SECTION 28 13 00
– ACCESS CONTROL SOFTWARE AND DATABASE MANAGEMENT

GENERAL

1.01 REFERENCE STANDARDS

A. UL 294 - Access Control System Units; Current Edition, Including All Revisions.

DEFINITIONS

2.01 ACS – ACCESS CONTROL SYSTEM

2.02 CSA – CLIENT SOFTWARE APPLICATION

2.03 DGM – DYNAMIC GRAPHICAL MAPS

2.04 ALPR – AUTOMATIC LICENSE PLATE RECOGNITION

2.05 SDK – SOFTWARE DEVELOPMENT KIT

2.06 GLM – GENETEC LIFECYCLE MANAGEMENT

2.07 SSM – SERVER SOFTWARE MODULE

2.08 UI – USER INTERFACE

2.09 USP – UNIFIED SECURITY PLATFORM

2.10 USW – UNIFIED WEB CLIENT

2.11 VMS – VIDEO MANAGEMENT SYSTEM

QUALIFICATIONS

3.01 THE SYSTEM PROGRAMMER SHALL HAVE ATTENDED MANUFACTURER TRAINING AND OBTAINED CERTIFICATION IN GENETEC™ SECURITY CENTER - SYNERGIS™ TECHNICAL CERTIFICATION.

3.02 OPTIONALLY, THE SYSTEM PROGRAMMER SHALL HAVE ATTENDED MANUFACTURER TRAINING AND OBTAINED CERTIFICATION IN GENETEC SECURITY CENTER - ENTERPRISE TECHNICAL CERTIFICATION.

3.03 THE SYSTEM PROGRAMMER SHALL BE A GENETEC CERTIFIED PARTNER WITH THE FOLLOWING LEVEL OF QUALIFICATION:

A. Certified Reseller or up

3.04 THE SYSTEM PROGRAMMER SHALL SUBMIT PROOF OF CERTIFICATIONS.

PRODUCTS

ELECTRONIC ACCESS CONTROL SYSTEM GENERAL REQUIREMENTS

5.01 THE ACS SHALL BE AN ENTERPRISE CLASS IP ACCESS CONTROL SOFTWARE SOLUTION. IT SHALL BE FULLY EMBEDDED WITHIN A UNIFIED SECURITY PLATFORM (USP). THE USP SHALL ALLOW THE SEAMLESS UNIFICATION OF THE ACS WITH AN IP VIDEO MANAGEMENT SYSTEM (VMS).

5.02 THE ACS SHALL BE HIGHLY SCALABLE TO SUPPORT CONFIGURATIONS CONSISTING OF THOUSANDS OF DOORS WITH FACILITIES SPANNING MULTIPLE GEOGRAPHIC AREAS.

5.03 THE ACS SHALL SUPPORT AN UNRESTRICTED NUMBER OF LOGS AND HISTORICAL TRANSACTIONS (EVENTS AND ALARMS) WITH THE MAXIMUM ALLOWED BEING LIMITED BY THE AMOUNT OF HARD DISK SPACE AVAILABLE.

5.04 THE ACS SHALL SUPPORT A VARIETY OF ACCESS CONTROL FUNCTIONALITIES, INCLUDING BUT NOT LIMITED TO:

A. Controller (Unit) management, door management, elevator management, and area management.

B. Cardholder and cardholder group management, credential management, and access rule management.

C. Badge printing and template creation.

D. Visitor Management.

E. People counting, area presence tracking, and mustering.

F. Offering a framework for third party hardware integration such as card and signature scanner.

5.05 MANUFACTURER:

A. Genetec Security Center SaaS:
   1. Synergis Enterprise

5.06 CERTIFICATION

A. The ACS shall be certified
   1. UL 294
   2. ULC-S319
   3. EN-60839-11-1
   4. CSPN

5.07 THE ACS SHALL SUPPORT CHANGING PASSWORDS OF VIDEO UNITS (FOR A LIST OF SUPPORTED UNITS, SEE THE SECURITY CENTER ADMINISTRATOR GUIDE):

A. The ACS shall show the strength of the current unit password.

B. The ACS shall have the ability to change the password manually or using a string password generator for single or multiple units.

C. The ACS shall have the ability to automatically update passwords on schedule.

D. The ACS shall keep the history for passwords and the ability to retrieve them.

E. The ACS shall have the ability to export passwords of units for safekeeping.

5.08 THE ACS SHALL SUPPORT MANAGING CERTIFICATES OF VIDEO UNITS USED FOR SECURE COMMAND AND CONTROL (HTTPS AND RTSPS) (FOR A LIST OF SUPPORTED UNITS, SEE THE SECURITY CENTER ADMINISTRATOR GUIDE):

A. Push Initial Certificate

B. Automatically switch from HTTP and RTSP to HTTPS and RTSPS

C. Allow certificate renewal

D. Manage certificates manually for a single device or a batch of devices

E. Automatically update upon configured schedule for single device or batch of devices

FAILOVER AND STANDBY REQUIREMENTS

6.01 THE USP SHALL SUPPORT NATIVE AND OFF-THE-SHELF FAILOVER OPTIONS.

6.02 FAILOVER DIRECTORY (ENTERPRISE ONLY)

A. The Standby Directory shall act as a replacement SSM on hot standby, ready to take over as the acting Directory in case the primary Directory fails. The failover shall occur in less than 1 minute. No action from the user shall be required.

B. The USP shall support up to five (5) Directories on standby, lined up to take over as the acting Directory in a cascading fashion.

C. The Standby Directory shall keep its configuration database synchronized with the primary Directory.

D. The Standby Directory shall support disaster recovery scenarios where a server can be located in another geographic area (or building) and only take over if all other Directories become offline.

E. The Standby Directory shall support synchronization of the configuration databases using a backup and restore mechanism. The synchronization period shall be configurable from 15 minutes to 1 week.

F. The Standby Directory shall support real-time synchronization of the configuration databases using SQL Mirroring or SQL Always On.

6.03 OFF-THE-SHELF STANDBY/FAILOVER OPTIONS (EXCLUDING THE VMS ARCHIVER) SHALL INCLUDE:

A. Native role failover across multiple servers

B. Windows Clustering

C. NEC ExpressCluster X LAN

ACS ACCESS MANAGEMENT

7.01 THE ACS SHALL BE BASED ON AN OPEN ARCHITECTURE ABLE TO SUPPORT MULTIPLE ACCESS CONTROL HARDWARE MANUFACTURERS. THE ACS SHALL BE ABLE TO INTEGRATE WITH MULTIPLE NON-PROPRIETARY INTERFACE MODULES AND CONTROLLERS, ACCESS READERS, AND OTHER THIRD-PARTY APPLICATIONS.

7.02 THE ACS SHALL BE AN IP ENABLED SOLUTION. ALL COMMUNICATION BETWEEN THE ACS AND HARDWARE CONTROLLERS SHALL BE BASED ON STANDARD TCP/IP PROTOCOL.

7.03 ACCESS MANAGER ROLE

A. The Access Manager Role shall be the server that synchronizes all access control hardware units under its control, such as door controllers and I/O modules. It shall also be able to validate and log all access activities and events when the door controllers and I/O modules are online.

B. The Access Manager Role shall maintain the communication link with the hardware controllers under its control. It shall also continuously monitor whether the controllers are online or offline.

C. Synchronization of hardware units shall be automated and transparent to users and shall occur in the background. It shall also be possible to manually synchronize units or to synchronize units on a schedule.

D. The Access Manager Role shall support doors and controllers located within one or more facilities. The Access Server shall support a minimum of 200 readers and up to 2000 readers per computer.

7.04 THE ACCESS SERVER SHALL STORE ALL ACCESS EVENTS ASSOCIATED WITH THE DOORS, AREAS, HARDWARE ZONES (HARDWARE INPUT POINTS), ELEVATORS, AND CONTROLLERS UNDER ITS DIRECT CONTROL.

ACS GLOBAL CARDHOLDER MANAGEMENT (ADDITIONAL LICENSE REQUIRED)

8.01 THE ACS SHALL SUPPORT GLOBAL CARDHOLDER MANAGEMENT AND SYNCHRONIZATION BETWEEN A CENTRAL INDEPENDENT SITE AND REMOTE INDEPENDENT SITES, ALL OF WHICH CAN HAVE THEIR OWN DIRECTORY AND DATABASES.

8.02 IT SHALL BE POSSIBLE TO SYNCHRONIZE THE FOLLOWING ENTITIES AND THEIR CONFIGURATION DATA:

A. Cardholders (incl. custom fields)

B. Cardholder groups

C. Credentials

D. Badge templates

8.03 CARDHOLDERS AND OTHER SYNCHRONIZED ENTITIES CAN BE ADDED CENTRALLY AND SYNCHRONIZED TO REMOTE SITES FOR CENTRAL CARDHOLDER MANAGEMENT.

8.04 CARDHOLDERS AND OTHER SYNCHRONIZED ENTITIES CAN BE ADDED AT REMOTE SITES AND SYNCHRONIZED TO THE CENTRAL SITE AND OTHER REMOTE SITES.

8.05 THE ACS SHALL SUPPORT THE ASSIGNMENT OF A SINGLE CARD PER CARDHOLDER ACROSS ALL AN ORGANIZATION'S SITES.

8.06 MANUAL AND SCHEDULED SYNCHRONIZATION SHALL BE SUPPORTED.

8.07 THE ACS SHALL SUPPORT MANUFACTURER OSDP COMMAND.

ACS HARDWARE COMPATIBILITY LIST

9.01 THE ACS SHALL HAVE AN OPEN ARCHITECTURE THAT SUPPORTS THE INTEGRATION OF THIRD-PARTY IP-BASED DOOR CONTROLLERS AND I/O MODULES. THE ACS SHALL SIMULTANEOUSLY SUPPORT MIXED CONFIGURATIONS OF ACCESS CONTROL HARDWARE FROM MULTIPLE VENDORS.

9.02 THE ACS SHALL SUPPORT SAM ONBOARD TO HOLD DESFIRE ENCRYPTION KEYS.

9.03 THE ACS SHALL SUPPORT 802.1X AUTHENTICATION.

9.04 THE ACS SHALL SUPPORT EMBEDDED CERTIFICATE VALIDATION ENGINE.

9.05 THE ACS SHALL SUPPORT THE USE OF TLS 1.2 AND CERTIFICATES.

9.06 THE ACS SHALL SUPPORT OSDP SECURE CHANNEL.

9.07 THE ACS SHALL SUPPORT OSDP TRANSPARENT READER MODE TO READ DESFIRE CREDENTIALS.

9.08 THE ACS SHALL SUPPORT MULTIPLE TYPES OF HARDWARE DEVICES: SINGLE-READER CONTROLLERS, 2-READER CONTROLLERS, 1- TO 64-READER CONTROLLERS, INTEGRATED READERS AND DOOR CONTROLLERS, AND POWER-OVER-ETHERNET (POE) ENABLED DOOR CONTROLLERS.

9.09 THE ACS SHALL SUPPORT MOST INDUSTRY STANDARD CARD READERS THAT OUTPUT CARD DATA USING OSDP AND WIEGAND PROTOCOL, AND CLOCK-AND-DATA.

9.10 THE ACS SHALL SUPPORT THE FOLLOWING IP-ENABLED CONTROLLERS. FOR A DESCRIPTION OF THE CAPABILITIES OF THE CONTROLLER, REFER TO THE SPECIFIC CONTROLLER'S A&E SPECIFICATIONS AND DESIGN:

A. Synergis Master Controller
B. Synergis Cloud Link
C. Synergis Cloud Link RoadRunner
D. Synergis IX
E. SharpV
F. HID VertX EVO
G. HID Edge
H. HID Edge EVO
I. PW6000 controllers
J. Mercury EP controllers
K. Mercury LP controllers
L. Mercury SIO module
M. Mercury M5 Bridge
N. Mercury MS Bridge
O. Assa Abloy Aperio RS485 8 to 1 hub

P. Assa Aperio AH40 (IP) hub

Q. Assa Abloy IP Locks (no DSR required)
   1. Corbin Russwin
   2. Sargent Passport
   3. Sargent Profile
   4. IN120
   5. IN220

R. Salto Sallis RS485 and PoE routers

S. Salto SVN

T. Schlage AD-300 and AD-400 electronic locks

U. Schlage Control wireless lock

V. Schlage NDE, LE, FE, and BE Networked wireless Mortise lock

W. Axis A1001

X. Axis A1601

Y. STid RS485 readers

Z. SSCP readers
   1. STid

AA. DDS AS34/TPL4

BB. SimonsVoss Smart Intego

CC. OSDP readers
   1. HID
   2. STid
   3. Cidron
   4. Allegion
   5. Wavelynx
   6. Deister
   7. PHG

SEAMLESS UNIFICATION WITH VMS

10.01 THROUGH THE USP, THE ACS SHALL SUPPORT INTEGRATION WITH AN IP VIDEO SURVEILLANCE SYSTEM OR MVS. INTEGRATION WITH AN IP VIDEO SURVEILLANCE SYSTEM SHALL PERMIT THE USER TO VIEW LIVE AND RECORDED VIDEO.

10.02 USERS SHALL BE ABLE TO ASSOCIATE ONE OR MORE VIDEO CAMERAS TO THE FOLLOWING ENTITY TYPES: DOORS, ELEVATOR AND HARDWARE ZONES (INPUT POINTS), AND MORE.

10.03 THE MONITORING UI SHALL PRESENT A TRUE UNIFIED SECURITY INTERFACE FOR ACCESS CONTROL AND VIDEO SURVEILLANCE. ADVANCED LIVE VIDEO VIEWING AND PLAYBACK OF ARCHIVED VIDEO SHALL BE AVAILABLE THROUGH THE MONITORING UI.

10.04 IT SHALL BE POSSIBLE TO VIEW VIDEO ASSOCIATED WITH ACCESS CONTROL EVENTS WHEN VIEWING A REPORT.

ACS CONTROLLER (UNIT) MANAGEMENT

11.01 THE ACS SHALL SUPPORT THE DISCOVERY, CONFIGURATION, AND MANAGEMENT OF IP ENABLED CONTROLLERS AND I/O MODULES (HARDWARE UNITS). A USER SHALL BE PERMITTED TO ADD, DELETE, OR MODIFY A CONTROLLER IF THEY HAVE THE APPROPRIATE PRIVILEGES.

11.02 THE ACS SHALL SUPPORT UNIT CONFIGURATION THROUGH A PRECONFIGURED DOOR TEMPLATE.

11.03 THE ACS SHALL SUPPORT AUTOMATIC UNIT DISCOVERY. THE USER SHALL ESTABLISH THE SETTINGS FOR DISCOVERY PORTS AND FOR THE TYPES OF UNIT DISCOVERY AND THE ACS SHALL AUTOMATICALLY DETECT ALL CONNECTED DEVICES.

11.04 THE ACS SHALL SUPPORT A UNIT SWAP UTILITY FOR SWAPPING OUT AN EXISTING CONTROLLER WITH A NEW CONTROLLER. THE UNIT SWAP UTILITY SHALL AVOID THE REPROGRAMMING OF THE SYSTEM WHENEVER A UNIT IS REPLACED. ALL LOGS AND EVENTS FROM THE OLD UNIT SHALL BE MAINTAINED.

11.05 THE ACS SHALL SUPPORT PRE-CONFIGURATION OF THE SYSTEM PRIOR TO THE PHYSICAL HARDWARE INSTALLATION.

11.06 THE ACS SHALL SUPPORT FIRMWARE UPGRADE IN BULK FROM THE APPLICATION.

11.07 THE ACS SHALL SUPPORT MIFARE DESFIRE CONFIGURATION CENTRAL MANAGEMENT.

11.08 THE ACS SHALL CENTRALLY MANAGE UNIT PASSWORD POLICY (PASSWORD STRENGTH, ROTATION, BULK UPDATE).

ACS CARDHOLDER AND CARDHOLDER GROUP MANAGEMENT

12.01 THE ACS SHALL SUPPORT THE CONFIGURATION AND MANAGEMENT OF CARDHOLDERS AND CARDHOLDER GROUPS. A USER SHALL BE ABLE TO ADD, DELETE, OR MODIFY A CARDHOLDER OR CARDHOLDER GROUP IF THEY HAVE THE APPROPRIATE PRIVILEGES.

12.02 CUSTOM FIELDS SHALL BE SUPPORTED FOR BOTH CARDHOLDERS AND CARDHOLDER GROUPS.

12.03 THE ACS SHALL PERMIT THE FOLLOWING ACTIVATION/EXPIRATION OPTIONS FOR A CARDHOLDER'S PROFILE: DELAYED ACTIVATION OF A CARDHOLDER'S PROFILE, EXPIRATION BASED ON THE DATE OF FIRST USE OF CREDENTIALS, OR EXPIRATION ON A USER-DEFINED DATE.

