SECTION 28 23 00
– VIDEO MANAGEMENT SYSTEM

GENERAL

RELATED WORK

2.01 DIVISION 14 - GENERAL ELEVATOR REQUIREMENTS

2.02 SECTION 28 13 00 – ELECTRONIC ACCESS CONTROL SYSTEM

DEFINITIONS

3.01 ACS – ACCESS CONTROL SYSTEM

3.02 CSA – CLIENT SOFTWARE APPLICATION

3.03 DGM – DYNAMIC GRAPHICAL MAPS

3.04 DVS – DIGITAL VIDEO SERVER

3.05 ALPR – AUTOMATIC LICENSE PLATE RECOGNITION

3.06 SDK – SOFTWARE DEVELOPMENT KIT

3.07 GLM – GENETEC LIFECYCLE MANAGEMENT

3.08 SSM – SERVER SOFTWARE MODULE

3.09 UI – USER INTERFACE

3.10 USP – UNIFIED SECURITY PLATFORM

3.11 USW – UNIFIED WEB CLIENT

3.12 VMS – VIDEO MANAGEMENT SYSTEM

QUALIFICATIONS

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

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

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

A. Certified Reseller or up

4.04 THE SYSTEM PROGRAMMER SHALL SUBMIT PROOF OF CERTIFICATIONS.

PRODUCTS

VMS GENERAL REQUIREMENTS

6.01 THE VMS SHALL SUPPORT UPDATING ITS CAMERA DRIVERS INDEPENDENT FROM THE VMS INSTALLATION. NEW DRIVERS SHALL BE RELEASED MULTIPLE TIMES A YEAR TO EXTEND SUPPORT FOR NEW DEVICES AND FEATURES.

6.02 THE VMS SHALL BE BASED ON A TRUE OPEN ARCHITECTURE THAT SHALL ALLOW THE USE OF NON-PROPRIETARY WORKSTATION AND SERVER HARDWARE, NON-PROPRIETARY NETWORK INFRASTRUCTURE, AND NON-PROPRIETARY STORAGE.

6.03 THE VMS SHALL OFFER A COMPLETE AND SCALABLE VIDEO SURVEILLANCE SOLUTION THAT SHALL ALLOW CAMERAS TO BE ADDED ON A UNIT-BY-UNIT BASIS.

6.04 THE VMS SHALL INTERFACE WITH ANALOG-TO-DIGITAL VIDEO ENCODERS AND IP CAMERAS AND WITH DIGITAL-TO-ANALOG VIDEO DECODERS, HEREAFTER REFERRED TO AS DIGITAL VIDEO SERVERS (DVS). THE VMS SHALL SUPPORT DVS FROM VARIOUS MANUFACTURERS.

6.05 THE VMS SHALL INTEGRATE DVS USING THE DVS NATIVE SDK OR USING THE FOLLOWING INDUSTRY STANDARDS TO INTERFACE TO THE DVS:

A. ONVIF

6.06 ALL VIDEO STREAMS SUPPLIED FROM ANALOG CAMERAS OR IP CAMERAS SHALL BE DIGITALLY ENCODED IN H.265, H.264, MPEG-4, MPEG-2, MJPEG, MXPEG, WAVELET, OR JPEG2000 COMPRESSION FORMATS AND RECORDED SIMULTANEOUSLY IN REAL TIME.

6.07 ALL AUDIO STREAMS SUPPLIED FROM IP VIDEO SERVERS SHALL BE DIGITALLY ENCODED IN G711 (U-LAW), G721, G723, OR AAC COMPRESSION FORMATS AND RECORDED SIMULTANEOUSLY IN REAL TIME.

6.08 EACH CAMERA'S BIT RATE, FRAME RATE, AND RESOLUTION SHALL BE SET INDEPENDENTLY FROM OTHER CAMERAS IN THE SYSTEM AND ALTERING THESE SETTINGS SHALL NOT AFFECT THE RECORDING AND DISPLAY SETTINGS OF OTHER CAMERAS.

6.09 THE VMS SHALL BE ABLE TO USE MULTIPLE CCTV KEYBOARDS TO OPERATE THE ENTIRE SET OF CAMERAS THROUGHOUT THE SYSTEM, INCLUDING BRANDS OF CAMERAS FROM VARIOUS MANUFACTURERS AND INCLUDING THEIR PTZ FUNCTIONALITIES (I.E., PELCO KEYBOARD CONTROLS PANASONIC DOME OR VICE-VERSA).

6.10 THE VMS SHALL BE ABLE TO RETRIEVE AND SET THE CURRENT POSITION OF PTZ CAMERAS USING XYZ COORDINATES.

6.11 THE VMS SHALL SUPPORT PTZ CAMERA PROTOCOLS FROM MULTIPLE MANUFACTURERS, INCLUDING ANALOG AND IP PROTOCOLS.

6.12 THE VMS SHALL ARBITRATE THE USER CONFLICT ON PTZ USAGE BASED ON USER LEVELS PER CAMERA.

6.13 THE VMS SHALL SUPPORT THE FOLLOWING LIST OF CCTV KEYBOARD:

A. American Dynamics 2078 ASCII, and American Dynamics 2088 ASCII

B. Bosch Autodome, Bosch Intuikey

C. DVTel

D. GE ImpactNet

E. Panasonic, Pelco ASCII, Pelco KBD-300, Pelco 9760, and Pelco P.

F. Radionics

G. Hanwha Techwin SSC-100, SPC-600, SPC-2010, SPC-6000, and SPC-7000.

H. Video alarm

I. Sony RM-NS1000

J. Panasonic WV-CU161C

K. Panasonic WV-CU950 Ethernet keyboard

6.14 THE VMS SHALL SUPPORT THE FOLLOWING LIST OF JOYSTICKS:

A. Axis 295

B. Axis T8310, T8311, T8312, T8313 Video Surveillance Control Board

C. Any USB joystick detected as a Windows Game Controller

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

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

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

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

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

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

6.16 THE VMS 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

6.17 THE VMS SHALL ALLOW FOR THE CONFIGURATION OF A TIME ZONE FOR EACH CAMERA CONNECTED TO A DVS. FOR PLAYBACK REVIEW, USERS SHALL HAVE THE ABILITY TO SEARCH FOR VIDEO BASED ON THE FOLLOWING OPTIONS:

A. Local time of the camera

B. Local time of the SSM

C. Local time of user’s workstation

D. GMT Time

E. Other time zone

6.18 AUDIO AND VIDEO STORAGE CONFIGURATION FOR THE SSM SHALL EITHER BE:

A. Internal or external IDE/SATA/SAS organized or not in a RAID configuration.

B. Internal or external SCSI/iSCSI/Fiber Channel organized or not in a RAID configuration.

C. Within the overall storage system, it shall be possible to include disks located on:
   1. External PCs on a LAN or WAN
   2. Network Attached Servers (NAS) on a LAN or WAN
   3. Storage Area Networks (SAN)

6.19 THE SSM SHALL NOT LIMIT THE ACTUAL STORAGE CAPACITY CONFIGURED PER SERVER.

6.20 MANUFACTURER:

A. Genetec Security Center:
   1. Omnicast Enterprise

CYBER SECURITY REQUIREMENTS

7.01 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.

7.02 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

7.03 THE USP SHALL LIMIT THE IP PORTS IN USE AND SHALL PROVIDE THE ADMINISTRATOR WITH THE ABILITY TO CONFIGURE THESE PORTS.

7.04 THE VMS SHALL SUPPORT ONLY SECURED MEDIA STREAM REQUESTS, UNLESS EXPLICITLY CONFIGURED OTHERWISE. SECURED MEDIA STREAM REQUESTS SHALL BE SECURED WITH STRONG CERTIFICATE-BASED AUTHENTICATION LEVERAGING RTSPS (RTSP OVER TLS). CLIENT AUTHENTICATION FOR MEDIA STREAM REQUESTS IS CLAIMS-BASED AND MAY USE A LIMITED LIFETIME SECURITY TOKEN.

7.05 THE VMS SHALL OFFER THE ABILITY TO ENCRYPT THE MEDIA STREAM, INCLUDING VIDEO, AUDIO, AND METADATA WITH AUTHENTICATED ENCRYPTION. MEDIA STREAM ENCRYPTION SHALL BE DONE AT REST AND IN TRANSIT AND BE A CERTIFICATE-BASED AES 128-BITS ENCRYPTION. THE VMS SHALL:

A. Allow encryption to be set on a per camera basis for all or some of the cameras.

B. Provide up to 20 different certificates for different groups of CSA or users who have been granted access to decrypted streams.

C. Not decrease the recording performance by more than 50% when encryption is enabled.

D. Use Secure RTP (SRTP) to encrypt the payload of a media stream in transit and allow multicast and unicast of the encrypted stream.

E. Use a random encryption key and change periodically.

F. Allow encrypted streams to be exported.

7.06 THE VMS SHALL SUPPORT END TO END ENCRYPTED STREAMS WITH CAMERAS SUPPORTING SECURE RTP (SRTP) BOTH IN UNICAST AND MULTICAST FROM THE CAMERA.

