 1.5 Seconds.

The ISMS must validate all PIV credentials via the external Certification Authorities at configurable periods between 1 hour and 24 hours.

Card readers must communicate to IFCs via a bi-directional supervised protocol on a physical RS485 transport layer. Additionally, the protocol shall be encrypted using AES-128 keys and authenticated using 256-bit Elliptic Curve Cryptography.

Each card reader shall have a manufacturer's unique serial number and the ISMS must prevent unauthorised reader substitution.

Card readers and IFCs must be able to show compliance to FIPS140-2 level 1 for communications and validation cryptography and FIPS140-2 level 3 for key storage.

ISMS shall support on demand PIV certificate validation

21. SITE PLANS

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

The designing and editing of a site plan shall allow:

- The basic editing tools to assist in the design and creation of the site plan.
- Assigning icons to ISMS functions and place these at any position on a site plan.
- Provision for drawing lines and shapes to form objects shall be available. These objects shall be able to be associated with ISMS items allowing ISMS item status to be visually indicated by the object.
- It shall be possible to place free text onto a site plan.
- An optional grid shall be available with snap-to-grid available for all objects and vertices.
- Individual objects within a site plan shall be able to be moved behind and in front of other objects using a layer scheme.
- An alignment tool shall be provided to align groups of objects in both x and y dimensions.
- External drawings shall be able to be imported into the ISMS from external drawing software. The ability to import common and the following drawing formats shall be supported:
 - EMF,
 - PDF,
 - PNG,
 - WMF.
- It shall be possible to design and load icons from external software for use in the ISMS.
- It shall be possible to design interactive buttons to reside on site plans. On activation, the buttons must be capable of performing multiple overrides for ISMS items simultaneously.

When an object is selected on a site plan, it shall present an interactive menu to the operator. All the following functionality must be included:

- View the current status of a door, input, or output,
- override a door, input, or output,
- monitor and acknowledge an alarm,
- open an access-controlled door,
- Change an unlock schedule on a door,
- move from one site plan to another,
- activate an intercom,

-
- override an alarm, access, or perimeter fence zone state,
 - generate a report.

Site plan usage shall support touch-screen technology and preclude the use of a mouse right-click as a separate function.

Site plans shall be capable of pan and zoom functionality.

All open site plans shall be updated immediately if that site plan is amended at any workstation.

Icon names shall use the item name by default, but a shortened name shall be configurable so as not to clutter the site plan with text.

The ISMS shall support a search functionality that when searching for an object, it will return a site plan containing the object.

There shall be provision for sending a copy of the currently visible site plan to a printer, email, or Windows clipboard, natively within the ISMS workstation application.

The site plan shall provide a means to show or hide objects at predetermined zoom levels to assist in reducing clutter on a highly populated plan.

When zooming out of the site plan, objects must amalgamate into a summarised indicator.

A site plan must support multiple floor layers in a single site plan item.

Whilst panning around a site plan, a secondary site plan must automatically present itself when the display pans over the location of that site plan that represents that sub-area.

Site plans shall allow icons for third party doors

Site plans shall allow background colour selection

Site Plans shall allow the user to customise its orientation

Site plans shall allow the user to implement the following:

- Provide options to hide and display items dependent on zoom levels
- Embedded site plans
- Have the ability to link separate panels and incorporate related items

Site plans shall allow intercom integration allowing for the following functions

- A fold away intercom Call queue which drives the navigation to the relevant intercom on the site plan
- Ringing behaviour on the intercom/door icons
- Popup controls to allow management of an intercom call

22. GUARD TOURS

The ISMS shall support multiple guard tours between check points.

- There shall be no imposed limit on the number of guard tours that can be configured.

Check points shall be card readers, inputs, or outputs.

- There shall be no imposed limit on the number of check points.

Multiple guard tours must be able to run concurrently.

The guard tour shall allow for flexible and configurable timing between check points which shall have (but not be limited to) the following:

- transition time;
 - the time period that it should take the guard to move from the last check point to the next check point,
 - this shall be configurable in hours, minutes and seconds,
 - the time shall be uniquely configurable for each check point,
- deviation;
 - the time allowed for the guard to be early or late at the check point,
 - this shall be configurable in hours, minutes and seconds,
 - the time shall be uniquely configurable for each check point,
- late;
 - the time period that has elapsed since the guard was expected at the check point wherein they are now considered as late to the check point,
 - this shall be configurable in hours, minutes and seconds,
 - the time shall be uniquely configurable for each check point.

The alarm priority for the guard tour events must be configurable.

User configurable instructions shall be available to assist operators when a guard tour alarm occurs.

The ISMS shall have an option to determine whether the guard must badge and open a door for a guard tour check point, or just present their card at the check point and not enter.

The ISMS shall be able to send an email and/or SMS alert to selected personnel based on guard tour events:

- it shall be possible to configure which events send alerts,
- it shall be possible to schedule when these alerts are sent.

The guard tour shall display in real-time the following information:

-
- the name of the guard,
 - the list of check points,
 - the time the guard is expected at each check point. This time shall display the deviation to indicate the time period the guard has to arrive at the check point.
 - This time period should update dynamically depending on the time the guard arrived at each check point.

The time the guard arrives at the check point.

The guard tour status should indicate (but not be limited to) the following:

- not due,
- due,
- early,
- overdue.

The guard tour shall stop if the guard arrives at an incorrect check point and an alarm shall be raised to indicate this.

The ISMS shall be configurable to restrict the individual guard tours that an operator can view.

The ISMS shall be configurable to determine whether an operator can view, edit or delete selected guard tours.

It shall be possible to display the real-time status of guard tours on a site map.

The guard tours shall be able to be started and stopped from the site map.

A site map showing the route of the guard tour shall be displayed.

It shall be possible to print a guard tour report directly from the site map.

The reports shall be configurable to filter based on the following criteria:

- date/time,
- guard tour,
- guard.

23. REPORTS

The ISMS shall provide report generation capabilities from the following sources of information:

- system activity data,
- cardholder access data,

-
- cardholder data fields,
 - cardholder access rights,
 - site configuration and setup data,

The report generation feature shall be easy to use and based on a “checkbox” style of parameter selection and preparation. The report preparation process shall provide features to simplify report generation by incorporating time selections such as “yesterday”, “last week”, “last month” etc. When these time-based selections are used in a saved report it will dynamically produce a report relevant to the time the report is run.

Report cover page, header, and footer, shall be configurable per report.

It shall be possible to re-order report columns.

It shall be possible to resize report columns.

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

It shall be possible to produce the following types of reports:

- any site activity,
- last known location of all cardholders on site, with cardholder count summary,
- unprocessed alarms, un-acknowledged alarms and doors temporarily overridden from secure to free,
- details pertaining to cardholders, including images,
- time-and-attendance based reports.

Reports shall be able to be saved for future use.

There shall be no limit imposed on the number of reports that can be saved.

It shall be possible to copy a report to be used as a template for another report.

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

- within the report editor,
- manually triggered from within a map display,
- triggered by a hardware or software event,
- a one-time or recurring schedule.

The ISMS shall generate and format reports as a background process. 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.

The ISMS shall have a screen preview function, so that reports can be previewed during report preparation and on-screen before they are printed.

The report generator shall be capable of exporting reports in the following formats:

- Adobe PDF (.PDF),
- Microsoft Word (.DOCX),
- Microsoft XPS (.XPS),
- Microsoft Excel (.XLSX),
- image file (.JPEG),
- CSV file with header (.CSV),
- CSV file without header (.CSV).

It shall be possible to email reports to nominated people or groups of people using the above format.

The email capability shall be available from within the ISMS itself. Applications that require reports to be generated, saved to a file and then emailed using an external email application will not be acceptable.

The report generator shall be capable of supporting wildcard searching when filtering data for reports.

It shall be possible for operators to change report parameters when generating reports.

Reports shall be able to be printed at any network-supported printers connected to the ISMS.

The ISMS shall be able to produce voltage reports for a networked energised fence.

- The energised fence voltage reports shall be displayed in graphical form showing the energised fence voltage along with the date and time.

The ISMS shall be able to produce temperature reports for a networked energised fence controller.

- The networked energised fence controller temperature voltage reports shall be displayed in graphical form showing the energised fence controller temperature along with the date and time

Operator privileges shall differentiate between:

- report preparation and configuration,
- report generation only (not allowed to change the configuration).

It shall be possible to generate reports with graphical representations of data for trend analysis in the following formats:

- bar graph,

-
- pie graphs,
 - line graphs,
 - summary report data shall be available in a table format.

ISMS shall be able to change the start of the reporting week as required

24. NOTIFICATIONS

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

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

It shall be possible to send notification of imminent card or competency expiry to an individual, their manager or other nominated person.

When emailing cardholder details, it shall be possible to send an image of the cardholder from their personal data record.

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

It shall be possible to schedule the notifications.

The notification may be triggered via a pre-configured alarm condition removing the need for operator intervention.

25. BULK NOTIFICATIONS

The ISMS shall allow for the broadcasting of notification messages to multiple recipients directly from the server.

The privilege to send the notification must be separate from the permission to create and see the setup of the notification.

Preconfigured messages shall be created that may then be sent with a single action by an operator or as a system triggered message.

The notification may be sent to groups filtered by previous access time, cardholder creation or modification date, access card type, or specific cardholder data criteria.

Notifications shall have the ability to be sent to dynamically updated groups based upon cardholder location in the ISMS.

26. AUDIT TRAIL

The ISMS server hard disk shall be used to record all system activity for auditing purposes.

All system activity event along with all details, including but not limited to the following list, shall be time stamped with the time of occurrence at the IFC and also the time the event was received by the server, to the nearest second, and shall be recorded in the system activity log for archiving:

- all access attempts (allowed and disallowed),
- alarm events,
- system events,
- operator activity.

The central control shall provide a facility to archive system data and event records to an archive file to free database space for further activity logging.

It shall be possible to archive the data to a network device by specifying a UNC path.

The archive process shall be initiated by either manual operation or automatically on a schedule.

It shall be possible to nominate the number of days of data that shall remain in the database after an archive process.

The ISMS reporting functionality shall return results from both live database and archive as a single contiguous report.

The system shall allow the workstations to acquire on demand subscriptions to the following and terminate these subscriptions after 5 minutes of inactivity

- Event Viewer
- Event Trail title
- Event Trail title

27. MOBILE DEVICE APPLICATION

The ISMS shall have a mobile device application which allows operators to remotely manage the ISMS via a smart phone or tablet. Dedicated devices with a single hardware option shall not be acceptable.

The mobile device application must be available on both Android and iOS operating systems.

The mobile device shall connect to the ISMS via:

- Wi-Fi or,
- mobile carrier data connection.

Mobile devices shall be enrolled in the ISMS by way of an authorisation code generated on the ISMS.

The mobile device connection must have the option of connecting to the ISMS server via an HTTPS proxy.

It shall be possible for the mobile device screen to lock after a preconfigured period of inactivity.