12.04 IT SHALL BE POSSIBLE TO SET A START DATE AND EXPIRATION DATE FOR THE ASSOCIATION OF A CARDHOLDER AND AN ACCESS RULE FOR TEMPORARY ACCESS.

12.05 IT SHALL BE POSSIBLE TO ASSOCIATE A PICTURE TO A CARDHOLDER'S PROFILE. THE PICTURE SHALL BE IMPORTED FROM A FILE, CAPTURED WITH A DIGITAL CAMERA, OR CAPTURED FROM A VIDEO SURVEILLANCE CAMERA. WHEN A CARDHOLDER EVENT OCCURS, THE PICTURE OF THE CARDHOLDER SHALL BE DISPLAYED IN THE MONITORING UI. THE ACS SHALL SUPPORT MULTIPLE STANDARD PICTURE FORMATS.

12.06 CARDHOLDER GROUPS SHALL ENABLE THE GROUPING OF CARDHOLDERS TO FACILITATE MASS CHANGES TO SYSTEM SETTINGS. IT SHALL BE POSSIBLE TO ASSIGN CARDHOLDER GROUPS TO ACCESS RULES, THUS AVOIDING THE ASSIGNMENT OF ONE CARDHOLDER AT A TIME.

12.07 IT SHALL BE POSSIBLE TO SEARCH BY PICTURE ASSOCIATION, CUSTOM FIELDS, NAMES, AND CREDENTIAL CODES.

12.08 IT SHALL BE POSSIBLE TO SELECT MULTIPLE CARDHOLDERS FOR IMMEDIATE DEACTIVATION OR REACTIVATION.

12.09 THE ACS SHALL SUPPORT THE SYNCHRONIZATION OF CARDHOLDERS AND CARDHOLDER GROUPS THROUGH ACTIVE DIRECTORY INCLUDING THE CREDENTIALS AND PICTURES OF THE CARDHOLDERS. (UP TO 9 ADDITIONAL CONNECTIONS CAN BE ADDED, AVAILABLE IN ENTERPRISE). IT SHALL BE POSSIBLE TO IMPORT CARDHOLDERS FROM AZURE AD.

12.10 UNUSED CREDENTIALS SHALL NOT BE AUTOMATICALLY DELETED.

12.11 IT SHALL SUPPORT THE IMPORT OF CARDHOLDERS, CREDENTIALS, AND CUSTOM FIELDS FROM AN EXTERNAL SYSTEM DATABASE OR CSV.

ACS CREDENTIAL MANAGEMENT

13.01 THE ACS SHALL SUPPORT THE CONFIGURATION AND MANAGEMENT OF CREDENTIALS, FOR EXAMPLE ACCESS CARDS AND KEYPAD PIN NUMBERS. A USER SHALL BE ABLE TO ADD, DELETE, OR MODIFY A CREDENTIAL IF THE USER HAS THE APPROPRIATE PRIVILEGES.

13.02 THE ACS SHALL SUPPORT READER TRANSPARENT MODE.

13.03 USERS SHALL BE ABLE TO ADD CUSTOM FIELDS (USER-DEFINED FIELDS) TO CREDENTIALS. CREATING A NEW CREDENTIAL SHALL BE ACCOMPLISHED EITHER MANUALLY OR AUTOMATICALLY.

13.04 AUTOMATIC CREATION SHALL ALLOW THE USER TO CREATE A CREDENTIAL ENTITY BY PRESENTING A CREDENTIAL TO A SELECTED READER. THE ACS SHALL READ THE CARD DATA AND ASSOCIATE IT TO THE CREDENTIAL ENTITY. IT SHALL BE POSSIBLE TO AUTOMATICALLY ENROLL ANY CARD FORMAT.

13.05 THE ACS SHALL SUPPORT HIGH ASSURANCE CREDENTIALS USING VALIDATION OF A CERTIFICATE, SUCH AS PIV, PIV-I, AND CIV.

13.06 THE ACS SHALL SUPPORT MULTIPLE CREDENTIALS PER CARDHOLDER WITHOUT NECESSITATING DUPLICATE CARDHOLDER INFORMATION. THE ACS SHALL AUTOMATICALLY DETECT AND PREVENT ATTEMPTS TO REGISTER AN ALREADY-REGISTERED CREDENTIAL.

13.07 IT SHALL BE POSSIBLE TO NATIVELY ENCODE DESFIRE CREDENTIALS FROM THE USER INTERFACE USING CUSTOMER'S OWN KEYS AND CONFIGURATION.

13.08 BATCH ENROLLMENT OF CREDENTIALS SHALL BE SUPPORTED.

13.09 THE ACS SHALL PROVIDE A WORKFLOW FOR BADGE ISSUANCE AND CARD REQUESTS.

13.10 THE ACS SHALL SUPPORT THE USE OF LICENSE PLATES AS A CREDENTIAL.

13.11 THE ACS SHALL SUPPORT DURESS PIN.

13.12 THE ACS SHALL NATIVELY SUPPORT THE CREATION AND MANAGEMENT OF MOBILE IDS IN THE SAME WAY AS OTHER CREDENTIALS.

13.13 THE ACS SHALL SUPPORT THE ABILITY TO PRINT AND ENROLL CREDENTIALS.

13.14 THE ACS SHALL SUPPORT THE ABILITY TO PRINT AND ENCODE SEOS AND MIFARE CREDENTIALS (REQUIRES A LICENSE).

ACS CUSTOM CARD FORMATS

14.01 A CUSTOM CARD FORMAT FEATURE SHALL ALLOW THE ADMINISTRATOR TO ADD ADDITIONAL CUSTOM CARD FORMATS USING AN INTUITIVE TOOL WITHIN THE CONFIGURATION UI. THE CUSTOM CARD FORMAT TOOL SHALL BE FLEXIBLE IN THE FOLLOWING WAYS:

A. Once enrolled, new custom card formats shall appear in the card format lists for manual card enrollment.

B. An unrestricted number of additional custom card formats can be added.

C. Shall support credential with up to 512 bits.

D. The administrator shall be able to set the following options when defining a new format:
   1. The order in which card fields appear in the user interface or CSA.
   2. Whether a field is hidden from or visible to an operator.
   3. Whether a field is read only or modifiable by an operator.
   4. Complex parity checking schemes.
   5. The order and location of a field's data. Location can be defined on a bit-by-bit basis.
   6. Application ID and keys for DESfire EV1 credentials.

ACS BADGE DESIGNER

15.01 THE BADGE DESIGNER SHALL ALLOW THE CREATION OF BADGE TEMPLATES THAT DEFINE THE CONTENT AND PRESENTATION FORMAT OF A CARDHOLDER BADGE TO BE PRINTED.

15.02 BADGE PRODUCTION SHALL CONSIST OF SELECTING THE CREDENTIAL, THE BADGE TEMPLATE, AND CLICKING PRINT.

15.03 BATCH PRINTING OF CARDS SHALL BE AVAILABLE.

15.04 THE CONTENTS OF A BADGE TEMPLATE CAN INCLUDE: CARDHOLDER'S FIRST AND LAST NAME, PICTURE, CUSTOM FIELDS, BITMAP GRAPHICS, LINES, OVALS, RECTANGLES, DYNAMIC TEXT LABELS LINKED TO CUSTOM FIELDS AND STATIC TEXT LABELS, AND BARCODES (INTERLEAVED 2 OF 5, EXTENDED CODE 39).

15.05 COPY AND PASTE OF BADGE TEMPLATE OBJECTS SHALL BE AVAILABLE.

15.06 IT SHALL BE POSSIBLE TO SET THE BORDER THICKNESS AND COLOR, THE FILL COLOR OF BADGE OBJECTS (CONTENT), AND THE COLOR OF TEXT LABELS.

15.07 SETTINGS, SUCH AS OBJECT TRANSPARENCY, TEXT ORIENTATION, AND AUTO-SIZING OF TEXT SHALL BE AVAILABLE OR TRANSPARENT TO THE USER.

15.08 SUPPORTED BADGE FORMATS SHALL BE (PORTRAIT AND LANDSCAPE): CR70 (2.875" X 2.125"), CR80 (3.37" X 2.125"), CR90 (3.63" X 2.37"), CR100 (3.88" X 2.63"), AND CUSTOM CARD SIZES.

15.09 DUAL-SIDED BADGES SHALL BE SUPPORTED.

15.10 A BADGE TEMPLATE IMPORT AND EXPORT FUNCTION SHALL BE AVAILABLE TO ALLOW THE SHARING OF BADGE TEMPLATES BETWEEN DISTINCT OR INDEPENDENT ACS.

15.11 CHROMAKEY SHALL BE SUPPORTED.

ACS DOOR MANAGEMENT

16.01 THE ACS SHALL SUPPORT THE CONFIGURATION AND MANAGEMENT OF DOORS. A USER SHALL BE ABLE TO ADD, DELETE, OR MODIFY A DOOR IF THEY HAVE THE APPROPRIATE PRIVILEGES.

16.02 THE ACS SHALL PERMIT MULTIPLE ACCESS RULES TO BE ASSOCIATED TO A DOOR.

16.03 IT SHALL BE POSSIBLE TO UNLOCK ALL DOORS FROM AN AREA AT ONCE.

16.04 THE ACS SHALL SUPPORT THE FOLLOWING FORMS OF AUTHENTICATION: CARD ONLY, CARD OR KEYPAD (PIN), OR CARD AND KEYPAD (PIN). IT SHALL BE POSSIBLE TO DEFINE A SCHEDULE FOR WHEN CARD ONLY OR CARD AND KEYPAD AUTHENTICATION MODES SHALL BE REQUIRED.

16.05 IT SHALL BE POSSIBLE TO SET AN EXTENDED GRANT TIME ON A PER-DOOR BASIS (IN ADDITION TO THE STANDARD GRANT TIME). CARDHOLDER PROPERTIES SHALL INCLUDE THE OPTION OF USING THE EXTENDED GRANT TIME. WHEN FLAGGED CARDHOLDERS ARE GRANTED ACCESS, THE DOOR SHALL BE UNLOCKED FOR THE DURATION OF THE EXTENDED GRANT TIME INSTEAD OF THE STANDARD GRANT TIME.

16.06 THE ACS SHALL ALLOW THE CONFIGURATION OF THE RELOCKING MODE ON DOORS SUCH AS ON DOOR OPEN, AFTER A DEFINITE TIME, OR ON DOOR CLOSE.

16.07 THE ACS SHALL SUPPORT THE ABILITY TO ENFORCE THE USE OF TWO VALID READS FROM DIFFERENT CARDHOLDERS TO GRANT ACCESS TO AN AREA.

16.08 THE ACS SHALL SUPPORT THE ABILITY TO ENABLE ACCESS RULES FOR OTHER CARDHOLDERS ONCE A SUPERVISOR HAS ACCESSED AN AREA.

16.09 THE ACS SHALL SUPPORT THE ABILITY TO ENABLE UNLOCKING SCHEDULE ON A DOOR ONCE AN EMPLOYEE HAS ENTERED THE FACILITY.

16.10 READERLESS DOORS.

A. The ACS shall support doors configured solely with a lock, a REX, and a door contact but without readers.

B. The implementation of a readerless door shall be possible with the use of standard access hardware IO modules. External hardware, such as timers, shall not be required.

C. Unlocking schedules shall be programmable for readerless doors.

D. Standard door activity reports shall also be possible with readerless doors.

16.11 UNLOCKING SCHEDULES AND EXCEPTIONS TO UNLOCKING SCHEDULES SHALL BE ASSOCIATED WITH A DOOR. AN UNLOCKING SCHEDULE SHALL DETERMINE WHEN A DOOR SHOULD BE AUTOMATICALLY UNLOCKED. THE ACS SHALL ALSO SUPPORT THE USE OF A SPECIFIC OFFLINE UNLOCKING SCHEDULE. EXCEPTIONS TO UNLOCKING SCHEDULES SHALL BE USED TO DEFINE TIME PERIODS DURING WHICH UNLOCKING SCHEDULES SHALL NOT BE APPLIED, SUCH AS DURING STATUTORY HOLIDAYS.

16.12 THE ACS SHALL SUPPORT ONE OR MORE CAMERAS PER DOOR. VIDEO SHALL THEN BE ASSOCIATED TO DOOR ACCESS EVENTS, SUCH AS ACCESS GRANT OR ACCESS DENIED.

ACS ELEVATOR MANAGEMENT

17.01 THE ACS SHALL SUPPORT THE CONFIGURATION AND MANAGEMENT OF ELEVATORS. A USER SHALL BE ABLE TO ADD, DELETE, OR MODIFY AN ELEVATOR IF THEY HAVE THE APPROPRIATE PRIVILEGES.

17.02 THE ACS SHALL BE ABLE TO CONTROL ACCESS TO SPECIFIC FLOORS USING A READER WITHIN THE ELEVATOR CAB. CONTROL SHALL BE AVAILABLE THROUGH THE USE OF A CONTROLLER WITH AN INTERFACE TO A READER AND TO MULTIPLE OUTPUT MODULES WITH RELAYS.

17.03 ELEVATOR FLOOR SELECTIONS SHALL BE TRACKED USING A CONTROLLER WITH AN INTERFACE TO MULTIPLE INPUT MODULES. FLOOR TRACKING SHALL BE AVAILABLE WITHIN AN ELEVATOR ACTIVITY REPORT.

17.04 THE ELEVATOR CONTROL MODULE SHALL CONTINUE TO FUNCTION IN OFFLINE MODE SHOULD COMMUNICATION BETWEEN THE ACS AND THE CONTROLLER FAIL.

17.05 THE ACS SHALL SUPPORT ONE OR MORE CAMERAS PER ELEVATOR CAB. VIDEO SHALL THEN BE ASSOCIATED TO ELEVATOR ACCESS EVENTS, SUCH AS ACCESS GRANTED OR ACCESS DENIED.

ACS VISITOR MANAGEMENT

18.01 THE ACS SHALL SUPPORT THE CONFIGURATION AND MANAGEMENT OF VISITORS. A USER SHALL BE ABLE TO ENROLL OR REMOVE A VISITOR IF THEY HAVE THE APPROPRIATE PRIVILEGES. THE ACS SHALL SUPPORT THE CHECK-IN AND CHECK-OUT OF VISITORS FROM THE MONITORING UI.

18.02 A VISITOR CHECK-IN WIZARD SHALL FACILITATE THE ENROLLMENT PROCESS, ALLOWING A USER TO SPECIFY THE VISITOR'S SPECIFIC INFORMATION.

18.03 IT SHALL BE POSSIBLE TO SET A HOST LEADING A GROUP OF VISITORS AND A TRAILING HOST WALKING BEHIND VISITORS, TRIGGERING ALERT IF A VISITOR IS NOT FOLLOWING THE DELEGATION.

18.04 THE ACS SHALL PERMIT THE FOLLOWING CREDENTIAL OPTIONS DURING VISITOR CHECK-IN:

A. Use an existing credential.

B. Automatically create a new credential.

C. Manually create a new credential.

18.05 THE ACS SHALL SUPPORT THE CREATION OF A POOL OF VISITOR CREDENTIALS IN ADVANCE. EXISTING VISITOR CREDENTIALS SHALL BE ASSIGNED TO VISITORS DURING THE CHECK-IN PROCESS.

18.06 THE ACS SHALL PERMIT CARDHOLDER GROUPS TO BE DESIGNATED AS "AVAILABLE FOR VISITORS". USERS SHALL BE ABLE TO DEFINE THE ACCESS PRIVILEGES FOR THE CARDHOLDER GROUPS (VISITOR CARDHOLDER GROUPS) IN ADVANCE. DURING VISITOR CHECK-IN, THE USER SHALL SELECT THE APPROPRIATE VISITOR CARDHOLDER GROUP TO ASSOCIATE WITH A VISITOR. ALL OF THE VISITOR CARDHOLDER GROUP ACCESS PRIVILEGES SHALL BE AUTOMATICALLY TRANSFERRED TO THE VISITOR. THIS FEATURE SHALL PERMIT THE CREATION OF MULTIPLE TYPES OF VISITOR GROUPS AND ASSOCIATED PRIVILEGES, SUCH AS FOR CONTRACTORS, VIPS, AND DAY VISITORS. VISITORS ADDED TO A VISITOR CARDHOLDER GROUP IN THE MONITORING UI SHALL BE AUTOMATICALLY UPDATED IN THE CONFIGURATION UI CARDHOLDER GROUP SCREEN.

18.07 A VISITOR'S PROFILE SHALL SUPPORT THE REAL-TIME MODIFICATION OF VISITOR INFORMATION AFTER A VISITOR HAS CHECKED IN.

18.08 THE ACS SHALL ALSO PROVIDE COMPREHENSIVE VISITOR TRACKING AND VISITOR REPORTING. THROUGH THE REAL-TIME TRACKING FEATURE, THE ACS SHALL GENERATE A REAL-TIME AND HISTORICAL VISITOR ACTIVITY LISTING IN THE MONITORING UI. THE ACS SHALL ALSO GENERATE VISITOR-SPECIFIC REPORTS THAT PROVIDE COMPREHENSIVE LISTINGS OF VISITORS AS WELL AS FULL DETAILS ON THEIR MOVEMENT.

