

**Access Control System**

Sielox™

Pinnacle™ Version 10L

March 2020

**A/E Specification Lite**

Subject to Change

Copyright © 2006-2020 by Sielox, LLC.

Published by:

Sielox, LLC

170 East Ninth Avenue
Runnemede, NJ 08078

856-939-9300 Phone
[www.sielox.com](http://www.sielox.com)

General

## Introduction: Complete System Proposal

* + 1. This document provides the information necessary to produce a complete proposal for a highly secure, easy-to-use and dependable Access Control System (ACS). The ACS shall provide the speed and flexibility of 32 bit multiple-technology controllers and be managed by a client/server application using an intuitive graphical operator interface on the Microsoft Server 2008 R2, 2012, 2012 R2, 2016, 2019, Windows 8.1 Pro or Windows 10 Systems. All devices, such as card readers, keypads, access cards, alarm inputs and outputs. The ACS shall include all computer hardware and software, field controllers, communication boards, power supplies, battery backup, [**electric hardware], [conduit], [raceways**], and all other equipment as indicated on the contract drawings and as specified herein. All material shall be the manufacturer'’ standard catalog products.

## System Description

* + 1. The ACS shall be a 32-bit native Microsoft Windows program with support for 64-Bit Operating Systems. OS options should include Microsoft Server 2008 R2, 2012, 2012 R2, 2016, 2019, Windows 8.1 Pro or Windows 10 Systems. Enterprise application with multi-operator and multi-threaded (multi-tasking) capability, allowing independent activities and monitoring to occur simultaneously at different locations. The Client workstation shall be easy to use and employ intuitive icon-based operator interface.
		2. The ACS shall be simple and economical enough to support a single site, yet powerful and flexible enough to manage multiple-sites, across a LAN or WAN network.
		3. ACS shall operate in a client/server or client/database server to hardware server or sever thin client (web based) when configuration on high-quality servers or work station computers running Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019, Windows 8.1 Pro or Windows 10 Enterprise operating system and with a Microsoft SQL 2016 Standard or Enterprise edition databases. SQL 2014 Express wit SP3 is included and will be acceptable for smaller or basic systems. The software shall be designed to support the manufacturer’s past & present generation access control hardware.
		4. The ACS shall allow ODBC database access either through a defined ODBC interface or an SDK library set.
		5. The ACS shall conform to standard networking protocols, including TCP/IP iP4 and iPv6 Ethernet Protocols.
		6. All core ACS hardware and software shall be developed and manufactured by the same manufacturer, and be made and supported I the U.S.A.

### Manuals

#### The manuals shall contain the following:

##### **Installation Guide**, this manual shall identify the operational requirements for the system and explain the theory of operation, design philosophy and specific functions.

##### **Operator’s Guide**, the operator’s manual shall fully explain all procedures and instructions for the operation of the system.

### Regulatory Requirements:

#### Systems shall be designed, manufactured, tested and installed in accordance with NFPA 70 (National Electrical Code), state codes, local codes, requirements of authorities having jurisdiction and in particular:

#### Equipment and materials for which there are UL standard testing requirements, listings, and labels shall be listed and labeled by UL or ETL, and meet or exceed all appropriate FCC Regulations.

## Warranty

### Manufacturer’s Warranty: Submit manufacturer’s standard warranty document executed by authorized company official. Manufacturer’s warranty is in addition to, and not a limitation of, other rights Owner may have under the Contract Documents.

## SOFTWARE MAINTENANCE

### The ACS manufacturer shall provide a minimum of two types of after warranty support

#### A Standard Protection plan and an Enhanced Service plan. Pricing for each option will be included in the bid.

### The ACS manufacturer shall support the current version of the ACS software and at least [2] full version back.

## Manufacturer Shall be: **Sielox, LLC**

170 East Ninth Avenue
Runnemede, NJ 08078

856-939-9300 Phone
[www.sielox.com](http://www.sielox.com)

### Server and Client Configuration

|  |  |
| --- | --- |
| Operating System | **Lite, Standard, Plus, and Clients:** Microsoft Server 2008 R2, 2012, 2012 R2, 2016, 2019, Windows 8.1 Pro or Windows 10 Professional/Enterprise**Professional:**Microsoft Server 2008 R2, 2012, 2012 R2, 2016, 2019, Windows 8.1 Pro or Windows 10 Professional/Enterprise |
| Microsoft SQL2014 Express Database Engine Guidelines | **Lite, Standard, and Plus:**Microsoft SQL 2104 Express included; greater than 128 readers or 10K cardholders OR 5K events per hour or 4 client workstations OR database partitioning requires Standard or Enterprise Editions of SQL which is not included.**Professional:**Standard or Enterprise Editions required (not included); SQL Express is included only to start up systems, MS SQL 2016 Standard or Enterprise required |
| Hard Disk Size | 1 - 500 GB - Raid 1 Mirror for Lite, 2 - 500GB Raid SATA Hot Swappable Raid 1 SATA HD for Standard, Plus, and Professional, computers/server should be upgradeable to RAID 5 if needed |
| Processor | **Lite and All Clients:** Pentium 4, Single Core 3.8 GHz or higher**Standard or Plus;** 4 Dual Core 3.8 GHz or higher**Professional:** Pentium 4 Duo Core 3.8GHz or higher |
| Memory | **Lite, Standard, Plus, and Clients:** 4GB**Lite, Standard, Plus Server:** 4GB**Professional** **Server:** 8GB |
| Monitor/Video | 19” LCD or Larger to suit application and desk space |
| Network Card | 10/100/1000 MB |
| Mouse | USB or wireless |
| Ports | 4 USB  |
| Keyboard | USB or wireless |
| Speakers | Built in or external as application and desk space allow |

###

### B. Multi-Hardware Communication Servers (**Option**)

#### The ACS shall support an advance distributed architecture allowing the use of multiple hardware communication servers.