The mobile device shall be able to manage ISMS alarms:

- Alarms shall be displayed in different colours to denote the priority.
- The alarms shall have a flashing indicator when unacknowledged.
- The alarms will have a constant colour indicator when acknowledged.
- When multiple instances of the same alarm occur within a user-defined time frame, the mobile device will present alarms as a group and display the number of alarms in each group.
- The application will display the following alarm status:
 - alarm condition is still in an active state,
 - alarm priority has been escalated,
 - multiple occurrences of the same alarm within a user-defined time frame.
- The mobile device operator will be able to view alarm details such as:
 - priority,
 - source of the alarm,
 - date and time,
 - alarm history,
 - contextual instructions on how to proceed resolving the alarm.
- The mobile device operator will be able to perform operations on the alarm such as:
 - add notes to the alarm,
 - acknowledge alarms,
 - process alarms.
- The mobile device operator will be able to filter alarms by (but not limited to) the following states:
 - priority,
 - acknowledged,
 - unacknowledged,
 - active,

-
- inactive,
 - division.

The mobile device shall be capable of monitoring the status of ISMS items such as (but not limited to):

- doors,
- access zones,
- alarm zones,
- fence zones,
- macros.

It shall be possible to search for items monitored by the mobile device by selecting from a list or entering part of the text relating to the item name.

The mobile device shall be able to override items such as (but not limited to):

- doors,
- access zones,
- alarm zones,
- fence zones,
- macros.

The mobile device shall be able to lock down an access zone such that all cardholder access is disabled, excluding specifically authorised cardholders.

The mobile device shall have the capability to display the individual cardholders that are located in any access zone configured on the ISMS server.

The mobile device application shall have the ability to read Mifare DESFire EV2 credentials using the native NFC antenna of the mobile device.

- It shall be possible for the mobile application using NFC antenna to log a cardholder into or out of an access zone in the same manner as if the cardholder presented their card to a fixed access control reader.
- The cardholder credentials shall be authenticated by the ISMS and displayed in the user interface, clearly indicating an access granted or denied decision.
- Access granted and denied decisions shall be indicated by different audio tones.
- It shall be possible to continuously read cards without pressing any additional "Read Card" buttons.

The mobile device shall be able to manage cardholders.

-
- It shall be possible to search for cardholders by selecting from a list or entering part of the text relating to the cardholder's name.
 - It shall be possible to search for cardholders based on (but not limited to):
 - card number,
 - user defined data fields such as company, department, employee ID number, licence plate etc.
 - The mobile device shall display (but not be limited to) the following cardholder information:
 - name,
 - the last entered access zone, including date/time,
 - image,
 - access groups,
 - user defined data fields,
 - access credentials.
 - Data fields such as email address, phone number etc. shall be hyperlinks to enable the operator to click on the field and automatically be taken to the default email or phone application.
 - If a cardholder is not authorised for access, or has no active access groups, or has no active token, a highlighted message shall appear on the screen to alert the operator.
 - It shall be possible to disable a cardholder's access via the mobile device.

The mobile device shall be able to validate a searched for cardholder:

- It shall be possible to conduct a spot check of cardholders whereby the operator can view the access credentials of the cardholder on the Mobile device and record whether the cardholder passes an ID check and has the appropriate access rights to their current location.
- The operator shall select a "Pass" or "Fail" which will be logged at the central server.
- It shall be possible for the operator to select user-definable reasons for the pass or fail.
- It shall be possible for the operator to enter free text into a notes field.
- It shall be possible to record the location of the mobile device to indicate where the spot check took place.

The mobile device shall be capable of reading barcodes.

-
- Upon reading a barcode, it shall search for, and display cardholder details based on the barcode identifier.
 - The barcode identifier associated with the cardholder must support alpha-numeric characters. Numeric only will not be accepted.
 - The mobile device shall be capable of reading (but not limited to) the following barcode formats:
 - Aztec Code 2D,
 - DataMatrix 2D,
 - PDF417 2D,
 - QR Code 2D,
 - Macro PDF417 2D,
 - Semacode 2D.

The mobile device shall be capable of reading supported cards

ISMS shall allow the mobile version of the application to connect securely from anywhere on the internet hence removing the need for the mobile end point to be on a VPN or corporate network.

The mobile application shall display a selected profile image for cardholders who have been assigned this feature.

28. COMPETENCIES

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.

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

Each competency will assume one of 4 different states:

- Active - The competency is currently valid for the cardholder.
- Expiry due - The competency is currently valid for the cardholder but will expire in a specified period.
- Expired - The competency has been assigned to the cardholder but has expired.
- Disabled - The competency, is temporarily disabled (or overridden) for the cardholder.

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.

Each competency shall be individually set per cardholder

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

Competencies shall be configured as required per access zone.

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

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

Access permission based on competency criteria must be determined at the IFC, independent of the ISMS being on-line.

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

Advance warning of a cardholder's competency about to expire shall be sent to the individual and/or other nominated persons via email.

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

29. RANDOM SELECTION

The ISMS shall have an integrated component for selecting cardholders using a completely random or pseudo-random criteria when they badge at a door.

The ISMS shall display a customisable message at a door's reader when the cardholder is selected.

The ISMS shall allow for configurable allowance or denial of access when the cardholder is selected.

The selection criteria shall be configurable with the following options:

- the maximum number of times that a single cardholder may be selected over a given period of time,
- the total number of cardholders that may be selected over a given period of time,
- that all cardholders must be selected at least once over a period of time.

The selection algorithm must be able to function on the IFC without the aid of the ISMS server.

The selection algorithm must be able to calculate the selection criteria across up to 30 doors in the system.

The selection algorithm must be able to differentiate between different groups of cardholders and assign a varying probability selection to each.

30. ELEVATOR CONTROL AND MANAGEMENT

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

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.

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

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

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.

The ISMS shall raise an alarm if the elevator reader stops communicating with its elevator controller.

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

- correct facility code,
- authorised card in database,
- correct issue number,
- authorised level,
- authorised time of day,
- correct PIN (If PIN entry is required).

The access mode for each floor of an 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:

- free access (no credential required),
- secure access (credential required),
- secure and PIN access (credential and PIN required),
- dual authorisation - access is granted when two different but legitimate cards are presented within a given time frame,
- escort - a second card is required to be presented from a cardholder who is nominated in a specified access group,
- shared code - The ISMS operator determines what the code will be and programs this into the ISMS. Access is allowed through the elevator when the correct 4-digit code is entered.

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

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

Where a low-level interface is specified:

- The interface between the access system elevator control equipment and the elevator switching control equipment shall be via dry relay contacts.
- The voltage from the elevator system connected to the relays shall not exceed 24 volts DC/AC.
- The elevator control system shall provide one relay contact per elevator shaft per level for the ISMS. This relay contact shall be used to interface with the elevator switching control equipment.
- 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.

Where a high-level interface is specified:

- The interface between the access system elevator control equipment and the elevator switching control equipment shall be via RS-232 or TCP/IP connection depending in the elevator system requirements.
- The elevator control equipment will provide feedback as to which level was selected by the cardholder.

31. CAR PARKING

The ISMS shall integrate car park management functionality.

Car parks may be allocated to a single cardholder or a group of cardholders.

Car park functionality for a group of cardholders:

- When occupancy of a group's car parks is reached the system shall disallow entry to members of that group until another group member has left the car parking area.
- The car parking functionality may allow for a cardholder to enter the parking area temporarily although there are no available parks for their group to ensure they do not cause a traffic jam at the entry point.
- If the cardholder that was allowed temporary entry does not leave the car park area after a configured period of time, then an alarm shall be raised in the ISMS.
- If another member of the parking group leaves the car park, then this shall allow the cardholder with temporary entry to remain in the car park.

The ISMS shall provide a real-time display to show the current occupancy of car parks.

The car parking system shall use standard readers and i/o devices to interface to barrier arms.

There shall be a terminal provided that gives feedback to a cardholder at the time of credential presentation.

The car parking system shall support all credentials specified in this tender including Bluetooth.

32. LOCKER SYSTEM

The ISMS shall include a locker management solution.

The lockers shall have the ability to be dedicated to a single person or allocated on-demand via a terminal when needed.

On-demand allocation of lockers shall not be reliant upon the ISMS server.

The lockers shall be able to be configured as either having an expiry period, or permanently assigned.

A quarantine state shall be configurable:

- To automatically occur when a locker allocation expires.
- With manual override for maintenance purposes.

The locker management system shall use standard readers and i/o devices to interface to locker bank hardware.

There shall be a terminal provided that gives feedback to a cardholder as to which locker they have been provided at the time of credential presentation.

A single terminal shall be able to support up to 256 lockers.

There shall be no limit to the total number of lockers in the system.

The locker management system shall support all credentials specified in this tender including Bluetooth.

33. PRE-PROGRAMMED OVERRIDE MACROS

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

Macro actions shall be capable of (but not limited to) the following:

- open doors,
- change door modes such as free, secure, secure with PIN, dual authority,
- anti-passback forgive,
- active and release zone lock down,

-
- reset the cardholder count in a zone,
 - switch an output on and off,
 - activate the generation of pre-configured reports,
 - start and stop a guard tour,
 - initiating another macro.

A macro shall be capable of activating multiple actions from within a single macro. There shall be no fixed limit to the number of actions that can be configured.

An operator shall be able to initiate the macro via either a menu item or by a site plan icon.

Macros shall be capable of being activated by any ISMS events.

Macro configuration 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 macros is not acceptable.

It shall be possible to initiate macros based on a on a time schedule.

Macros shall be able to execute Microsoft Windows command line actions.

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

Each macro shall be able to contain multiple command line entries.

The configuration and execution of command line macros shall be user account name and password protected. These usernames and passwords shall be obscured on entry and transmitted and stored at the central command ISMS server in an encrypted format.

34. VISITOR MANAGEMENT KIOSK

The ISMS shall allow visitors to self-register as defined in this section.

The kiosk shall operate on a workstation provided to the specification defined in “System Servers and Workstation Hardware”.

The kiosk shall support touch screen functionality.

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

Visit details shall be recorded in the ISMS event database.

Attributes associated with the visit shall be configurable and set as mandatory or optional fields. These shall include:

- the reception where the visitor(s) will be expected to arrive,
- the visitor category,
- the person the visitor(s) will be meeting,
- visitor arrival time,

-
- visitor departure time,
 - building access rights to be given to the visitor(s),
 - visitor photo-ID image.

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

A welcome (default) screen shall be customer configurable to allow branding and imagery to be displayed.

The kiosk shall support visitor site induction.

- The induction feature shall be customer configurable, incorporating the following features:
 - induction videos,
 - multi-choice questionnaire depending on induction level required,
 - multiple questionnaires,
 - induction hint feature to allow the visitor to request a hint for questions,
 - notify the host that the visitor requires induction assistance,
 - a condition of entry screen,
 - a privacy statement screen.