7.07 THE USP SHALL SUPPORT ENCRYPTION FOR ALL COMMUNICATIONS WITH ITS DATABASES.

7.08 THE USP SHALL PROVIDE IN ITS MAIN USER INTERFACE A VISUAL LIST SHOWING THE STATE OF ALL CONFIGURATION ITEMS RELATING TO THE CYBER SECURITY HARDENING OF THE FEATURES OF THE SYSTEM.

7.09 THE USP SHALL PROVIDE RECOMMENDATIONS RELATING TO THE PASSWORDS USED TO ACCESS THE HARDWARE UNITS IN THE SYSTEM. THE RECOMMENDATION SHOULD DISPLAY IF THE PASSWORDS USED ON THE UNITS ARE WEAK, AVERAGE, STRONG, OR VERY STRONG.

7.10 THE USP SHALL PROVIDE THE ABILITY TO MANUALLY OR AUTOMATICALLY CHANGE THE VIDEO UNIT PASSWORDS WITH MANUFACTURER'S NATIVE API, STANDARD GENETEC PROTOCOL OR ONVIF. THE VMS SHALL SUPPORT PASSWORD CHANGE FOR VIDEO UNITS AS FOLLOWS:

A. In batch or per unit

B. On schedule

C. From an event

D. Based on manufacturer's policies

E. The USP shall allow backup of last 5 passwords.

F. The USP shall allow copying password to clipboard to be used in the device webpage if the user has the appropriate privileges.

G. The USP shall provide the ability to export the video unit passwords if the user has the appropriate privileges.

7.11 THE USP SHALL PROVIDE RECOMMENDATIONS RELATING TO THE FIRMWARE OF THE HARDWARE UNITS ENROLLED IN THE SYSTEM. RECOMMENDATIONS SHOULD DISPLAY IF THE FIRMWARE IS UP TO DATE, OUT OF DATE, OR IF IT HAS KNOWN SECURITY VULNERABILITIES.

FAILOVER AND STANDBY REQUIREMENTS

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

8.02 FAILOVER DIRECTORY:

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 one 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.

8.03 STANDBY ARCHIVER. REFER TO SECTION 2.05 STANDBY ARCHIVER FOR MORE INFORMATION.

8.04 OFF-THE-SHELF STANDBY/FAILOVER OPTIONS (EXCLUDING THE VMS ARCHIVER) SHALL INCLUDE: (ADDITIONAL LICENSE REQUIRED PER SERVER THAT WILL FAILOVER, ENTERPRISE ONLY)

A. Windows Clustering

B. NEC ExpressCluster X LAN

ARCHIVING

9.01 THE ARCHIVER (ROLE) SHALL USE AN EVENT AND TIMESTAMP DATABASE FOR THE ADVANCED SEARCH OF AUDIO/VIDEO ARCHIVES. THIS DATABASE SHALL USE MICROSOFT SQL.

9.02 THE ARCHIVER SHALL PROTECT ARCHIVED AUDIO/VIDEO FILES AND THE SYSTEM DATABASE AGAINST NETWORK ACCESS AND NON-ADMINISTRATIVE USER ACCESS.

9.03 THE ARCHIVER SHALL DIGITALLY SIGN RECORDED VIDEO USING AN EDDSA SIGNATURE ALGORITHM BASED ON A PUBLIC/PRIVATE KEY CRYPTOGRAPHY.

9.04 THE ARCHIVER SHALL OFFER A PLUG AND PLAY TYPE HARDWARE DISCOVERY SERVICE WITH THE FOLLOWING FUNCTIONALITIES:

A. Automatically discover DVS units as they are attached to the network.

B. Discover DVS units on different network segments, including the Internet, and across routers with or without network address translation (NAT) capabilities.

9.05 THE ARCHIVER SHALL HAVE THE CAPACITY TO CONFIGURE THE KEY FRAME INTERVAL (I-FRAME) IN SECONDS OR NUMBER OF FRAMES.

9.06 THE ARCHIVER SHALL PROVIDE A PRE-ALARM AND POST-ALARM RECORDING OPTION THAT CAN BE SET BETWEEN ONE SECOND AND 5 MINUTES ON A PER CAMERA BASIS.

9.07 THE ARCHIVER SHALL PROVIDE THE FUNCTIONALITY OF STORING OF VIDEO AND AUDIO STREAMS BASED ON TRIGGERING EVENTS, SUCH AS:

A. Digital motion detection

B. Digital input activation

C. Macros

D. Through SDK application recording

9.08 THE ARCHIVER SHALL PERFORM VIDEO MOTION DETECTION ON EACH INDIVIDUAL CAMERA BASED ON A GRID OF 1320 MOTION DETECTION BLOCKS. ALL OF THE VIDEO MOTION DETECTION SETTINGS ARE CONFIGURABLE ON SCHEDULE. A GLOBAL SENSITIVITY THRESHOLD IS AVAILABLE TO REDUCE MOTION DETECTION SENSITIVITY WHEN THE VIDEO SIGNAL IS NOISY OR WHEN A LOT OF FALSE HITS ARE INCURRED. VIDEO MOTION DETECTION ITSELF CAN BE SET INTO FOUR DIFFERENT MODES:

A. Full Screen: All 1320 blocks on screen are activated, and a general threshold for the overall motion in the entire image can be set, and when it is reached, it can trigger recording and a motion event or a custom event.

B. Full Screen Unit: This is the same as the Full Screen, but the motion detection takes place in the DVS.

C. Detection Zone: Six overlapping zones can be defined in the 1320 blocks on screen with each of these zones having its own threshold, and, when that threshold is reached, each one of them can trigger recording and a motion event or a custom event. Each zone triggering its own event allows for the configuration of directional motion detection events and other complex motion detection logic.

D. Detection Zone Unit: This is the same as the Detection Zone, but the motion detection takes place in the DVS and only one zone is supported.

E. Disabled: No motion detection is performed on this camera.

9.09 THE ARCHIVER SHALL BE ABLE TO DETECT MOTION IN VIDEO WITHIN 200 MILLISECONDS AND NOT ONLY ON KEY FRAMES.

9.10 THE ARCHIVER SHALL ALLOW FOR MULTIPLE RECORDING SCHEDULES TO BE ASSIGNED TO A SINGLE CAMERA. EACH SCHEDULE SHALL BE CREATED WITH THE FOLLOWING PARAMETERS:

A. Recording mode:

1. Continuous
2. On Motion/Manual
3. Manual
4. Disabled

B. Recurrence pattern:
1. Once on specific days
2. Specific days on a yearly basis
3. Specific days on a monthly basis
4. Specific days on a weekly basis
5. Daily

9.11 TIME COVERAGE:
1. All day.
2. Specific time range(s).
3. Daytime or nighttime based on the times of sunrise and sunset that are automatically calculated from the time of year and a geographical location. Provision shall be given to offset the calculated sunrise or sunset time by plus or minus 3 hours.

9.12 THE ARCHIVER SHALL ALLOW EACH CAMERA (VIDEO SOURCE) TO BE ENCODED MULTIPLE TIMES IN THE SAME OR DIFFERENT VIDEO FORMATS (H.265, H.264, MPEG-4, MPEG-2, MJPEG, MXPEG, WAVELET, OR JPEG2000), LIMITED ONLY BY THE CAPABILITIES OF EACH DVS.

9.13 WHENEVER MULTIPLE VIDEO STREAMS ARE AVAILABLE FROM THE SAME CAMERA, USERS SHALL BE FREE TO USE ANY ONE OF THEM BASED ON THEIR ASSIGNED USAGE. THE STANDARD VIDEO STREAM USAGES ARE:

A. Live

B. Recording

C. Remote

D. Low resolution

E. High resolution

9.14 THE ARCHIVER SHALL ALLOW THE VIDEO QUALITY TO VARY ACCORDING TO PREDEFINED SCHEDULES. SUCH SCHEDULES SHALL HAVE THE SAME CONFIGURATION FLEXIBILITY AS THE RECORDING SCHEDULES MENTIONED EARLIER. THE VIDEO QUALITY SHALL BE BASED ON, BUT NOT LIMITED TO, THE FOLLOWING PARAMETERS:

A. Maximum bit rate

B. Maximum frame rate

C. Image quality

D. Key frame interval

9.15 THE ARCHIVER SHALL HAVE THE ABILITY TO DYNAMICALLY BOOST THE QUALITY OF THE "RECORDING STREAM" (SEE PREVIOUS BULLET) BASED ON SPECIFIC EVENTS:

A. When recording is started manually by a user.

B. When recording is triggered by a macro, an alarm or detected motion.

9.16 THE ARCHIVER SHALL HAVE THE CAPACITY TO COMMUNICATE WITH THE DVS USING 128 BITS SSL ENCRYPTION.

9.17 THE ARCHIVER SHALL HAVE THE CAPACITY TO COMMUNICATE WITH THE DVS USING HTTPS SECURE PROTOCOL.

9.18 THE ARCHIVER SHALL HAVE THE CAPACITY TO RECEIVE MULTICAST UDP STREAMS DIRECTLY FROM THE DVS.

9.19 FOR NETWORK TOPOLOGIES THAT RESTRICT THE DVS FROM SENDING MULTICAST UDP STREAMS, THE ARCHIVER SHALL REDIRECT AUDIO/VIDEO STREAMS TO ACTIVE VIEWING CLIENTS ON THE NETWORK USING MULTICAST UDP.