#### The multi-hardware communication server architecture shall also allow linked inputs and outputs between different hardware servers.

#### The ACS shall provide support for drag and drop and Cut and Paste of Controllers setting across hardware communication servers and within the same Hardware Server, allowing hardware communication servers and door/reader’s to be easily added to an existing configuration.

### C. System Field Controller

#### The ACS shall support the legacy controllers, hardware will be 100% backwards compatible to all legacy hardware.

#### The controllers shall be 100% distributed intelligence architecture. Each controller shall operate independently of one another. If the ACS Controller communication is lost, it will NOT revert to a degraded mode of operation. The ACS Controller will continue operation without losing any features for cardholders or alarm functions, and it will retain a minimum of 10,000 events which will be downloaded to the server upon the restoration of network communications. The failure of any ACS controller will result in a Maximum of 1 or 2 Card Readers doors in the off-line condition. Any controller offline condition that affects more than 1 or 2 readers will be considered unacceptable. Controllers that control 4, 8 or 16 readers are not acceptable to the Owner.

#### The controllers shall provide intelligent interface to intrusion detection and duress alarm devices, card reader devices, door locking and gate control mechanisms, elevator systems, local alarm devices, Intercom systems, and other auxiliary systems that may be part of a building security systems.

#### The ACS [AC-1700] controllers shall incorporate a 32-bit CPU, using high speed processing for maximum reliability. The design shall allow for a mixture of Readers and I/O support on a single board to facilitate expansion capabilities. Basic Controller

##### 1 or 2 Reader Controller [AC-1700] – Provides support for up to two card readers each with support for; door strike, door contact, and request-to-exit devices. All aspects of each input and output can be completely configured to meet owner’s needs. Any controller that supports 4, 8 or 16 readers per controller will be considered unacceptable.

##### Each Controller [AC-1700] shall have a minimum of 4 auxiliary inputs – each input could be independently configured to be Supervised 4 states or unsupervised 2 states. All aspects of shunting and other timing features shall also be independently configured.

##### Each Controller [**AC-1700**] shall have a Minimum of 4 auxiliary outputs – each output should be capable of being supervised and completely programmable. Relays are assignable to activate in the normally open or normally closed positions. The outputs will be assignable to trip on any system event, either alarm type event or on any Card holders type event. Each relay on the controller [**AC-1700**] shall be removable and field replaceable.

##### Each Controller [**AC-1700**] shall support the expansion of at least 56 auxiliary inputs and or outputs.

##### On board Ethernet Connection, and Network speed direct into controller CPU. A POE option should also be available. The POE option will power the Controller and up to two card readers attached to the [**AC-1700**] ACS Controller.

##### Each Controller [**AC-1700**] shall support up to 32 Allegion – Schlage AD and NDE series locks. The introduction of wireless locks shall not replace the use of the 2 hard wired reader ports enabling the controller to communicate with up to 34 doors.

#### Controllers shall incorporate the following basic features as minimums;

##### Cards stored on Controller 50,000 with one access level per cardholder

##### Cards stored on Controller 25,000 with three access levels per cardholder

##### Buffered events shall be a Minimum of 10,000

##### Equipment and materials for which there are ETL or UL standard testing requirements,

##### A Web based onboard port which will allow for remote; testing, status reports, rebooting of controller, input and output tests as well as the ability to remotely update the controllers’ firmware. (flash memory updates). This Maintenance port will remain operational even when the controller is communicating through the RS-485 port for day to day operation.

##### User-defined dry contact relays/outputs with or without supervision

##### User-defined SPDT dry contacts relays/outputs, shall be a minimum of 2 Amps max at 24 VDC or 24 VAC, and be removable (sockets) and field replaceable.

##### The ACS controller should run in a voltage range of 11.5 VDC to 18 VDC max.

i) All inputs and outputs of the ACS Controller shall be able to be supervised.

j) All communication through the Ethernet Port and RS-485 will have AES 256 encryption.

k) Provide support for FIPs 201 and CAC Card Standards.

l) Standard coin battery for memory and clock retention.

m) Secure SD card (standard type) for door configuration, database backup and end-user and

 field technician use, as well as remote setup without a network/computer.

 (Construction Mode)

n) The System shall have no limit to the number of Facilities codes that each controller will

 accept.

o) The controller will have LED indicators for the following, RS-485 ports, RS-232 ports,

 network port, relay’s (outputs), storage device on controller. Any ACS that does not have

 these field trouble shooting aids will be considered unacceptable.

#### All database information shall be stored at the controller level resulting in 100% of decision making being performed at the controller. Any controller that has a degraded mode of option will NOT be aceptable and will be rejected.

#### Controllers shall support direct wiring of a 1 or 2 Wiegand output readers without the need for a separate reader interface board, including any proprietary formats that may need to be incorporated in the to owners system.

#### Controllers shall be compatible with any identification device that transmits data using Wiegand, ANSI or Custom ANSI, or other industry standard protocols. This shall include but not limited to Proximity, HID, AWID, INDALA, Bar code, Magnetic stripe, Iclass, Corporate 1000, Smart Card, Weigand Readers, Keypads and Biometric readers or any combination of the above type readers.

 12. Local (server-independent) Anti-Passback per Terminal Controller (TC) and server based global and

 Soft Anti-Passback supporting up to 20 TC’s (40 Readers) per defined zone, each independent of

 Location:

###### **Hard** APB Card must be used to exit before it ca be used to enter or card must be used to enter before it can be used to exit. If this is out of sequence access is denied.