Visitors shall be able to search for themselves in the system and carry out the following functions:

- add or update their details,
- capture a photograph via a camera connected to the kiosk,

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

If the visitor has been assigned an access token, then the visitor shall be able to present their token as identification.

The kiosk shall support business card scanning via a Dymo Executive Business Card Scanner.

The kiosk shall support passport and driver licence scanning via ScanShell products.

For pre-arranged visits, the visitor shall be able to pick the visit from a drop-down list.

The visitor shall be allowed to print a visitor label.

Visitors shall be able to advise their host via the ISMS that they have arrived via email or SMS message.

Hosts shall be able to assign themselves to the visitor by badging at a Card Reader.

Hosts shall be able to set the status of visitors to ensure current status of each visitor is always known. Host options shall include:

- marking a visitor on or off site,
- reprinting a badge for a visitor,
- updating visitor details such as arrival and departure times,
- assigning an access card to the visitor.

Tour groups shall be catered for.

- Tour group members are not individually named, however the number of people in the group shall be recorded.

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

The kiosk shall support a QR Code scanner.

- Upon creating an appointment, the visitor may be emailed a QR code which can be used to sign in.
- The QR code if used for signing in shall also be used for signing out.

35. DOOR FUNCTIONALITY – CONNECTED TO CONTROLLER

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

- access reader,
- emergency release switch input,
- reception control switch input.

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

- exit reader,
- push button request to exit,
- emergency exit break-glass.

A push button request to exit shall record the exit in the event database.

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

- The door relock time shall support three modes of operation:
 - the door lock output will relock immediately on door open
 - the door lock output will relock after a door open/close cycle

-
- the door lock output will relock after the configured time regardless of open-close cycles
 - The period of unlock shall be extended should a cardholder have a suitable privilege.

All entry and exit methods shall be recorded in the event in the event database.

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

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.

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 first being released by the ISMS.

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

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

It shall be possible to disable the reader audible warning.

It shall be possible to generate the audible warning via a relay connected elsewhere in the ISMS including any other IFC.

Should a valid request to access a door be generated and access not taken, this will be recorded as a different event and the door will be re-secured.

The ISMS shall have a lock down feature whereby cardholders who would usually have access to doors are denied access.

- It shall be possible to assign specific cardholders the right to access a door when the door is in lock down, whilst refusing access to all other cardholders.

It shall be possible to create an interlock relationship between groups of doors for situations such as airlocks whereby a door cannot be opened until other doors or inputs are closed.

- Up to 20 doors shall be included in any interlock group.
- It shall be possible to configure interlock groups via GUI drag and drop functionality without the requirement to write scripted logic.
- It shall be possible to assign outputs that advise cardholders that there is an interlocked state active.

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

- When a card is presented at a reader, images from the cardholder database (as many as required) shall be displayed in the challenge view of an operator GUI.

-
- Associated with the images, it shall be possible to display a video image from one or more assigned cameras.
 - 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.
 - In challenge mode it shall be possible for the operator to view the status of the cardholder's cards and competencies for informing the cardholder, at the time of entry, if any expiries are imminent.
 - Related data fields shall also be able to be displayed, associated with the cardholder (name details, department etc).
 - 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.
 - The challenge mode shall be configurable to either:
 - Automatically grant access to a valid card and display the current access decision (granted or denied) to the challenge operator.
 - Require operator intervention to grant access to a valid cardholder.
 - Should a second challenge be requested while an unanswered challenge remains in the ISMS, the second and subsequent challenges shall queue automatically awaiting response.
 - 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.
 - The ISMS shall allow challenge events to be managed from a single full-screen view per operator or multiple filtered views, as dictated by the specification.

36. DOOR FUNCTIONALITY – DATA ON CARD

Where specified, doors shall be managed using an offline door locking system.

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

The offline doors shall be fully integrated into the ISMS as described below:

- Card technology shall be contactless Mifare Classic, Mifare Plus, or Mifare DESFire EV2.
- Card encoding shall be carried out as a single encode operation for both online and offline door readers.
- Operational data shall be transferred between the ISMS and offline doors automatically, without the need for specific operator actions. This data shall include:

-
- multiple levels of door low battery voltage alarms,
 - access activity from all doors,
 - blacklisted card information,
 - changes to cardholder access privileges.
- Access privileges based on time and day shall be available, with full flexibility in specifying the time intervals or day types for any cardholder.
 - It shall be possible to configure the ISMS to ensure access updates for offline doors are enforced within a given period of time, configurable as a minimum of 1 day.
 - Access privilege changes must not require connection of a management device to the escutcheon (eliminating the need to update each door escutcheon when a user is added or removed).
 - The ability to specify an extended door opening time for specific cardholders shall also be available for offline doors.
 - Offline doors shall support partitioning to allow specific administrators to control and assign access privileges within their own environment/facility.

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

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

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

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

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

The offline escutcheons should be able to hold an audit trail of at minimum the last 1000 events.

The offline 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 cardholder with privilege to change the escutcheon mode.

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

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).

A handheld programming device may be used for the purposes of:

- diagnosing problems,

-
- performing an emergency opening of an offline escutcheon,
 - updating software,
 - provide power to the escutcheon to allow resolving a no battery voltage situation,
 - initialising hardware.

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). One or all may be used.

The hardware range shall include the ability to upgrade offline doors to online via wireless through a wireless gateway.

37. DOOR FUNCTIONALITY – WIRELESS CONNECTIVITY

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

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.

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.

The ISMS shall provide real-time access decisions as described elsewhere in this specification.

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

Card encoding shall be carried out as a single encode operation for both online and wireless door readers

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

- Wireless hubs shall be able to be wired in series with RS485 compatible cable.
- 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).
- AES-128 encryption shall apply for communication between the hub and each wireless reader.
- Up to 16 (installer selectable) channels per hub shall be available to ensure each wireless escutcheon or cylinder is configured with reliable communication.
- Hardware shall not use proprietary batteries. Batteries must be commonly available types.

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

The wireless doors shall be fully integrated into the ISMS as described below:

- Card technology shall be contactless Mifare Classic, Mifare Plus, or Mifare DES-Fire EV2.
- Operational data shall be transferred between the ISMS and wireless doors automatically, without the need for specific operator actions. This data shall include:
 - multiple levels of door low battery voltage alarms,
 - access activity,
 - blacklisted card information,
 - changes to cardholder access privileges.

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

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

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

38. FIELD HARDWARE – INTELLIGENT FIELD CONTROLLER (IFC)

The IFC shall be the main controller in the field. The ISMS shall communicate directly with all IFCs.

The IFC shall use a Linux operating system, this OS shall be specifically re-developed for a security purpose. Applications on a general-purpose OS such as Windows CE, Arduino, or a standard Linux kernel shall not be accepted.

The IFC shall incorporate an ARM processor with a processing speed of at least 1.2GHz; at least 4 Gigabytes of non-volatile FLASH eMMC and 512 Megabytes of RAM. The IFC shall incorporate boot code in a protected sector of the flash memory.

During IFC firmware upgrades, this shall be checked and verified as the true firmware pack during the upgrade process.

The IFC shall be intelligent such that in the event of failure of communications to the ISMS, for whatever reason, the IFC shall continue to allow or deny access based on the full security criteria at time of disconnection.

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 server for access decisions will not be considered.

The IFC shall buffer activity data and immediately transmit it to the central control server upon re-establishment of communications.

Should communications fail with the ISMS, each IFC shall be capable of buffering up to 1,000,000 events.

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

ISMS that only time stamp the event upon receipt at the central control hardware shall not be acceptable.

The IFC shall be capable of storing up to 2,000,000 card records with associated access criteria.

The IFC shall be capable of storing up to 1,000,000 mobile credentials with associated access criteria.

The IFC shall be capable of storing up to 1,000,000 biometric credentials with associated access criteria.

The IFC shall support the use of six-state end-of-line circuits and enunciate whether the circuit is open, closed, alarm, trouble, open circuit tampered, or short circuit tampered as separate conditions.

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

The IFC shall include tamper protection for the front and the back of the unit. The front of the unit shall be tamper protected for enclosure open, and the rear of the unit to detect if the unit has been removed from the wall.

The IFC shall operate from a DC power source with battery backup.

IFC's shall have power source options that enable:

- DC power supply with standby power at the power source.
- Power over Ethernet (802.3at Type 2 compliant) and must have a capability to maintain a 7Ah battery for standby power.
- Automatic detection and reporting of a PoE loss.

The IFC shall be capable of automatically detecting and reporting a low power condition.

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

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

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

The IFC shall be allocated to a time zone appropriate to the IFC location to cater for regionally and globally located IFCs.

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

When specified, the IFC shall be fitted with 2 Ethernet ports providing a fail-over communication capability.

The IFC shall have IPv6 address support.

The IFC shall support DHCP addressing.

The IFC shall be able to automatically obtain an IP address from a standard DHCP server.

The ISMS shall natively support WAN and NAT configurations to communicate with IFCs on distributed networks.

The IFC shall support DNS operation.

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

The IFC shall be provided with a pre-configured IP address to allow offline initial configuration via a web browser application when required.

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 using a conventional web browser.

The IFC diagnostic web interface shall:

- Not share common log on credentials with any other installed site.
- Have the ability to be disabled from the ISMS system.

Should excessive network broadcast traffic occur (resulting from a denial-of-service attack or similar), an alarm shall be generated.

The IFC shall support a high security configuration that disables unnecessary ports and legacy communication methods, this shall be achieved by an onboard jumper or DIP switch.

All ISMS data communication between the central server and IFCs shall be fully authenticated and encrypted using an industry standard asymmetric encryption algorithm equivalent to AES-256 or stronger.

All data communication between IFCs, IFCs and ISMS shall use an industry standard asymmetric encryption algorithm for mutual authentication and session key negotiation. This algorithm shall be equivalent to ECC P-384 or stronger. Session keys shall be re-negotiated on a regular basis at intervals no longer than 30 hours.

The IFC shall store and encrypt its cryptographic keys within its dedicated hardware for protection.

The IFC shall use Trusted Execution Environment (TEE) based on the ARM Platform Security Architecture.

Data onboard the IFC shall be encrypted at rest to prevent unauthorised access.

Communication between the management application and IFCs shall be continuous and monitored for interruption.

IFC variants shall enable remote communication to alarm monitoring stations with connection options:

- RS232 multi-communication port.
- TCP/IP for alarm transmission.

The IFC shall support logic functionality by way of configurable logic blocks.

- The IFC logic functionality shall be able to be run independent of the ISMS server being online.
- The following items shall be useable as input parameters to logic blocks:
 - physical input states,
 - output states (both physical and logical),
 - door states,
 - other logic block states.
- Up to ten logic block input parameters shall be configurable in AND/OR combinations to cause a logic block to operate.
- When a logic block change state according to the input parameters then the following types of items may change to reflect the state of the logic block:
 - virtual output (software based),
 - physical relay.
- The state change of the logic block shall have configurable timing options with at least the following:
 - explicit,
 - delay on,
 - delay off,
 - pulsed,
 - maximum on time,
 - latched.
- The IFC logic block shall be able to trigger actions across multiple IFCs, independent of the ISMS server being online.

