SECTION 281000 – ACCESS CONTROL SYSTEM

28.11.00 Access Control Applications:

This document includes a general description, functional requirements, operational characteristics, and criteria for the Access Control System (ACS).

28.12.00 General Requirements:

28.12.01 This shall document the general description, functional requirements, operational characteristics, and criteria for the Access Control System (ACS).

28.12.02 The Codes and Regulations listed below form a part of this specification to the extent referenced. Work shall be performed in accordance with the applicable international, federal, state, and local codes or standards current at the commencement of installation. The following list summarizes applicable standards:

A. UL 294, UL 1076, ULC

B. CE

C. FCC – Part 15, Part 68

D. NFPA 70, NEC

E. IEEE, RS 170 variable standard

F. Microsoft® Open Database Connectivity (ODBC) interface)

G. ISO Software Coding Standards

H. RoHS

28.12.04 Where more than one code or regulation is applicable, the more stringent shall apply.

28.12.05 Cable installation, identification and termination shall be performed in addition to the applicable codes above.

28.13.00 Access Control Software and Database Management:

28.13.11 Access Control Software shall be Access Control System shall be {Access It! Universal.NET from RS2 Technologies LLC} no substitutions shall be acceptable. The ACS shall use a single seamlessly integrated Microsoft SQL relational database for all functions utilizing a fully multi-tasking multi-threading Microsoft Windows operating system.

A. Annual Software Maintenance Fees shall not be acceptable. Access Control Software shall be supported by the manufacturer to the authorized reseller at no annual fee. The current major version of the released version and the previous released version of the

software and all sub-versions of the current and previous major version shall be supported.

B. Reader License charges. There shall be no Reader License Fees, software having Reader License Fees based on the number of readers supported by the software package shall be unacceptable.

C. Upgrades or expansion of the ACS to a larger size system in scale shall not require installation of a different and or new ACS application or require the administrator / operator to learn a different and or new interface from the previous version.

D. The ACS shall be written using recognized standard software coding techniques. The ACS shall be written to support multiple languages without re-engineering. The ACS software shall be written to Microsoft's published standards for User Interface Design, Secure Coding Practices and Database Implementation Guidelines.

E. The ACS software developer shall be a Microsoft Certified Independent Software Vendor.

F. The ACS shall support N-Tier architecture where the expansion of the system architecture will allow for end-user deployment based upon their system architectural needs. The ACS shall allow but not require the separation of the database, application server, web server, and client interface. The ACS shall require that all connections to the database are performed through a trusted link from the client or internet browser interface.

G. The ACS shall support Centralized distribution (publishing) of applications using Windows Terminal Server, Citrix, or utilizing IIS for the web client using a standard internet browser such as Internet Explorer, Mozilla Firefox, Google Chrome, Apple Safari, and/or by means of a mobile computing platform using a Tablet PC, PDA device, or Smart Phone.

H. The ACS architecture shall support Microsoft Windows Clustering, Hot-Standby, Fault Tolerant Servers, Fault Tolerant Hot Standby Servers, and Virtual Servers.

I. The ACS shall only be able to connect to and interface with data sources utilizing a Windows Service.

J. The ACS shall be capable of importing or updating Cardholder data using the following source types.

1. Microsoft Access
2. Microsoft Excel
3. Microsoft SQL Server
4. ASCII Text (delimited file)

K. The ACS (RS2 Access It! Universal.NET) shall support

1. {**RS2 Universal Standard Series} supports up to:
2. 1000 System Control Panels (SCP)
3. Support for 256 Tasks per SCP
4. 64,000 Access Control Readers, 64 readers per SCP.