###### **Zoned** (universal) APB enforcing anti-Passback rules for up to 40 readers or 20 controllers in a defined area.

###### **Soft** APB Card must be used to exit before it can be used to enter or card must be used to enter before it can be used to exit. If this is out of sequence, access is granted and a soft anti-Passback violation event is posted.

###### **Timed** APB is time or group of times will automatically reset all APB logic forgiving anyone that may have resulted in an APB violation.

#### The ACS Controller [**AC-1700**]:

b) System architecture shall provide for controllers to communicate with Legacy controllers via point-to-point RS-485 2 wire, up to 4,000 feet from the Main Controller.

c) Local APB defined as being server-independent and performed at the entrance and exit point of a single 2-Reader Terminal Controller module.

#### The Controllers [**AC-1700**] shall have the capability of being upgraded (flashed) either from host computer or Maintenance Port directly to the board.

### Card Reader / Keypad

#### The ACS shall support proximity card, Wiegand, Magnetic Stripe, and barcode technologies to include the following manufacturers:

##### Sielox Mirage SG, Mirage 2, Performa, and AC-160 Keypad Readers

##### Integrated Biometric Readers

##### FIPS 201, PIV, TWIC, and CAC Reader Standards

##### Morpho V-Flex, V-Prox, V-Pass, V-Smart and V-Station

##### ALLEGION Aptiq Readers

##### HID including: iCLASS, Corporate 1000, BioCLASS, MultiClass and Indala

##### AWID Proximity Readers [26-75] bit

##### Sentex Passport Readers

##### Any Wiegand formatted Reader, [26-75] bit

##### Select [**Specified**] barcode Reader

##### FarPointe Readers

#### The Allegion AptiQ proximity reader shall be low profile, weatherized and have a read range of up to [five] inches. The reader shall communicate to the controller through a five conductor, stranded, shielded 18 AWG cable for distances up to 500 feet. The reader shall utilize a [26] bit wiegand data output and operate at [13.56 MHz]. The reader shall be available in industry standard switch plate size and mullion mount. The reader shall be suitable for indoor and outdoor applications and feature bi-color LED status indicator. The reader shall be powered by 12 VDC, supplied by the controller.

### Access Cards and Key Tags

#### The ACS shall be compatible with the following access control cards:

##### Sielox Performa – Proximity Plus, Cards and Key Tags/Fobs

##### ALLEGION AptiQ – Proximity, Cards and Key Tags/Fobs

##### AWID – Proximity, Cards and Key Tags/Fobs

##### HID – Proximity, Cards and Key Tags/Fobs

##### HID iClass – Contactless Smart Card/Corporate 1000, Cards and Key Tags/Fobs

##### Sentex Passport Credentials

##### Any Wiegand Card or Tag or Fob, 26-75 bit

##### US Government Issued PIV, TWIC, and CAC Credentials

##### FarPointe Proximity Cards and Key Tags

#### Allegion AptiQ Proximity cards shall be approximating the Thickness of a standard credit card. The card shall utilize 13.56 MHz operating technology. The card shall be compatible with the ACS manufacturer’s card readers. The card shall be available with pre-programmed customer-specific ID numbers and available in clamshell or graphics quality direct print. The graphics-quality direct print card shall also be available in a dual-technology proximity/magnetic stripe card.

## ACS Software Platform

### Basic Functions and Scalability / Expandability

#### The basic functions of the ACS software shall be:

##### Access granted, with card, tag, pin, or a combination of several.

##### Monitoring of all alarms and card events and general system activity.

##### Perform database management tasks like back-up, repair, and maintenance.

##### Database reporting, including errors and status.

##### Device or Controller Status and door lock override and control.

#### The ACS manufacturer shall provide a minimum of four levels of product scalability from entry to enterprise levels. Each low level will be expandable without penalty or the repurchase of an entire system. Any System Manufacture that cannot provide a scalable system to meet the end users growth will be considered unacceptable.

#### The ACS shall provide straightforward expandability with the following capabilities:

##### Support for one (1) online readers with maximum unlimited capacity

##### Support for one (1) cardholders with a maximum unlimited capacity

##### Support an unlimited number of cardholder custom fields

##### Support an unlimited number of client (thick) and Web (thin) workstations

##### Support an unlimited number of hardware communication servers

##### Support an unlimited number of addressable controllers

##### Support an unlimited number of total access levels and time zones

##### Support a maximum of 99 individual expiring access levels per cardholder, each with the ability of having the independent activation dates.

##### Support a maximum of 99 alarms levels, each customizable

##### Unlimited inputs and outputs, all programmable and customizable

##### Unlimited User defined Users (computer operators) Levels

##### Support an Unlimited number of Database Partitions

##### Support an unlimited number of Allegion – Schlage AD, NDE, LE, and RU/RM Series Locks.

##### Support an unlimited number of ASSA Abloy – Aperio Series Locks

### Operating System

* + 1. The ACS shall be a 32-bit Access Control Software, with 64-Bit support. ACS shall operate in a client/server or client/database server to hardware server or sever thin client (web based) when configuration on high-quality servers or work station computers running Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019, Windows 8.1 Pro or Windows 10 Enterprise operating system and with a Microsoft SQL 2016 Standard or Enterprise edition databases. SQL 2014 Express with SP3 is included and will be acceptable for smaller or basic systems. The software shall be designed to support the manufacturer’s past & present generation access control hardware.
			1. This ACS shall allow the ACS to take full advantage of these and other features inherent in the Microsoft family of products.
			2. Operating Systems including:
				1. Multi-operator and multi-threaded (multi-tasking) operation on an open architecture system
				2. Complete support for most standard networking protocols, including: TCP/IP, UDP
				3. Graphical operator interface, pull-down menus, mouse and keyboard control, standard Windows type environment.