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

- tamper,

-
- tamper return to normal,
 - unit stopped responding,
 - card error,
 - maintenance warning,
 - alarm sector state change,
 - user set alarm,
 - user unset alarm,
 - card trace,
 - wrong PIN,
 - access denied,
 - duress,
 - zone count maximum,
 - zone count minimum,
 - door open too long,
 - forced door,
 - door not locked,
 - power failure,
 - battery failure,
 - system reboot,
 - intercom.

The IFC shall communicate with and control the following equipment:

- biometric access readers,
- card access readers with PIN keypads,
- elevator access equipment,
- alarm monitoring input/output panels and equipment,
- alarm response equipment.

All communications links between the IFCs and 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.

Communication between IFCs and downstream devices shall support a high-speed serial protocol of at least 1Mbit/second.

IFC variants shall support up to 10 high speed serial communication ports.

The IFC shall support up 80 devices comprising a combination of readers, I/O devices and sensors.

Devices connected to the high-speed communication serial port shall contain a manufacturer's unique serial number.

When connected to an IFC, the serial number of the downstream device shall be reported to the ISMS.

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

The IFC shall have OSDP reader support.

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

- Activate and latch a relay in response to an alarm. Relay to remain latched until alarm processed.
- Activate a relay for pre-set "pulse" time. The relay to release after the "pulse" time lapses.
- Relay activation to "mirror" or "follow" the alarm input activation.

The ISMS shall incorporate relay outputs that can be activated according to time schedules, rather than alarm event.

The IFC shall support direct third-party communications with:

- Building management systems
- 3rd party API systems
- High level interfaced elevator systems

The IFC must comply with in ceiling space/plenum installation standards.

The IFC shall meet Compliances

- UL294 – Level 3
- UL2610 – Proprietary, Centralised station, mercantile
- UL2043
- IEC/ASNZS 60839-11-1
- ASNZS 2201.1
- EN BS50131

-
- FIPS 140-2 Level 3
 - CE/UKCA
 - FCC

39. ENCRYPTED END OF LINE DEVICE – CLASS 5

Encrypted end of line devices shall be available to provide secure monitoring of alarm inputs, i.e. passive infrared sensors, contacts.

The End of Line Device (ELD) must conform to the AS/NZS 2201 Class 5 Intruder Alarm Standard.

The ELD is required to fit securely inside the housing of a AS/NZS 2201 complaint PIR.

Alarm input devices must connect to the ISMS via an ELD.

The ELD must communicate with the ISMS using encrypted communications.

The ELD shall support the following I/O to the alarm device:

- alarm input,
- tamper input,
- anti-masking input,
- walk test output,
 - the walk test output shall support either a positive or negative output voltage during testing.

Events relating to the ELD shall be visible at the ISMS.

The ELD shall be encapsulated in a protective resin and plastic casing to prevent tampering.

The ELD shall support self-discovery on the ISMS.

The ELD shall be identifiable via a manufacturer's unique serial number both indelibly marked on the ELD and at the ISMS.

When connected to an IFC, the unique number of the ELD shall be reported to the ISMS.

The ELD is required to generate an alarm for the following conditions:

- attempted substitution of the ELD,
- external tamper sensor activated,
- communications lost to ISMS,
- alarm input triggered,
- anti-mask input triggered.

The ELD shall be upgradeable via software uploaded from the ISMS without any intervention at the ELD.

Each ELD shall be identified on the operator GUI by means of a user definable unique plain language descriptor. The plain language descriptor shall be at least 60 characters in length.

It shall be possible to connect up to thirty ELDs to a single IFC.

The ELD shall support a serial wiring configuration.

The ELD shall operate at temperatures between -10°C to +70°C

40. ENCRYPTED END OF LINE DEVICES

Encrypted end of line devices shall be available to provide secure monitoring of alarm inputs, i.e. passive infrared sensors, contacts.

The purpose of the ELD is to overcome the security weakness created by non-authenticated sensor inputs using a balanced resistor network.

The ELD shall be small enough to fit inside the housing of a PIR.

Alarm input devices must connect to the ISMS via an ELD.

The ELD must communicate with the ISMS using encrypted communications.

The ELD shall support the following I/O to the alarm device:

- alarm input,
- tamper input,
- anti-masking input,
- walk test output,
 - the walk test output shall support either a positive or negative output voltage during testing.

Events relating to the ELD shall be visible at the ISMS.

The ELD shall be encapsulated in a protective resin and plastic casing to prevent tampering.

The ELD shall support self-discovery on the ISMS.

The ELD shall be identifiable via a manufacturer's unique serial number both indelibly marked on the ELD and at the ISMS.

When connected to an IFC, the unique number of the ELD shall be reported to the ISMS.

The ELD is required to generate an alarm for the following conditions:

- attempted substitution of the ELD,

-
- external tamper sensor activated,
 - communications lost to ISMS,
 - alarm input triggered,
 - anti-mask input triggered.

The ELD shall be upgradeable via software uploaded from the ISMS without any intervention at the ELD.

Each ELD shall be identified on the operator GUI by means of a user definable unique plain language descriptor. The plain language descriptor shall be at least 60 characters in length.

Communication sessions between IFCs and ELDs shall use certificate exchange protocols using keys with a minimum strength of ECC P-256.

Data communication between IFCs and ELDs shall use a minimum of AES-128 encryption.

It shall be possible to connect up to thirty ELDs to a single IFC.

The ELD shall support a serial wiring configuration.

The ELD shall operate between -10°C to +70°C.

41. ACCESS CONTROL READERS – MIFARE TECHNOLOGY

The reader shall support the following technologies:

- Mifare Classic,
- Mifare Plus,
- Mifare DESFire EV1,
- Mifare DESFire EV2,
- NFC.

The reader shall be capable of reading the CSN of the Mifare card and store the CSN in the ISMS database

The readers shall support self-discovery on the ISMS.

- Readers shall contain a manufacturer's unique serial number.
- When connected to an IFC, the serial number of the reader shall be reported to the ISMS.
- Once assigned to a function within an IFC, if any attempt is made to substitute readers in the field without authorisation, an alarm shall be generated.

Data communication rate between IFCs and readers shall be at least 1Mbit/second.

Communication sessions between IFCs and readers shall use certificate exchange protocols using keys with a minimum strength of ECC P-256.

Data communication between IFCs and readers shall be encrypted and use a minimum of AES-128.

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

Readers shall be upgradeable via software downloaded from the ISMS without any intervention at the reader.

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

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

Where a card only reader is specified, the reader shall include:

- Integrated reader module supporting the technologies listed above.
- The card only reader option shall include an audible beeper and red/green LEDs to provide user feedback.
 - A steady red LED shall indicate door secure.
 - A flashing red LED shall indicate access denied.
 - A steady green LED shall indicate door free access.
 - A flashing green LED shall indicate access granted.
 - It shall be possible to turn off the reader LED indication via the ISMS software.
- The beeper shall give different beeps to indicate:
 - access granted,
 - access denied,
 - second card required when dual card authorisation or escort mode is programmed,
 - it shall be possible to turn off the reader beeper via the ISMS software.
- The readers must comply with at least IP68 environmental protection rating.
- The readers must comply with an impact rating of at least IK07
- A vandal resistant enclosure having an impact rating of at least IK08 rating shall be available where:

-
- Vandal covers shall be fixed to the wall surface using tamper-resistant screws.
 - Vandal covers shall have bevelled edges to limit the ability for persons to use the reader as an aid to climbing the building.
 - All external surfaces shall be bevelled and without protruding parts to meet anti-ligature requirements.
 - The reader must be RoHS compliant
 - The reader shall operate with a temperature range of -30°C to +70°C.

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

- integrated reader module supporting the technologies listed above,
- a minimum of a 3.5" LED colour display indicating:
 - card required,
 - PIN required,
 - access denied,
 - intruder alarm set,
 - intruder alarm unset,
 - free access,
 - second card required.
- The display shall support multiple languages which shall be selectable from the ISMS software.
- The reader shall display information to the user using a combination of text and graphics.
- The reader shall display the date and time.
- a PIN pad fully integrated with the reader,
- the PIN pad shall be backlit,
- The PIN pad shall include:
 - numerical 0 to 9 keys,
 - a cancel key,
 - an enter/accept key,
 - two soft keys that vary according to the current usage of the keypad.
 - An option with no reader module, for use as an AMT.

-
- Menus shall be accessible by logging on with either a card or a PIN.
 - The reader shall be capable of (but not limited to) carrying out the following functions:
 - Arm alarm zones; A minimum of 50 per reader must be supported.
 - Disarm alarm zones; A minimum of 50 per reader must be supported.
 - View Alarms; A minimum of 100 per reader must be supported.
 - Acknowledge alarms; A minimum of 100 per reader must be supported.
 - View alarm history; A minimum of 100 per reader must be supported.
 - Change the door to free access mode.
 - Change the door to secure access mode.
 - Change the door to operate from a user defined schedule.
 - Turn outputs on and off. A minimum of 50 per reader must be supported.
 - View the status of inputs. A minimum of 100 per reader must be supported.
 - Isolate inputs. A minimum of 100 per reader must be supported.
 - User definable custom images shall be displayed on the screen when the reader is idle.
 - The reader shall support the following image formats:
 - PNG,
 - JPG,
 - JPEG.
 - It shall be possible to adjust the reader beeper via the ISMS software to the following volume levels:
 - off,
 - quiet,
 - normal,
 - loud.
 - The reader shall have the ability to display the status of alarms and indicate the status of physical and logical items via LEDs on front panel.
 - The reader shall support at least 8 indication LEDs.
 - It shall be possible to turn off the reader indicator LEDs via the ISMS software.

-
- Tamper detection shall be provided against the unit being removed from the mounting surface.
 - Keypad readers must comply with a minimum IP66 environmental protection rating.
 - Keypad readers must comply with an impact rating of at least IK08.
 - The keypad reader shall operate with a temperature range of -30°C to +70°C.

All readers must be RoHS compliant.

42. ACCESS CONTROL READERS – MULTI TECHNOLOGY

The reader shall support the following technologies:

- Proximity 125 kHz
- Mifare Classic,
- Mifare Plus,
- Mifare DESFire EV1,
- Mifare DESFire EV2,
- NFC,
- Bluetooth LE.

The reader shall be capable of reading the CSN of the Mifare card and store the CSN in the ISMS database

The readers shall support self-discovery on the ISMS.

- Readers shall contain a manufacturer's unique serial number.
- When connected to an IFC, the serial number of the reader shall be reported to the ISMS.
- Once assigned to a function within an IFC, if any attempt is made to substitute readers in the field without authorisation, an alarm shall be generated.

Data communication rate between IFCs and readers shall be at least 1Mbit/second.

Communication sessions between IFCs and readers shall use certificate exchange protocols using keys with a minimum strength of ECC P-256.