9.20 THE ARCHIVER SHALL HAVE THE CAPACITY TO REDIRECT AUDIO/VIDEO STREAMS TO ACTIVE VIEWING CLIENTS ON THE NETWORK USING UNICAST UDP OR TCP.

9.21 THE ARCHIVER SHALL EMPOWER THE ADMINISTRATOR WITH A FULL RANGE OF DISK MANAGEMENT OPTIONS:

A. The Archiver shall allow the administrator to choose which disks to use for archiving and to set a maximum quota for each.

B. The Archiver shall allow the administrator to spread the archiving of different cameras on different disk groups (groups of disks controlled by the same controller) so that archiving could be carried out in parallel on multiple disks.

C. The Archiver shall have the capacity to move video archives to the Azure Cloud. The archives will be moved after a preset number of days.

9.22 THE ARCHIVER SHALL EMPOWER THE ADMINISTRATOR WITH A FULL RANGE OF ARCHIVE MANAGEMENT OPTIONS:

A. The Archiver shall provide a graphical representation of video sequences and recording gaps.

B. The Archiver shall provide a way to identify the location of the video sequences.

9.23 THE ARCHIVER SHALL OFFER THE FOLLOWING OPTIONS TO CLEAN UP OLD ARCHIVES, ON A CAMERA-BY-CAMERA BASIS:

A. After a preset number of days.

B. Deleting oldest archives first when disks run out of space.

C. Stop archiving when disks are full.

9.24 THE ARCHIVER SHALL ALLOW IMPORTANT VIDEO SEQUENCES TO BE PROTECTED AGAINST NORMAL DISK CLEANUP ROUTINES.

9.25 USERS SHALL HAVE THE FOLLOWING OPTIONS WHEN PROTECTING A VIDEO SEQUENCE:

A. Until a specified date

B. For a specified number of days

C. Indefinitely (until the protection is explicitly removed)

9.26 THE ARCHIVER SHALL ALLOW THE ADMINISTRATOR TO PUT A CAP ON THE PERCENTAGE OF STORAGE SPACE OCCUPIED BY PROTECTED VIDEO.

9.27 THE ARCHIVER SHALL KEEP A LOG AND COMPILE STATISTICS ON DISK SPACE USAGE.

A. The statistics shall be available by disk group or for the whole Archiver.

B. The statistics shall show the percentage of protected video over the total used disk space.

9.28 THE ARCHIVER SHALL HAVE THE CAPACITY TO DOWN-SAMPLE VIDEO STREAMS FOR STORAGE SAVING PURPOSES. THE DOWN-SAMPLING OPTIONS AVAILABLE ARE THE FOLLOWING:

A. For H.264, MPEG-4, and H.265, streams the down-sampling options are: all key frames, 1 fps, 2 sec./frame, 5 sec./frame, 10 sec./frame, 15 sec./frame, 30 sec./frame, 60 sec./frame, 120 sec./frame.

B. For MJPEG streams the down-sampling options are: 15 fps, 10 fps, 5 fps, 2 fps, 1 fps, 2 sec./frame, 5 sec./frame, 10 sec./frame, 15 sec./frame, 30 sec./frame, 60 sec./frame, 120 sec./frame.

9.29 THE ARCHIVER SHALL SUPPORT DVS WITH EDGE RECORDING CAPABILITIES AND OFFER THE FOLLOWING CAPACITY:

A. The ability to playback the video recorded on the DVS at different speeds.

B. The ability to offload (video trickling) the video recorded on the DVS on schedule, on event, or manually to store it on the Archiver.

C. It shall be possible to filter the video that is being offloaded using one or multiple of the following filters:
   1. Time interval
   2. Playback request
   3. Video analytic events
   4. Motion events
   5. Bookmarks
   6. Alarms
   7. Input pin events
   8. Unit offline events

9.30 THE ARCHIVER SHALL BE PROVIDED WITH PROVEN PERFORMANCE AND SCALABILITY FIGURES:

A. The Archiver's performance shall be guaranteed during the rebuild of a disk from a raid 5 disk group. The rebuild process shall not affect the recording and playback capabilities.

B. The recommended server specification from the Genetec Security Center Hardware Requirement shall allow Archiver to perform up to 300 cameras or 300Mbs throughput first limit reached.

C. The high-performance archiver specification from the Genetec Security Center Hardware Requirement shall allow Archiver to perform: (For prequalified machines)
   1. Up to 500 cameras or 500Mbs throughput first limit reached with a 1Gbps NIC.
   2. Up to 700 cameras or 1300Mbs throughput first limit reached with a 10Gbps NIC.

9.31 THE ARCHIVER SHALL PROVIDE THE ABILITY TO ENCRYPT THE MEDIA STREAM COMING FROM THE DVS INCLUDING THE VIDEO, AUDIO AND METADATA: (ADDITIONAL LICENSE REQUIRED)

A. Media encryption shall be optional and can be activated on a per DVS basis.

B. Media encryption shall be performed with AES 128-bits.

C. Media encryption shall encrypt all video, audio and metadata at rest and in transit. Once media encryption is turned on for a DVS all media stored or redirected by the Archiver shall be encrypted and shall require the private key to be decoded.

D. It shall be possible to export the encrypted media into a non-encrypted ASF file.

AUXILIARY ARCHIVER (ADDITIONAL LICENSE REQUIRED)

10.01 THE AUXILIARY ARCHIVER SHALL BE USED TO PRODUCE REDUNDANT ARCHIVES (VIDEO, EVENTS, OR BOOKMARKS) FOR ANY CAMERA IN THE SYSTEM, ON A CASE-BY-CASE BASIS.

10.02 THE AUXILIARY ARCHIVER SHALL HAVE THE ABILITY TO RECORD A CAMERA ON A DIFFERENT SCHEDULE THAN THE ARCHIVER.

10.03 THE AUXILIARY ARCHIVER SHALL HAVE THE ABILITY TO ARCHIVE ANY OF THE STANDARD VIDEO STREAMS FOR ARCHIVING. THE STANDARD VIDEO STREAM USAGES ARE: LIVE, RECORDING, REMOTE, LOW RESOLUTION, AND HIGH RESOLUTION.

10.04 THE AUXILIARY ARCHIVER SHALL HAVE THE CAPACITY TO MOVE VIDEO ARCHIVES TO THE AZURE CLOUD.

STANDBY ARCHIVER (REQUIRES AN ADDITIONAL LICENSE PER DVS THAT WILL FAILOVER)

11.01 THE STANDBY ARCHIVER SHALL ACT AS A REPLACEMENT ARCHIVER ROLE ON HOT STANDBY, READY TO TAKE OVER THE FUNCTIONS OF THE PRIMARY ARCHIVER ROLE. THE FAILOVER WILL OCCUR IN LESS THAN 1 MINUTE. NO ACTION FROM THE USER WILL BE REQUIRED.

11.02 THE STANDBY ARCHIVER ASSIGNED TO AN ARCHIVER ROLE ENTITY SHALL AUTOMATICALLY PROVIDE PROTECTION FOR ALL DVS CONNECTED TO THAT ARCHIVER ROLE.

11.03 THE STANDBY ARCHIVER SHALL PROTECT THE PRIMARY ARCHIVER ROLE AGAINST THE FOLLOWING FAILURES:

A. Server failure (hardware or software).

B. Storage failure, such as Archiver Role detects that it cannot read or write to any of its allocated disks.

11.04 IT SHALL BE POSSIBLE FOR A SINGLE USP SERVER TO ACT AS THE STANDBY SERVER OF MULTIPLE ARCHIVER ROLES.

A. Each Archiver role shall have priority value if multiple Archiver Roles fail at the same time on the same standby server.

11.05 IT SHALL BE POSSIBLE FOR ANY ARCHIVER ROLE IN THE SYSTEM TO BE DESIGNATED AS ANOTHER'S STANDBY AND VICE-VERSA.

11.06 FOR EACH ARCHIVER ROLE IT SHALL BE POSSIBLE TO SET UP TO 2 STANDBY ARCHIVER SO THAT IF THE FIRST FAILOVER ARCHIVER FAILS THE FAILOVER WILL AUTOMATICALLY OCCUR TO A THIRD SERVER.

11.07 THE STANDBY ARCHIVER SHALL HAVE THE ABILITY TO ACT AS A REDUNDANT ARCHIVER.

11.08 IT SHALL BE POSSIBLE TO SET A DIFFERENT RETENTION PERIOD FOR THE ARCHIVER AND THE REDUNDANT ARCHIVER.

11.09 THE REDUNDANT ARCHIVER SHALL MAINTAIN AN EXACT COPY OF EVERYTHING RECORDED BY THE DEFAULT ARCHIVER, I.E., AUDIO/VIDEO ARCHIVES, EVENTS, AND BOOKMARKS.

11.10 REDUNDANCY SHALL BE CONFIGURED ON A CAMERA-BY-CAMERA BASIS.

11.11 THE REDUNDANT ARCHIVER SHALL HAVE TO ABILITY TO USE A MULTICAST VIDEO STREAM FROM THE DVS AND SHALL NOT REQUIRE AN ADDITIONAL CONNECTION TO ANY DVS.