### Database

#### The ACS software shall utilize Microsoft SQL Server 2008 R2, 2012, 2012 R2, 2016, 2019, or SQL Express for smaller or basic systems

### Networking

#### Networking capability shall be necessary to implement large scale and/or multi-location systems with ACS devices including intelligent field controllers and/or remote clients while overall control of the network is maintained at a central location. Local Area Networks (LAN) or Wide Area Networks (WAN) may be required.

#### The ACS shall support IP Tunneling and VPN communications in a multi-cast network environment.

#### A diagnostic utility (CKP Ping) shall be supplied to allow the operator to verify network communications between a server and workstations or between multiple workstations using LAN topology.

#### The ACS shall support Workstation LAN Disconnect messaging with automatic reconnect options as outlined below:

##### When LAN communications with the server is interrupted, a Network Status message shall be displayed at each effected workstation. The dialog box shall be accompanied by a system beep that continues until the “Silence” button is clicked, the ACS is closed or the user logs in, whichever happens first. The ACS shall receive new events or alarms at the workstation while disconnected or while Pinnacle is closed.

##### When LAN communications are restored, the Network Status message shall be updated. A system beep shall accompany the new message with a “Connect” button enabled. Clicking the “Connect” button shall cause the ACS to restart and the user to be prompted to log in again.

### Administration and Operating Features

#### The ACS shall provide an easy-to-operate graphical interface for security operators while performing complex access control, security management and reporting functions. The provided graphical operator interface (GUI) shall be designed following Microsoft Window’s guidelines.

#### The features below shall be standard without the need for any add-on software.

##### The ACS shall provide interactive on-line help with extensive on-line manual. The on-line manual shall be available to allow the operator to obtain detailed help without having to consult a manual.

##### Each workstation shall have access to all features if password level allows. Password levels shall be individually customized to allow or disallow operator access to a program function.

##### The operator shall have ability to view and operate up to four independently configured Events screens simultaneously. Each screen shall be capable of displaying its own title, filter, columns and cardholder image.

##### Each workstation shall have the option of having an Alarm Pop-up window appear to alert of pending alarms. The window shall also contain alarm response instructions and a field to enter security console operator comments. The ACS shall have the ability to cascade a maximum of ten Alarm Pop-Up windows per workstation.

##### Each workstation shall have the ability to filter alarms, events, and time controlled zones. Users shall be capable of defining alarms, events, and time controlled filters that will be displayed at each workstation. The set-up of an ACS will also allow the ability to trigger an email notification off a filtered event.

##### Alarm routing shall be provided so that if an alarm is unacknowledged for a preset amount of time the alarm will automatically appear on another user’s workstation. The system shall provide a minimum of 99 levels of alarm priority.

##### The ACS shall provide a device find feature on the device configuration screen.

##### The ACS shall provide for .wav files or system beep to be associated with alarm events for alarm annunciation. The playback frequency of the audible alarms shall be configurable from 1 to 10 times or until the alarm is acknowledged.

##### The ACS shall support the ability to perform a lock down via an input and be configurable to control one, many or all doors/locks in the system. When the button is reset, the lock should return the state it should be in at the time of the reset.

##### The ACS shall support the ability to perform a block of any or all readers associated with the lockdown which restricts access to all blocked readers except to those responders assigned a privileged access level.

##### The ACS shall support up to 8 privilege cardholders per reader as well as up to 16 privilege access groups per system.

##### The ACS shall provide the following Input and Output Linking:

###### **Local** = I/O Linking within the same Controller

###### **Regional** = I/O Linking within the same Controller Group [**AC-1700’s**] of controllers

###### **Global** = I/O Linking across [**AC-1700**] Controllers within the same server

###### **Universal** (when using hardware communication servers for enhanced communications)

##### The ACS shall provide the ability for an access level to shunt on or off an input in response to a card read. The shunt shall be either momentary, toggle or latch.

##### The ACS shall provide the ability for an access level to activate an output in response to a card read. The output shall activate for the momentary toggle or latch activation time set in the output configuration, and should be able to be controlled with a time zone.

##### The ACS shall provide n-screen image enhancements that allow color, brightness, and contrast control, along with image cropping, and red eye removal.

##### The ACS shall provide an Image Library feature that allows up to nine images to be associated with one cardholder record.

##### The ACS shall automatically activate and deactivate temporary access levels for a cardholder without affecting the cardholder’s regular access level.

##### The ACS shall provide a cardholder quick entry screen that allows the operator to configure and issue a card from that single screen.

##### The ACS shall provide First Person Rule (FPR, or snow day option), this feature disables the “Time-Unlock” door schedule until an authorized cardholder is admitted prior to the “Timed Unlock.

##### The ACS shall support entry of card internal identification number in decimal or hexadecimal formats.

##### The ACS shall support of multiple card formats, across multiple controllers and readers, independently configurable on a per controller [AC-1700] basis, including card only, card + PIN, or ANSI and Custom ANSI format. The following should be pre-programmed for speedy installation of the ACS system:

###### 26-bit Std & 33-bit CKP Wiegand

###### 26-bit Std & 33-bit CKP Wiegand + Pin

###### ANSI Mag/Custom Wiegand

###### HID Corp 1000

###### HID Corp 1000 + PIN

##### The ACS shall provide a library consisting of over 19 standard reports or “canned reports” using formula queries and Boolean statements.

##### A Crystal reports engine for customization shall allow reports to be tailored to exact requirements of who, what, when, where. The system shall use a Report “wizard” technique to assist the operator in generating all reports. Additional crystal reports license shall not be acceptable.