18.09 IT SHALL BE POSSIBLE TO EXEMPT A VISITOR FROM ANY ANTIPASSBACK RULES IN EFFECT.

18.10 THE OPERATOR SHALL BE ABLE TO PRINT VISITOR BADGES DURING THE CHECK-IN PROCESS. THE PRINTING OF BOTH PAPER BADGES (VISITOR WITHOUT AN ASSIGNED CREDENTIAL) AND ACTUAL CREDENTIALS SHALL BE SUPPORTED.

18.11 VISITOR MANAGEMENT AND REPORTING SHALL BE AVAILABLE THROUGH THE WEB CLIENT AS WELL.

18.12 IT SHALL BE POSSIBLE TO LOCATE A VISITOR'S INFORMATION OR PROFILE BY SWIPING THE VISITOR'S CREDENTIAL (CARD) AT A USB READER.

18.13 IT SHALL BE POSSIBLE TO TAG THE PERSON VISITED TO THE VISITOR'S PROFILE.

18.14 IT SHALL BE POSSIBLE TO REQUIRE THAT THE VISITOR MUST HAVE AN ESCORT TO ENTER AN AREA AND THAT THE ESCORT MUST BADGE-IN TO CONFIRM THE ACCESS OF THE VISITOR.

ACS PEOPLE COUNTING & AREA PRESENCE TRACKING (MUSTERING)

19.01 THE ACS SHALL SUPPORT PEOPLE COUNTING (OR AREA PRESENCE TRACKING). THE ACS SHALL BE ABLE TO MONITOR AND REPORT THE NUMBER OF CARDHOLDERS IN AN AREA IN REAL-TIME AND FOR ALL AREAS. MONITORING SHALL BE BASED ON THE ENTIRE ACCESS CONTROL INFRASTRUCTURE, FOR BOTH LOCAL AREAS AND THOSE IN REMOTE GEOGRAPHIC LOCATIONS. PEOPLE COUNTING CAN ALSO BE USED TO PERFORM MUSTERING.

19.02 IT SHALL BE POSSIBLE TO CONTROL THE MAXIMUM OCCUPANCY OF AN AREA BY SETTING A THRESHOLD AND USER NOTIFICATION WHEN REACHING THE LIMIT.

19.03 THE ACS SHALL REPORT AREA PRESENCE COUNTS IN THE UI. AREA PRESENCE TRACKS SHALL DYNAMICALLY TRACK THE TOTAL NUMBER OF CARDHOLDERS IN AN AREA. DISPLAYED DATA SHALL BE UPDATED DYNAMICALLY.

19.04 THE ACS SHALL SUPPORT MUSTERING THROUGH THE USE OF MOBILE READERS (REQUIRES ADDITIONAL SOFTWARE AND HARDWARE FROM THIRD-PARTY).

19.05 THE ACS SHALL PROVIDE A NATIVE DEDICATED MUSTERING TASK USING A USB, MOBILE, OR WALL READER.

19.06 THE ACS SHALL BE ABLE TO GENERATE AN AREA PRESENCE REPORT LISTING THE CARDHOLDERS LOCATED IN ONE OR MORE AREAS, ACCESSIBLE THROUGH THE MONITORING UI. IT SHALL BE POSSIBLE TO FILTER THE REPORT BY AREA AND TIME PERIOD. THE REPORT SHALL ALSO INCLUDE ACTIVITY FROM SUB-AREAS (NESTED AREAS).

19.07 THROUGH PEOPLE COUNTING, THE ACS SHALL BE ABLE TO GENERATE FIRST PERSON IN AND LAST PERSON OUT EVENTS. THE FIRST PERSON IN EVENT SHALL DETECT WHEN THE FIRST CARDHOLDER ENTERS AN EMPTY AREA. THE LAST PERSON OUT EVENT SHALL DETECT WHEN THE LAST CARDHOLDER LEAVES AN AREA. IT SHALL BE POSSIBLE TO TRIGGER ACTIONS FROM BOTH EVENTS SUCH AS SENDING A MESSAGE OR TRIGGERING AN ALARM.

19.08 THE ACS SHALL BE ABLE TO DETERMINE THE ENTRY OF A CARDHOLDER BASED ON A DEDICATED SENSOR.

19.09 THE ACS SHALL PROVIDE A VISUAL HTML DASHBOARD TO AID WITH THE EVACUATION THAT CAN RUN ON MOBILE DEVICES.

19.10 THE ACS SHALL PROVIDE THE ABILITY TO GLOBALLY VIEW ALL EVACUATIONS SIMULTANEOUSLY OR PER AREA.

19.11 ON AN EVACUATION, THE ACS SHALL SET ALL CARDHOLDERS AS UNKNOWN UNTIL THEY REACH A MUSTERING POINT.

19.12 IT SHALL BE POSSIBLE TO MARK A CARDHOLDER AS SAFE OR UNSAFE FROM THE WEB EVACUATION ASSISTANT.

19.13 IT SHALL BE POSSIBLE TO FILTER BY CARDHOLDER GROUPS OR CUSTOM FIELDS IN THE MUSTERING DASHBOARD.

19.14 THE ACS SHALL SUPPORT WALL-MOUNTED READERS AND MOBILE-HANDLED DEVICES FOR MUSTERING.

19.15 THE ACS SHALL PROVIDE DISTINCT VISUAL INDICATION AS AN AREA IS BEING EVACUATED.

19.16 THE ACS SHALL HAVE THE ABILITY TO CONFIGURE A MUSTERING POINT PER AREA.

19.17 THE ACS SHALL HAVE THE ABILITY TO RESET APB AT THE END OF AN EVACUATION.

ACS CUSTOM FIELDS (USER-DEFINED FIELDS)

20.01 THE ACS SHALL PERMIT THE CREATION OF CUSTOM FIELDS. UP TO 1,000 CUSTOM FIELDS SHALL BE SUPPORTED.

20.02 CUSTOM FIELDS SHALL BE SUPPORTED FOR THE FOLLOWING ENTITIES: CARDHOLDERS, CARDHOLDER GROUPS, CREDENTIALS, AND VISITORS.

20.03 SUPPORTED CUSTOM FIELDS SHALL INCLUDE TEXT, INTEGERS, DECIMAL NUMBERS, DATES, BOOLEAN, AND IMAGES (GRAPHICS).

20.04 USERS SHALL BE ABLE TO DEFINE A DEFAULT VALUE FOR A CUSTOM FIELD.

20.05 THE CREATION OF NEW CUSTOM FIELD TYPES SHALL BE POSSIBLE. NEW CUSTOM FIELD TYPES SHALL BE BASED ON THE STANDARD CUSTOM FIELDS SUPPORTED. THEY SHALL SUPPORT USER-DEFINED VALUES FROM WHICH AN OPERATOR MUST MAKE A SELECTION.

20.06 ADMINISTRATORS HAVE THE ABILITY TO DEFINE WHICH USERS CAN VIEW AND MODIFY SPECIFIC CUSTOM FIELDS. THIS SHALL LIMIT THE ACCESS TO CUSTOM FIELD DATA TO USERS WITH PRE-DEFINED PRIVILEGES. THE ACS SHALL SUPPORT QUERYING AND REPORT GENERATION USING CUSTOM FIELDS.

20.07 CUSTOM FIELDS CAN BE GROUPED AND ORDERED WITHIN THESE GROUPS AS DEFINED BY THE USER.

20.08 VALUES FOR CUSTOM FIELDS CAN BE IMPORTED USING THE IMPORT TOOL.

ACS IMPORT TOOL

21.01 THE ACS SHALL SUPPORT AN INTEGRATED IMPORT TOOL TO FACILITATE THE IMPORT OF EXISTING CARDHOLDER AND CREDENTIAL DATA. THE IMPORT OF DATA SHALL BE THROUGH THE USE THE CSV FILE FORMAT. THE TOOL SHALL BE AVAILABLE FROM THE CONFIGURATION UI.

21.02 IT SHALL BE POSSIBLE TO CONNECT TO AN EXTERNAL MICROSOFT SQL OR ORACLE DATABASE TO IMPORT CARDHOLDERS.

21.03 THE IMPORT TOOL SHALL ALSO SUPPORT THE ABILITY TO MANUALLY IMPORT DATA THAT HAS BEEN EXPORTED FROM A THIRD-PARTY DATABASE IF IT IS IN CSV FORMAT.

21.04 THE IMPORT TOOL SHALL PERMIT THE IMPORT OF THE FOLLOWING DATA:

A. Cardholder name, descriptions, picture, email, and status.

B. Cardholder group information.

C. Credential name, status, format, and card number (including credentials with custom formats).

D. Partition information.

E. Custom fields.

F. Activation date and expiration date.

G. Update cardholder group association.

21.05 FULL FLEXIBILITY IN SELECTING THE FIELDS TO BE IMPORTED DURING AN IMPORT SESSION SHALL BE AVAILABLE.

21.06 THE OPTION TO USE A CUSTOM AND UNIQUE CARDHOLDER KEY SHALL BE SPECIFIED DURING THE IMPORT PROCESS TO ENSURE THAT CARDHOLDERS WITH DUPLICATE NAMES WILL NOT HAVE THEIR DATA OVERWRITTEN. CARDHOLDER KEY GENERATION SHALL BE AUTOMATED. THE END USER SHALL HAVE THE OPTION TO SELECT WHICH FIELDS WILL BE USED TO CREATE THIS UNIQUE KEY, FOR EXAMPLE CREDENTIAL NUMBER, CUSTOM FIELDS, OR CARDHOLDER NAME.

21.07 THE ACS SHALL ALSO SUPPORT RE-IMPORTING A CSV FILE CONTAINING NEW INFORMATION TO UPDATE EXISTING INFORMATION IN THE ACS DATABASE. RE-IMPORTING SHALL ENABLE BULK AMENDMENTS TO EXISTING ACCESS CONTROL DATA.

GENERAL CLIENT SOFTWARE REQUIREMENTS

22.01 THE CLIENT SOFTWARE APPLICATIONS (CSA) SHALL PROVIDE THE USER INTERFACE FOR USP CONFIGURATION AND MONITORING OVER ANY NETWORK AND BE ACCESSIBLE LOCALLY OR FROM A REMOTE CONNECTION.

22.02 THE CSA SHALL CONSIST OF THE CONFIGURATION UI FOR SYSTEM CONFIGURATION AND THE MONITORING UI FOR MONITORING. THE CSA SHALL BE WINDOWS-BASED AND PROVIDE AN EASY-TO-USE GRAPHICAL USER INTERFACE (UI).

22.03 THE CSA FOR MONITORING SHALL SUPPORT RUNNING IN 64-BIT MODE.

22.04 THE SERVER ADMINISTRATOR SHALL BE USED TO CONFIGURE THE SERVER DATABASE(S). IT SHALL BE WEB-BASED AND ACCESSIBLE LOCALLY ON THE SSM OR ACROSS THE NETWORK.

22.05 THE CSA SHALL SEAMLESSLY MERGE ACCESS CONTROL, LICENSE PLATE RECOGNITION (ALPR), AND VIDEO FUNCTIONALITIES WITHIN THE SAME USER APPLICATION.

22.06 THE USP SHALL USE THE LATEST USER INTERFACE (UI) DEVELOPMENT AND PROGRAMMING TECHNOLOGIES SUCH AS MICROSOFT WPF (WINDOWS PRESENTATION FOUNDATION), THE XAML MARKUP LANGUAGE, AND THE .NET SOFTWARE FRAMEWORK.

22.07 ALL APPLICATIONS SHALL PROVIDE AN AUTHENTICATION MECHANISM, WHICH VERIFIES THE VALIDITY OF THE USER. AS SUCH, THE ADMINISTRATOR (WHO HAS ALL RIGHTS AND PRIVILEGES) CAN DEFINE SPECIFIC ACCESS RIGHTS AND PRIVILEGES FOR EACH USER IN THE SYSTEM.

22.08 LOGGING ON TO A CSA SHALL BE DONE EITHER THROUGH LOCALLY STORED USP USER ACCOUNTS AND PASSWORDS OR USING THE OPERATOR'S WINDOWS CREDENTIALS WHEN ACTIVE DIRECTORY INTEGRATION IS ENABLED. (FIRST LICENSE OF ACTIVE DIRECTORY INTEGRATION INCLUDED, ADDITIONAL LICENSES REQUIRED FOR MORE)

22.09 WHEN INTEGRATED WITH MICROSOFT'S ACTIVE DIRECTORY, THE CSA AND USP SHALL AUTHENTICATE USERS USING THEIR WINDOWS CREDENTIALS. AS A RESULT, THE USP WILL BENEFIT FROM ACTIVE DIRECTORY PASSWORD AUTHENTICATION AND STRONG SECURITY FEATURES. (FIRST LICENSE OF ACTIVE DIRECTORY INTEGRATION INCLUDED, ADDITIONAL LICENSES REQUIRED FOR MORE)

22.10 WHEN INTEGRATED WITH AN EXTERNAL IDENTITY PROVIDER SUCH AS WINDOWS ACTIVE DIRECTORY, ADFS (ACTIVE DIRECTORY FEDERATION SERVICES) OR AN OPEN ID CONNECT/SAML2 IDENTITY PROVIDER (EX.: AZURE AD), THE CSA AND USP SHALL AUTHENTICATE USING A SINGLE-SIGN ON EXPERIENCE TO THE USERS. AS A RESULT, THE USP WILL BENEFIT FROM REUSING THE SAME CREDENTIAL THROUGHOUT ENTERPRISE APPLICATIONS.

22.11 THE CSA SHALL SUPPORT MULTIPLE LANGUAGES, INCLUDING BUT NOT LIMITED TO THE FOLLOWING: ENGLISH, FRENCH, ARABIC, CZECH, DUTCH, GERMAN, HEBREW, HUNGARIAN, ITALIAN, JAPANESE, KOREAN, NORWEGIAN, PERSIAN (FARSI), POLISH, PORTUGUESE (BRAZILIAN), SIMPLIFIED AND TRADITIONAL CHINESE, RUSSIAN, SPANISH, SWEDISH, THAI, TURKISH, AND VIETNAMESE.

22.12 TO ENHANCE USABILITY AND OPERATOR EFFICIENCY, THE CONFIGURATION UI AND MONITORING UI SHALL SUPPORT MANY OF THE LATEST UI SUCH AS:

A. A customizable Home Page that includes favorite and recently used tasks.

B. Task-oriented approach for administrator/operator activities where each type of activity (surveillance, visitor management, individual reports, and more) is an operator task.

C. Consolidated and consistent workflows for video, ALPR, and access control.

D. Single click functionality for reporting and tracking. The Monitoring UI shall support both single-click reporting for access control, ALPR, and video, as well as single-click tracking of areas, cameras, doors, zones, cardholders, elevators, ALPR entities, and more. Single-click reporting or tracking shall create a new task with the selected entities to report on or track.

22.13 CONFIGURATION UI AND MONITORING UI HOME PAGE AND TASKS

A. The Configuration UI and Monitoring UI shall be task oriented.

B. A task shall be user interface design patterns whose goal is to simplify the user interface by grouping related features from different systems such as video and access, in the same display window. Features shall be grouped together in a task based on their shared ability to help the user perform a specific task.

C. Tasks shall be accessible via the Home Page of either the Configuration or the Surveillance CSA.

D. Newly created tasks shall be accessible via the Configuration UI or the Monitoring UI taskbar.

E. Similar tasks shall be grouped into the following categories:
   1. Operation: Access control management, LRP management, and more.
   2. Investigation: access control activity reports, visitor activity reports, alarm reports, and more.
   3. Maintenance: Access control, troubleshooters, audit trails, health-related reports, and more.

F. An operator shall be able to launch a specific task only if they have the appropriate privileges.

G. The Home Page content shall be customizable through the use of privileges to hide tasks that an operator should not have access to and through a list of favorite and recently used tasks. In addition, editing a USP XML file to add new tasks on the fly shall also be possible.

H. The configuration of the operator parameters shall be able to be imported and exported for both the Configuration and Monitoring UI.

22.14 THE CONTRACTOR SHALL PROVIDE UP TO XX NUMBER OF SIMULTANEOUS CLIENTS, INCLUDING THICK CLIENT, WEB, AND MOBILE CONNECTIONS.

CONFIGURATION USER INTERFACE (UI)

23.01 GENERAL

A. The Configuration UI application shall allow the administrator or users with appropriate privileges to change the system configuration. The Configuration UI shall provide decentralized configuration and administration of the USP system from anywhere on the IP network.

B. The configuration of all embedded ACS, VMS, and ALPR systems shall be accessible via the Configuration UI.

C. The Configuration UI shall have a home page with single-click access to various tasks.

D. The Configuration UI shall include a variety of tools such as troubleshooting utilities, import tools, and a unit discover tool, amongst many more.