Data communication between IFCs and readers shall be encrypted and use a minimum of AES-128.

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

Readers shall be upgradeable via software downloaded from the ISMS without any intervention at the reader.

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

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

Where a card only reader is specified, the reader shall include:

- Integrated reader module supporting the technologies listed above.
- The card only reader option shall include an audible beeper and red/green LEDs to provide user feedback.
 - A steady red LED shall indicate door secure.
 - A flashing red LED shall indicate access denied.
 - A steady green LED shall indicate door free access.
 - A flashing green LED shall indicate access granted.
 - It shall be possible to turn off the reader LED indication via the ISMS software.
- The beeper shall give different beeps to indicate:
 - access granted,
 - access denied,
 - second card required when dual card authorisation or escort mode is programmed,
 - it shall be possible to turn off the reader beeper via the ISMS software.
- The readers must comply with at least IP68 environmental protection rating.
- The readers must comply with an impact rating of at least IK07
- A vandal resistant enclosure having an impact rating of at least IK08 shall be available where:
 - Vandal covers shall be fixed to the wall surface using tamper-resistant screws.
 - Vandal covers shall have bevelled edges to limit the ability for persons to use the reader as an aid to climbing the building.
 - All external surfaces shall be bevelled and without protruding parts to meet anti-ligature requirements.
- The reader must be RoHS compliant

-
- The reader shall operate with a temperature range of -30°C to +70°C.

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

- integrated reader module supporting the technologies listed above,
- a minimum of a 3.5" LED colour display indicating:
 - card required,
 - PIN required,
 - access denied,
 - intruder alarm set,
 - intruder alarm unset,
 - free access,
 - second card required.
- The display shall support multiple languages which shall be selectable from the ISMS software.
- The reader shall display information to the user using a combination of text and graphics.
- The reader shall display the date and time.
- a PIN pad fully integrated with the reader,
- the PIN pad shall be backlit,
- The PIN pad shall include:
 - numerical 0 to 9 keys,
 - a cancel key,
 - an enter/accept key,
 - two soft keys that vary according to the current usage of the keypad.
- Menus shall be accessible by logging on with either a card or a PIN.
- The reader shall be capable of (but not limited to) carrying out the following functions:
 - Arm alarm zones; a minimum of 50 per reader must be supported.
 - Disarm alarm zones; a minimum of 50 per reader must be supported.
 - View alarms; a minimum of 100 per reader must be supported.
 - Acknowledge alarms; a minimum of 100 per reader must be supported.

-
- View alarm history; a minimum of 100 per reader must be supported.
 - Change the door to free access mode.
 - Change the door to secure access mode.
 - Change the door to operate from a user defined schedule.
 - Turn outputs on and off; a minimum of 50 per reader must be supported.
 - View the status of inputs; a minimum of 100 per reader must be supported.
 - Isolate inputs; a minimum of 100 per reader must be supported.
 - User definable custom images shall be displayed on the screen when the reader is idle.
 - The reader shall support the following image formats:
 - PNG,
 - JPG,
 - JPEG.
 - It shall be possible to adjust the reader beeper via the ISMS software to the following volume levels:
 - off,
 - quiet,
 - normal,
 - loud.
 - The reader shall have the ability to display the status of alarms and indicate the status of physical and logical items via LEDs on front panel.
 - The reader shall support at least 8 indication LEDs.
 - It shall be possible to turn off the reader indicator LEDs via the ISMS software.
 - Tamper detection shall be provided against the unit being removed from the mounting surface.
 - Keypad readers must comply with a minimum IP66 environmental protection rating.
 - Keypad readers must comply with an impact rating of at least IK08.
 - The keypad reader shall operate with a temperature range of -30°C to +70°C.

All readers must be RoHS compliant.

The keypad reader shall support a backlight feature for dark environments.

43. ACCESS CONTROL READERS – LONG RANGE

The requirement for long range access control readers will be specified in accompanying documents. When required, these readers shall meet the following specification.

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

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

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

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

A short-range access card or token shall have the ability to be temporarily associated with a booster to allow the data from the card or token to be transmitted to the long-range reader.

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

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

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

44. READER – BLUETOOTH AND NFC

The system shall have the capability to use a mobile device as an access credential in place of a traditional access control card.

Connectivity between the mobile device and access control reader shall be via BLE communication or NFC technology (subject to the capability of the mobile device).

In addition to BLE and NFC support, the access control reader must support multiple card and communication technologies to allow for scenarios where a mobile device may not be available. The reader shall support the following:

- Proximity 125 kHz,
- Mifare Classic,
- Mifare Plus,
- MIFARE DESFire EV1,
- MIFARE DESFire EV2.

Any communication between the ISMS and a cloud server shall be limited to those initiated by outbound requests from the ISMS only to ensure system security.

It shall be possible to configure the Bluetooth functionality of the reader via the ISMS.

The options for configuration shall include:

- enable/disable reader BLE functionality,
- enable/disable second factor authentication whereby the user must present their mobile device and enter a PIN or biometric identification,
- enable/disable the ability of the reader to advertise its name via BLE,
- adjust the overall transmit power of the reader,
- enable/disable the ability for the mobile device to automatically connect to the access control reader,
- adjust the signal strength threshold for auto connection to the access control reader,
- enable/disable the ability for the mobile device to manually connect to the access control reader,
- adjust the read range for manual connection to the access control reader.

It shall be possible to apply a global setting for all readers.

It shall be possible to apply a setting for individual readers.

It shall be possible to configure and calibrate the BLE functionality of the reader via an application on the mobile device. The configuration and calibration options shall include:

- enable/disable reader BLE functionality,
- enable/disable second factor authentication whereby the user must present their mobile device and enter a PIN or biometric identification,
- enable/disable the ability of the reader to advertise its name via BLE,
- adjust the overall transmit power of the reader,
- enable/disable the ability for the mobile device to automatically connect to the access control reader,
- adjust the signal strength threshold for auto connection to the access control reader by placing the mobile device at the distance where it is required to operate and selecting a calibration button,
- enable/disable the ability for the mobile device to manually connect to the access control reader,
- adjust the read range for manual connection to the access control reader by placing the mobile device at the distance where it is required to operate and selecting a calibration button.

Provisioning of a mobile device to be used as an access credential shall be carried out within the ISMS core software. Obtaining credential details via a third-party application or web site will not be acceptable.

Provisioning of the access credential shall be a two-step process to ensure security.

- An email shall be sent to the user who will confirm acceptance of the access credential on their mobile device.
- After acceptance, a confirmation code of no less than 6 digits shall be sent via SMS to the mobile device, whereby the user will enter this into the mobile device access control application to enable its operation.

The time allowed for the credential to be accepted shall be configurable within the ISMS. After the time has expired, the credential will need to be re-issued.

Systems that use a single step provisioning process are not acceptable. This is to avoid instances where the ISMS operator incorrectly enters an email address or mobile device number and an incorrect person receives the access credential.

It shall be possible to remove authorisation of access credentials via the ISMS should a mobile device be lost.

It shall be possible to re-issue access credentials via the ISMS should a mobile device be replaced.

It shall be possible to re-issue access credentials to another cardholder.

When the mobile device is presented to the reader, the access decision shall be made at the IFC. Systems where the access decision is made at the ISMS server or in the cloud are not acceptable.

In addition to using the mobile device as an access control credential, the following functionality shall be available via the mobile device access control application:

- arm and disarm an alarm zone,
- change the mode of a door from secure to free access, and vice versa,
- change the scheduled access mode of a door,
- activate/deactivate relay outputs anywhere on the system. The relays do not necessarily have to be connected to the access controller which is connected to the Bluetooth reader,
- receive messages from the ISMS via push notifications.

ISMS shall support Bluetooth Tag tracking utilising Bluetooth Low Energy specification outline for ibeacon and Eddystone.

45. ACCESS CONTROL READERS – BIOMETRIC (FINGERPRINT)

Where specified, biometric (fingerprint) readers are required for this project.

The reader shall be designed for wall mounting, positioned to allow ease of use for the user.

Where required, visual (LED and LCD graphic display) and audible feedback shall be provided to indicate:

- reposition the finger for a valid read,
- access granted,
- access denied.

The reader shall include a Mifare/DESFire contactless smartcard reader for verification mode where the fingerprint template is stored on a card.

The reader shall support encryption for both data in transit and data at rest for all biometric templates.

Tamper protection shall be provided against the unit being opened and against the unit being removed from the mounting surface.

The sensor resolution shall be 500dpi or greater and FBI PIV-IQS certified

Fingerprint read time shall be less than one second.

The reader shall be able to detect and reject artificial fingers presented to the reader.

46. ACCESS CONTROL READERS – BIOMETRIC (CONTACTLESS)

Where specified, contactless biometric readers are required for this project.

The reader shall be designed for wall mounting, positioned to allow ease of use for the user.

The reader shall acquire a biometric scan from a hand waved within sensor range without requiring contact to any surface.

Where required, visual (LED and LCD graphic display) and audible feedback shall be provided to indicate:

- pass hand through the sensor again for a valid read,
- access granted,
- access denied.

The reader shall include a Mifare/DESFire contactless smartcard reader for verification mode where the hand template is stored on a card.

The reader shall support encryption for both data in transit and data at rest for all biometric templates.

Tamper protection shall be provided against the unit being opened and against the unit being removed from the mounting surface.

Hand read time shall be less than one second.

The reader shall be able to detect and reject artificial hands presented to the reader.

47. ALARM MANAGEMENT TERMINAL – ACCESS CONTROL

AMTs shall be provided to allow keypad functionality as described in this section.

The AMT shall support self-discovery on the ISMS.

- AMTs shall contain a manufacturer's unique serial number.
- When connected to an IFC, the serial number of the AMT shall be reported to the ISMS.
- Once assigned to a function within an IFC, if any attempt is made to substitute AMTs in the field without authorisation, an alarm shall be generated.

Data communication rate between IFCs and AMTs shall be at least 1Mbit/second.

Communication sessions between IFCs and AMTs shall use certificate exchange protocols using keys with a minimum strength of ECC P-256.

Data communication between IFCs and AMTs shall use a minimum of AES-128.

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

AMTs shall be upgradeable via software downloaded from the ISMS without any intervention at the AMT.

Each AMT shall be identified independently on the ISMS by means of a unique plain language descriptor. The plain language descriptor shall be at least 60 characters in length.

The AMT must have a secure idle state to prevent unauthorised usage.

Where an AMT is specified, it shall include:

- The AMT must have a colour display, size being a minimum of 3.5".
- The display shall support multiple languages which shall be selectable from the ISMS software.
- The AMT shall display information to the user using a combination of text and graphics.
- The AMT shall display the date and time.

The AMT keypad shall be backlit.

The AMT keypad pad shall include:

- numerical 0 to 9 keys,
- a cancel key,
- an enter/accept key,
- two soft keys that vary according to the current usage of the AMT.