5. 512,000 Inputs, 512 per SCP
6. 512,000 Outputs 512 per SCP
7. Supports multi-drop OSDP readers with EP/LP SIO devices.
7. Unlimited Cardholders
8. Multiple Cards per Cardholder
9. 32,737 Access Levels
10. 128 Access Levels per Card
11. 255 Timezones, with 12 start/stop intervals each
12. 255 Holidays, across 8 Holiday Groups/Types
13. Anti-Passback with Occupancy Counting
14. Virtualization Support
15. Video Integration Support
16. Zenitel Intercom integration support.
17. Biometric Integration Support
18. Web Client / Thin Client Support
19. Fully Integrated Graphical Mapping (Floor Plans with Active ICONs)
20. Definable Report Support, with the ability to Hyperlink recorded video directly from with-in a Report to play back recorded video in a single step operation.
21. Workstation can be used for other tasks while reports are being generated.
22. User Definable Macro Support.
23. Macro Utilization report.
24. Calendar display on Macro screen.
25. Outlook ICS files may be imported for Macro Schedules 26. Macros may be set to automatically delete after scheduled execution.
27. Macros may be pinned to the Ribbon Bar for immediate access.
28. Macros may be placed on Graphic Floor Plans (Maps) for immediate access.
29. Unassigned Access Level Interval and Timezone report assists with system organization and clean up.
30. Windows Authentication allows log in without entering separate password.
31. Diagnostics permits viewing all Access It! Universal.NET messages in Windows Event Viewer.

32. System Status screen has direct links to filtered views such as Unlocked Doors, Active Cards, Installed SCPs, SIOs, Readers, Inputs, Outputs, Unlocked Doors, and other System Status Categories.

33 Ability to create a mandatory custom drop down database field for cardholder information

34 Advanced Hardware Filter Views.

35 Dynamic Search capabilities

36 Lifesafety power integration K. Lock Integration support for:

1. Allegion – Schlage AD-400 No Substitution

L. The ACS {RS2 Access It! Universal.NET Enterprise} shall support (**add additional detail if required. Delete un-used section and all words in parenthesis unless the spec is an RS2 ONLY specification.

1. {**RS2 Universal Enterprise Series} supports up to:

2. Multiple Sites, (Partitioning, or Segmenting)

3. 1000 System Control Panels (SCP) M. Lock Integration support for:

1. Allegion

N. ACS Software and Field Hardware Warranty. The ACS Software shall be warranted for a period of 90 Days from the date of shipment from the manufacturer to be free of defects and will function in substantial accordance to the published specification.

1. ACS Field Hardware shall be warranted for a period of three (3) years from the date of shipment from the manufacturer, will be free from defects and will function in general accordance with the product specifications.

2. ACS Third Party Device warranties are transferred from the manufacturer to the contractor, which may then transfer third party warranties to the owner. Specific third party warranty details, terms and conditions, remedies and procedures, are either expressly stated on, or packaged with, or accompany such products. The warranty period may vary from product to product. These products include but are not limited to devices that are directly interconnected to the SMS field hardware or computers and are purchased directly from the SMS manufacturer. Examples may include but not be limited to; Credential Printers, Reader Heads, Biometric Devices, Computers etc.

O. The Access Control System shall use one of the following Operating Systems, Windows 7 Professional, Windows 8 Professional, Windows 8.1 Professional, Windows 10 Professional, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016. Other Operating Systems such as but not limited to - Windows Home editions, Linux, Unix, Sun, or Apple shall not be acceptable.

1. The ACA shall use Microsoft SQL Server Express 2008 R2 or higher as the database engine. Substitutions shall not be acceptable.

P. The ACS shall be capable of utilizing a Web client. The Web client shall be capable of being utilized via any standard Browser to include but not limited to Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera, Apple Safari, IOS Browser, and Android Browser. The Web client shall be device aware such that it shall display according to the device it is being used from with larger buttons on a mobile device such as a Tablet or Phone. The Web client shall require the User to log in and shall utilize User Groups to allow commands / functions available to the User if at a Desktop (i.e. change reader mode, find, a cardholder/card, interact with cardholder/card, execute a Macro, change an Access Level,

Q. ACS Software Interface

1. The ACS Software shall be Microsoft Windows compliant having a Microsoft "Outlook" type structure, having the following features / functions:

2. The ACS shall display a "Ribbon Bar" (Tool Bar) at the top of the screen containing buttons for the functions which may be utilized pertaining to the current selected Menu / screen.