E. The Configuration UI shall include a static reporting interface to:
   1. View historical events based on entity activity. The user shall be able to perform such actions as printing a report and troubleshooting a specific access event from the reporting view.
   2. View audit trails that show a history of user/administrator changes to an entity.

F. Common entities such as users, schedules, alarms, and many more, can be reused by all embedded systems (ACS, VMS, and ALPR).

ACS CLIENT USER INTERFACE (UI)

24.01 THE MONITORING UI SHALL FULFILL THE ROLE OF A UNIFIED SECURITY INTERFACE THAT IS ABLE TO MONITOR VIDEO, ALPR, AND ACCESS CONTROL EVENTS AND ALARMS, AS WELL AS VIEW LIVE AND RECORDED VIDEO.

24.02 THE MONITORING UI SHALL PROVIDE A GRAPHICAL USER INTERFACE TO CONTROL AND MONITOR THE USP OVER ANY IP NETWORK. IT SHALL ALLOW ADMINISTRATORS AND OPERATORS WITH APPROPRIATE PRIVILEGES TO MONITOR THEIR UNIFIED SECURITY PLATFORM, RUN REPORTS, AND MANAGE ALARMS.

24.03 TO ENHANCE USABILITY AND OPERATOR EFFICIENCY, THE MONITORING UI SHALL SUPPORT THE FOLLOWING UI CONCEPTS:

A. Dynamically adaptive interface that adjusts in real-time to what the operator is doing.

B. Dynamic controls loaded with entity-specific widgets (for example, door and camera widgets).

C. Use of transparent overlays that can display multiple types of data in a seamless fashion.

D. Display tile menus and quick commands.

E. Consolidated and consistent workflows.

F. Tile menus and quick commands easily accessible within every display tile of the user workspace.

G. Single-click functionality for reporting and tracking. The Monitoring UI shall support both single-click reporting for access control, ALPR, and video, as well as single-click tracking of areas, cameras, doors, zones, cardholders, elevators, ALPR entities, and more. Single-click reporting or tracking shall create a new task with the selected entities to report on or to track.

24.04 MONITORING UI HOME PAGE AND TASKS

A. Similar tasks shall be grouped into the following categories:
   1. Operation: Access control/LRP/video surveillance, visitor management, mustering, access control and video alarm monitoring, and more.
   2. Investigation: Video bookmark/motion/archive reports, access control activity reports, visitor activity reports, alarm reports, ALPR activity reports, and more.
   3. Maintenance: Access control and video configuration reports, troubleshooters, audit trails, and more.

24.05 DYNAMICALLY ADAPTIVE UI, CONTROLS SECTION, AND WIDGETS

A. The Monitoring UI shall dynamically adapt to what the operator is doing. This shall be accomplished through the concept of widgets that are grouped in the Monitoring UI Controls section.

B. Widgets shall be mini-applications or mini-groupings in the Monitoring UI Controls section that let the operator perform common tasks and provide them with fast access to information and actions.

C. With a single click on an entity (for example, door or camera) the specific widgets associated to that entity appear and other non-relevant widgets disappear dynamically (instantly). Widgets shall bring the operator information such as door status and camera stream information, as well as user actions, such as door unlock, PTZ controls, and more.

D. Specific widgets include those for a door, camera, alarm, zone, display tile, video stream (statistics), PTZ camera, and more.

24.06 OPERATOR WORKFLOWS

A. A workflow shall be a sequence of operations an operator or administrator shall execute to complete an activity. The “flow” relates to a clearly defined timeline or sequence for executing the activity.

B. The Monitoring UI shall be equipped with consistent workflows for the ALPR, video, and access control systems that it unifies.

C. Generating or printing a report, setting up or acknowledging an alarm, or creating an incident report shall follow the same process (workflow) whether the operator is working with video, ALPR, or access control, or with both video and access control.

24.07 EACH TASK WITHIN THE MONITORING UI SHALL CONSIST OF ONE OR MORE OF THE FOLLOWING ITEMS:

A. Event list.

B. Logical tree. Doors, cameras, zones, ALPR units, and elevators shall be grouped under Areas in a hierarchical fashion.

C. Entities list of all entities being tracked.

D. Display tiles with various patterns (1 x 1, 2 x 2, and more).

E. Display tile menu with various commands related to cameras, doors, PTZ, and tile controls.

F. Control section with widgets.

24.08 THE MONITORING UI SHALL SUPPORT MULTIPLE EVENT LISTS AND DISPLAY TILE PATTERNS, INCLUDING:

A. Event/alarm list layout only

B. Display tile layout only

C. Display tile and alarm/event list combination

D. ALPR map and alarm/event list combination

24.09 USER WORKSPACE CUSTOMIZATION

A. The user shall have full control over the user workspace through a variety of user-selectable customization options. Administrators shall also be able to limit what users and operators can modify in their workspace through privileges.

B. Once customized, the user shall be able to save their workspace.

C. The user workspace shall be accessible by a specific user from any client application on the network.

D. Display tile patterns shall be customizable.

E. Event or alarm lists shall span anywhere from a portion of the screen up to the entire screen and shall be resizable by the user. The length of event or alarm lists shall be user-defined. Scroll bars shall enable the user to navigate through lengthy lists of events and alarms.

F. The Monitoring UI shall support multiple display tile patterns (e.g., 1 display tile (1x1 matrix), 16 tiles (8x8 matrix), and multiple additional variations).

G. The Monitoring UI shall support as many monitors as the PC video adapters and Windows Operating System are capable of accepting.

H. Additional customization options include show/hide window panes, show/hide menus/toolbars, show/hide overlaid information on video, resize different window panes, and choice of tile display pattern on a per task basis.

24.10 THE MONITORING UI SHALL PROVIDE AN INTERFACE TO SUPPORT THE FOLLOWING TASKS AND ACTIVITIES COMMON TO ACCESS CONTROL, ALPR, AND VIDEO:

A. Monitoring the events from a live security system (ACS and/or VMS and/or ALPR).

B. Generating reports, including custom reports.

C. Monitoring and acknowledging alarms.

D. Creating and editing incidents and generating incident reports.

E. Displaying dynamic graphical maps and floor plans, as well as executing actions from dynamic graphical maps and floor plans.

F. Management and execution of hot actions and macros.

24.11 THE MONITORING UI SHALL BE ABLE TO MONITOR THE ACTIVITY OF THE FOLLOWING ENTITIES IN REAL-TIME: AREAS, ALPR ENTITIES, DOORS, ELEVATORS, CAMERAS, CARDHOLDERS, CARDHOLDER GROUPS, ZONES (INPUT POINTS), AND MORE. THE MONITORING UI SHALL PROVIDE AN INTERFACE TO SUPPORT THE FOLLOWING ACCESS CONTROL TASKS AND CAPABILITIES:

A. Monitoring and management of access events and alarms.

B. Viewing of cardholder picture or badge IDs.

C. Verification of cardholder picture IDs against live video.

D. Visitor management.

E. People counting or mustering, including resetting the people count in an area.

F. Door control, including remotely unlocking doors, overriding a door's unlocking schedules, and enabling door maintenance mode.

G. Forgiving antipassback.

H. Generation of ACS configuration and activity reports.

I. Viewing of HTML files including alarm instructions.

24.12 ENTITY MONITORING

A. The USP shall permit the user to select multiple entities to monitor from the Monitoring UI by adding the entities one by one to the tracking list.

B. The Monitoring UI shall provide the option to filter which events shall be displayed in the display tile layout, event list layout, or both.

C. It shall be possible to lock a Monitoring UI display tile so that it only tracks the activity of a specific entity (for example, a specific door or camera).

D. The user shall be able to drag and drop an event from an event list (or an alarm from an alarm list) onto a display tile to view a license plate read, cardholder picture ID, badge ID, or live/archived video, among other options.

E. Event, alarm, monitoring/tracking, and report lists shall contain cardholder pictures where applicable.

F. The user shall be permitted to start or pause the viewing of events within each display tile.

24.13 DISPLAY TILE PACKING AND UNPACKING

A. The Monitoring UI shall support single-click unpacking and packing for, areas, doors, zones, and alarms.

B. The packing and unpacking of entities shall allow operators to quickly obtain additional information and camera views of a specific entity.

C. The unpacking of an entity shall display associated entities. For example, unpacking a door with multiple associated cameras shall display all cameras associated with that door. Unpacking shall reconfigure the display tiles to be able to display all associated entities. For example, unpacking a door (or a zone or alarm) that is currently in a 1 x 1 tile configuration and

that has 3 cameras tied to it will create a 1 x 3 display tile arrangement for viewing all associated entities.

D. Packing will return the display to the original tile pattern.

24.14 THE FOLLOWING ADDITIONAL TOOLS OR UTILITIES SHALL BE AVAILABLE FROM THE MONITORING UI: CREATE CREDENTIALS, CREATE CARDHOLDERS, AND ACCESS CONTROL TROUBLESHOOTER.

SERVER ADMINISTRATOR USER INTERFACE REQUIREMENTS

25.01 THE SERVER ADMINISTRATOR SHALL BE USED TO CONFIGURE THE SSM AND THE DIRECTORY ROLE (MAIN CONFIGURATION) AND ITS DATABASE(S), TO APPLY THE LICENSE, AND MORE.

25.02 THE SERVER ADMINISTRATOR SHALL BE A WEB-BASED APPLICATION. THROUGH THE SERVER ADMINISTRATOR, IT SHALL BE POSSIBLE TO ACCESS THE SSM ACROSS THE NETWORK OR LOCALLY ON THE SERVER.

25.03 ACCESS TO THE SERVER ADMINISTRATOR SHALL BE PROTECTED VIA LOGIN NAME, PASSWORD, AND ENCRYPTED COMMUNICATIONS.

25.04 THE SERVER ADMINISTRATOR SHALL ALLOW THE ADMINISTRATOR (USER) TO PERFORM THE FOLLOWING FUNCTIONS:

A. Manage the system license.

B. Configure the database(s) and database server for the Directory Role.

C. Activate/Deactivate the Directory Role.

D. Manually back up the Directory Role database(s) and/or restore the server database(s), as well as configure scheduled backups of the databases.

E. Define the client-to-server communications security settings.

F. Configure the network communications hardware, including connection addresses and ports.

UNIFIED WEB CLIENT (UWC) GENERAL REQUIREMENTS

26.01 THE USP SHALL SUPPORT A UNIFIED WEB CLIENT (UWC) FOR ACCESS CONTROL, VIDEO, AND AUTOMATIC LICENSE PLATE RECOGNITION (ALPR).

26.02 THE UWC SHALL BE A TRULY THIN CLIENT WITH NO DOWNLOAD REQUIRED OTHER THAN AN INTERNET WEB BROWSER OR STANDARD WEB BROWSER PLUGINS.

26.03 THE UWC SHALL BE PLATFORM INDEPENDENT AND RUN WITHIN MICROSOFT EDGE, MS INTERNET EXPLORER, FIREFOX, SAFARI, AND GOOGLE CHROME.

26.04 THE UWC SHALL BE DESIGNED AS AN HTML5 APPLICATION.

26.05 THE UWC SHALL SUPPORT DISPLAY ON TABLET FORMAT.

26.06 THE UWC WILL SUPPORT NATIVE H.264 VIDEO IN THE WEB CLIENT.

26.07 WEB PAGES FOR THE WEB CLIENT SHALL BE MANAGED AND PUSHED BY THE WEB CLIENT SERVER. MICROSOFT IIS OR ANY OTHER WEB HOSTING SERVICE SHALL NOT BE REQUIRED GIVEN THAT ALL THE WEB PAGES SHALL BE HOSTED BY THE MOBILE SERVER.

26.08 THE WEB CLIENT SERVER SHALL PROVIDE THE ABILITY TO DEFINE A UNIQUE URL TO ACCESS THE WEB CLIENT, TO ENSURE THE SECURITY OF THE APPLICATION.

26.09 THE UWC SHALL PROVIDE THE ABILITY TO LOAD A CAMERA LAYOUT.

26.10 THE UWC SHALL PROVIDE THE ABILITY TO CONFIGURE, SAVE, AND RELOAD PRIVATE CAMERA LAYOUTS.

26.11 THE UWC SHALL PROVIDE THE ABILITY TO CONTROL PTZ CAMERAS.

26.12 FUNCTIONALITIES:

A. Log in support shall be available using:

1. Username and password
2. Active Directory (First Active Directory integration included, addition licenses required for more)

B. Ability for user to change their password.

C. Encrypted communications for all transactions.

D. Print reports and export to CSV file.

E. Access Control.
1. Cardholder and group (add/modify/delete)
2. Credential management (add/modify/delete)
3. Access rules management (add/modify/delete)
4. Visitor management (check-in/modify/check-out)
5. Unlock door
6. Override the unlocking schedule on a door
7. Door Activities report

F. Alarms.
1. Alarm report

G. Threat Level management.

H. Automatic License Plate Recognition (ALPR).
1. Live monitoring of the ALPR cameras
2. ALPR reads and hits report
3. Addition of plate numbers to hotlists

SMARTPHONE AND TABLET APP GENERAL REQUIREMENTS

27.01 THE USP SHALL SUPPORT MOBILE APPS FOR VARIOUS OFF-THE-SHELF DEVICES. THE MOBILE APPS SHALL COMMUNICATE WITH THE USP OVER ANY WI-FI OR CELLULAR NETWORK CONNECTION.

27.02 MOBILE APPS SHALL COMMUNICATE WITH THE USP VIA A MOBILE SERVER ROLE (MSR). ALL COMMUNICATION BETWEEN THE MOBILE APPS AND MSR SHALL BE BASED ON STANDARD TCP/IP PROTOCOL AND SHALL USE THE TLS ENCRYPTION WITH DIGITAL CERTIFICATES TO SECURE THE COMMUNICATION CHANNEL.

27.03 SUPPORTED DEVICE MANUFACTURERS SHALL INCLUDE (REFER TO MOBILE APP SPECIFICATIONS FOR LATEST COMPATIBILITY LIST):

A. Apple devices running iOS 13.0 or later

B. Android devices 10.0 or later

27.04 IT SHALL BE POSSIBLE TO DOWNLOAD THE MOBILE APPS FROM THE CENTRAL APPLICATION STORE (APPLE ITUNES APP STORE, GOOGLE PLAY).

27.05 IT SHALL BE POSSIBLE TO PUSH CONFIGURATION TO MOBILE DEVICES THROUGH A MOBILE DEVICE MANAGEMENT SOLUTION SUCH AS VMWARE WORKSPACE ONE OR MICROSOFT INTUNE.

27.06 FUNCTIONALITIES

A. Core
1. Ability to logon/logoff the UPS using an authorized use profile of the system.
2. Ability to support passive authentication from a single sign-on provider (OpenID Connect or SAML2 identity provider).
3. Ability to use biometric features (thumbprint, face ID, etc.) to perform connection to the system.
4. Ability to change the picture or the password of the user of the mobile app.
5. Ability to view the current Threat Level of the system.
6. Ability to change the current Threat Level of the system.

7. Ability to execute hot actions configured in the user profile.
8. Ability to view entities from the USP:
    a. Cameras
    b. Doors
    c. ALPR cameras
    d. Web Tile Plugins
    e. Layouts
    f. Camera Sequences
    g. Macros
    h. Maps (geographical maps only)
9. Ability to navigate the system hierarchical view of the entities and search entities in the system.

B. Video
1. Ability to view live and recorded video from the cameras of the USP. A maximum of eight cameras shall be displayed.
2. Ability to view video in native format (H.264).
3. Ability to display live and recorded video side-by-side for a specific camera.
4. Ability to perform digital zoom on cameras.
5. Ability to perform actions on cameras, such as add a bookmark, control a PTZ, control the iris/focus function, save a snapshot, and start/stop recording.
6. Ability to view camera layouts.
7. Ability to view camera sequences.
8. Ability to run a camera events report.
9. Ability to change the video quality on the cameras displayed on the mobile app.
10. Ability to use the camera of the smartphone and stream a live video feed to a video recorder in the system

C. Access Control
1. Ability to view the door state and the door lock state.
2. Ability to perform actions on a door such as unlock the door, set the door in maintenance mode, and override the door unlocking schedule.

D. Automatic License Plate Recognition
1. Ability to view live events raised by an ALPR camera.
2. Ability to view the read image, context image, and all metadata captured by the ALPR camera.
3. Ability to run an ALPR event report.
4. Ability to add a license plate to a hotlist on the system.

E. Alarm Management
1. Ability to receive push notifications to notify mobile operators that an alarm was received.
2. Ability to view all active alarms assigned to the mobile operator.
3. Ability to perform action on an alarm such as acknowledge, forward, or alternate-acknowledge an active alarm.
4. Ability to view entities attached to the alarm.

F. Map
1. Ability to display a geographical map with USP entities geo-located on the map.
2. Ability to view any entity configured on the map.
3. Ability to go to pre-defined map locations using preset buttons.
4. Ability to search for entities or locations on the map.