CLOUD ARCHIVING

12.01 THE VMS SHALL SUPPORT THE AUTOMATIC TRANSFER OF VIDEO RECORDED ON THE ARCHIVER TO THE CLOUD, BASED ON THE AGE OF THE VIDEO.

12.02 THE ARCHIVER SHALL ENCRYPT RECORDINGS USING AES-256 PRIOR TO TRANSFERRING VIDEO TO THE CLOUD.

12.03 THE ARCHIVER SHALL ROTATE THE ENCRYPTION KEY AT EVERY FILE. THE ENCRYPTION KEY SHALL BE ENCRYPTED WITH A CERTIFICATE KEPT IN AZURE KEY VAULT.

12.04 THE VMS SHALL SUPPORT TLS ENCRYPTION BETWEEN THE ON-PREMISES ARCHIVER AND THE CLOUD.

12.05 THE VMS SHALL ALLOW USERS TO SEARCH VIDEO STORED IN THE CLOUD THROUGH THE SAME FUNCTIONALITY USED WHEN QUERYING VIDEO THAT IS STORED LOCALLY.

12.06 THE VMS WILL MAINTAIN A LOCAL CACHE OF VIDEO DOWNLOADED FROM THE CLOUD TO PLAYBACK RECORDINGS WITHOUT REQUIRING AN ADDITIONAL TRANSFER.

12.07 THE VMS SHALL SUPPORT DIFFERENT TIERS TO SUPPORT THE VIDEO SEQUENCES.

A. The VSM shall allow users to differentiate the video sequences available for real-time and delayed retrieval.

B. The VMS shall automatically move video sequences from the real-time access to delayed retrieval after a configurable delay.

VMS MEDIA STREAMING

13.01 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).

13.02 THE MEDIA ROUTER ROLE SHALL SUPPORT MULTIPLE TRANSPORT PROTOCOLS, SUCH AS UNICAST TCP, UNICAST UDP, AND MULTICAST UDP.

13.03 THE MEDIA ROUTER SHALL SUPPORT IGMP (INTERNET GROUP MANAGEMENT PROTOCOL) TO ESTABLISH MULTICAST GROUP MEMBERSHIPS:

A. IGMP v3, including SSM (Source-Specific Multicast) shall be supported.

13.04 THE MEDIA ROUTER ROLE USING REDIRECTOR AGENTS SHALL BE RESPONSIBLE FOR REDIRECTING A STREAM FROM A SOURCE IP ENDPOINT TO A DESTINATION IP ENDPOINT.

13.05 THE REDIRECTOR AGENTS SHALL BE CAPABLE OF CONVERTING A STREAM FROM AND TO ANY SUPPORTED TRANSPORT PROTOCOLS:

A. Multicast UDP to Unicast TCP

B. Multicast UDP to Unicast UDP

C. Unicast TCP to Multicast UDP

D. Unicast UDP to Multicast UDP

13.06 IT SHALL BE POSSIBLE TO LIMIT THE NUMBER OF CONCURRENT LIVE AND PLAYBACK VIDEO REDIRECTIONS FOR EACH REDIRECTOR AGENT IN ORDER TO BETTER CONTROL THE BANDWIDTH ACROSS MULTIPLE SITES.

13.07 IT SHALL BE POSSIBLE TO LIMIT THE BANDWIDTH CONSUMED BY LIVE AND PLAYBACK VIDEO FROM THE CSA TO BETTER CONTROL THE BANDWIDTH ACROSS MULTIPLE SITES. THE SSM SHALL BE ABLE TO PRIORITIZE VIDEO STREAMING TO THE CSA BASED ON USER LEVEL.

13.08 IT SHALL BE POSSIBLE TO PROTECT THE MEDIA ROUTER ROLE AGAINST HARDWARE OR SOFTWARE UNAVAILABILITY BY CONFIGURING ANOTHER MEDIA ROUTER ROLE TO ACT AS A HOT STANDBY SERVER.

13.09 MULTIPLE REDIRECTOR AGENTS SHALL BE USED ON A LARGE VMS INSTALLATION TO INCREASE THE SERVICE AVAILABILITY AND TO PROVIDE AUTOMATIC LOAD BALANCING.

VMS VIDEO ARCHIVES TRANSFER CAPABILITIES

14.01 ARCHIVE TRANSFER SHALL PROVIDE THE ABILITY TO:

A. Transfer video from a server to another server in the same system.

B. Transfer video from a federated server to another server.

C. Transfer video from camera storage to a server.

14.02 IT SHALL BE POSSIBLE TO PROGRAM VIDEO TRANSFERS EITHER ON A RECURRENT SCHEDULE, OR TO TRIGGER THEM MANUALLY OR UPON CONNECTION.

14.03 IT SHALL BE POSSIBLE TO FILTER THE VIDEO OF INTEREST FOR A TRANSFER. THE VIDEO OF INTEREST SHALL BE DEFINED WITH THE FOLLOWING FILTERS:

A. All archives when the camera was offline.

B. Alarms.

C. Playback request from the edge.

D. Video analytics events.

E. Motion events.

F. Bookmarks.

G. Input triggers.

H. Time range.

14.04 IT SHALL BE POSSIBLE TO DEFINE THE LENGTH OF VIDEO BEFORE AND AFTER THE EVENT USED AS A FILTER TO DETERMINE THE VIDEO OF INTEREST.

14.05 THE USP SHALL OFFER AN INTERFACE FOR DISPLAYING ALL VIDEO ARCHIVE TRANSFER REQUESTS. THIS INTERFACE SHALL DISPLAY ALL THE CURRENT, REQUESTED AND SCHEDULED VIDEO TRANSFER REQUESTS. IT SHALL BE POSSIBLE TO EDIT, TRIGGER, AND CANCEL VIDEO ARCHIVE TRANSFERS FROM THIS INTERFACE.

14.06 THE USP SHALL OFFER AN INTERFACE FOR QUERYING PAST VIDEO TRANSFERS AND THEIR OUTCOME.

WEARABLE CAMERA MANAGER

15.01 A BODY-WORN CAMERA, ALSO KNOWN AS A WEARABLE CAMERA, IS A VIDEO RECORDING SYSTEM THAT IS TYPICALLY USED BY LAW ENFORCEMENT WITH THE PURPOSE OF GATHERING VIDEO EVIDENCE AND PUBLIC INTERACTION.

15.02 A BODY-WORN CAMERA STATION IS A PHYSICAL DEVICE OR SOFTWARE USED TO AUTOMATICALLY UPLOAD MEDIA FROM A BODY-WORN CAMERA INTO THE VMS SYSTEM.

15.03 THE WEARABLE CAMERA MANAGER SHALL BE USED TO CONFIGURE AND MANAGE BODY-WORN CAMERA DEVICES, CONFIGURE CAMERA STATIONS, ADD OFFICERS (WEARABLE CAMERA USERS), UPLOAD CONTENT TO AN ARCHIVER, AND SET THE RETENTION PERIOD FOR UPLOADED EVIDENCE.

15.04 THE WEARABLE CAMERA MANAGER SHALL ALLOW FOR AUTOMATIC OFFICER CREATION AND HARDWARE SERIAL NUMBER ASSOCIATION.

15.05 THE WEARABLE CAMERA MANAGER SHALL SUPPORT THAT ACTIVATION AND DEACTIVATION OF OFFICERS.

15.06 THE WEARABLE CAMERA MANAGER SHALL SUPPORT THE UPLOADING OD THE FOLLOWING TYPES OF DATA:

A. Video

B. Audio

C. Metadata

15.07 THE SYSTEM SHALL ASSIGN MULTIPLE ARCHIVERS TO THE WEARABLE CAMERA MANAGER FOR PERFORMANCE AND LOAD BALANCE PURPOSES.

15.08 THE WEARABLE CAMERA MANAGER SHALL AUTOMATICALLY UPLOAD DATA WHEN THE BODY-WORN CAMERA IS CONNECTED TO THE BODY-WORN CAMERA DOCKING STATION.

15.09 THE WEARABLE CAMERA EVIDENCE REPORT SHALL LOG THE USER, THE EVIDENCE NAME, THE CAPTURE TIME, THE UPLOAD TIME, AND THE CONVERSION STATUS AND PROGRESS.

15.10 THE WEARABLE CAMERA EVIDENCE REPORT SHALL SUPPORT QUERIES BASED ON THE FOLLOWING FILTERS:

A. Time range

B. During the last year, month, weeks, days, hours, minutes, seconds

C. Specific range

D. Date and time options

E. Capture time

F. Upload time

G. Conversion status

H. Error

I. Pending

J. In progress

K. Completed

15.11 THE SYSTEM SHALL GENERATE AN EVIDENCE READY EVENT WHEN THE UPLOADED VIDEO AND CONVERSION IS COMPLETED.

15.12 THE MONITORING UI INVESTIGATION TASK SHALL SUPPORT THE POSSIBILITY TO SEARCH AND INVESTIGATE BODY WEARABLE CAMERA ARCHIVES.