3. When the Advanced Window Control is enabled the ACS shall allow all screens to be moved independently. The ACS shall support multiple monitors when Windows is utilizing an Extended Desktop and has multiple display monitors present.

4. The ACS shall permit advanced device commands to be shown or to be hidden at the option of the user.

5. The ACS shall have a user selectable setting to determine the number of Traced Card/Cardholder/Reader events to pull from the database for display in the tracking screen on startup from 1 – 100.

6. The ACS shall permit Users to select that screens to be displayed in a Tab format (Advanced Window Control) permitting a User to quickly and easily move between screens without requiring one screen to be closed prior to moving to the next screen.

7. The ACS shall permit a User to relocate Tabs and to separate Tabs (screens) for most efficient use.

8. The ACS shall be capable of allowing a User to only work with a single Site (Segment) at a time or to work with multiple Site(s) (Segments) at the same time, as the User's password permissions dictate.

9. The ACS shall be capable of permitting the use of "Non-Modal dialogs" via a menu selectable check box.

10. The ACS shall be capable of tracking Cardholders, Cards, or Readers in a separate Tracking Screen\Window for those items being Tracked (watched).

    a. The ACS shall be capable of permitting a User to set the number of historical Tracking events to search for and display when the workstation is

started (signed in/logged in) allowing the User to immediately view the last X (up to 100) Tracked / Watched item events without creating and running a report.

R. The ACS shall have a User selectable real time "Mustering" screen. This screen shall permit the User to select the "Ares(s)" of interest, the Refresh Interval (which will

continue to update the selected area(s) of interest every X selected seconds, Omit cards not used in X hours from being shown, and Print Reports from the Mustering screen.

S. The ACS shall be capable of having Digital Video Recording / Network Video Recording integrations.

U. IP - Wireless and POE Locksets

1. Allegion

V. Intrusion Detection System Integration

1. Bosch (7412 and 9414 versions G, GV2, GV3 (8.05 and 8.13) and GV4, and B series panels)
2. DMP (XR-100N, XR-150N, XR-500N, XR-550N versions 100 and 200)

X. Mobile Access Control / Mustering

1. Telaeris - XpressEntry

Y. Destination Dispatch Elevator Control

1. Otis – Compass Destination Entry

28.14.00 Access Control System Hardware:

28.14.11 The ACS shall communicate with, monitor, and use open architecture System Control Processor (SCPs), which shall support 64 controlled openings per, EP – 1502, EP – 2500, EP – 4502 EP-4502 with Auxiliary Authentication Module (AAM), the Lp4502, LP2500, LP1502, LP1501 SCPs. The EP – 1501 and LP-1501 (SCP) shall support a total of 17 openings. The ACS shall be capable of communicating with a minimum of 1,000 SCPs concurrently for a minimum of 64,000 controlled openings. The ACS shall not employ reader licenses which limit the number of Readers the ACS shall control. The ACS shall be capable of communicating with the SCPs using Hardwire (direct RS-232, or RS-485), Dialup modem using POTS (Plain Old Telephone system), and TCP/IP network communications. Each SCP shall be capable of maintaining in its memory a Real-time clock, 256 Holidays, 128 TimeZones each having 12 start\stop Time Intervals, 32,000 Access Levels, 256 Tasks (predefined routines with 256 steps per Task), 8 Card Formats (up to 19 digit card codes, 8 Facility (Site) codes, supports Open Supervised Device Protocol (OSDP) multi-drop support with series 3 Mercury hardware, supports AntiPassback (areas, hard, soft, timed, nested), occupancy count rules, device configurations for the devices (Readers, Inputs, Outputs) controlled by the SCP, and a minimum of 50,000 event transactions if the SCP is unable to communicate to the ACS, the SCP stores Card numbers for entry decisions.