G. Incident management
1. Ability to view active incidents, sort and group them for a customized view.
2. Ability to trigger incidents manually.

3. Ability to get all details about an incident including related incidents, entities and documents.
4. Ability to take ownership of an incident and respond to the defined standard operating procedure geared towards incident resolution.

27.07 IT SHALL BE POSSIBLE TO SEND A MESSAGE FROM THE CLIENT USER INTERFACE TO A MOBILE OPERATOR.

27.08 IT SHALL BE POSSIBLE TO SEND A LIVE OR PLAYBACK VIDEO SEQUENCE FROM THE CLIENT UI TO A MOBILE OPERATOR.

27.09 IT SHALL BE POSSIBLE TO VIEW MOBILE OPERATORS WHO ENABLED LOCATION TRACKING ON A MAP IN THE SYSTEM. THE LOCATION OF THE MOBILE OPERATOR SHOULD BE UPDATED IN REAL TIME.

HEALTH MONITOR

28.01 THE USP SHALL MONITOR THE HEALTH OF THE SYSTEM, LOG HEALTH-RELATED EVENTS, AND CALCULATE STATISTICS.

28.02 USP SERVICES, ROLES, AGENTS, UNITS, AND CLIENT APPS WILL TRIGGER HEALTH EVENTS.

28.03 THE USP SHALL POPULATE THE WINDOWS EVENT LOG WITH HEALTH EVENTS RELATED TO USP ROLES, SERVICES, AND CLIENT APPS.

28.04 A DEDICATED ROLE, THE HEALTH MONITORING ROLE, SHALL PERFORM THE FOLLOWING ACTIONS:

A. Monitor the health of the entire system and log events.

B. Calculate statistics within a specified time frame (hours, days, months).

C. Calculates availability for clients, servers and video/access/ALPR units.

28.05 A HEALTH MONITORING TASK AND HEALTH HISTORY REPORTING TASK SHALL BE AVAILABLE FOR LIVE AND HISTORICAL REPORTING.

28.06 A HEALTH MONITORING DASHBOARD TASK SHALL BE AVAILABLE IN THE CLIENT APPLICATION USER INTERFACE TO PROVIDE A LIVE DISPLAY, SUCH AS PIE CHARTS AND EVENT LISTS, FOR QUICK VISUAL ASSESSMENT ON THE GENERAL HEALTH OF THE SYSTEM.

28.07 A WEB-BASED, CENTRALIZED HEALTH DASHBOARD SHALL BE AVAILABLE TO REMOTELY VIEW UNIT AND ROLE HEALTH EVENTS OF THE USP.

28.08 DETAILED SYSTEM CARE STATISTICS WILL BE AVAILABLE THROUGH A WEB-BASED DASHBOARD PROVIDING HEALTH METRICS OF USP ENTITIES AND ROLES, INCLUDING UPTIME AND MEAN-TIME-BETWEEN-FAILURES.

28.09 ALL HEALTH EVENTS RAISED IN THE SYSTEM CAN BE USED FOR AUTOMATING THE USP EVENT/ACTION MANAGEMENT.

28.10 HEALTH EVENTS SHALL BE ACCESSIBLE VIA THE SDK (CAN BE USED TO CREATE SNMP TRAPS).

28.11 THE HARDWARE INVENTORY REPORT SHALL DISPLAY LEVELS OF ENCRYPTION, PASSWORD STRENGTH, AND RECOMMENDED FIRMWARE VERSION.

USP GENERAL REQUIREMENTS

29.01 THE UNIFIED SECURITY PLATFORM (USP) SHALL BE AN ENTERPRISE CLASS IP-ENABLED SECURITY AND SAFETY SOFTWARE SOLUTION.

29.02 THE USP SHALL SUPPORT THE SEAMLESS UNIFICATION OF IP ACCESS CONTROL SYSTEM (ACS), IP VIDEO MANAGEMENT SYSTEM (VMS), AND IP AUTOMATIC LICENSE PLATE RECOGNITION SYSTEM (ALPR) UNDER A SINGLE PLATFORM. THE USP USER INTERFACE (UI) APPLICATIONS SHALL PRESENT A UNIFIED SECURITY INTERFACE FOR THE MANAGEMENT, CONFIGURATION, MONITORING, AND REPORTING OF EMBEDDED ACS, VMS AND ALPR SYSTEMS, AND ASSOCIATED EDGE DEVICES.

29.03 FUNCTIONALITIES AVAILABLE WITH THE USP SHALL INCLUDE:

A. Configuration of embedded systems, such as ACS, ALPR, and VMS systems.

B. Live event monitoring.

C. Live video monitoring and playback of archived video.

D. Alarm management.

E. Reporting, including creating custom report templates and incident reports.

F. The Federation™ feature for global monitoring, reporting, and alarm management of multiple remote and independent ACS, VMS, and or ALPR systems spread across multiple facilities and geographic areas. (Additional license required)

G. Microsoft Active Directory integration for synchronizing USP user accounts and ACS cardholder accounts. (First integration included, addition licenses required for more)

H. SIP Intercom device integration for bi-directional communication.

I. Integration with third party video analytics systems and databases via plug-ins require additional licenses.

J. Dynamic graphical map viewing.

29.04 THE USP SHALL BE DEPLOYED IN ONE OR MORE OF THE FOLLOWING TYPES OF INSTALLATIONS:

A. Unified access, ALPR, video platform, and any combination thereof.

B. Standalone access control, video, or ALPR platform.

C. Unified access and video platform that federates multiple remote ACS, VMS, and ALPR.

D. Standalone access control that federates multiple independent remote ACS.

29.05 LICENSING:

A. A single central license shall be applied centrally on the configuration server.

B. There shall be no requirement to apply a license at every server computer or client workstation.

C. Based on selected options, one or more embedded systems shall be enabled or disabled.

29.06 HARDWARE AND SOFTWARE REQUIREMENTS:

A. The USP and embedded systems (video, license plate recognition, and access control) shall be designed to run on a standard PC-based platform loaded with a Windows operating system. The preferred operating system shall be coordinated with the Owner following the manufacturer supported operating systems.

B. The core client/server software shall be built in its entirety using the Microsoft .NET software framework and the C# (C-Sharp) programming language.

C. The USP database server(s) shall be built on Microsoft's SQL Server. The preferred SQL version shall be coordinated with the Owner and compatible with the USP.

D. The USP shall be compatible with virtual environments, including VMware and Microsoft Hyper-V.

E. The USP shall use the latest user interface (UI) development and programming technologies such as Microsoft WPF (Windows Presentation Foundation), the XAML markup language, and .NET software framework.

USP ARCHITECTURE

30.01 THE USP SHALL BE BASED ON A CLIENT/SERVER MODEL. THE USP SHALL CONSIST OF A STANDARD SERVER SOFTWARE MODULE (SSM) AND CLIENT SOFTWARE APPLICATIONS (CSA).

30.02 THE USP SHALL BE AN IP ENABLED SOLUTION. ALL COMMUNICATION BETWEEN THE SSM AND CSA SHALL BE BASED ON STANDARD TCP/IP PROTOCOL AND SHALL USE TLS ENCRYPTION WITH DIGITAL CERTIFICATES TO SECURE THE COMMUNICATION CHANNEL.

30.03 THE SSM SHALL BE A WINDOWS SERVICE THAT CAN BE CONFIGURED TO START WHEN THE OPERATING SYSTEM IS BOOTED AND RUN IN THE BACKGROUND. THE SSM SHALL AUTOMATICALLY LAUNCH AT COMPUTER STARTUP, REGARDLESS OF WHETHER OR NOT A USER IS LOGGED ON THE MACHINE.

30.04 USERS SHALL BE ABLE TO DEPLOY THE SSM ON A SINGLE SERVER OR ACROSS SEVERAL SERVERS FOR A DISTRIBUTED ARCHITECTURE. THE USP SHALL NOT BE RESTRICTED IN THE NUMBER OF SSM DEPLOYED.

30.05 THE USP SHALL SUPPORT THE CONCEPT OF THE FEDERATION FEATURE WHEREBY MULTIPLE INDEPENDENT ACS, VMS, AND ALPR INSTALLATIONS CAN BE MERGED INTO A SINGLE LARGE VIRTUAL SYSTEM FOR CENTRALIZED MONITORING, REPORTING, AND ALARM MANAGEMENT. (ADDITIONAL LICENSE REQUIRED)

30.06 THE USP SHALL PROTECT AGAINST POTENTIAL DATABASE SERVER FAILURE AND CONTINUE TO RUN THROUGH STANDARD OFF-THE-SHELF SOLUTIONS.

30.07 THE USP SHALL SUPPORT UP TO ONE THOUSAND INSTANCES OF CSA CONNECTED AT THE SAME TIME. HOWEVER, AN UNRESTRICTED NUMBER OF CSA CAN BE INSTALLED AT ANY TIME. (UNRESTRICTED WITH ENTERPRISE)

30.08 THE USP SHALL SUPPORT AN UNRESTRICTED NUMBER OF LOGS AND HISTORICAL TRANSACTIONS (EVENTS AND ALARMS) WITH THE MAXIMUM ALLOWED BEING LIMITED BY THE AMOUNT OF HARD DISK SPACE AVAILABLE.

30.09 ROLES-BASED ARCHITECTURE:

A. The USP shall consist of a role-based architecture, with each SSM hosting one or more roles.

B. Each role shall execute a specific set of tasks related to either core system, automatic license plate recognition (ALPR), video (VMS), or access control (ACS) functionalities, among many others. Installation shall be streamlined through the ability of the USP to allow administrators to:
   1. Deploy one or several SSM across the network prior to activating roles.
   2. Activate and deactivate roles as needed on each and every SSM.
   3. Centralize role configuration and management.
   4. Support remote configuration.
   5. Move roles over from one SSM to another.

C. Each role, where needed, shall have its own database to store events and role-specific configuration information.

D. Roles without databases, such as The Federation feature, Active Directory, and Global Cardholder Management, shall support near real-time standby without any third-party failover software being required.

E. Directory Role:
   1. The Directory Role shall manage the central database that contains all the system information and component configuration of the USP.
   2. The Directory Role shall authenticate users and give access to the USP based on predefined user access rights or privileges, and security partition settings.
   3. The Directory Role shall support the configuration/management of the following components common to the ACS, ALPR, and VMS sub-systems:
      a. Security Partitions, users, and user groups
      b. Areas
      c. Zones, input/output (IO) linking rules, and custom output behavior
      d. Alarms. Schedules, and scheduled tasks
      e. Custom events
      f. Macros or custom scripts
   4. The Directory Role shall support the configuration/management of the following components specific to VMS:
      a. Video servers and their peripherals (for example audio, IOs, and serial ports)
      b. PTZ
      c. Camera sequences
      d. Recording and archiving schedules
   5. The Directory Role shall support the configuration/management of the following components specific to ACS:
      a. Door controllers, and input and output (IO) modules
      b. Doors, Elevators, and Access rules
      c. Cardholders and cardholder groups, credentials, and badge templates
   6. The Directory Role shall support the configuration/management of the following components specific to ALPR:
      a. ALPR units and cameras
      b. Hotlists, permit lists, and overtime rules

F. The Video Archiver Role shall be responsible for managing cameras and encoders under its control and archiving.

G. The Media Router Role shall be responsible for routing video and audio streams across local and wide area networks from the source (for example DVS) to the destination (for example CSA).

H. The Access Manager Role shall be responsible for synchronizing access control hardware units under its control, such as door controllers and I/O modules. This role shall also be responsible for validating and logging all access activities and events when the door controllers and I/O modules are online.

I. The Automatic License Plate Recognition (ALPR) Role shall be responsible for synchronizing fixed ALPR units (cameras) and mobile ALPR applications under its control. The ALPR Role shall also be responsible for logging all ALPR activities and events.

J. The Zone Manager Role shall be responsible for managing all software zones (collection of inputs) and logging associated zone events. Zones shall consist of inputs from both access control and video devices.

K. The Health Monitoring Role shall be responsible for monitoring and logging health events and warnings from the various client applications, roles, and services that are part of the USP. This role shall also be responsible for logging events within the Windows Event Log and for generating reports on health statistics and health history.

L. The Data Ingestion Role shall be responsible for ingesting data from external sources in order to enhance the system reporting and dashboarding capabilities.

M. Optional Roles
   1. The Federation Role shall be responsible for creating a large virtual system consisting of hundreds or thousands of independent and remote ACS, VMS, and/or ALPR systems. (Additional license required)
   2. The Active Directory Role shall be responsible for synchronizing user accounts and cardholder accounts with a Microsoft Active Directory server. (Additional license required)
   3. The Plug-in Manager Role shall be responsible for the communication between the USP and third-party systems such as video analytics, access control, video, ALPR, and building management systems. (Additional license required)
   4. The Web SDK Role shall be responsible for connecting the USP to any application or interface developed with the Web Service SDK. Applications developed with the Web Service SDK shall be platform independent and rely on the REST protocol for communications. (Additional license required)
   5. The Communication Management Role shall be responsible for registering the SIP communication endpoints and for managing the call routing.

30.10 SERVER MONITORING SERVICE (WATCHDOG):

A. The USP shall include a Server Monitoring Service that continuously monitors the state of the Server Software Module (SSM) service.

B. The Server Monitoring Service shall be a Windows service that automatically launches at system startup, regardless of whether or not a user is logged into his account.

C. The Server Monitoring Service shall be installed on all PCs/servers running an SSM. In the event of a malfunction or failure, the Server Monitoring Service shall restart the failed service. As a last resort, the Server Monitoring Service shall reboot the PC/server should it be unable to restart the service.

USP ACCESS CONTROL, VIDEO, AND ALPR UNIFICATION

31.01 THE MONITORING UI SHALL PRESENT A TRUE UNIFIED SECURITY INTERFACE FOR LIVE MONITORING AND REPORTING OF THE ACS, VMS, AND ALPR. ADVANCED LIVE VIDEO VIEWING AND PLAYBACK OF ARCHIVED VIDEO SHALL BE AVAILABLE THROUGH THE MONITORING UI.

31.02 THE CONFIGURATION UI SHALL PRESENT A TRUE UNIFIED SECURITY INTERFACE FOR THE CONFIGURATION AND MANAGEMENT OF THE ACS, VMS, AND ALPR.

31.03 THE USER SHALL BE ABLE TO ASSOCIATE ONE OR MORE VIDEO CAMERAS TO THE FOLLOWING ENTITY TYPES: AREAS, DOORS, ELEVATORS, ZONES, ALARMS, INTRUSION PANELS, ALPR CAMERAS, AND MORE.

31.04 IT SHALL BE POSSIBLE TO VIEW VIDEO ASSOCIATED TO ACCESS CONTROL EVENTS WHEN VIEWING A REPORT.

31.05 IT SHALL BE POSSIBLE TO VIEW VIDEO ASSOCIATED TO INTRUSION PANEL EVENTS WHEN VIEWING A REPORT.

31.06 IT SHALL BE POSSIBLE TO VIEW VIDEO ASSOCIATED TO ALPR EVENTS WHEN VIEWING A REPORT.

USP ALARM MANAGEMENT

32.01 THE USP SHALL SUPPORT THE FOLLOWING ALARM MANAGEMENT FUNCTIONALITY:

A. Create and modify user-defined alarms. An unrestricted number of user-defined alarms shall be supported.

B. Assign a time schedule or a coverage period to an alarm. An alarm shall be triggered only if it is a valid alarm for the current time period.

C. Set the priority level of an alarm and its reactivation threshold.

D. Define whether to display live or recorded video, still frames or a mix once the alarm is triggered.

E. Provide the ability to display live and recorded video within the same video tile using picture-in-picture (PiP) mode.

F. Provide the ability to group alarms by source and by type.

G. Define the time period after which the alarm is automatically acknowledged.

H. Define the recipients of an alarm. Alarm notifications shall be routed to one or more recipients. Recipients shall be assigned a priority level that prioritizes the order of reception of an alarm.

I. Define the alarm broadcast mode. Alarm notifications shall be sent using either a sequential or an all-at-once broadcast mode.

J. Define whether to display the source of the alarm, one or more entities, or an HTML page.

K. Specify whether an incident report is mandatory during acknowledgment.

32.02 THE WORKFLOWS TO CREATE, MODIFY, ADD INSTRUCTIONS AND PROCEDURES, AND ACKNOWLEDGE AN ALARM SHALL BE CONSISTENT FOR ACCESS CONTROL, ALPR, AND VIDEO ALARMS.

32.03 ALARMS SHALL BE FEDERATED, ALLOWING GLOBAL ALARM MANAGEMENT ACROSS MULTIPLE INDEPENDENT USP, ACS, AND VMS SYSTEMS.

32.04 THE USP SHALL ALSO SUPPORT ALARM NOTIFICATION TO AN EMAIL ADDRESS OR ANY DEVICE USING THE SMTP PROTOCOL.

32.05 THE ABILITY TO CREATE ALARM-RELATED INSTRUCTIONS SHALL BE SUPPORTED THROUGH THE DISPLAY OF ONE OR MORE HTML PAGES FOLLOWING AN ALARM EVENT. THE HTML PAGES SHALL BE USER-DEFINED AND CAN BE INTERLINKED.