##### An Alarms report shall be included with the standard reports offered by the ACS. The report shall give the operator the ability to selectively record new, acknowledged and cleared alarms.

##### Duress code for card and PIN applications shall allow a cardholder to utilize duress PIN when forced to access a card and PIN door. The duress PIN shall unlock the door and send an alarm event to the operator.

##### The ACS shall provide a maintenance port password for technicians accessing the ACS controllers so that unauthorized persons do not gain direct serial port access to the controllers.

### Passwords

#### Passwords shall be programmed to either never expire or to expire in a user definable number of days.

#### The system shall permit the Administrator to allow blank passwords or to specify that passwords be at least a user definable amount of characters long.

#### The system shall permit the Administrator to never lock out accounts or to lock out accounts after a user defined number of bad attempts and to continue that lock out until either the Administrator resets it or to forgive the lockout after a user defined number of minutes.

 4. The ACS system will have an option of supporting Window Authentication. Any ACS that can not

 support Microsoft Windows Authentication will not be acceptable.

### Extended System Applications and Utilities

#### The ACS shall provide operator-friendly, stand-alone system applications designed to assist, configure, or maintain the ACS software. The utilities shall include but not be limited to the following:

##### **Administration Management Utility**: A utility that scans the system looking for unused or otherwise unnecessary items that can be removed. The application shall enable the operator to select from the following:

###### Unused Access Levels

###### Duplicate Access Levels

###### Inactive Cardholders

###### Expired Cardholders

###### Cardholders with No Cards Issued

###### Cardholders with No Access Levels Assigned

###### Cardholders who have Not Used Their Card for a Specified Timeframe

###### Past Holidays

##### **Report Utility**: Shall allow the operator to generate reports without having to log into the ACS main application. The utility shall be capable of accepting a series of command lien parameters so that report templates can be configured and saved to the desktop. Allowing the report to be run by clicking on the ICON speeding up the process of gathering data and displaying information in an emergency.

##### **Event-Link Utility**: A utility that receives filtered events and is capable of displaying the contents of the image library for a corresponding cardholder. The application shall be capable of displaying an event grid to allow the operator to refer back to recent events and view the corresponding images.

##### **Event-Counter Utility**: An application that increments and decrements a counter based on operator defined ACS events. The application shall be capable of controlling up to four (4) devices (inputs, outputs, doors, and readers) that are triggered by the counter’s value. Two Event Grids; one for incrementing, the other for decrementing events shall be displayed on the operator screen once the application has been launched. Each grid shall be capable of being defined by the Operator. The application shall also support Play/Pause and will display the current counter value and allow the Operator to change the value at any time.

##### **Network Communication Verification**: An application that allows the operator to verify network communications between a server and workstations or between multiple workstations using LAN topology.

##### **Door Control Utility**: An application that allows the operator to unlock, lock or momentarily unlock selected doors. The utility shall also provide the capability of displaying a lock/unlock icon on the desktop in addition to the Door Control Utility window. The utility shall also display all events triggered by the ACS.

##### **Independent Report Processing Utility**: Shall allow the operator to execute reports for pre-configured reports and formulas.

##### **Scheduler Utility**: A utility that allows the scheduling of reports to a predetermined email destination.

##### **N-Man Rule / Occupancy Restriction Utility**: A utility that is fully configurable to allow access and limiting occupancy to a secured area. The utility employs a rule for transitioning between two occupancy levels as well as determining which events are permissible. The utility shall feature the following:

###### Control up to four (4) devices (inputs, outputs, doors or readers) via commands that are triggered by the utility’s counter value

###### The ability to allow the user to select one (1) incrementing filter that increases the counter value and one (1) decrementing filter that decreases the counter value

###### A display of Event Grids for filtered events impacting the counter value with such grids capable of being configured by the user, support Play/Pause and display on the first five (5) columns of the transaction table

###### A display of a current value counter with the ability for the user to reset the value at any time

###### A manual override for each device in the event an immediate override is necessary

###### The ability to allow the user to use a text name to customize the Counter Name

###### A rule option to allow the user to configure the required number of admitted events (counter value) within a specified time

###### A set of rules further restricting counter verses time where the user shall have the ability to choose the source of sequential events that make up a transaction. Available events are as follows:

No Restrictions

Different Cardholders at the Same Device

Different Cardholders at Different Devices

Same Cardholder at Different Devices

Same Cardholder at Same Device

###### A Counter Value Rule that allows the user to configure the counter value as follows:

Initial Value

Current Value

Minimum Counter Value

Maximum Counter Value

Enable Negative Counter Values

###### The utility shall allow the user to set the counter value to a certain value at a particular timeframe.

###### The utility shall provide the user with the option of allowing the counter value to be reset after each transition.

###### The utility shall be capable of saving/retrieving the configuration using standard open, save, and save as commands in the file menu.

##### **Email Report Scheduler**: will allow scheduled report generation with direct E-mailing

###### Send Standard or Customized filter reports to anyone, anywhere, anytime, to their assigned workstation.

### Event Monitor

#### The ACS shall provide an operator friendly event monitoring screen that utilizes navigation bars and icons. From this screen the operator shall have the ability to quickly access the following:

##### Monitor

###### The monitor shall be a configurable viewer window capable of displaying of four independent event screens.

###### The monitor view shall be capable of toggling a cardholder image display. When this feature is turned on, a cardholder photo for any reader event displayed in the viewer window will appear.

##### Event Viewer Pop-Up Menu

###### The ACS shall give the operator the ability to perform additional functions via a pop-up menu window by right clicking on an event.