28.14.13 System Input Output (SIO), Reader Interface Modules (RIM), such as the MR-50 single (opening) reader interface, MR-52 dual opening or single opening with in out reader interface control, and MR-51E single opening control supports dual readers for IN \ OUT control or the Series 3 MR-50, MR-52, MR-62e.

28.14.15 System Input Output (SIO), 16 dry contact Input modules with 2 Form C output relays, and 16 form C relay Output modules, such as the MR-16IN, or the MR-16OUT or the series 3 MR-16IN, MR 16-OUT, SIO devices.

28.14.16 The ACS shall also have the capability to integrate \ communicate with wireless \ IP locksets, Intrusion Systems, and Biometrics.

28.14.17 The ACS shall be capable of utilizing PVC badge printer having a Windows compliant \ capable Windows Driver for the Operating System being utilized for the ACS Workstation Software. The ACS shall utilize standard Dot Matrix, Laser, and Ink jet printers for report purposes having a Windows Driver for the workstation the printer is connected to.

28.15.00 Access Control Hardware Devices:

28.15.11 Allegion MFG. (NO SUBSTITUTIONS)

28.15.11.1 Schlage Electronics WRI400 (Wireless reader interface)

28.15.12 Schlage Card Reader. MT15 BLK. No Substitutions.

28.15.13 PIM 400-1501 16 Door wireless smart controller

28.15.14.1 Schlage Electronics AD400 (4 battery per spec)

28.15.15 Schlage Electronics M490 Maglock

28.16.00 Access Control Interfaces:

28.16.15 Video Surveillance Interfaces:

A. The ACS shall be capable of having the following integration interfaces at a minimum.

1. CCTV – The ACS shall have the ability to send an ASCII command via RS-232 to a video switcher.

2. DVR / NVR – The ACS shall have the ability to have an interface to authorized DVR / NVR units listed below, to pull live video or recorded video to the ACS. The ACS shall not store or manipulate the video, the ACS shall only request the video stream, in order to maintain any watermarking, and or chain of custody for legal uses.

3. American Dynamics

4. Avigilon (Avigilon Control Center version Client\Server v.5.x)

5. Bosch

6. Digital Watchdog (Digital Watchdog Spectrum 2.5 and up)

7. eXacq (eXacqVision Enterprise VMS-Hybrid Z Server Client 7.0.1.81045 / Server7.0.1.81035)
8. Genetec (Omnicast 4.7)
9. HIKvision
10. March networks (8000 Series Hybrid NVRs Command VMS)
11. Milestone (Milestone XProtect XProtect 2016)
12. OnSSI (OnSSI Ocularis PRO / Ent / ULT 4 and 5)
13. Panasonic
14. Pelco (Digital Sentry DSNVS, DSSRV, Endura)
15. Salient Systems (CompleteView ONE CompleteView 4.3.0.88) 16. VideoInsight (Video Insight Software 5.5.36.4)

28.17.00 Access Control Identification Management System:

The ACS shall have a seamlessly integrated ID Management System module capable of producing PVC credentials.

A. The ACS ID Management System module shall use the same SQL database as the ACS uses.

B. There shall be a minimum of 32 User Definable database fields for Cardholder Credential purposes. The ACS ID Management module shall have the capability to add an unlimited number of additional User Definable fields to the database.

C. Each ACS ID Management module, User definable field shall be capable of being a Text field, Pull down list field, Date Combo field, or Text field with Required entry.

D. The ACS ID Management module shall have the capability to capture Photo's from a web (USB) camera having a suitable windows driver, a camera or scanner with a TWAIN interface, import images from BMP, JPG, JPEG, GIF, and PNG file types.

E. The ACS ID Management module shall have the capacity to have an unlimited number of Badge forms (templates). Badge forms (templates) may contain graphics, any and all Cardholder data fields, static text, photo (image), and may contain those items only when specific criteria is met as defined using a "IF" statement. Fields shall be capable of being printed as a Barcode when the Badge Type (template) is printed or viewed.

F. The ACS shall be capable of integrating with the following Visitor Management Systems.

1. STOPware
2. EasyLobby

END OF SECTION 281000