32.06 ALARM UNPACKING AND PACKING SHALL BE SUPPORTED WHERE ALL THE ENTITIES ASSOCIATED TO AN ALARM CAN BE DISPLAY IN THE MONITORING UI WITH THE SINGLE CLICK OF A BUTTON.

32.07 THE USER SHALL HAVE THE ABILITY TO ACKNOWLEDGE ALARMS, CREATE AN INCIDENT UPON ALARM ACKNOWLEDGEMENT, AND PUT AN ALARM TO SNOOZE.

32.08 THE USER SHALL BE ABLE TO SPONTANEOUSLY TRIGGER ALARMS BASED ON SOMETHING HE OR SHE SEES IN THE SYSTEM.

32.09 AN ALARM SHALL BE CONFIGURED IN SUCH A WAY THAT IT REMAINS VISIBLE UNTIL THE SOURCE CONDITION HAS BEEN ACKNOWLEDGED.

32.10 THE USER SHALL BE ABLE TO INVESTIGATE AN ALARM WITHOUT ACKNOWLEDGING IT.

USP THREAT LEVELS

33.01 THE USP SHALL SUPPORT THREAT LEVELS TO DYNAMICALLY CHANGE THE SYSTEM BEHAVIOR TO RESPOND TO CRITICAL EVENTS.

33.02 THREAT LEVELS SHALL BE ACTIVATED AND DEACTIVATED BY THE CSA OPERATOR WITH THE RIGHT PRIVILEGE.

33.03 THREAT LEVELS SHALL BE SET ON AN AREA OR ON THE ENTIRE SYSTEM.

33.04 THREAT LEVELS SHALL AFFECT THE SYSTEM BEHAVIOR BY EXECUTING ANY ACTION AVAILABLE IN THE USP SUCH AS: TRIGGER OUTPUT, START RECORDING, BLOCK CAMERA, OVERRIDE RECORDING QUALITY, ARM ZONE, SET A DOOR IN MAINTENANCE MODE, AND MORE.

33.05 THE FOLLOWING SPECIFIC ACTIONS SHALL BE AVAILABLE WITH THREAT LEVEL:

A. Set minimum security clearance to restrict or permit access to cardholders on specific areas on top of the restrictions imposed by the access rules.

B. Set minimum user level to automatically log out user from the USP.

C. Set reader mode to change how the doors are accessed (for example card and PIN, or card or PIN).

33.06 A VISIBLE NOTIFICATION SHALL BE DISPLAYED IN ALL OPERATOR CSA WHEN A THREAT LEVEL IS ACTIVATED.

USP ADVANCED TASK MANAGEMENT

34.01 USP SHALL SUPPORT AN INFRASTRUCTURE FOR MANAGING MONITORING UI TASKS USED FOR LIVE MONITORING, DAY-TO-DAY ACTIVITIES, AND REPORTING.

34.02 ADMINISTRATORS SHALL BE ABLE TO ASSIGN TASKS AND LOCK THE OPERATOR'S WORKSPACE. THE USER MANAGEMENT OF THEIR WORKSPACE SHALL BE LIMITED BY THEIR ASSIGNED PRIVILEGES.

34.03 OPERATORS SHALL BE ABLE SAVE THEIR TASKS AS EITHER PUBLIC TASKS OR PRIVATE TASKS AND IN A SPECIFIC PARTITION. PUBLIC TASKS SHALL BE AVAILABLE TO ALL USERS. PRIVATE TASKS SHALL ONLY BE AVAILABLE TO THE OWNER OF THE TASK.

34.04 OPERATORS SHALL BE ABLE TO SHARE THEIR TASKS BY SENDING THEM TO ONE OR MORE ONLINE USERS. RECIPIENTS SHALL HAVE THE OPTION TO ACCEPT THE SENT TASK.

34.05 OPERATORS SHALL BE ABLE TO DUPLICATE A TASK.

USP REPORTING

35.01 THE USP SHALL SUPPORT REPORT GENERATION (DATABASE REPORTING) FOR ACCESS CONTROL, ALPR, VIDEO, AND INTRUSION.

35.02 EACH AND EVERY REPORT IN THE SYSTEM SHALL BE A USP TASK, EACH ASSOCIATED WITH ITS OWN PRIVILEGE. A USER SHALL HAVE ACCESS TO A SPECIFIC REPORT TASK IF THEY HAVE THE APPROPRIATE PRIVILEGE.

35.03 THE WORKFLOWS TO CREATE, MODIFY, AND RUN A REPORT SHALL BE CONSISTENT FOR ACCESS CONTROL, ALPR, AND VIDEO REPORTS.

35.04 REPORTS SHALL BE FEDERATED, ALLOWING GLOBAL CONSOLIDATED REPORTING ACROSS MULTIPLE INDEPENDENT USP, ACS, VMS, AND ALPR SYSTEMS.

35.05 ACCESS CONTROL AND ALPR REPORTS SHALL SUPPORT CARDHOLDER PICTURES AND LICENSE PLATE PICTURES, RESPECTIVELY.

35.06 THE USP SHALL SUPPORT THE FOLLOWING TYPES OF REPORTS:

A. Alarm reports

B. Video-specific reports (archive, bookmark, motion, and more)

C. Configuration reports (cardholders, credentials, units, access rules, readers/inputs/outputs, and more)

D. Activity reports (cardholder, cardholder group, visitor, credential, door, unit, area, zone, elevator, and more)

E. ALPR-specific reports (mobile ALPR playback, hits, plate reads, reads/hits per day, reads/hits per ALPR zone, and more)

F. Health activity and health statistics reports

G. Other types of reports, including visitor reports, audit trail reports, incident reports, and time and attendance reports

35.07 GENERIC REPORTS, CUSTOM REPORTS AND REPORT TEMPLATES:

A. The user shall the option of generating generic reports from an existing list, generating reports from a list of user-defined templates, or creating a new report or report template.

B. The user shall be able to customize the predefined reports and save them as new report templates. There shall be no need for an external reporting tool to create custom reports and report templates. Customization options shall include setting filters, report lengths, and timeout period. The user shall also be able to set which columns shall be visible in a report. The sorting

of reported data shall be available by clicking on the appropriate column and selecting a sort order (ascending or descending).

C. All report templates shall be created within the Monitoring UI.

D. These templates can be used to generate reports on a schedule in PDF or Excel formats.

E. An unrestricted number of custom reports and templates shall be supported.

35.08 A REPORTING TASK LAYOUT SHALL CONSIST OF PANES WITH SETTINGS (REPORT LENGTH, FILTERS, GO AND RESET COMMANDS, ETC.), THE ACTUAL REPORT DATA IN COLUMN FORMAT, AND A PANE WITH DISPLAY TILES. THE USER SHALL BE ABLE TO DRAG AND DROP INDIVIDUAL RECORDS IN A REPORT ONTO ONE OR MORE DISPLAY TILES TO VIEW A CARDHOLDER'S PICTURE ID, PLAYBACK A VIDEO SEQUENCE, OR AN ALPR EVENT.

35.09 THE USP SHALL SUPPORT COMPREHENSIVE DATA FILTERING FOR MOST REPORTS BASED ON ENTITY TYPE, EVENT TYPE, EVENT TIMESTAMP, CUSTOM FIELDS, AND MORE.

35.10 THE REPORTING TASK SHALL HAVE THE ABILITY TO DISPLAY RESULTS THROUGH GRAPHICS SUCH AS LINE CHARTS, BAR CHARTS, STACKED BAR CHARTS, DOUGHNUT CHARTS, AND PIE CHARTS.

35.11 THE USER SHALL BE ABLE TO CLICK ON AN ENTITY WITHIN AN EXISTING REPORT TO GENERATE ADDITIONAL REPORTS FROM THE MONITORING UI.

35.12 THE USP SHALL SUPPORT THE FOLLOWING ACTIONS ON A REPORT: PRINT REPORT, EXPORT REPORT TO A PDF/MICROSOFT EXCEL/CSV FILE, EXPORT THE GRAPHICS CHART IN JPG/PNG, AND AUTOMATICALLY EMAIL A REPORT BASED ON A SCHEDULE AND A LIST OF ONE OR MORE RECIPIENTS, INCLUDING USERS WITH ACCOUNTS OUTSIDE THE UPS.

USP DASHBOARDS

36.01 THE USP SHALL SUPPORT THE ABILITY TO CREATE DASHBOARDS.

36.02 OPERATORS SHALL BE ALLOWED TO VIEW DASHBOARDS IF THEY ARE GRANTED THE APPROPRIATE PRIVILEGE. MODIFICATION TO THE DASHBOARDS SHOULD ALSO BE ALLOWED TO USERS GRANTED THE APPROPRIATE PRIVILEGE.

36.03 DASHBOARDS IN THE SYSTEM SHALL BE A USP TASK. A USER SHALL HAVE ACCESS TO A SPECIFIC DASHBOARD TASK IF THEY HAVE THE APPROPRIATE PRIVILEGE.

36.04 DASHBOARDS SHALL BE SAVED EITHER IN A PRIVATE FOLDER OR A PUBLIC FOLDER.

36.05 A DASHBOARD SHALL CONSIST OF A CANVAS WITH VARIOUS WIDGETS DISPLAYED ON THE CANVAS. ALL WIDGETS SHOULD OFFER THE ABILITY TO SPECIFY LOCATION AND SIZE TO THE WIDGET, A TITLE TO THE WIDGET, A BACKGROUND COLOR TO THE WIDGET, AND THE ABILITY TO REFRESH PERIODICALLY THE CONTENT OF THE WIDGET.

36.06 DASHBOARD WIDGET TYPES SHALL BE:

A. Image: provides the ability to display an image (JPG, PNG, GIF, BMP) on a dashboard.

B. Text: provides the ability to display a text on a dashboard. The text style shall be configurable, so font, size, color, and alignment can be specified by the user.

C. Tile: provides the ability to display any entity of the USP inside of a tile.

D. Web page: provides the ability to display a URL on a dashboard.

E. Entity Count: provides the ability to display the total number of a specific entity type in the USP.

F. Reports: provides the ability to display the results of any saved reports in the system. The results shall be displayed either by showing the total number of results in the report, a set of top results from the report, or a visual graph from the data returned by the report.

36.07 IT SHALL BE POSSIBLE TO EXTEND THE WIDGETS OF A DASHBOARD USING THE SDK. THIS WILL PROVIDE THE ABILITY TO DEVELOP CUSTOM WIDGETS TO THE SYSTEM.

36.08 THE USP SHALL SUPPORT THE FOLLOWING ACTIONS ON A DASHBOARD: PRINT DASHBOARD, EXPORT DASHBOARD TO PNG FILE, AND AUTOMATICALLY EMAIL A REPORT BASED ON A SCHEDULE AND A LIST OF ONE OR MORE RECIPIENTS.

USP FEDERATION FEATURE: MONITORING OF REMOTE SYSTEMS (ADDITIONAL LICENSE REQUIRED FOR EACH FEDERATED SITES AND ENTITIES)

37.01 THE USP SHALL SUPPORT THE CONCEPT OF A FEDERATION FEATURE FOR ACCESS CONTROL, VIDEO, AND ALPR.

37.02 THE FEDERATION FEATURE SHALL ALLOW MULTIPLE INDEPENDENT USP SYSTEMS (FEDERATED SYSTEMS) TO BE UNIFIED INTO A LARGER VIRTUAL SYSTEM (THE FEDERATION FEATURE). THIS SHALL FACILITATE THE GLOBAL MONITORING OF MULTIPLE INDEPENDENT USP SYSTEMS.

37.03 THE FEDERATION FEATURE SHALL SUPPORT THE UNIFICATION OF MULTIPLE INDEPENDENT VIDEO SURVEILLANCE SYSTEMS OR VMS.

37.04 THE FEDERATION FEATURE SHALL SUPPORT THE UNIFICATION OF MULTIPLE INDEPENDENT ACCESS CONTROL SYSTEMS OR ACS.

37.05 THE FEDERATION FEATURE SHALL SUPPORT THE UNIFICATION OF MULTIPLE INDEPENDENT LICENSE PLATE RECOGNITION SYSTEMS OR ALPR.

37.06 ENTITIES THAT SHALL FEDERATED AND MONITORED CENTRALLY FROM THE FEDERATION FEATURE SHALL INCLUDE ALARMS, AREAS, CAMERAS, CARDHOLDERS AND CARDHOLDER GROUPS, CREDENTIALS, DOORS, ELEVATORS, ALPR EVENTS, AND ZONES (MONITORED INPUTS).

37.07 THE FEDERATION FEATURE SHALL SUPPORT A CLOUD-BASED DEPLOYMENT, WHEREBY THE SERVICE AND INFRASTRUCTURE WILL BE UPDATED AUTOMATICALLY AND PROVISIONED BY THE SERVICE PROVIDER, WITHOUT NEED FOR ON-SITE HARDWARE.

37.08 THE FEDERATION FEATURE SHALL SUPPORT GLOBAL ALARM MANAGEMENT FROM THE MONITORING UI FOR ACCESS CONTROL, VIDEO, AND ALPR.

37.09 THE FEDERATION FEATURE SHALL SUPPORT GLOBAL REPORT GENERATION FROM THE MONITORING UI FOR ACCESS CONTROL, VIDEO, AND ALPR.

37.10 THE FEDERATION FEATURE SHALL SUPPORT DOZENS OF OPERATOR ACTIONS ON REMOTE (FEDERATED) ENTITIES FROM THE MONITORING UI (FOR EXAMPLE GENERATING A GLOBAL REPORT TAKING INTO ACCOUNT EVENTS FROM MULTIPLE INDEPENDENT SITES OR ACKNOWLEDGING REMOTE ALARMS).

USP ZONE MANAGEMENT

38.01 THE USP SHALL SUPPORT THE CONFIGURATION AND MANAGEMENT OF ZONES FOR INPUT POINT MONITORING VIA THE ZONE MANAGER ROLE. A USER SHALL BE ABLE TO ADD, DELETE, OR MODIFY A ZONE IF THEY HAVE THE APPROPRIATE PRIVILEGES.

38.02 A ZONE SHALL MONITOR THE STATUS OF ONE OR MORE INPUTS POINTS. ZONE MONITORING OR INPUT POINT MONITORING SHALL BE POSSIBLE THROUGH THE USE OF A CONTROLLER AND ONE OR MORE INPUT MODULES. INPUTS FROM VIDEO CAMERAS OR VIDEO ENCODERS SHALL ALSO BE ACCESSIBLE VIA A ZONE.

38.03 DEPENDING ON THE HARDWARE INSTALLED, SUPERVISED INPUTS SHALL BE SUPPORTED. DEPENDING ON THE INPUT MODULE USED, BOTH 3-STATE AND 4-STATE SUPERVISION SHALL BE AVAILABLE.

38.04 A SCHEDULE SHALL BE DEFINED FOR A ZONE, INDICATING WHEN THE ZONE WILL BE MONITORED.

38.05 CUSTOM EVENTS SHALL PROVIDE FULL FLEXIBILITY IN CREATING CUSTOM EVENTS TAILORED TO A ZONE. USERS SHALL BE ABLE TO ASSOCIATE CUSTOM EVENTS TO STATE CHANGES IN MONITORED INPUTS.

38.06 THE ACS SHALL SUPPORT ONE OR MORE CAMERAS PER ZONE. VIDEO SHALL THEN BE ASSOCIATED TO ZONE STATE CHANGES.

38.07 INPUT/OUTPUT (IO) LINKING

A. Zone management shall support Input/Output (IO) Linking. I/O Linking shall allow one or more inputs to trigger one or more outputs.

B. I/O Linking shall be available in offline mode when communication between the server and hardware is not available.

C. Custom Output Behaviors shall provide full flexibility in creating a variety of complex output signal patterns: simple pulses, periodic pulses, variable duty-cycle pulses, and state changes.

D. Through the “trigger an output” action, the ACS shall support the triggering of outputs with custom output behaviors.

USP USER AND USER GROUP SECURITY, PARTITIONS, AND PRIVILEGES MANAGEMENT

39.01 THE USP SHALL SUPPORT THE CONFIGURATION AND MANAGEMENT OF USERS AND USER GROUPS. A USER SHALL BE ABLE TO ADD, DELETE, OR MODIFY A USER OR USER GROUP IF THEY HAVE THE APPROPRIATE PRIVILEGES.