The AMT shall be capable of (but not limited to) carrying out the following functions:

- Arm alarm zones; a minimum of 50 per AMT must be supported.
- Disarm alarm zones; a minimum of 50 per AMT must be supported.
- View alarms; a minimum of 100 per AMT must be supported.
- Acknowledge alarms; a minimum of 100 per AMT must be supported and be decoupled from the ISMS.
- View alarm history; a minimum of 100 per AMT must be supported.
- Turn outputs on and off; a minimum of 50 per AMT must be supported.
- View the status of inputs; a minimum of 100 per AMT must be supported.
- Isolate inputs; a minimum of 100 per AMT must be supported.

User definable custom images shall be displayed on the screen when the AMT is idle.

Customisable message shall be displayed as the AMT utilised for entry and exit.

The AMT shall support the following image formats:

- PNG,
- JPG,
- JPEG.

It shall be possible to customise the AMT audio tones for Access Granted and Access Denied together with icons.

To adjust the AMT beeper via the ISMS software to the following volume levels:

- off,
- quiet,
- normal,
- loud.

Multiple AMTs can be used anywhere attached to the ISMS to remotely manage assigned intruder alarm zones.

The AMT shall have the ability to display the status of alarms and indicate the status of physical and logical items via LEDs on front panel.

The AMT shall support at least 8 indication LEDs.

It shall be possible to turn off the AMT indicator LEDs via the ISMS software.

Tamper detection shall be provided against the unit being removed from the mounting surface.

AMT readers must comply with a minimum IP66 environmental protection rating.

AMTs must comply with an impact rating of at least IK08.

The AMT shall operate within a temperature range of -30°C to +70°C.

A mobile App shall be utilised to access the AMT while using dual factor authorisation.

Cipher Pad function can be enabled to enhanced cardholder security.

48. ALARM MANAGEMENT TERMINAL – PERIMETER

AMTs shall be provided to allow keypad functionality as described in this section.

The AMT shall support self-discovery on the ISMS.

- AMTs shall contain a manufacturer's unique serial number.
- When connected to an IFC, the serial number of the AMT shall be reported to the ISMS.
- Once assigned to a function within an IFC, if any attempt is made to substitute AMTs in the field without authorisation, an alarm shall be generated.

Data communication rate between IFCs and AMTs shall be at least 1Mbit/second.

Communication sessions between IFCs and AMTs shall use certificate exchange protocols using keys with a minimum strength of ECC P-256.

Data communication between IFCs and AMTs shall use a minimum of AES-128.

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

AMTs shall be upgradeable via software downloaded from the ISMS without any intervention at the AMT.

Each AMT shall be identified independently on the ISMS by means of a unique plain language descriptor. The plain language descriptor shall be at least 60 characters in length.

The AMT must have a secure idle state to prevent unauthorised usage.

Where an AMT is specified, it shall include:

- The AMT must have a colour display, size being a minimum of 3.5".
- The display shall support multiple languages which shall be selectable from the ISMS software.
- The AMT shall display information to the user using a combination of text and graphics.
- The AMT shall display the date and time.

The AMT keypad shall be backlit.

The AMT keypad pad shall include:

- numerical 0 to 9 keys,
- a cancel key,
- an enter/accept key,
- two soft keys that vary according to the current usage of the AMT.

The AMT shall be capable of (but not limited to) carrying out the following functions:

- Arm alarm zones; a minimum of 50 per AMT must be supported.
- Disarm alarm zones; a minimum of 50 per AMT must be supported.
- View alarms; a minimum of 100 per AMT must be supported.
- Acknowledge alarms; a minimum of 100 per AMT must be supported.
- View alarm history; a minimum of 100 per AMT must be supported.
- Turn outputs on and off; a minimum of 50 per AMT must be supported.
- View the status of inputs; a minimum of 100 per AMT must be supported.
- Isolate inputs; a minimum of 100 per AMT must be supported.

Where an AMT is specified to control perimeter fence system, it shall be capable of (but not limited to) carrying out the following perimeter electric fence system functions:

- Override fence zones as follows:
 - arm,
 - disarm,
 - isolated (lock out zone(s) for maintenance).
- Display Fence Zone status ("Armed", "Disarmed", "Alarms in System") on the front panel LEDs.

-
- Display the Fence Zone status details such as High Voltage, Low Voltage and Iso-lated.
 - Display current fence return voltages.
 - Display fence return voltage range for the past seven days.
 - Display backup battery status and voltage.
 - Display current ambient temperature of the Electric Fence Controller.
 - Display the temperature range for the past seven days.

User definable custom images shall be displayed on the screen when the AMT is idle.

The AMT shall support the following image formats:

- PNG,
- JPG,
- JPEG.

It shall be possible to adjust the AMT beeper via the ISMS software to the following volume levels:

- off,
- quiet,
- normal,
- loud.

Multiple AMTs can be used anywhere attached to the ISMS to remotely manage assigned intruder alarm zones.

The AMT shall have the ability to display the status of alarms and indicate the status of physical and logical items via LEDs on front panel.

The AMT shall support at least 8 indication LEDs.

It shall be possible to turn off the AMT indicator LEDs via the ISMS software.

Tamper detection shall be provided against the unit being removed from the mounting surface.

AMT readers must comply with a minimum IP66 environmental protection rating.

AMTs must comply with an impact rating of at least IK08.

The AMT shall operate within a temperature range of -30°C to +70°C.

49. ACCESS CARDS AND TOKENS

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

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.

All cards shall meet ISO standards.

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

The access token data shall include:

- support for up to 2008-bit card numbers,
- where a proprietary card number format is offered, the card format shall include:
 - a unique site code not used for any other system worldwide,
 - a unique cardholder identification number at least 7 digits long,
 - 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.

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

Uniquely identifiable information shall be stored in the access token in a secure format.

Transmission of data between the proximity access token and the proximity reader shall be in a secure format.

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.

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.

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.

50. TOKEN – MIFARE CLASSIC TECHNOLOGY

The cards shall incorporate Mifare Classic technology.

The card number must be a number specifically encoded to a sector of the card. It shall not be the CSN.

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

The encoded card data shall incorporate data consisting of:

- the assigned card number,
- a site-specific key consisting of 32 hexadecimal characters.

Card encoding shall be an integral part of card production.

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

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

Where multiple sectors on the Mifare card are configured for different applications, single pass card encoding shall be used.

51. TOKEN – MIFARE PLUS TECHNOLOGY

The cards shall incorporate Mifare Plus technology.

The card number must be a number specifically encoded to a sector of the card. It shall not be the CSN.

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

The Mifare Plus “S” variant shall be provided.

The encoded card data shall incorporate data consisting of:

- the assigned card number,
- a site-specific key consisting of 32 hexadecimal characters,
- the 32 hexadecimal key shall optionally be sourced from a customer specified key-safe.

Card encoding shall be an integral part of card production.

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

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

Where multiple sectors on the Mifare card are configured for different applications, single pass card encoding shall be used.

52. TOKEN – MIFARE DESFIRE TECHNOLOGY

The cards shall incorporate DESFire technology.

The card number must be a number specifically encoded to an application on the card. It shall not be the CSN.

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

The DESFire EV2 variant shall be provided.

The encoded card data shall incorporate data consisting of:

- the assigned card number.
- a site-specific key consisting of 48 hexadecimal characters.

The 48 hexadecimal key shall optionally be sourced from a customer specified key-safe

Card encoding shall be an integral part of card production.

The application unlock key and the DESFire CAD unlock key shall be user definable.

53. CREDENTIAL – BLUETOOTH AND NFC ON MOBILE DEVICE

An application shall be provided that enables a mobile device to be recognised as a valid credential for the ISMS.

The mobile device access control application shall have a built-in help system.

Credentials shall be managed with strong encryption.

It shall be possible to enable two factor authentication with the addition of either:

- PIN, or
- biometric (where supported by the mobile device).

The second authentication factor shall be selected by the user at the time of registration.

Where biometric authentication is deployed, no biometric information shall ever leave the device, this includes during the initial registration and authentication.

It shall be possible to connect the mobile device access control application to the reader for access control verification:

- Manual connection; whereby the user must interact with the mobile device access control application to request access. Interaction must be no more complex than opening the application and touching an icon relating to the reader.
- Auto-connection; whereby the phone is authorised with a reader when the signal strength reaches a configured threshold, and does not have to open the application and touch an icon.

Provisioning of the access credential shall be a two-step process to ensure security. After acceptance, a confirmation code of no less than 6 digits shall be sent to the mobile device,

whereby the user will enter this into the mobile device access control application to enable its operation.

The mobile device access control application shall support multiple sites without requiring the device holder to change any settings to move between sites.

The mobile device access control application shall support a digital ID:

- Displaying all the information as is available in the integrated card design program.
- The digital ID shall display the time that the information was verified on the ISMS server.
- If the digital ID is not able to verify with the ISMS server, then this shall be displayed as an additional message overlaying the digital ID.

54. CREDENTIAL - BIOMETRIC

The requirement for biometric authentication will be specified in accompanying documents. When required the following specifications shall be met.

The biometric readers and associated technology shall be fully integrated into the system. All biometric enrolment and template management user interfaces shall be provided seamlessly in the standard central control system user interface.

The operator shall not have to access a separate biometric template database to manage biometric templates.

The identification time (time to identify a presented biometric from the database) shall be less than 2 seconds.

The reader shall have tamper protection against removal of the reader from the wall, and removal of the reader fascia from the base.

Enrolment shall be carried out at a USB capable enrolment reader specifically provided for this purpose.

The enrolled biometric templates shall conform to the following:

- Each template shall be based on three separate presentations to obtain the best template.
- A second template associated with a second biometric (in case the primary biometric temporarily cannot be used for any reason) shall be enrolled.
- Two optional duress biometric templates shall be able to be captured and stored in the reader.
- The enrolment user interface shall provide visual and audible guidance for correct biometric presentation during enrolment.
- The enrolment user interface shall display a quality score associated with the biometric capture and warn the operator if the quality of the template is low.

-
- The enrolment user interface shall provide an indication of the enrolment quality of the presented biometrics. The level of quality threshold for accepting presented biometrics shall be adjustable by the operator.

When identification mode (1 to many, or 1:N) is specified:

- The enrolment reader shall read the biometrics and store them as biometric templates in a central database.
- The biometric templates defined above shall be a subset of the cardholder record.
- During the biometric read process, the presentation of a biometric at a reader shall initiate a database inquiry at the reader. If the biometric is determined to be of a valid cardholder, the associated access will then be verified by the access controller before access is granted.

When verification mode 1 to one, or 1:1 is specified:

- The enrolment reader shall read the biometrics and store the template data onto a Mifare Classic, Mifare Plus, or DESFire card.
- When the card is to be encoded, the user shall be prompted to enrol the biometrics and the card shall then be encoded with both the system identification data and the biometric data.
- There shall be a configurable option whether to save cardholder biometrics to the central database or discard after encoding to card.
- During the biometric read process, the biometric read at a reader shall be compared with the template data read from the card. If the biometric is determined to be a match, then the associated access will be verified by the access controller before access is granted.
- An authorised system operator shall be able to generate and download a Mifare A key to all readers in the system.
- The A key shall be either generated automatically as a random hexadecimal key, or manually entered.
- On a Mifare Classic or Mifare Plus card, the Mifare sectors where the biometric template data is to be stored shall be user definable.