15.13 THE WEARABLE CAMERA MANAGER SHALL BE PROVIDED WITH THE FOLLOWING PROVEN PERFORMANCE AND SCALABILITY FIGURES:

A. A Wearable Camera Manager can support up to 1000 body-worn camera entities

B. Upon officer incident recording

C. Dedicated Archiver for when more than 20 concurrent officers are uploading video at the same time
   1. Maximum of 100 current officers uploading at the same time
   2. Maximum of 300 officers per Archiver

D. Upon officer continuous recording

E. Dedicated Archiver if more than 5 concurrent officers are uploading video at the same time
   1. Maximum of 30 concurrent officers uploading at the same time
   2. Maximum of 100 officers per Archiver

SECURITY VIDEO ANALYTICS

16.01 THE ANALYTICS SHALL BE COMPLETELY UNIFIED WITH THE VIDEO MANAGEMENT SYSTEM.

16.02 CONFIGURATION SHALL NATIVELY BE PERFORMED IN THE CONFIGURATION INTERFACE OF THE VIDEO MANAGEMENT SYSTEM.

16.03 THE ANALYTICS SHALL FEATURE DEDICATED CONFIGURATION POSSIBILITIES FOR THE FOLLOWING SCENARIOS:

A. Perimeter protection

B. Positional tracking

C. Area protection

D. Direction control

E. Object detection

F. Stopped vehicle detection

G. Tailgating Detection

16.04 EACH OF THE SCENARIOS SHALL TRIGGER EVENTS IN THE VIDEO MANAGEMENT SYSTEM, WHICH CORRESPOND TO THEIR FUNCTIONALITY.

16.05 ADDITIONAL TO THESE SCENARIOS, THE ANALYTICS SHALL ALLOW TO CONFIGURE CUSTOM INTRUSION DETECTION AND OBJECT DETECTION SCENARIOS AS WELL AS ALLOW TO IMPORT SETTINGS TO ALLOW MAXIMUM FLEXIBILITY.

16.06 THE ANALYTICS LICENSE SHALL ALLOW TO CONFIGURE ANY ONE OF THESE SCENARIOS PER CAMERA.

16.07 THE ANALYTICS SHALL ALLOW AT LEAST TWO DIFFERENT DETECTION VARIANTS:

1. Trigger an alarm if a motion pattern moves from zone A (source) through zone B into zone C (sink).
2. Trigger an alarm if a motion pattern moves anywhere inside a specified zone.

16.08 THE ANALYTICS SHALL SUPPORT AN UNLIMITED NUMBER OF DETECTION AREAS.

16.09 THE ANALYTICS FEATURE RAIN-FILTERS TO FILTER OUT DISTURBANCES.

16.10 THE ANALYTICS SHALL FEATURE LIVE CONFIGURATION TO IMMEDIATELY SEE THE EFFECTS OF PARAMETER CHANGES IN THE CONFIGURATION INTERFACE WITHOUT PRIOR SAVING NEW CONFIGURATIONS.

16.11 THE CONFIGURATION OF THE ANALYTICS SHALL BE POSSIBLE ON RECORDED VIDEO STREAMS.

16.12 THE ANALYTICS SHALL OFFER THE POSSIBILITY TO CONFIGURE OBJECT MOVEMENT PATHS.

16.13 THE ANALYTICS SHALL NOT EMPLOY TRIPWIRES OR CROSSLINES.

16.14 AREAS AND THE SCENES PERSPECTIVE (NEAR & FAR OBJECT SIZE) SHALL BE CONFIGURED ON-SCREEN USING A POINT-AND-CLICK INTERFACE.

16.15 THE ANALYTICS SHALL FEATURE FILTERS FOR MOVEMENT SPEED, DISTANCE, AND DIRECTION TO DETECT EVENTS.

16.16 THE ANALYTICS SHALL FEATURE OPTIONS TO SEPARATELY SHOW OR HIDE AREAS, AREA NAMES, AND DETECTION OVERLAYS.

16.17 THE ANALYTICS SHALL BE FULLY SERVER-BASED, WITH NO CALCULATION ON CAMERAS NECESSARY.

16.18 THE ANALYTICS SHALL OPERATE WITH COLOR, THERMAL, AND INFRARED CAMERAS.

16.19 THE ACCURACY OF THE ANALYTICS SHALL BE EVALUATED AND APPROVED BY THE CPNI VIDEO ANALYTICS ASSESSMENT PROGRAMME AND SHALL BE LISTED IN THE CPNI CATALOGUE OF SECURITY EQUIPMENT (CSE).

CAMERA INTEGRITY MONITOR

17.01 DESCRIPTION:

A. Automatically checks camera feeds to detect if cameras have been tampered with.

B. Can be used for near-real-time alerting of tampering events or as a maintenance tool.

C. Reports can be run on detected tampering events.

17.02 DETAILS:

A. It shall be completely unified with the Video Management System.

B. It shall be possible to set the detection sensitivity per camera stream between low, medium, and high.

C. It shall be possible to choose on which servers the analytics shall run.

D. The camera stream used for analytics shall be configurable.

E. It shall be possible to define how many cameras are being analyzed at the same time.

F. To utilize minimum hardware resources, it shall be definable how often camera streams are analyzed.

G. There shall be an overview over which cameras are configured to be analyzed.

PRIVACY PROTECTOR

18.01 DESCRIPTION:

A. Automatically obscures all movement in surveillance videos in real-time.

B. Live privacy masking of moving objects (such as people and vehicles).

C. Completely unified with the video management system.

D. Native configuration in the configuration interface of the video management system.

18.02 DETAILS:

A. Certified with a valid EuroPriSe certification seal.

B. Privacy masking can be removed either per camera or for all cameras currently viewed. Masking for all cameras viewed can be removed and added either manually with a button or automatically with an action.

C. Indoor / outdoor modes using flexible background modeling:
   1. Indoor: Learning model with up to 10 different illumination states – this allows to adapt to fast lighting changes such as lights switching on and off.
   2. Outdoor: Foreground detection based on edge detection rather than color – this allows to adapt to heavily changing lighting conditions such as clouds temporarily blocking sunlight.

D. Detects movements using an absolute difference image, calculated by subtracting the current frame from a calculated background model.

E. Masks movements using blocks, thus obscuring the outline of an object or person.

F. Three different scrambling methods: Pixelation, Colorize, and Transparency.

G. Masking grids can be configured in a point-and-click interface.

H. Past preview mode to see configuration changes in the configuration interface without necessity to save the configuration.

I. Zones can be freely definable polygons with a point-and-click interface.

J. Option to set analysis resolution to optimize performance.

K. No calculation on the camera necessary, completely server based.

L. Option to define zones, which should always or never be pixelated.

M. Option to choose input stream and output stream parameters, including resolutions, frame rate, and encoding.

N. Utilizes server-side hardware acceleration to maximize the amount of cameras analyzed per server.

PEOPLE COUNTER

19.01 THE ANALYTICS SHALL FEATURE DEDICATED CONFIGURATION POSSIBILITIES FOR THE FOLLOWING SCENARIOS:

A. People counting

B. Crowd estimation

19.02 DESCRIPTION:

A. Automatically counts people in a camera's field of view.

B. Provides live dashboard widgets dedicated for people counting and crowd estimation.

C. Completely unified in the video management system.

D. Native configuration in the configuration interface of the video management system.

19.03 DETAILS:

A. Based on deep-learning models trained on person detection to exclude non-human objects.

B. Dedicated dashboard widgets for people counting with the following features:
   1. Charts: visualization of counts in line- or bar-charts
   2. Throughput: Show number of persons in given time frame.
   3. Occupancy: Show how many people are in an area (IN minus OUT)

C. Counts adults and children.

D. Counts crowds of 5 up to more than 300 people in a single frame

E. Counts persons in wheelchairs.

F. Triggers events if more than a defined amount of people is counted in a single frame.

G. Supports top-down camera views.

H. Supports bi-directional counting.

I. Supports tilted camera views.

J. Option to show/hide overlays with detected persons and counting line with dedicated people, crowds, counting lines, and areas.

K. No GPU required to run.

L. The occupancy widget support resetting the count at a defined time option to define zones, which should always or never be pixelated.

M. Supports organizing cameras into areas and show these areas in widgets.

N. Utilizes server-side hardware acceleration to maximize the amount of cameras analyzed per server.

O. Counts can be integrated to external systems using CSV exports and a .NET SDK.

GENERAL CLIENT SOFTWARE REQUIREMENTS

20.01 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.

20.02 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).

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

20.04 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.

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

20.06 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.

20.07 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.

20.08 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 INTEGRATION INCLUDED, ADDITIONAL LICENSES REQUIRED FOR MORE)

20.09 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 INTEGRATION INCLUDED, ADDITIONAL LICENSES REQUIRED FOR MORE)

20.10 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. (ADDITIONAL LICENSE REQUIRED)

20.11 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.

20.12 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.

20.13 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: 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, 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.

20.14 THE CONTRACTOR SHALL PROVIDE UP TO 5 NUMBER OF SIMULTANEOUS CLIENTS.

CONFIGURATION USER INTERFACE (UI)

21.01 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).

21.02 VIDEO MANAGEMENT SYSTEM:

A. The Configuration UI shall allow the administrator or users with appropriate privileges to change video configuration.

B. The Configuration UI shall provide the ability to change video quality, bandwidth, and frame rate parameters on a per camera (stream) basis for both live and recorded video.

C. The Configuration UI shall provide the ability to change video quality by a selection of predefined video quality template.

D. The Configuration UI shall provide the ability to configure brightness, contrast, and hue settings for each camera on the same DVS.