###### The menu shall contain the following elements: Sort Ascending by Column Title, Sort Descending by Column Title, View Only Records for Specified Column Title and View All.

##### Pending Alarms

###### The ACS shall notify the operator of how many alarm events are pending.

###### The ACS shall activate a Pending Alarm icon/button on the Operator Screen. The button/icon shall indicate the number of alarms pending and shall increment as the ACS receives additional alarms.

###### The ACS shall allow the operator to acknowledge the alarm and remove it once the alarm condition is resolved.

###### The ACS shall allow the operator to acknowledge the alarm and leave it displayed on the screen.

###### The ACS shall allow the operator to override any requirements for comments and remove the alarm from the activity list.

###### The ACS shall allow the operator to enter comments about the alarm. Comments shall be stored in the event history file and be kept available for reports.

###### The ACS shall allow the operator to arrange the alarm activity display in ascending or descending order based on column title.

###### The ACS shall allow the operator to print selected records or all records that appear in the alarm activity window.

###### The ACS shall allow the operator to filter certain alarm characteristics so that only those events with of the same type are displayed.

##### Reports Screen

###### The Reports Screen shall allow the operator to access built-in reports directly from the Monitor screen. The Reports screen shall display both the name of each report and description of what it includes. Operators shall be allowed to configure reports specifically for devices, events, and cardholders.

##### System Reminders

###### System Reminders shall notify the operator whether or how many Operator Actions have been performed and will require operator intervention to undo the action. These actions shall include door unlock, output on and input shunt. Reminders shall be configurable and shall be capable of posting once, every [**X**] hours, once every [**X**] month.

#### Operator Actions

##### Operator Actions shall allow the operator to take actions on devices through the ACS software interface. Actions shall include refreshing controllers, locking and unlocking doors, shunt on/or inputs, and turn on/off outputs.

##### Operator should be able to perform Actions from the Event Screen.

#### Scheduling Messages

##### The ACS shall have the ability to schedule custom messages to each workstation.

#### The cardholder database screen elements shall provide for but not limited to the following:

##### **Cardholder name** - Fields shall be provided for last name, first name and middle initial.

##### **Activation date** - Shall default to the date the cardholder record was created but shall be capable of being modified if required.

##### **Expiration date** - Shall have a built-in default period of five years but shall be capable of being modified if required.

##### **Cardholder status** - shall allow the operator to effect a cardholder record either active or inactive.

##### **Class field** - shall allow the operator to select a class for each cardholder. The ACS shall include Employee and Visitor as standard classes and shall be capable of creating additional classes.

##### **Badge field** - shall allow the operator to select a badge style and associate it with a cardholder.

##### **Last admitted event** - shall display the last “admitted” card read from a cardholder.

##### **Display image** - shall allow the operator to choose whether a cardholder image is displayed.

##### **Display signatures** - shall allow the operator to choose whether a cardholder signature is displayed.

##### **Capture images and signatures** - shall allow the operator to capture cardholder signatures or images.

##### **Miscellaneous information** - shall display the following pertinent information in a separate window examples are:

###### Date Created

###### Created By

###### Last Modified

###### Modified By

###### Number of Badges Printed

###### Number of APB Forgiven

##### **Access Levels**

###### Access levels will allow for assignment to card holders. Access levels are defined as the combination of where the card holder can go (card reader) and when the cardholder can go (time and holiday schedules)

###### Shall have up to 99 access levels assigned to each cardholder. If the number of access levels exceeds 3, in any one controller, the ACS server shall assist cardholders to gain access to the reader/door.

##### **Cards**

###### The ACS shall allow the cardholders to have more than one card type without the need to create separate cardholder records for each card type. The ACS shall not limit the card types that each user can use, and will not limit the number of facility codes within the system at any time. Any ACS that limits the quantity of facility codes in any way will not be acceptable.

###### Shall have lost card/return card buttons in the card information window that will allow the operator to quickly change cardholder status. For audit reasons this feature shall not delete the cardholder record but only the card information itself that has been modified. Any ACS that deletes the card from the card holders record will not be acceptable

###### Shall provide a feature that permits the operator to quickly view a cardholder’s card history by clicking a single button. The history shall display on the operator screen and shall show all cards issued to a cardholder along with the disposition of each card.

##### **Custom Fields**

###### The software shall support an unlimited number of operator-defined custom fields. The custom field feature shall allow the operator to configure each custom field to be either unique text, drop down lists, or calendar fields. Any ACS that cannot meet this flexibility will be considered unacceptable.

##### **Database Partitioning** (**Option**)

###### The ACS shall have the capability of partitioning the database by dividing a single system into multiple segments that are each independently operated and managed.

###### The database partitioning shall utilize centralized cardholder administration that will permit the system administration to create cardholders and assign them to one or more partitions as required.

###### The System Administrator shall have full access to all partitions including the ability to modify and delete.

###### Partitions shall be distinct in that information in one partition is concealed from other partitions.

###### A partition shall consist of cardholders, cardholder custom fields, devices, access levels, time zones, holidays, and filters.

###### The ACS shall allow users to share devices across partitions at the discretion of the device’s owner; owners of a shared device shall have the ability to control shared devices but not modify or delete.

###### Cardholder, custom fields, time zones, holidays, access levels and filters shall be unique to each partition. Partition users shall have the ability to customize this information.

###### The ACS shall selectively limit database access through the use of Permissions and Passwords. User Permissions shall determine which screens can be viewed and which functions the user can carry out.

###### New cardholders shall be assigned a default Access Level for a corresponding partition until subsequently modified by a user for that partition.

##### **Image Library**

###### The ACS software shall support a feature that allows up to nine images to be associated with one cardholder record.