55. RS485 FIBRE TRANSCEIVER REQUIREMENTS

The fibre transceiver shall provide two independent data channels operating as either multi-mode or single-mode devices (depending on the model).

Each channel will be capable of transparently supporting data speeds of 1MB/S on a single fibre.

Each data channel will be capable of handling 2-wire half-duplex RS485 data as per the TIA/EIA standards.

The multi-mode fibre transceiver shall be capable of supporting distances up to 4km between fibre transceivers.

The single-mode fibre transceiver shall be capable of supporting distances up to 40km between fibre transceivers.

Up to 60 devices per RS485 channel shall be supported.

The fibre transceiver shall support the following network topologies:

- point-to-point,
- multi-drop,
- redundant self-healing ring topology.

The fibre transceiver will provide indication of port faults and network damage which shall support the following:

- LED indication at the unit,
- relay output at the unit,
- configurable to indicate either local or global (all transceivers) faults.

LED indicators on the fibre transceiver shall indicate the following:

- data activity,
- synchronisation status,
- fault status,
- fault location.

Each channel shall support individually selectable RS485 biasing via a dip-switch.

The operating temperature for the fibre transceiver will be -40°C to +75°C.

The fibre transceiver shall have reverse polarity protection.

Mean time between failure for the fibre transceiver should be no less than 100,000 hours.

56. ENERGISED PERIMETER INTRUDER DETECTION - STRUCTURE

The physical fence part of the energised intruder detection system shall be a multi-wire Energised Security Fence (ESF) which consists of a horizontally spaced grid of conductive wires supported by a specially made carrier fence. This will comprise of insulated components exclusively used for a security fence, and support posts retro-fitted to an existing solid and/or mesh type fence or wall.

The system shall be installed in accordance with the manufacturer's installation instructions.

The operating voltage for the energised fence shall be a high voltage short duration pulse, managed and continually monitored to deter intrusion by giving any intruder a high voltage pulse should they touch any part of the grid of conductive wires whilst earthed or in contact with other conductive elements.

All energised fence wires must deliver a deterrent pulse to an intruder touching a wire and earth, or attempting to penetrate between any adjacent wires.

The ESF shall contain intermediate insulating posts at a spacing not greater than three metres to minimise ability to spread the grid of conductive wires creating a viable opening in the energised fence.

Physical hardware (e.g. tensioning devices, springs and insulators) should be inherently designed to suit security applications. Items designed and used for agricultural applications will not be acceptable.

Intermediate insulating components shall have a minimum electrical tracking distance of not less than 80mm.

Intermediate insulating components shall have no area where the conductive wires can be trapped easily between insulator surfaces of the insulating components if the conductive wire is demounted from its nominal position on the insulating component.

Shielding of insulating components should be designed to direct the conductive wire to an earth contact to maximise alarm generation if the conductive wire is demounted from its nominal position.

The retention mechanism of the conductive wire on the insulating components shall be designed to break during climbing attempts where a load greater than 30kg is applied in a direction away from the physical fence structure.

All structural climb points must be fitted with additional intrusion detection and anti-climb protection.

The conductive wires shall be attached to the inner face of the barrier security fence and access gates when installed within 1.5m of ground level. The barrier security fence provides a physical separation barrier between the general public and the exposed pulsed conductive wires.

Unless otherwise specified, the conductive wires shall extend at least 0.6 metres above the top of the existing barrier security fence fabric or a minimum of 1.0 metre above a wall.

Each energised fence circuit on the same fence control device must be capable of being operated independently.

Where two fence circuits are operating within the same detection zone, shorting of one conductive wire to earth or another conductive element (excluding second conductive wire) should not directly affect the performance and detection of the second conductive wire.

Each access gate or perimeter access door shall be fitted with a switching device that will detect the opening of the gate/door. The switching device and/or attached controls shall ensure all high voltage pulses on or around the gate/door are effectively shorted to earth or disabled at the fence controller.

Opening of a perimeter access door or gate should annunciate an alarm condition on the system and inhibit the deterrent pulses on that gate.

Each active fence circuit shall be individually configurable for all functionalities.

Anti-climb configuration at strain points shall be provided, above the physical barrier. The fence circuit shall be routed around strain posts and connected to strainers such that it forms part of the continuous electrical circuit and does not constitute a parallel, redundant or dead-end path.

Re-tensioning of fence wires must be possible without the need to reposition anti-climb elements.

All joints between conductive elements in a fence circuit shall be clamped and not rely solely on tension of the conductive wire to maintain the integrity of the electrical connection. This excludes the external pressure contact between gate switch halves.

All metal components of the system must be protected against the environment using aluminium alloy, or steel with zinc-based galvanising.

- Copper based components are not permitted.
- Stainless steel should not be mechanically or electrically coupled to aluminium or zinc galvanised components without measures to prevent galvanic corrosion.

Security posts shall be galvanised to ensure maximum environmental protection and performance.

The termination point of the conductive wire should be at the tensioning device.

Tensioning devices should be attached to the ESF structure by insulated mounting hardware. Tensioners that are attached to the ESF structure by wire hooks shall not be acceptable.

Fine pitch tensioning capability shall be provided for ease of adjustment during installation and maintenance.

The tensioning of the conductive wire shall be integrated into the tensioning device directly attached to the security fence post. Independent tensioning devices shall not be acceptable.

Re-tensioning of conductive wire must be possible without the need to reposition the configuring links.

Where springs are attached to the grid of conductive wires, an indication of the tension of the conductive wire must be clearly visible on the spring device.

Where springs are attached to the grid of conductive wires, the spring must be in direct electrical contact to the tensioning device.

Springs used in the tensioning of the conductive wire should be of a single continuous wire which forms part of the conductive circuit.

Any spring which form part of the conductive circuit should have a means of physically limiting the length of extension of the spring.

Each conductive wire shall be capable of deterring and detecting potential intruders by means of a high voltage pulse and detecting the following types of attack:

- cutting or disconnecting any wire,
- shorting any wire to ground or the support fence,
- shorting adjacent but different polarity wires,
- shunting the wires with an electrically conductive material to reduce the pulse voltage.

Each active fence circuit shall always be monitored.

The system shall be configured in accordance with the specific contract drawings.

The system shall generate an alarm within four seconds if any one wire is cut or continuously short circuited to an adjacent wire or to earth.

The shorting together of any conductive wires, or cutting of any wires, shall have no impact on the deterrent or detection capability of the remaining active fence circuits and zones.

The shorting together of any conductive wires, or cutting of any wires, shall raise an alarm in the ISMS.

The system shall generate minimal nuisance alarms in any environmental conditions of wind, rain, or temperature, nor from wildlife of less than five kilograms.

The system shall have a false alarm rate no greater than one false alarm per fence line kilometre per week.

All fence pulses shall be synchronised so that the pulses on adjacent fence sections do not occur at a time interval less than permitted in the current version of relevant standards (IEC60335-2-76).

When specified, local control at field cabinets shall be provided via an AMT.

Fully adjustable lightning diverter and protection devices shall be connected to each ESF circuit connection.

An independent earthing system must be provided for the ESF earth return with a physical separation of 10m from any other earthing system.

Where the ESF abuts to, attaches to or passes over any metallic structure, that structure must be grounded or earthed using a separate earthing system.

When specified, the ESF must be capable of interfacing with an emergency shutdown system, which in the event of an incident will electronically deactivate and isolate the high voltage deterrent pulses on the conductive wire array.

- The emergency shutdown when specified shall be a fail-safe interface, carried out at each of the field cabinets to minimise dependency on site communication systems.

The system manufacturer shall support the product for a minimum period of ten years from the time at which the product is superseded.

The system must be formally inspected and assessed by a manufacturer approved representative, to the manufacturer's published standard.

Full system documentation meeting the manufacturer's compliance, minimum quality, safety codes, and instruction must be provided to the system end user representative.

An annual preventative maintenance program must be offered to check and maintain the ESF to an operational and safe condition.

57. ENERGISED SECURITY FENCE CONTROLLER – STAND ALONE

The physical fence part of the energised intruder detection system shall be a multi-wire ESF which consists of a horizontally spaced grid of conductive wires supported by a specially made carrier fence. This will comprise of insulated components exclusively used for a security fence, and support posts retro-fitted to an existing solid and/or mesh type fence or wall.

The ESF controller shall generate pulses at intervals of not less than 1.1 seconds.

The ESF controller shall be available as a single fence circuit or dual fence circuit option.

The ESF controller shall be capable of delivering 2.3 Joules when configured as a live/earth system, i.e. alternate wires have a voltage or are earthed.

The ESF controller shall be capable of delivering 4.6 Joules when configured as a dual-pulse system, i.e. alternate conductive wires have positive to negative voltages.

The ESF controller shall provide an optional reduced voltage operating mode to provide full detection capability as per high voltage but with reduced deterrent.

An alternative ESF controller shall be available with the following capabilities where the project requires:

- When configured as a live/earth system, the ESF Controller shall be capable of increasing the output from 2.3 Joules to 3.6 Joules per fence circuit. This is triggered when there is a drop in voltage from one high voltage pulse to the next, which has reached a pre-defined alarm threshold.
- When configured as a dual-pulse system, the ESF Controller shall be capable of increasing the output from 4.6 Joules to 7.2 Joules. This is triggered when there is a drop in voltage from one high voltage pulse to the next, which has reached a pre-defined alarm threshold. Output is measured across alternate wires.
- The ESF shall return to the standard output after 20 minutes.

The conductive wire pulses shall be synchronised so that the pulses on adjacent fence sections occur within time intervals as permitted in the reference standards.

The ESF controller shall operate within an ambient temperature range of -20°C to +50°C.

The ESF controller shall have temperature sensors to monitor the internal temperature of its enclosure and adjust performance as follows:

- 75°C. Over-temperature.
 - An indicator LED on the front panel shall flash and the ESF controller shall reduce its pulse rate to reduce the internal temperature
- 85°C Critical temperature.
 - The ESF controller must stop generating pulses and turn off.

The ESF controller shall have indicator LEDs on the front panel to indicate the following:

- over temperature alarm,
- service alarm,
- tamper,
- mains power failure,
- battery test failed, or battery missing,
- high voltage mode,
- low voltage mode,
- fence circuit pulsing with return voltage measurement in the form of a bar-LED indicator,
- synchronisation status:
 - off,
 - synchronisation conflict,
 - correct synchronisation.

The ESF controller shall have a service mode to allow a service technician to easily isolate and locally control fence circuits.

This service mode shall be accessible at the ESF controller by means of a special key.