E. The Configuration UI shall provide the capability to enable audio recording on DVS units that support audio.

F. The Configuration UI shall provide the ability to change the audio parameters, serial port and I/O configuration of individual DVS units.

G. The Configuration UI shall provide the capability to rename all DVS units based on system topology and to add descriptive information to each DVS.

H. The Configuration UI shall provide the ability to set recording schedules and modes for each individual camera. The recording mode can be:
   1. Continuous
   2. On motion and Manual
   3. Manual only
   4. Disabled

I. The Configuration UI shall support the creation of schedules to which any of the following functional aspects can be attached:
   1. Video quality (for each video stream per camera)
   2. Recording (for each camera)
   3. Motion detection (for each detection zone per camera)
   4. Brightness, Contrast, and Hue (for each camera)
   5. Camera sequence execution

J. The Configuration UI shall support the creation of unlimited recording schedules and the assigning of any camera to any schedule.

K. The Configuration UI shall detect and warn user of any conflict within assigned schedules.

L. The Configuration UI shall provide the capability to set a PTZ protocol to a specific DVS serial port and shall allow mixing domes of various manufacturers within a system.

M. User shall have the ability to configure a return to home function after a predefined time of inactivity for PTZ cameras. This period of inactivity time shall be configurable from 1 to 7200 seconds.

VMS CLIENT USER INTERFACE (UI)

22.01 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.

22.02 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.

22.03 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. A dynamic controls section loaded with entity-specific widgets (e.g., 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.

22.04 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.

22.05 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.

22.06 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.

22.07 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. Controls section with widgets.

22.08 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

22.09 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 his or her 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 (for example one 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.

22.10 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.

22.11 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.

22.12 THE MONITORING UI SHALL INCLUDE ADVANCED VIDEO CAPABILITIES, INCLUDING:

A. Advanced live video viewing functionality.

B. Advanced archive playing and video playback functionality.

C. Monitoring and management of video system events and alarms.

D. Intercom or duplex audio.

E. Generation of video reports.

F. Control of PTZ cameras.

G. Creating and monitoring archive transfer requests.

H. Display metadata overlaid on live or playback video.

22.13 THE MONITORING UI SHALL LEVERAGE THE GRAPHICAL PROCESSING UNIT (GPU) FOR VIDEO DECODING.

A. The following GPU technologies shall be supported:
   1. NVidia CUDA
   2. Intel Quick Sync

B. The Monitoring UI shall have the ability to decode video through the optimal simultaneous use of the GPU and Computer Processing Units (CPU).

22.14 THE LIVE VIDEO VIEWING CAPABILITIES OF THE MONITORING UI SHALL INCLUDE:

A. The ability to display all cameras attached to the USP and all cameras attached to federated systems.

B. Support for live video monitoring on each and every display tile within a task in the user's workspace.

C. The USP shall support uninterrupted video streaming. The CSA shall keep existing video connections active in the event that an SSM (except Archiver) becomes unavailable.

D. The ability to drag and drop a camera into a display tile for live viewing.

E. The ability to drag and drop a camera into a display tile for live viewing on an analog monitor connected to an IP hardware decoder (converting an IP encoded stream into an analog video signal).

F. The ability to drag and drop a camera from a map into a display tile for live viewing.

G. Support for digital zoom on live camera video streams.

H. The ability for audio communication with video units with audio input and output.

I. The ability to control pan-tilt-zoom, iris, focus, and presets.

J. The ability to bookmark important events for later retrieval on any archiving camera and to uniquely name each bookmark in order to facilitate future searches.

K. The ability to start/stop recording on any camera in the system that is configured to allow manual recording by clicking on a single button.

L. The ability to activate or de-activate viewing of all system events as they occur.

M. The ability to switch to instant replay of the video for any archiving camera with the simple click of button.

N. The ability to take snapshots of live video and be able to save or print the snapshots.

O. The ability to view the same camera multiple times in different tiles.

22.15 THE VIDEO PLAYBACK (ARCHIVE PLAYING) CAPABILITIES OF THE MONITORING UI SHALL INCLUDE:

A. Support for audio and video playback for any time span.

B. Support for video playback on each and every display tile.

C. The ability to instantly replay the video for any archiving camera with the simple click of a button.

D. The ability to select between instant synch of all video streams in playback mode, allowing operators to view events from multiple angles or across several camera fields, or non-synchronous playback.

E. The ability to simultaneously view the same camera in multiple tiles at different time intervals.

F. The ability to control playback with:
   1. Pause
   2. Lock Speed
   3. Forward and Reverse Playback at: 1x, 2x, 4x, 6x, 8x, 10x, 20x, 40x, 100x
   4. Forward and Reverse Playback frame by frame
   5. Slow Forward and Reverse Playback at: 1/8x, 1/4x, 1/3x, 1/2x
   6. Loop playback between two time markers

G. The ability to display a single timeline or one timeline for each selected video stream, which would allow the operator to navigate through the video sequence by simply clicking on any point in the timeline.

H. The ability to display the level of motion at any point on a timeline.

I. The ability to clearly display bookmarked events on the timeline(s).

J. The ability to query archived video using various search criteria, including, but not limited to, time, date, camera, and area.

K. The tool necessary for searching video and associated audio based on user-defined events or motion parameters.

L. The ability to define an area of the video field in which to search for motion as well as define the amount of motion that will trigger search results. The Monitoring UI shall then retrieve all archived video streams that contain motion that meets the search parameters. There shall be a graphical timeline on which the time of each search hit shall be indicated.

M. The ability to browse through a list of all bookmarks created on the system and select any bookmarked event for viewing.

N. The ability to add bookmarks to previously archived video for easier searching and retrieval.

O. Support for digital zoom on playback video streams.

P. Still image export to PNG, JPEG, GIF, and BMP format with Date and Time stamp, and Camera Name on the image (snapshot).

Q. Tools for exporting video and a self-contained video player on various media such as USB keys or CD/DVD-ROM. This video player shall be easy to use without training and shall still support reviewing video metadata, such as bookmark, or navigating the video with functions like panoramic camera view dewarping.

R. Tools for exporting video sequences in standard video formats, such as ASF or MP4.

S. The ability to encrypt exported video files.

T. The ability for an operator to load previously exported video files from their computer or network.

U. The ability for queries to be saved upon closing the CSA and reappear when the application is reopened.

V. The ability to dynamically block, on demand, video stream dynamically to lower-level users to prevent access, for a specific time, to live and recorded video.

W. A tool building and exporting a set of videos into a single container. This tool shall allow the operator to build sequences of video to create a storyboard and allow the export of synchronous cameras.

X. The ability to store the video export and still image export at a pre-defined storage location.

Y. An interface with the ability to list, search, and manipulate previously generated video exports.

Z. The ability to export sequences of video in open standards including ASF and MP4.

22.16 THE MONITORING UI SHALL PROVIDE AN INTERFACE TO SUPPORT THE FOLLOWING ALPR TASKS AND CAPABILITIES:

A. Monitoring and management of ALPR events and alarms.

B. Viewing of license plate picture(s) and context images.

C. Viewing of license plate data (e.g., license plate reads)

D. Verification of ALPR data against live and recorded video.

22.17 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 and/or event list layout.

C. It shall be possible to lock a Monitoring UI display tile so that it only tracks the activity of a specific entity (e.g., 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.

22.18 DISPLAY TILE PACKING AND UNPACKING:

A. The Monitoring UI shall support single-click unpacking and packing for ALPR hits, ALPR reads, areas, doors, zones, camera sequences, 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.

22.19 VISUAL TRACKING:

A. The Monitoring UI shall support the ability to manually track a moving target with the single click of a button.

B. The ability to switch from one camera view to an adjacent camera shall be done within a single display tile.

C. Switching between camera streams shall be accomplished by simply clicking on a semi-transparent shape or overlay.

D. Visual tracking shall be available with both live and recorded video.

SERVER ADMINISTRATOR USER INTERFACE REQUIREMENTS

23.01 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.

23.02 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.

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

23.04 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.

G. Configure system SMTP settings (mail server and port).

H. Configure event and alarm history storage options.

UNIFIED WEB CLIENT (UWC) GENERAL REQUIREMENTS

24.01 THE USP SHALL SUPPORT A UNIFIED WEB CLIENT (UWC) FOR ACCESS CONTROL AND VIDEO.

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

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

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

24.05 THE UWC SHALL SUPPORT DISPLAY ON TABLET FORMAT.

24.06 THE UWC SHALL SUPPORT NATIVE H.264 VIDEO IN THE WEB CLIENT.

24.07 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.

24.08 THE CONTRACTOR SHALL PROVIDE UP TO 5 NUMBER OF SIMULTANEOUS WEB CLIENTS.

24.09 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.

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

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

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

24.13 FUNCTIONALITIES:

A. Log in support shall be available using:
   1. Username and password
   2. Active Directory.
      (First integration included, additional licenses required for more)
   3. Ability for user to change their password.