###### The ACS software shall permit the operator to perform the following functions from the Image Library Menu:

Capture new photo images

Display photo images

Select multiple capture devices

Load photo image from a file

Delete the photo image

Print a badge using a selected image

Configure the encoder to be used for magnetic stripe encoding

Select a printer and an encoder

Edit the image by enhancing the color settings

Crop the image

Frame the image in a vignette

Red eye removal

Flip image horizontally or vertically

Launch the badge designer application

###### The ACS software shall have a cardholder search engine that can search on a list of fields in the cardholder database and display the results of the cardholders matching the search criteria. Capabilities shall include searching for a single cardholder or group of cardholders.

###### The ACS software shall have the ability to automatically load the proper cardholder database information into the appropriate intelligent filed controller(s) without any operator intervention.

### Elevator Control – Hardware & Software:

### Hardware and Software Type:

#### The ACS software shall support up to 60 floors of elevator control using the ACS manufactured 32-bit controller.

#### The ACS software shall provide for any card read to activate any floor based on the access level assigned the cardholder, with wiring back through an input for individual floor monitoring, and floor call button selection can be controlled by day of week as well as time of day. Standard access controller shall be used and not require separate elevator control module

Software only Type:

 1. The ACS shall support a software interface to the new software control Kiosk

 systems like ThyssenKrupp Elevator Inc, Schindler Elevator Inc. The ACS system will support

 this with an IP/Network Connection only. Any ACS that needs extra hardware or a third party

 Interface will not be acceptable. The system will use current Access levels in the ACS to support

 the elevator software request for access control rights and record all activity.

 2. This software only interface will be a real-time system that uses hardware and software

 components from both Sielox and [**ThyssenKrupp**] **[Schindler] [OTIS]**. It will use Microsoft

 .NET technology for web, executable, and service components.

### Time Zones and Holidays

#### The ACS shall be equipped with two standard built-in time zones:

##### **Never** - When a new access level is created, all access for the readers in that level is set to never. Access shall be granted only after the operator applies a positive time zone to that reader.

##### **Always** - When a new reader is created, it is configured to always report card transactions for display on the event monitor and inclusion in the event history file.

#### The ACS shall be capable of configuring an unlimited number of time zones, limited only controller restriction, each containing up to eight start and stop intervals.

#### Each time zone shall be capable of crossing midnight as well as including weekdays, weekends and holidays all within the same time zone.

#### The ACS shall be capable of defining holidays to override the normal operation of time zones, and must have a Minimum of 20 available for programming.

### Output’s [**ALOC**] and Input [**ALIC**] as part of Access Level

#### The ACS shall incorporate Access Level Output Control (ALOC) and Access Level Input Control. This shall provide the ability to control outputs or shunt inputs based on an access level.

#### ALOC shall be capable of sending momentary signals to activate elevator call buttons for so that only authorized cardholders can access certain floors.

#### Access Level Input Control (ALIC) shall be capable of momentarily shunting alarm inputs up to 12 hours, to latch them in a shunted state or to toggle the shunt.

### Reporting

#### Report Generator

##### Report generation software shall provide the capability to print or view the reports on-screen at operator direction. All reports shall provide the operator with the capability to set up the page, to view the report on-screen prior to printing, or to send the report to a file. Report processing shall not degrade system performance.

#### Standard Reports

##### The operator shall have the capability to initiate standard reports for information contained in the database. The operator shall have the ability to select the columns, sort by a selected field and display the report on-screen or at any designated printer. A fixed number of pre-defined reports are required. The system shall allow the operator to determine if cardholders’ images will be included in selected reports. The system shall also allow the operator to customize the title of each report that is generated. Finally, the system shall be able to produce cardholder dossiers.

##### The system shall allow executables to be placed on the Desktop to run selected reports at a particular time.

##### The ACS shall provide the ability to create custom reports that are tailored to exact requirements of the operator.

##### The following standard reports shall be available as Standard:

###### Access Level Input Control

###### Access Level Output Control

###### Access Levels

###### Cardholder Summary

###### Cardholder Track

###### Cardholders

###### Event Archive

###### Filters

###### Groups

###### Input/Output Links

###### Last Admitted Event

###### Network Configuration

###### Reader Access

###### Reader Track

###### Time Zones

###### APB Zones

 (17) Alarms

 (18) Argos Event Archive

 (19) User Authentication

 (20) Muster Reports

##### The ACS shall allow the operator to save a report as a file so that it can be emailed or exported to another computer or saved to media. Shall have the ability to export reports to the following Minimum formats:

###### Adobe Acrobat (PDF)

###### Rich Text Format

###### Comma-Separated Values

###### MS Excel 97-2000 (XLS)

###### MS Excel 97-2000 Data Only

###### HTML 3.2, and 4.0

###### ODBC

###### Crystal Reports (RPT)

###### Report Definition

###### Tab-Separated Text, & Plain Text

###### Columns with Space, and without Space

###### MS Word

###### XML

(14) Record Style

#### Muster Reporting

##### The ACS shall have the ability to create a muster report using Last Admitted Event logging – either generated via muster station assembly or via any Admitted event outside the boundary of the evacuation area. This report shall include each Cardholder, the name of the reader generating the event, the Date/Time of the event, and the type of Admitted event. Area groups shall also be supported.

##### The system shall have the ability to save a muster report set-up to the desktop for immediate refreshing as needed.

### Archive / Backup

#### The ACS shall place no limit on the size of the event archive file.

#### The ACS shall incorporate an administrative archive backup tool that enables the operator to manage the size of the event archive file by periodically copying a portion of its contents into backup files and removing it from the live event archive file. This utility shall be able to run daily, weekly, monthly or annually. This backup utility shall be configurable and provide for a schedule. This shall run in the background and not require operator intervention.