The ESF controller shall provide battery management as follows:

- trickle charge; slow charge rate when battery is below 10 VDC,
- bulk charge; maximum charge rate for fast battery recovery,
- float charge; slow charge rate to accommodate temperature variations,
- battery save; reduce electric pulse rate to save battery power.

The ESF controller shall support external power supplies such as additional backup batteries or solar cells to be connected.

The ESF controller shall operate in a standalone mode such that it does not require any external system software for its configuration and control.

Configuration shall be via dip-switches inside the ESF controller.

The fence circuits shall be armed and disarmed via input signals from an external switch, keypad, or alarm panel.

The ESF controller shall have output relays to indicate the following:

- system alarm,
- power supply failure,
- primary fence circuit alarm,
- armed status,
- secondary fence circuit alarm, for the dual fence circuit ESF controller.

The ESF controller shall have the capability to be changed from a standalone unit to a networked unit which is connected to an ISMS via a dip-switch, without the need to change any firmware within the ESF controller.

58. ENERGISED SECURITY FENCE CONTROLLER - NETWORKED

The ESF controller shall deliver an electric pulse through the fence wires to maximise the intruder deterrent and detection capabilities whilst meeting global safety standards.

The ESF controller shall operate in a networked environment and be controlled and monitored by the ISMS.

The ESF controller shall generate pulses at intervals of not less than 1.1 seconds.

The ESF controller shall be available as a single fence circuit (single zone) or dual fence circuit (dual zone) option.

The ESF controller shall be capable of delivering 2.3 Joules when configured as a “live/earth” system, i.e. alternate wires have a voltage or are earthed.

The ESF controller shall be capable of delivering 4.6 Joules when configured as a dual-pulse system, i.e. alternate conductive wires have positive to negative voltages.

The ESF controller shall provide an optional reduced voltage operating mode to provide full detection capability as per high voltage but with reduced deterrent.

The ESF controller shall support self-calibrating alarm thresholds that vary the required voltage drop to generate an alarm in response to long-term environmental factors.

An alternative ESF controller shall be available with the following capabilities where the project requires:

- When configured as a live/earth system, the ESF Controller shall be capable of increasing the output from 2.3 Joules to 3.6 Joules per fence circuit. This is triggered when there is a drop in voltage from one high voltage pulse to the next, which has reached a pre-defined alarm threshold.
- When configured as a dual-pulse system, the ESF controller shall be capable of increasing the output from 4.6 Joules to 7.2 Joules. This is triggered when there is a drop in voltage from one high voltage pulse to the next, which has reached a pre-defined alarm threshold. Output is measured across alternate wires.
- The ESF shall return to the standard output after 20 minutes.

The conductive wire pulses shall be synchronised so that the pulses on adjacent fence sections occur within time intervals as permitted in the reference standards.

The ESF controller shall operate within an ambient temperature range of -20°C to +50°C.

The ESF controller shall have temperature sensors to monitor the internal temperature of its enclosure and adjust performance as follows:

- 60°C Temperature warning.
 - It shall be possible to activate a relay to turn on an external cooling fan.
- 75°C Over-temperature.
 - An indicator LED on the front panel shall flash and the ESF controller shall reduce its pulse rate to reduce the internal temperature
- 85°C Critical temperature.
 - The ESF controller must stop generating pulses and turn off.

The ESF controller shall have indicator LEDs on the front panel to indicate the following:

- over temperature alarm,
- service alarm,
- tamper,
- mains power failure,
- battery test failed, or battery missing,
- high voltage mode,
- low voltage mode,
- fence circuit pulsing with return voltage measurement in the form of a bar-LED indicator,
- synchronisation status:
 - off,

-
- synchronisation conflict,
 - correct synchronisation.

The ESF controller shall have a service mode to allow a service technician to isolate and locally control fence circuits.

- An event shall be sent to the system when the ESF controller is in service mode.
- The service mode shall be capable of being enabled from the ISMS.
- This service mode shall be toggled at the ESF controller by means of a special key when enabled by the ISMS.

The ESF controller shall provide battery management as follows:

- trickle charge; slow charge rate when battery is below 10 VDC,
- bulk charge; maximum charge rate for fast battery recovery,
- float charge; slow charge rate to accommodate temperature variations,
- battery save; reduce electric pulse rate to save battery power.

The ESF controller shall support external power supplies such as additional backup batteries or solar cells to be connected.

The ESF controller shall support self-discovery on the ISMS.

- ESF controller shall contain a manufacturer's unique serial number.
- When connected to an IFC, the serial number of the ESF controller shall be reported to the ISMS.
- Once assigned to a function within an IFC, if any attempt is made to substitute ESF controllers in the field without authorisation, an alarm shall be generated.

Data communication rate between IFC and the ESF controller shall be at least 1Mbit/second.

Communication sessions between IFC and ESF controller shall use certificate exchange protocols using keys with a minimum strength of ECC P-256.

Data communication between IFCs and ESF controllers shall use a minimum of AES-128.

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

ESF controllers shall be upgradeable via software downloaded from the ISMS without any intervention at the controller.

59. SYSTEM INTEGRATION

The ISMS shall support OPC AE protocol.

-
- The OPC AE interface shall allow third party OPC clients to subscribe to receive alarms and events from the ISMS.
 - When an alarm is processed, the OPC AE client shall send an event processed message back to the ISMS to process the alarm on the ISMS.
 - The ISMS shall support multiple simultaneous OPC AE connections.

The ISMS shall support OPC DA protocol.

- The OPC interface shall support OPC DA specification 2.0 and 3.0.
- The OPC DA interface shall allow the status of system components to be reported to an external OPC DA client.
- The OPC Interface shall allow third party OPC DA clients to generate system component overrides including but not limited to alarm zone and access zone overrides.
- The ISMS shall support multiple simultaneous OPC DA connections.

The ISMS shall support a REST Web Service API.

- The ISMS cardholder functionality shall support a REST Web Service to allow an external system to create, remove, and modify cardholders, including assigning access rights.
- The ISMS alarms and events functionality shall support a REST Web Service to allow external systems to receive alarms and events from the ISMS.
- The ISMS shall provide a REST Web Service that will allow a third-party system to perform actions in the ISMS such as open doors, disarm alarm zones, and turn an IFC output on.
- The ISMS shall support a REST Web Service that will allow a third-party system to interrogate the status of ISMS items such as doors, alarm zones, and IFC inputs.

The ISMS shall allow data exchange with other applications using XML protocols.

- The system shall provide an XML interface to allow for the import, export, and synchronisation of data in an on-going basis from other applications directly into the cardholder database both in a real-time manner and in a batch-oriented approach. A developer's kit with a sample application shall be readily available.
- The system shall provide an XML interface to allow for updating access control schedules from other applications directly into the ISMS database in both a real-time manner and in a batch-oriented approach. A developer's kit with sample application shall be readily available.

The system shall provide a tool which allows configuration and synchronisation of cardholder data with third party systems via a csv file. The CSV import functionality shall support the following functionality:

- manually triggered data import,

-
- schedule triggered data import,
 - images imported via flat file.

An API that communicates directly to the IFC shall be available.

- The API shall allow third party systems to pass events to the IFC and for the events to appear in the ISMS event window.
- It shall be possible for the IFC to be programmed to trigger actions based upon these external events. For example, a video analytic alarm from a video management system is passed to the IFC, the IFC in turn will lock doors and raise an alarm.
- It shall be possible for a third-party system to send a card number and site code to the IFC to act as a “virtual card reader”.
- The API shall allow the third-party system to interact directly with the IFC with no reliance on the ISMS server.

The ISMS shall support the BACnet communications protocol.

- BACnet communication will be via TCP/IP.
- The IFC will communicate with BACnet devices with no need for server intervention.
- The BACnet integration will enable the IFC to monitor BACnet objects for state changes and raise alarms accordingly.
- The BACnet integration will enable the IFC to change BACnet object states in response to events.

The ISMS shall support the SNMP communications protocol.

Events from third party systems shall be managed in the same way as inputs connected directly to IFCs.

Interactions with third party systems shall be logged in the ISMS.

ISMS shall support smart sensor integration which detects the following

- Masking
- Air quality
- Volatile organics
- Vaping
- Gunshot
- Tetrahydrocannabinol (THC)
- Fine particulate matter (PM 2.5 and PM10)

-
- Ammonia
 - Nitrogen dioxide
 - Carbon monoxide
 - Carbon dioxide
 - Help keyword
 - Aggression
 - Barometric pressure
 - Light level
 - Temperature
 - Humidity
 - Tampered
 - Sound level

The system shall support biometric reader integration which can read all four fingerprints on a cardholder's hand.

The ISMS shall have the ability to integrate with SIP intercoms and provide the following functionality

- Answer calls from the ISMS
- Call a SIP intercom from ISMS
- Please a call on hold
- Hanging up a call
- View video for an intercom at 720p resolution
- Grant access

60. VIDEO MANAGEMENT SYSTEM INTEGRATION

The ISMS shall be capable of concurrently interfacing with VMS from multiple vendors.

It shall be possible for the ISMS to view live video from multiple cameras within its interface.

The ISMS shall be capable of viewing stored (archived) video from the VMS within its interface.

Where supported by the integrated VMS, it shall be possible to operate camera controls such as:

- PTZ,

-
- pause,
 - forward,
 - rewind.

It shall be possible to maximise a camera window.

- Whilst a camera window is maximised, the other camera windows should be changed to live thumbnail images to ensure the operator is able to see activity in all cameras.

It shall be possible to drag a camera icon from a site plan into a video view to dynamically be able to view cameras in an ad hoc manner.

It shall be possible to drag a camera icon from a list into a video view to dynamically be able to view cameras in an ad hoc manner.

It shall be possible to find a camera from a search box.

Where supported by the integrated VMS, it shall be possible for the ISMS to send a message to the VMS to move cameras to priests.

Where supported by the integrated VMS, it shall be possible for the ISMS to receive motion detection and video analytic events from the VMS.

61. REST API

The ISMS shall support a RESTful web API.

The RESTFUL API shall support client certificate pinning for connection security.

The RESTful API shall be authenticated and secured using TLS client certificates (2048-bit RSA).

The RESTFUL API shall support HTTPS for data transfer.

Rest API should allow Cardholder data Synchronisation between ISMS servers

Rest API shall be able to interface to the Visitor Management setup on the ISMS in order to set up the following

- Create Visitor
- Modify any Visit attributes
- Delete Visitor

ISMS shall allow Restful APIs to create, amend and delete access schedules as a requirement for a single source of truth.

Restful API shall allow for mixed key-and-certificate authentication

Restful APIs are utilised for Active Directory Cardholder Synchronisation

The system shall support Events and Cardholder data Synchronisation from a source to destination servers by utilising Rest APIs.

The web-based client shall use REST API via an API Gateway that has no persistent storage.

The ISMS shall send updates to web-based client session through use of Rest APIs via API Gateway.

REST API shall allow the users to redact Personal Identifiable Information (PII) from the system in order to meet GDPR requirements