39.02 THE USP SHALL SUPPORT USER AUTHENTICATION WITH CLAIMS-BASED AUTHENTICATION USING EXTERNAL PROVIDERS. EXTERNAL PROVIDERS SHALL INCLUDE:

A. ADFS (Active Directory Federation Services)

B. Azure Active Directory (through OpenID Connect)

C. Ping Identity (through OpenID Connect)

D. KeyCloak (through OpenID Connect)

E. Other Open ID Connect / SAML2 authentication agents

39.03 COMMON ACCESS RIGHTS AND PRIVILEGES SHARED BY MULTIPLE USERS SHALL BE DEFINED AS USER GROUPS. INDIVIDUAL GROUP MEMBERS SHALL INHERIT THE RIGHTS AND PRIVILEGES FROM THEIR PARENT USER GROUPS. USER GROUP NESTING SHALL BE ALLOWED.

39.04 USER PRIVILEGES SHALL BE EXTENSIVE IN THE USP. ALL CONFIGURABLE ENTITIES FOR THE USP, INCLUDING ACCESS CONTROL, VIDEO, AND ALPR SHALL HAVE ASSOCIATED PRIVILEGES.

39.05 SPECIFIC ENTITIES, SUCH AS CARDHOLDERS, CARDHOLDER GROUPS, AND CREDENTIALS SHALL INCLUDE A MORE GRANULAR SET OF PRIVILEGES, SUCH AS THE RIGHT TO ACCESS CUSTOM FIELDS AND CHANGE THE ACTIVATION OR PROFILE STATUS OF AN ENTITY.

39.06 PARTITIONS:

A. The USP shall limit what users can view in the configuration database via security partitions (database segments). The administrator, who has all rights and privileges, shall be allowed to segment a system into multiple security partitions.

B. All entities that are part of the USP can be assigned to one or more partitions.

C. A user who is given access to a specific partition shall only be able to view entities (components) within the partition to which they have been assigned. Access is given by assigning the user as an accepted user to view the entities that are members of a particular partition.

D. A user or user group can be assigned administrator rights over the partition.

39.07 IT SHALL BE POSSIBLE TO SPECIFY USER AND USER GROUP PRIVILEGES ON A PER PARTITION BASIS.

39.08 ADVANCED LOGON OPTIONS SHALL BE AVAILABLE SUCH AS DUAL LOGON AND MORE.

39.09 IT SHALL BE POSSIBLE TO SPECIFY AN INACTIVE PERIOD FOR THE MONITORING UI AFTER WHICH TIME THE APPLICATION SHALL AUTOMATICALLY LOCK, WHILE STILL PRESERVING ACCESS TO CURRENTLY DISPLAYED CAMERA FEEDS.

39.10 IT SHALL BE POSSIBLE TO REVIEW USED PERMISSIONS AND DETERMINE:

A. For any entity in the system, which user group or user can view or modify it.

B. For any user group or user in the system, what are its privileges.

C. For any privilege in the system, which used group or used is allowed to perform the underlying action.

USP EVENT/ACTION MANAGEMENT

40.01 THE USP SHALL SUPPORT THE CONFIGURATION AND MANAGEMENT OF EVENTS FOR VIDEO AND ALPR. A USER SHALL BE ABLE TO ADD, DELETE, OR MODIFY AN ACTION TIED TO AN EVENT IF HE HAS THE APPROPRIATE PRIVILEGES.

40.02 THE USP SHALL RECEIVE ALL INCOMING EVENTS FROM ONE OR MORE ACS, VMS, AND/OR ALPR. THE USP SHALL TAKE THE APPROPRIATE ACTIONS BASED ON USER-DEFINE EVENT/ACTION RELATIONSHIPS.

40.03 THE USP SHALL RECEIVE AND LOG THE FOLLOWING EVENTS:

A. System-wide events

B. Application events (clients and servers)

C. Area, camera, door, elevator, and ALPR events (reads and hits)

D. Cardholder and credential events

E. Unit events

F. Zone events

G. Alarm events

H. ALPR events

I. First Person In and Last Person Out events and antipassback events

J. Intrusion events

K. Asset management events

L. Health monitoring events.

40.04 THE USP SHALL ALLOW THE CREATION OF CUSTOM EVENTS.

40.05 THE USP SHALL HAVE THE CAPABILITY TO EXECUTE AN ACTION IN RESPONSE TO AN ACCESS CONTROL, VIDEO, AND ALPR EVENT.

40.06 THE USP SHALL ALLOW A SCHEDULE TO BE ASSOCIATED WITH AN ACTION. THE ACTION SHALL BE EXECUTED ONLY IF IT IS AN APPROPRIATE ACTION FOR THE CURRENT TIME PERIOD.

USP SCHEDULES AND SCHEDULED TASKS

41.01 SCHEDULES

A. The USP shall support the configuration and management of complex schedules. A user shall be able to add, delete, or modify a schedule if they have the appropriate privileges.

B. The USP shall provide full flexibility and granularity in creating a schedule. The user shall be able to define a schedule in 1-minute or 15-minute increments.

C. Daily, weekly, ordinal, and specific schedules shall be supported.

41.02 SCHEDULED TASKS

A. The USP shall support scheduled tasks for access control, video, and ALPR.

B. Scheduled tasks shall be executed on a user-defined schedule at a specific day and time. Recurring or periodic scheduled tasks shall also be supported.

C. Scheduled tasks shall support all standard actions available within the USP, such as sending an email, emailing a report or triggering incidents.

USP MACROS AND CUSTOM SCRIPTS

42.01 THE USP SHALL ENABLE USERS TO AUTOMATE AND EXTEND THE FUNCTIONALITIES OF THE SYSTEM THROUGH THE USE OF MACROS OR CUSTOM SCRIPTS FOR ACCESS CONTROL, VIDEO, AND ALPR.

42.02 CUSTOM MACROS SHALL BE CREATED WITH THE USP SOFTWARE DEVELOPMENT KIT (SDK).

42.03 A MACRO SHALL BE EXECUTED EITHER AUTOMATICALLY OR MANUALLY.

42.04 IN THE MONITORING UI, A MACRO SHALL BE LAUNCHED THROUGH HOT ACTIONS.

USP DYNAMIC GRAPHICAL MAPS (DGM)

43.01 THE USP SHALL SUPPORT MAPPING FUNCTIONALITY FOR ACCESS CONTROL, VIDEO SURVEILLANCE, INTRUSION DETECTION, ALPR, AND EXTERNAL APPLICATIONS.

43.02 THE USP SHALL PROVIDE A MAP CENTRIC INTERFACE WITH THE ABILITY TO COMMAND AND CONTROL ALL THE USP CAPABILITIES FROM A FULL SCREEN MAP INTERFACE.

43.03 IT SHALL BE POSSIBLE TO SPAN THE MAP OVER ALL SCREENS OF THE USP CLIENT STATION. IN THE SCENARIO WHERE THE MAP IS SPANNED OVER ALL THE SCREENS OF THE USP CLIENT STATION IT SHALL BE POSSIBLE TO NAVIGATE THE MAP INCLUDING PAN AND ZOOM, AND THE MAP'S MOVES SHALL BE SYNCHRONIZED BETWEEN ALL SCREENS. SPANNING THE MAP OVER MULTIPLE SCREENS MUST PROVIDE THE SAME COMMAND AND CONTROL CAPABILITIES THAN IN A SINGLE SCREEN DISPLAY.

43.04 THE DGM SHALL SUPPORT THE FOLLOWING FILE FORMAT AND PROTOCOL FOR IMPORTING MAP BACKGROUND:

A. PDF

B. JPG

C. PNG

D. Web Tile Map Service (WMTS) and Web Map Service (WMS) defined by the Open Geospatial Consortium (OGC)

E. BeNomad

F. AutoCAD (DWG & DXF)

43.05 THE DGM SHALL PROVIDE THE FOLLOWING ONLINE MAP PROVIDERS FOR USE AS MAP BACKGROUND AND PROVIDE THE ABILITY TO MANAGE THEIR SERVICE LICENSE IF THEY REQUIRE ONE:

A. Google Map, aerial, terrain (Licensed)

B. Bing Map, aerial, satellite, hybrid (Licensed)

C. ESRI ArcGIS (Licensed)

D. OpenStreet Map aerial (Licensed)

E. OVI hybrid

43.06 IT SHALL BE POSSIBLE TO CONFIGURE A MIXED SET OF MAPS MADE OF GIS, ONLINE PROVIDERS AND PRIVATE IMPORTED FILES AND LINK THEM TOGETHER.

43.07 THE DGM SHALL PROVIDE THE ABILITY TO DISPLAY ALL NATIVE ENTITIES OF THE USP INCLUDING:

A. Cameras, fix, and PTZ
B. Doors
C. Camera sequences
D. Areas
E. Intrusion areas
F. Intrusion zones
G. License Plate Recognition cameras
H. Digital inputs
I. Digital outputs
J. Intercoms
K. Alarms
L. Macros
M. Police Car Patrollers

43.08 THE DGM SHALL PROVIDE THE ABILITY TO DRAW AND DISPLAY INFORMATION OVER THE MAP IN THE FORM OF:

A. Vectoral shapes: line, rectangles, polygons, ellipse
B. Pictures
C. Text

43.09 THE DGM SHALL PROVIDE THE ABILITY TO DISPLAY ANY TYPE OF THIRD-PARTY ENTITIES INTEGRATED THROUGH AN SDK.

43.10 THE DGM SHALL PROVIDE THE ABILITY TO DISPLAY LAYER OF INFORMATION IN KEYHOLE MARKUP LANGUAGE (KML) FORMAT.

43.11 THE DGM SHALL PROVIDE THE ABILITY TO THE OPERATOR TO MANAGE LAYERS OF ENTITIES DISPLAYED OVER THE MAP, BEING ABLE TO TURN THEM ON AND OFF AND CHANGING THE SUPERPOSITION ORDER.

43.12 THE DGM SHALL PROVIDE THE ABILITY TO IMPORT DATA LAYERS FROM ONE OR MORE ESRI ARCGIS SERVERS.

43.13 THE DGM SHALL PROVIDE THE OPERATORS WITH THE ABILITY TO MANAGE LAYERS THAT ARE IMPORTED FROM ESRI ARCGIS. THE OPERATORS SHALL BE ABLE TO TURN THE LAYERS ON AND OFF, AS WELL AS SORT THE LAYERS.

43.14 THE DGM SHALL OFFER BUILT-IN MAP DATA BACKUP AND RESTORE FOR BOTH MAP BACKGROUNDS AND LAYERS OF ENTITIES.

43.15 THE DGM SHALL PROVIDE THE ABILITY TO IMPORT CONFIGURATIONS FROM AN EXTERNAL FILE SUCH AS:

A. AutoCAD layer for objects
B. CSV, Excel file

43.16 THE DGM SHALL OFFER FAILOVER CAPABILITIES.

43.17 THE DGM SHALL SCALE UP TO SEVERAL THOUSANDS OF ENTITIES ON A SINGLE MAP AND HUNDREDS OF MAPS.

43.18 THE DGM SHALL PROVIDE A MEANS TO UPDATE A MAP BACKGROUND WITHOUT AFFECTING THE MAP OBJECT CONFIGURATION.

43.19 THE DGM SHALL OFFER A USER-FRIENDLY GRAPHICAL MAP DESIGNER TO CONFIGURE THE MAPS.

43.20 THE DGM SHALL PROVIDE USER FRIENDLY AND INTUITIVE NAVIGATION THAT INCLUDES:

A. The ability to create hierarchies of maps to facilitate navigation within and between various sites and buildings.

B. The ability to define favorites for recurrent position recall.

C. The possibility to create links between maps. The map links shall allow the link from one map to multiple maps representing the floors of a building. Navigating between floors of a building shall keep the level of the map.

D. A common user experience regarding navigation into the map for both GIS and private maps.

43.21 IT SHALL BE POSSIBLE TO MONITOR THE STATE OF ENTITIES ON THE MAP. IT SHALL BE POSSIBLE TO CUSTOMIZE THE ICONS OF ANY ENTITIES REPRESENTED ON THE MAP.

43.22 THE DGM SHALL OFFER THE ABILITY TO OPTIONALLY SET A GRAPHICAL DISPLAY NOTIFICATION OF THE MOTION DETECTION.

43.23 THE DGM SHALL OFFER A SMART SELECTION TOOL TO ACCESS THE VIDEO. BY CLICKING THE LOCATION THE USER WANTS TO SEE, THE DGM WILL AUTOMATICALLY SELECT THE CAMERAS THAT CAN SEE THIS LOCATION AND MOVE THE PTZ TOWARDS THAT LOCATION. THIS SMART SELECTION TOOL SHALL TAKE OBSTACLES INTO CONSIDERATION AND NOT DISPLAY CAMERAS THAT CANNOT SEE THE LOCATION BECAUSE OF A WALL.

43.24 IT SHALL BE POSSIBLE TO SELECT A LOCATION BY DRAWING A ZONE OF INTEREST ON THE DGM, AND TO DISPLAY ALL THE ENTITIES THAT ARE PART OF THAT ZONE OF INTEREST AT ONCE.

43.25 THE USER SHALL BE ABLE TO SELECT AND DISPLAY THE CONTENT OF MULTIPLE USP ENTITIES ON THE MAP IN POP-UP WINDOWS.

43.26 THE USER SHALL BE ABLE TO MOVE, RESIZE, AND PIN THE USP ENTITY POP-UP WINDOWS TO THE MAP.

43.27 IT SHALL BE POSSIBLE TO ACCESS LIVE AND PLAYBACK VIDEO FROM THE MAP.

43.28 IT SHALL BE POSSIBLE TO MONITOR ALL ENTITY EVENT NOTIFICATIONS FROM THE DGM. USERS SHALL BE ABLE TO TURN NOTIFICATIONS ON AND OFF PER ENTITY.

43.29 THE DGM SHALL OFFER THE ABILITY TO FULLY OPERATE ALARM MONITORING. IT SHALL BE POSSIBLE TO:

A. Center the map on entities related to the alarm.

B. Visualize the Alarm notifications on the map and access the related videos from the map.

C. Trigger and receive alarms.

D. Act on the alarm from the DGM, including acknowledgements, forwarding, and investigation.

E. Visualize that an alarm occurred in an underlying linked map.

43.30 THE DGM SHALL PROVIDE THE FOLLOWING SEARCH CAPABILITIES:

A. Search and center by entity name.

B. From the Display of an entity in the USP, locate the entity on the map and offer the ability to select another one close-by.

C. By street address, city, landmark, point of interest (using geocoder license from Google, ESRI, or other providers).

43.31 ANY UPDATE OF MAP CONTENT BY AN ADMINISTRATOR SHALL BE IMMEDIATELY AND DYNAMICALLY PUSHED TO ALL DGM USERS.

43.32 THE DGM SHALL SUPPORT THE USE OF GIS MAPS OR PRIVATE MAPS OR A COMBINATION OF BOTH FOR MAP BACKGROUND.

43.33 THE DGM SHALL BE COMPATIBLE WITH ANY GIS COMPLIANT MAPS WITH THE OGC AND SUPPORTING WMTS AND WMS. THIS INCLUDES, BUT IS NOT LIMITED TO, ESRI MAPS. THE DGM SHALL ALLOW THE SELECTION OF THE APPROPRIATE GIS LAYERS.

43.34 THE DGM SHALL PROVIDE AN INTUITIVE BUILT-IN MAP DESIGNER FOR ENTITY POSITIONING ON THE MAP USING DRAG AND DROP. ANY CONFIGURATION SHALL BE GRAPHIC.

43.35 IT SHALL BE POSSIBLE TO EDIT AND CONFIGURE MULTIPLE MAP OBJECTS AT ONCE.

43.36 ALL MAP DESIGN MODIFICATIONS SHALL BE LOGGED IN AN AUDIT TRAIL.

43.37 VARIOUS ACTIONS SHALL BE AVAILABLE WITHIN MAPS FOR EXECUTION THROUGH SIMPLE AND INTUITIVE DOUBLE-CLICK, RIGHT-CLICK, OR DRAG-AND-DROP FUNCTIONALITY. EXAMPLES OF ACTIONS AVAILABLE THROUGH MAPS SHALL INCLUDE UNLOCKING A DOOR AND ACKNOWLEDGING AN ALARM.

43.38 THROUGH THE FOLLOWING FUNCTIONALITY, THE DGM SHALL ALLOW THE MANAGEMENT OF USP ALARMS FROM THE MAP:

A. Locate on the map entities related to the alarm.

B. Display entities of the alarm with a specific icon, color, transparency level, and blinking rate.

C. List, select, and locate alarms.

D. Auto center the map on the highest priority alarm.

E. Handle the alarm from the map, including acknowledgement, forwarding, and investigation.

F. All map containers, such as hotspots or map links shall reflect the alarm status of the contained entities.

43.39 IT SHALL BE POSSIBLE TO ADD ADVANCED FUNCTIONALITY TO MAPS OBJECT USING THE SDK. ANY FUNCTIONALITY AVAILABLE THROUGH THE USP SDK SHALL BE AVAILABLE WITHIN MAPS.