### Photo ID Badging System

#### The ACS Photo ID Badging System shall provide the ability to import images from bitmap file formats, digital cameras, TWAIN cameras, scanners, or live video.

#### The system shall provide a complete, integrated photo ID imaging system, which will run on the Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019, Windows 8.1 Pro or Windows 10.

#### All system components shall be readily available off-the-shelf items from nationally or internationally recognized vendors. Proprietary hardware elements will not be permitted.

#### The video capture card must be a high resolution, non-proprietary board.

#### The Badging sub-system shall be fully integrated with the host server database; i.e. all badge holder images and all badge holder data are stored on the ACS host server. All enrollment and badge production processes must occur on the client workstation.

#### The imaging system shall utilize a commercially available imaging compression technique, e.g. JPEG using 15-20K per image.

#### The software shall support remote viewing of badge images on ACS terminals utilizing standard Ethernet communications.

#### The badge design and badge production components must provide the capability to:

##### Design custom badge formats

##### Have a full array of drawing tools

##### Define static and dynamic text

##### Move text, justify text, use multiple fonts and sizes

##### Use custom colors

##### Import industry standard graphics for logos and backgrounds

##### Capture photos from video board and digital camera

##### Capture signatures from signature capture pad

##### Use scanners for import of photos or signatures via TWAIN drivers

##### Have photo enhancement controls – hue, intensity, brightness, contrast, red eye removal

##### Create standard barcodes

##### Encode Mag Stripe on badges

##### Create and print dual-sided badges

##### Preview and print dossier page

 O. Visitor Management Interface - Easy Lobby

 Visitor Management: The ACS shall support real-time integration with a designated visitor management package that shall store and retrieve specific fields of information about the arrival and departure of visitors to the facility. Minimum capability and options shall include:

###### Visitor Badging and reporting

###### Photo capture

###### Pre-registration of visitors and groups

###### Multi-tenant building requirements

###### Compatible with signature pads, business

###### Card scanners and driver's license scanners

###### Watch/Lookout List keeps out unwanted visitors

###### Easy import & update of employee directory, work Stations must be able to be on the Network for site with multiple lobbies.

P. Schlage Wireless Locks – up to 32 Schlage locks per 1700 controller

* + - 1. The ACS shall have a direct interface to the Schlage AD series and NDE series locks. Any ACS that requires a third party interface either software or hardware will be considered unacceptable.

 The interface **MUST** allow the ACS to communicate and control the locks as follows:

 a. Cardholder card information

 b. Access Levels including;

 1. Doors the users is allowed to enter

 2. Day of the week the users allowed to enter

 3. Time of Day the users allowed to enter

 4. Holiday/Vacation time associated with the cardholders rights

 c. Alarm Information:

 1. Door Forced alarms

 2. Door Held open too long alarms

 d. History

 1. Report all Valid and Invalid Card reads

 2. Report any Alarm active as programmed into the hardware system

 3. Report Loss of Communication, Low Battery

 4. Scheduled unlocking or locking of Door

 5. System operator (Computer User) remotely unlocking or locking of Door

 e. Operator Actions

 1. Must be able to Lock, Unlock, and Momentarily Unlock a door by an operator

 2. Must be able to Block access to a reader

 f. Schedules

 1. Must be able to put Doors on an unlock schedule

 2. Must be able to Block access to a reader

g. Card Reader types Supported

 1. Prox, I Class, Mifare, Desfire, Magstripe, Keypad, NFC

. Card or Credential types Supported

 1. Prox, I Class, Mifare, Desfire, Magstripe, NFC, FIPS 201

h. Lock Toggle while using Access control card, separate toggle card not acceptable

###  Q) Von Duprin Exit Hardware Interface – RU/RM Interface - Remote dogging ready, undogging and monitoring.

1. The ACS shall have a direct interface to Von Duprin Model 98, 99, 33A and 35A Exit Hardware.
2. The RU/RM interface **MUST** allow the ACS to communicate, monitor and control Von Duprin Model 98, 99, 33A and 35A RIM Exit Devices.
3. The ACS shall support remote undogging for centralized lockdown.
4. The ACS shall communicate, monitor and report door position status.
5. The ACS shall support remote dogging ready and undogging of the exit device (Electric latch retraction).
6. The ACS shall monitor and report REX activation from doors fitted with Von Duprin Model 98, 99, 33A and 35A RIM Exit Devices.

R) ASSA Abloy Wireless Aperio Locks – up to 32 Aperio locks per 1700 controller

The interface **MUST** allow the ACS to communicate and control the locks as follows:

 a. Cardholder card information

 b. Access Levels including;

 1. Doors the users is allowed to enter

 2. Day of the week the users allowed to enter

 3. Time of Day the users allowed to enter

 4. Holiday/Vacation time associated with the cardholders rights

 c. Alarm Information:

 1. Door Forced alarms

 2. Door Held open too long alarms

 d. History

 1. Report all Valid and Invalid Card reads

 2. Report any Alarm active as programmed into the hardware system

 3. Report Loss of Communication, Low Battery

 4. Scheduled unlocking or locking of Door

 5. System operator (Computer User) remotely unlocking or locking of Door

 e. Operator Actions

 1. Must be able to Lock, Unlock, and Momentarily Unlock a door by an operator

 2. Must be able to Block access to a reader

 f. Schedules

 1. Must be able to put Doors on an unlock schedule

 2. Must be able to Block access to a reader

f. Card Reader types Supported

1. Prox, I Class, SEOS, Mifare, Desfire

h. Lock Toggle while using Access control card, separate toggle card not acceptable

  **END**