B. Encrypted communications for all transactions.

C. Print reports and export to CSV file.

D. Customer logo customization shall be available for multi-tenant and hosted services applications.

E. Video:
   1. Live and playback video at 320 x 240, 640 x 480 or 1280 x 1024 @ 15 fps
   2. Video export
   3. 1, 4, 6 or 9 tiles
   4. Basic PTZ Controls (Pan/Tilt, Zoom, go to presets, start pattern)
   5. Start / Stop recording
   6. Sample web page for customers to see how to view video for their own development
   7. Add bookmarks

F. Alarms:
   1. Alarm report

G. Threat Level.

SMARTPHONE AND TABLET APP GENERAL REQUIREMENTS

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

25.02 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.

25.03 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

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

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

25.06 FUNCTIONALITIES:

A. Core
   1. Ability to logon/logoff to the USP using an authorized user 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 four 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, 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 ad door lock state.
2. Ability to perform actions on a door such as unlock the door, set the door in maintenance mode, override the door unlocking schedule.
3. Ability to monitor live cardholder activities per door, such as cardholder name, pictures, access denied and reason for access denied.

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 (Included w enterprise)
1. Ability to display a geographic map with USP entities geo-located on the map.
2. Ability to view any entity configured on the map.
3. Ability to search entities or location on the map.

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

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

25.09 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

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

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

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

26.04 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.

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

26.06 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.

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

26.08 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.

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

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

SESSION INITIATION PROTOCOL (SIP) COMMUNICATION MANAGEMENT (CM)

27.01 AN OPERATOR OF THE USP SHALL BE ABLE TO, WITHIN THE USP MONITORING UI, INITIATE CALLS TO AND ANSWER CALLS FROM OTHER OPERATOR AND EDGE VOICE DEVICES SUCH AS INTERCOMS, EMERGENCY CALL STATIONS, INFORMATION DESKS, SOFTPHONES, OR PHONE DEVICES.

27.02 THE USP SHALL SUPPORT CM BETWEEN THE USP CLIENT USER INTERFACE AND SIP ENDPOINT DEVICES.

27.03 SIP ENDPOINTS SHALL BE ABLE TO REGISTER TO THE USP USING A STANDARD SIP PROTOCOL.

27.04 THE USP SHALL SUPPORT CM BETWEEN TWO SIP ENDPOINT DEVICES.

27.05 THE USP SHALL ALLOW THE CONFIGURATION OF SIP TRUNK CONNECTIONS TO MULTIPLE SIP SERVERS SUPPORTING SIP TRUNKS.

27.06 THE CM SHALL SUPPORT THE MANAGEMENT OF CALLS TO AND FROM OTHER SIP SERVERS CONNECTED THOUGH SIP TRUNKS.

27.07 THE USP SHALL SUPPORT THE CONFIGURATION OF PAGING ZONES FOR PRE-RECORDED AND LIVE MESSAGE ANNOUNCEMENTS.

27.08 THE CM IS A SERVICE OF THE USP AND SHALL NOT REQUIRE THE ADDITION OF ANY THIRD-PARTY SOFTWARE.

27.09 THE CM SHALL SUPPORT THE FOLLOWING VIDEO CODECS:

A. H.264
B. H.263
C. H.263+ (1998)

27.10 THE CM SHALL SUPPORT THE FOLLOWING AUDIO CODECS:

A. PCMA (G.711 aLaw)
B. PCMU (G.711 uLaw)
C. G.722
D. G.729
E. iLBC
F. GSM
G. telephone event
H. Speex (Narrowband)

I. Speex (Wideband)
J. Speex (Ultrawideband)
K. L.16
L. L.16-44-1
M. G.728
N. G.726-16
O. G.726-24
P. G.726-32
Q. G.723
R. G.726-40

27.11 THE CM SHALL CERTIFY SIP DEVICES FROM THE FOLLOWING MANUFACTURERS:

A. 2N Telekomunikace
B. Algo
C. Axis
D. Baudisch
E. Castel
F. Cisco
G. Code Blue
H. Commend
I. EMCOM
J. Grandstream networks
K. Jacques
L. Mobotix
M. Siedle
N. TalkaPhone
O. TOA Corporation
P. Valcom
Q. Vingtor-Stentofon
R. Zenitel
S. Intelbras

27.12 THE CM SHALL ALLOW BIDIRECTIONAL AUDIO AND VIDEO RECORDING OF CALL SESSIONS. THE USP SHALL OFFER THE FOLLOWING RECORDING CAPABILITIES:

A. Automatic cleanup of call session files after a programmable number of days.
B. Deactivation of call recording between operators.
C. Deactivation of call recording with specific operators.
D. Deactivation of call recording with specific voice devices.
E. Selection of the storage path for call session recordings.

27.13 THE CM SHALL PROVIDE THE CAPABILITY TO REACH A PHYSICAL LOCATION IDENTIFIED BY ITS OWN EXTENSION NUMBER REGARDLESS OF THE USER CONNECTED TO THE USP.

27.14 THE CM SHALL PROVIDE THE FLEXIBILITY FOR THE ADMINISTRATOR TO DEFINE THE NETWORK PORTS USED TO COMMUNICATE BETWEEN THE USP SERVERS AND THE FOLLOWING:

A. USP Operator Client User Interfaces

B. SIP devices

C. SIP servers

27.15 THE CM SHALL PROVIDE THE CAPABILITY TO CREATE RING GROUPS. A RING GROUP IS A GROUP OF CALL NUMBERS GROUPED UNDER A SINGLE CALL NUMBER. IT SHALL BE POSSIBLE TO SET A RING GROUP TO SIMULTANEOUSLY OR SEQUENTIALLY CALL THE MEMBERS OF THE GROUP. DWELL TIME FOR SEQUENCE MODE SHALL BE CONFIGURABLE.

27.16 THE CM SHALL ALLOW THE AUTOMATIC ROUTING OF CALLS THROUGH THE CONFIGURATION OF A COLLECTION OF RULES (DIAL PLAN). DIAL PLANS SHALL SUPPORT THE FOLLOWING CAPABILITIES:

A. Match a phone number with regular expression.

B. Route calls based on matching the phone numbers from which calls are made.

C. Route calls based on matching the destination phone numbers to which calls are made.

D. Change the phone extension from which calls are received.

E. Change the phone extensions to which calls are sent.

F. A combination of any of the above capabilities in a configured priority and based on a schedule.

27.17 DIAL PLANS SHALL BE APPLICABLE TO CALLS BETWEEN SIP ENTITIES REGISTERED TO THE USP AS WELL AS TO AND FROM EXTERNAL SIP SERVERS.

27.18 THE USP SHALL UNIFY, WITHIN A SIMPLE USER INTERFACE, THE WORKFLOW BETWEEN THE ASSOCIATED SECURITY ENTITIES OF A CALL SESSION, INCLUDING THE CALL BOX, CAMERAS, DOORS, INTRUSION ZONES AND OUTPUTS.

27.19 THE USP SHALL SUPPORT VIDEO AND AUDIO CALLS:

A. Between USP Client User Interfaces

B. To and from USP Client User Interfaces and SIP devices

C. Between SIP devices

27.20 THE USP SHALL PROVIDE AN ADVANCED AND FRIENDLY CALL MANAGEMENT USER INTERFACE THAT ALLOWS OPERATORS TO:

A. Connect standard USB headsets and webcams to USP Client User Interface workstations so that USP users can make voice and video calls through the USP Client User Interface.

B. Display the video associated with the call and switch between multiple video sources.

C. Receive incoming call notifications directly through a notification tray.

D. Initiate, answer, forward, place on hold, or cancel calls from a dedicated call dialog box.

E. Control cameras, doors, zones, and device outputs during a call.

F. Create a customizable list of contacts, so that users can quickly call their contacts. Contact lists shall include other USP users, as well as SIP devices.

G. Dial a phone number to make a call.

H. Dial a DTMF sequence during a call.

I. Monitor the availability status of a user and set its own availability status.

J. Access a history log of calls that the operator both initiated and received. This log shall show the time of the call, duration, direction and the reason for its ending. It shall be possible to redial one of the entries in the log.

27.21 THE USP SHALL ALLOW AN OPERATOR TO MANAGE UP TO 10 CALLS SIMULTANEOUSLY. THE CALL QUEUE SHALL SHOW THE STATUS OF EACH CALL: INCOMING, IN CALL, OR ON HOLD. IT SHALL BE POSSIBLE TO HOLD AND RESUME A CALL DIRECTLY FROM THE CALL QUEUE.