43.40 THE DGM SHALL OFFER LASSO TOOLS FOR:

A. Displaying entities at one location through a single action.

B. Triggering an action on all entities at one a location in a single click.

C. Editing multiple entities at one location simultaneously.

43.41 THE DGM SHALL ALLOW THE DISPLAY OF USP ENTITIES SELECTED FROM THE MAP ON A REMOTE MONITOR (VIDEO WALL).

43.42 THE DGM SHALL PROVIDE THE ABILITY TO SEARCH WITHIN THE MAP BY ENTITY NAME.

43.43 THE DGM SHALL ALLOW THE USE OF KML OVERLAY MAP INFORMATION FOR BOTH GIS AND PRIVATE MAPS. MOVABLE OBJECTS SHALL BE SUPPORTED USING KML.

43.44 THE CONTRACTOR SHALL PROVIDE LICENSES FOR EACH ENTITY THAT IS REQUIRED TO BE SHOWN ON THE GRAPHICAL MAPS.

USP AUDIT AND USER ACTIVITY TRAILS (LOGS)

44.01 THE USP SHALL SUPPORT THE GENERATION OF AUDIT TRAILS. AUDIT TRAILS SHALL CONSIST OF LOGS OF OPERATOR/ADMINISTRATOR ADDITIONS, DELETIONS, AND MODIFICATIONS.

44.02 AUDIT TRAILS SHALL BE GENERATED AS REPORTS. THEY SHALL BE ABLE TO TRACK CHANGES MADE WITHIN SPECIFIC TIME PERIODS. QUERYING ON SPECIFIC USERS, CHANGES, AFFECTED ENTITIES, AND TIME PERIODS SHALL ALSO BE POSSIBLE.

44.03 FOR ENTITY CONFIGURATION CHANGES, THE AUDIT TRAIL REPORT SHALL INCLUDE DETAILED INFORMATION OF THE VALUE BEFORE AND AFTER THE CHANGES.

44.04 THE USP SHALL SUPPORT THE GENERATION OF USER ACTIVITY TRAILS. USER ACTIVITY TRAILS SHALL CONSIST OF LOGS OF OPERATOR ACTIVITY ON THE USP SUCH AS LOGIN, CAMERA VIEWED, ALPR EVENT VIEWED, BADGE PRINTING, VIDEO EXPORT, AND MORE.

44.05 THE ACS SHALL SUPPORT THE FOLLOWING ACTIONS ON AN AUDIT AND ACTIVITY TRAIL REPORT: PRINT REPORT AND EXPORT REPORT TO A PDF/ MICROSOFT EXCEL/CSV FILE.

USP INCIDENT REPORTS

45.01 INCIDENT REPORTS SHALL ALLOW THE SECURITY OPERATOR TO CREATE REPORTS ON INCIDENTS THAT OCCURRED DURING A SHIFT. BOTH VIDEO-RELATED AND ACCESS CONTROL-RELATED INCIDENT REPORTS SHALL BE SUPPORTED.

45.02 THE OPERATOR SHALL BE ABLE TO CREATE STANDALONE INCIDENT REPORTS OR INCIDENT REPORTS TIED TO ALARMS.

45.03 THE OPERATOR SHALL BE ABLE TO LINK MULTIPLE VIDEO SEQUENCES TO AN INCIDENT, ACCESS THEM IN AN INCIDENT REPORT, AND CHANGE THE DATE OR TIME OF THE SEQUENCES LATER ON.

45.04 IT SHALL BE POSSIBLE TO CREATE A LIST OF INCIDENT CATEGORIES, TAG A CATEGORY TO AN INCIDENT, AND FILTER THE SEARCH WITH THE CATEGORY AS A PARAMETER.

45.05 INCIDENT REPORTS SHALL ALLOW THE CREATION OF A CUSTOM FORM ON WHICH TO INPUT INFORMATION ON AN INCIDENT.

45.06 INCIDENT REPORTS SHALL ALLOW ENTITIES, EVENTS, AND ALARMS TO BE ADDED TO SUPPORT AT THE REPORT'S CONCLUSIONS.

45.07 INCIDENT REPORTS SHALL ALLOW THE USE OF A CUSTOM LOGO, THE DEFAULT MISSION CONTROL LOGO OR NO LOGO AT ALL.

USP DATA INGESTION

46.01 USP SHALL ALLOW THE POSSIBILITY TO IMPORT EXTERNAL DATA FROM OUTSIDE SOURCES TO ENHANCE UNIFICATION OF DATA SOURCES WITHIN THE USP.

46.02 EACH DATA SOURCE SHALL BE DEFIED BY A SET OF FIELDS AND FIELD TYPES THAT DESCRIBE THE DATA SOURCE. FIELD TYPES SHALL BE:

A. String

B. 32-bit and 64-bit integer

C. Floating point number

D. Boolean

E. Timestamp

F. Binary (in a file or base 64)

46.03 THE VISUALIZATION OF EACH DATA POINT FROM A DATA SOURCE SHALL BE CONFIGURABLE TO DETERMINE WHAT FIELDS FROM THE DATA SHOULD BE DISPLAYED. THE CONFIGURATION OF EACH FIELD SHOULD BE:

A. Which fields are displayed or hidden

B. What order are the fields displayed

C. A label to specify the name of the filed (to have a key:value format)

D. An option to specify how to display the field (text value, image, clipboard value, hyperlink to a web page, hyperlink to an entity in the system, sound file)

46.04 A PRIVILEGE SHOULD BE AVAILABLE FOR EACH DATA SOURCE TO ALLOW OR DENY ACCESS TO SPECIFIC USERS AND USER GROUPS OF THE USP.

46.05 INGESTED DATA SHALL BE AVAILABLE IN THE USP REPORTING SYSTEM.

46.06 INGESTED DATA SHALL BE AVAILABLE TO DISPLAY IN THE USP DASHBOARDS.

USP THIRD PARTY INTEGRATION

47.01 MICROSOFT ACTIVE DIRECTORY INTEGRATION: (FIRST INTEGRATION INCLUDED, ADDITIONAL LICENSES REQUIRED FOR MORE)

A. The USP shall support a direct connection to one or multiple Microsoft Active Directory server via the Active Directory Role(s). Active Directory integration shall enable the synchronization of information from the Active Directory server to the USP.

B. Active Directory integration shall permit the central management of the USP users, user groups, cardholders, and cardholder groups.

C. The USP shall support ADFS for user login.

D. The USP shall be able to connect to and synchronize data from multiple Active Directory servers (up to 10).

E. The USP shall support Azure AD for cardholder synchronization.

F. The USP shall support synchronizing Active Directory Universal Groups as well as security groups belonging to other domains within the same forest.

G. The USP shall support Microsoft Active Directory encryption using LDAP SSL.

H. When enabled, Active Directory shall manage user logon to the USP client applications through the user's Windows credentials. Logging on to the USP shall utilize native Active Directory password management and authentication features.

I. It shall be possible to synchronize the following USP entities and their information from Active Directory with the USP:
   1. Users (username, first and last names, email address, and more)
   2. User groups (user group name, description, and group email address)
   3. Cardholders (first and last names, description, email, picture and more)
   4. Cardholder groups (cardholder group name, description, and group email address)
   5. Active Directory attributes to USP custom fields

J. When enabled, the addition, removal, or suspension of a user's Windows account in Active Directory shall result in the creation, deletion, or disabling of the equivalent user account in the USP.

K. When enabled, the addition, removal, or suspension of a user's Windows account in Active Directory shall result in the creation, deletion, or disabling of the equivalent cardholder account in the USP.

L. Supported synchronization methods for additions, modification, and deletions of synchronized entities shall include on first logon (users only), manual synchronization, and scheduled synchronization.

M. The USP shall support user connections across independent organizations by connecting to an external identity provider using claims-based authentication such as ADFS (Active Directory Federation Services), Azure Active Directory, other OpenID Connect & SAML2 providers.

47.02 ADDITIONAL THIRD-PARTY INTEGRATIONS

A. The USP shall support multiple approaches to integrating third party systems. These shall include: Software Development Kits (SDKs), REST-based Web Service SDKs, RTSP Service SDKs, and more. (SDK package and license required)

B. The USP architecture shall support the addition of new connectors to integrate to third party system integration, such as: (Additional license required)
   1. ALPR integrations with pay stations, permit vendors, pay-by-phone vendors, and ticketing vendors
   2. Building management systems
   3. Access Control ecosystem (such as IDscanner, card synchronization, Guardtour, Morpho Biometrics, Advanced Enrollment)
   4. Videowall (Barco, Eizo)
   5. Intelligent Keys (Salto SVN, Medeco XT, CLIQ, ILOQ (future))
   6. Gunshot Detection (Shot Spotter, Guardian GunShot)
   7. Dynamic Logbook: Customizable forms with reporting capabilities

USP SOFTWARE DEVELOPMENT KIT (SDK) (ADDITIONAL LICENSE REQUIRED)

48.01 A USP SDK SHALL BE AVAILABLE TO SUPPORT CUSTOM DEVELOPMENT FOR THE PLATFORM.

48.02 THE SDK SHALL INCLUDE FUNCTIONALITIES SPECIFIC TO THE EMBEDDED AUTOMATIC LICENSE PLATE RECOGNITION (ALPR), ACCESS CONTROL (ACS), AND VIDEO (VMS) SYSTEMS.

48.03 INTEGRATION WITH EXTERNAL APPLICATIONS AND DATABASES SHALL BE POSSIBLE WITH THE SDK.

48.04 THE SDK SHALL SUPPORT AN API TO ALLOW THIRD PARTY ACCESS CONTROL HARDWARE INTEGRATION.

48.05 THE SDK SHALL ENABLE END-USERS TO DEVELOP NEW FUNCTIONALITY (USER INTERFACE, STANDALONE APPLICATIONS, OR SERVICES) TO LINK THE USP TO THIRD PARTY BUSINESS SYSTEMS AND APPLICATIONS SUCH AS BADGING SYSTEMS, HUMAN RESOURCES MANAGEMENT SYSTEMS (HRMS), AND ENTERPRISE RESOURCE PLANNING (ERP) SYSTEMS.

48.06 THE SDK SHALL BE BASED ON THE .NET FRAMEWORK.

48.07 THE SDK SHALL SUPPORT DYNAMIC OR TRANSACTIONAL UPDATES TO THE USP CONFIGURATION. IT SHALL ALSO SUPPORT CHANGE NOTIFICATION OF USP ENTITY CONFIGURATION.

48.08 THE SDK SHALL PROVIDE AN EXTENSIVE LIST OF PROGRAMMING FUNCTIONS TO VIEW AND/OR CONFIGURE CORE ENTITIES SUCH AS: USERS AND USER GROUPS, ALARMS, CUSTOM EVENTS, AND SCHEDULES, AND MORE.

48.09 THE SDK SHALL PROVIDE AN EXTENSIVE LIST OF PROGRAMMING FUNCTIONS TO VIEW AND CONFIGURE ACS, VMS, AND ALPR.

48.10 THE SDK SHALL PROVIDE AN EXTENSIVE LIST OF PROGRAMMING FUNCTIONS TO VIEW AND CONFIGURE MOST ACS ENTITIES SUCH AS CARDHOLDERS, CARDHOLDER GROUPS, VISITORS, CREDENTIALS, ACCESS RULES (MODIFY ONLY), AND CUSTOM FIELDS.

48.11 THE SDK SHALL BE ABLE TO RECEIVE REAL TIME EVENTS FROM THE FOLLOWING USP ENTITIES: USERS AND USER GROUPS, AREAS, ZONES, CAMERAS, VIDEO UNITS, DOORS, DOOR CONTROLLERS (UNITS), ELEVATORS, CARDHOLDERS, CARDHOLDER GROUPS, AND CREDENTIALS.

48.12 THE SDK SHALL BE ABLE TO QUERY THE HISTORY OF EVENTS FOR AREAS, CAMERAS, ZONES, ALARMS, CARDHOLDERS, CREDENTIALS, VISITORS, DOORS, QUERY LICENSE PLATE READ EVENTS, LICENSE PLATE HIT EVENTS, GENERATE A LICENSE PLATE HITS REPORT, GENERATE A LICENSE PLATE READS REPORT.

48.13 THE SDK SHALL SUPPORT THE FOLLOWING ALARM FUNCTIONS: VIEW ALARMS IN REAL TIME, ACKNOWLEDGE ALARMS, CHANGE PRIORITY, AND CHANGE RECIPIENT.

EXECUTION

WARRANTY

50.01 THE PRODUCT SHALL PERFORM IN ALL MATERIAL RESPECTS IN ACCORDANCE WITH THE ACCOMPANYING USER MANUAL, AND THE MEDIA ON WHICH THE SOFTWARE PRODUCT RESIDES WILL BE FREE FROM DEFECTS IN MATERIALS AND WORKMANSHIP UNDER NORMAL USE. SOFTWARE DEFECTS ARE COVERED THROUGH SERVICE RELEASES AND CUMULATIVE UPDATES WHICH ARE AVAILABLE FOR A PERIOD OF 1 YEAR FROM THE DATE OF THE SOFTWARE PURCHASE.

50.02 EXTENDED WARRANTY, UP TO 5 YEARS, SHALL BE AVAILABLE THROUGH THE PURCHASE OF THE GENETEC ADVANTAGE SUPPORT SERVICE WHICH INCLUDES THE FOLLOWING ADDITIONAL SERVICES OVER THE STANDARD WARRANTY:

A. Access to phone support and online chat for technical assistance
B. Online case management
C. Online system availability monitor
D. Access to Major and Minor Release Upgrades
E. 24/7 pager support and dedicated support specialist (Additional cost)

DEPLOYMENT SERVICES AND SYSTEM COMMISSIONING (PER DAY CHARGE PLUS TRAVEL, CONSULT GENETEC INC. ON NUMBER OF RECOMMENDED DAYS TO SPECIFY)

51.01 GENERAL REQUIREMENTS:

A. The contractor shall engage the services of the USP vendor to assist in the management of the deployment of the USP at the end-user site on projects that involve:
   1. Multiple contractors or subcontractors that will be responsible for deploying the USP at multiple client sites in different geographical regions.
   2. Complex enterprise installations involving advanced functionality (for example The Federation feature, failover, plugins) and/or multiple systems (for example access control, video, ALPR) and/or third-party integrations.
   3. Extensive use of customized solutions/plugins developed by the vendor that will be integrated into the USP.

B. The USP vendor services shall include Deployment Management and System Configuration and Commissioning.

51.02 DEPLOYMENT MANAGEMENT SERVICE:

A. The Deployment Management service from the vendor shall include a Project Manager acting as the single point of contact for all communications between the contractor and the vendor organization and who will be responsible for:
   1. Conducting a Risk Assessment of the impact of potential risk factors on the operation of the vendor's USP.
   2. Providing a project plan for the deployment of the vendor's USP.
   3. Managing the development and deployment of the custom solution components that will be integrated into the vendor's USP (if applicable).
   4. Providing a scope of work detailing the services to be provided by the vendor to assist in the deployment of the vendor’s USP.
   5. Coordinating and scheduling the vendor field services with the contractor to assist with the deployment of the vendor’s USP.
   6. Providing regular project status updates to the contractor regarding the development of custom solutions (if applicable) and the deployment of the vendor’s USP.

51.03 SOLUTION ARCHITECT SERVICE:

A. The Solution Architect service from the vendor shall include a Solutions Architect Engineer acting as a single technical point of contact throughout the deployment of the USP, and who will be responsible for:
   1. Assisting the contractor/subcontractor with the design and architecture of the vendor’s USP.
   2. Conducting technical consultation activities that may include fit/gap analysis, system design reviews, device compatibility assessments, functional and technical design reviews, as well as performance reviews of the vendor’s USP.
   3. Conducting a system assessment and ensuring best practices of the vendor’s USP are followed.
   4. Providing upgrade and migration strategy for the vendor’s USP where applicable.
   5. Providing documentation regarding the system architecture, system design, hardware specifications and compatibility requirements, camera bandwidth calculations, and best practices as they relate to the vendor’s USP.

51.04 SYSTEM CONFIGURATION AND COMMISSIONING SERVICE:

A. The System Configuration and Commissioning service from the vendor shall include a Field Engineer who will be responsible for:
   1. Assisting the contractor's or subcontractor's onsite/remote technicians with the configuration and commissioning of the vendor's USP at the client site.
   2. Conducting a test of the USP following the deployment of the system using real-world operator scenarios to ensure optimal system performance.
   3. Providing the contractor with a Service Report detailing the tasks completed during the deployment of the USP at the client site, as well as any recommendations for improving the performance of the USP that must be implemented by the contractor.
   4. Providing a knowledge transfer of the vendor's USP to the contractor following the deployment of the USP at the client site.

MANUFACTURER END USER OPERATOR TRAINING (PER HALF-DAY CHARGE PLUS EXPENSES)

52.01 THE CONTRACTOR SHALL ENGAGE THE SERVICES OF THE USP VENDOR TO ASSIST IN THE END USER TRAINING OF THE USP AT THE END-USER SITE.

END OF SECTION 28 13 00