27.22 THE USP SHALL OFFER A CALL WINDOW. IT SHALL BE POSSIBLE WITHIN THE CALL WINDOWS TO:

A. Switch between cameras associated with the call participant.

B. Open and lock doors associated with the call participant.

C. Arm and Disarm zones associated with the call participant.

D. Trigger outputs associated with the call participant.

E. Put on hold, resume, forward, and end a call.

F. Mute the microphone.

G. Hide the webcam video feed.

27.23 THE USP SHALL HAVE A BUILT-IN ADDRESS BOOK. THE ADDRESS BOOK SHALL BE AVAILABLE IN THE CALL DIALOG BOX, IN WHICH USERS CAN VIEW AND MANAGE THEIR LIST OF CONTACTS. FROM THE ADDRESS BOOK, USERS SHALL BE ABLE TO DO THE FOLLOWING:

A. Call a contact by simply double-clicking the contact name.

B. See the availability status of their contacts (users and SIP Devices).

C. Quickly display a contact's information, such as photo, name, and number.

D. Filter their contacts by type (SIP Device or User).

E. Create a list of favorites by adding and removing contacts.

F. Search for and call numbers that appear in the contact list.

27.24 THE USP SHALL PROVIDE A GRAPHICAL DIAL PAD TO ALLOW THE OPERATOR TO MAKE CALLS AND DIAL DTMF TONES DURING A CALL.

27.25 THE USP SHALL PROVIDE THE ABILITY TO SEND PUBLIC ANNOUNCEMENTS VIA A MICROPHONE OR UPLOADED PRE-RECORDED MESSAGES. THE USERS SHALL BE ABLE TO DO THE FOLLOWING:

A. Create paging zones.

B. Associate any SIP callable entity with a paging zone.

C. Upload pre-recorded messages.

D. Trigger a live or pre-recorded message.

27.26 THE USP SHALL PROVIDE CALL REPORTING CAPABILITIES TO ALLOW FOR THE INVESTIGATION OF THE ACTIVITIES DURING SPECIFIC CALL SESSIONS. THE REPORT SHALL PROVIDE THE CAPABILITY TO REPLAY AUDIO RECORDINGS AND WATCH CALL SESSIONS THAT HAVE ASSOCIATED VIDEO. THE CALL REPORT SHALL PROVIDE FILTERS TO QUERY THE CALL RECORDS BY:

A. Date and time

B. Call session duration

C. Involved users and call stations

D. Call events and actions

E. Actions taken by a user on doors, intrusion zones, and outputs during the call session

27.27 THE USP SHALL GIVE THE CAPABILITY TO EXPORT A CALL SESSION, INCLUDING BIDIRECTIONAL AUDIO, ASSOCIATED VIDEO, AND LOG JOURNAL OF THE CALL SESSION.

27.28 IT SHALL BE POSSIBLE TO PLACE THE VOICE DEVICES AS ICONS ON A MAP THAT SHALL DISPLAY THE CALL STATUS OF THE VOICE DEVICE WITH A COLOR CODE. A RIGHT CLICK ON THE VOICE DEVICE MAP ICON SHALL ALLOW THE USER TO:

A. Answer or reject an incoming call.

B. Initiate a call to the device.

C. Put on hold and resume a call with the device.

27.29 IT SHALL BE POSSIBLE FOR AN OPERATOR TO SELECT AND BROADCAST HIS OR HER AVAILABILITY STATUS, WITH THE POSSIBLE STATUSES BEING AVAILABLE, AWAY AND BUSY. THIS STATUS WILL APPEAR WITH A COLOR CODE IN THE CALL DIALOG BOX OF OTHER OPERATORS.

27.30 THE CONTRACTOR SHALL PROVIDE UP TO 5 NUMBER OF SIP CONNECTIONS.

27.31 IT SHALL BE POSSIBLE TO DO A FAILOVER AND BIDIRECTIONAL AUDIO AND VIDEO RECORDING FOR EACH SIP DEVICE.

27.32 IT SHALL BE POSSIBLE TO DO SIP PUBLIC ADDRESS.

27.33 THE CM SHALL PROVIDE THE ABILITY TO BROADCAST PUBLIC ADDRESSING MESSAGES TO A COLLECTION OF SIP DEVICES INCLUDED IN A PAGING ZONE. THE PA (PUBLIC ADDRESS) FEATURE SHALL SUPPORT THE FOLLOWING CAPABILITY:

A. Define paging zones and assign SIP entities for each of them

B. Broadcast live and pre-recorded messages

USP GENERAL REQUIREMENTS

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

28.02 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.

28.03 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, additional licenses required for more)

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

I. Integration with third party video analytics systems via plug-ins (Additional license required)

J. Dynamic graphical map viewing.

28.04 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, ALPR, or video platform.

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

D. Standalone video platform that federates multiple independent remote VMS.

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

F. Standalone access control that federates multiple independent remote ALPR.

28.05 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.

28.06 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

29.01 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).

29.02 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.

29.03 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.

29.04 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.

29.05 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)

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

29.07 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)

29.08 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.

29.09 THE USP SHALL SUPPORT UNINTERRUPTED VIDEO STREAMING. THE CSA SHALL KEEP EXISTING VIDEO CONNECTIONS ACTIVE IN THE EVENT THAT AN SSM (EXCEPT ARCHIVER) BECOMES UNAVAILABLE.

29.10 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 (e.g., 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. 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. (First integration included, additional licenses required for more)
    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, ALPR, video, 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.
6. The Web Server Role shall be responsible for managing incoming Web Client connection and hosting the web pages for the Web Client. The Web Server Role acts as a proxy for the client connections and can be installed in a DMZ for additional security.
7. The Media Gateway Role shall be responsible for connecting any video stream to a third-party system using standard RTSP/RTSPS protocol. This role shall provide access to live and playback video. (Requires the SDK packages, additional license required)

29.11 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

30.01 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.

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

30.03 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.

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

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

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

30.07 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.

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

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

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

30.11 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.

30.12 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.

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

30.14 THE USER SHALL BE ABLE TO SPONTANEOUSLY TRIGGER ALARMS BASED ON SOMETHING THEY SEE IN THE SYSTEM.

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

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

USP THREAT LEVELS

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

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

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

31.04 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.

31.05 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).

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

USP REMOTE TASK

32.01 THE USP SHALL PROVIDE, THROUGH A REMOTE TASK, CAPABILITIES TO REMOTELY MONITOR AND CONTROL THE CONTENT OF OTHER WORKSTATIONS RUNNING THE CSA (MONITORING UI) THAT ARE PART OF THE SAME SYSTEM.

32.02 THE USP SHALL SUPPORT VIDEO WALL APPLICATIONS BY CONNECTING AND CONTROLLING MULTIPLE WORKSTATIONS AND MONITORS SIMULTANEOUSLY.

32.03 THE REMOTE TASK SHALL BE A GRAPHICAL INTERFACE SHOWING A REPLICATION OF THE REMOTE WORKSTATION RUNNING THE CSA (MONITORING UI).

32.04 THE REMOTE TASK SHALL ALLOW THE CONNECTION TO OTHER WORKSTATIONS USING A LOW BANDWIDTH MODE TO RECEIVE ONLY SNAPSHOTS OF VIDEO VIEWED REMOTELY.

32.05 THE REMOTE TASK SHALL ALLOW THE CONNECTION TO OTHER WORKSTATIONS USING A SPY MODE TO REMAIN INVISIBLE TO THE REMOTELY CONNECTED WORKSTATION. THE SPY MODE OPTION SHOULD BE AVAILABLE TO THE USER WITH PERMISSION TO ACCESS THE FEATURE.

32.06 THE FUNCTIONALITY PROVIDED BY THE REMOTE MONITORING AND CONTROL CAPABILITY SHALL INCLUDE:

A. Remote monitoring and control of the monitoring and alarm monitoring tasks.
B. Ability to remotely switch cameras, doors and zones into display tiles.
C. Ability to remotely control live and playback video.
D. Ability to remotely change the tile pattern.
E. Ability to remotely create and delete tasks.
F. Ability to remotely start/stop task cycling.
G. Ability to remotely go into full screen mode.
H. Ability to remotely save and reload the workspace.

USP ADVANCED TASK MANAGEMENT

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

33.02 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.

33.03 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.

33.04 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.

33.05 OPERATORS SHALL BE ABLE TO DUPLICATE A TASK.

USP REPORTING

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

34.02 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.

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

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

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

34.06 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

34.07 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.

34.08 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.

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

34.10 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.

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

34.12 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.

USP DASHBOARDS

35.01 THE USP SHALL SUPPORT THE ABILITY TO CREATE DASHBOARDS.

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

35.03 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.

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

35.05 A DASHBOARD SHALL CONSIST OF A CANVAS WITH CARIOUS 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.

35.06 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.

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

35.08 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)

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

36.02 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.

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

36.04 ENTITIES THAT SHALL BE 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).

36.05 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.

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

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

36.08 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

37.01 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.

37.02 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.

37.03 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.

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

37.05 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.

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

37.07 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. IO 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

38.01 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.

38.02 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

38.03 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.

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

38.05 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.

38.06 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.

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

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

38.09 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.

38.10 IT SHALL BE POSSIBLE TO REVIEW USER 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 user group or user is allowed to perform the underlying action.

USP EVENT/ACTION MANAGEMENT

39.01 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.

39.02 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.

39.03 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. Unit events

E. Zone events

F. Alarm events

G. ALPR events

H. Health Monitoring events

39.04 THE USP SHALL ALLOW THE CREATION OF CUSTOM EVENTS.

39.05 THE USP SHALL HAVE THE CAPABILITY TO EXECUTE AN ACTION IN RESPONSE TO AN ACCESS CONTROL, VIDEO, AND ALPR EVENT. THE USP SHALL SUPPORT THE FOLLOWING LIST OF ACTIONS, WITHOUT BEING LIMITED TO:

A. Add bookmark

B. Arm intrusion detection area

C. Arm zone

D. Block and unblock video

E. Bypass input

F. Cancel postpone intrusion detection area arming

G. Clear input bypass

H. Clear task

I. Display a camera on an analog monitor

J. Display an entity in the CSA

K. Email a report

L. Email a snapshot

M. Export report
N. Forgives antipassback violation
O. Go home
P. Go to preset
Q. Import from file
R. Override recording quality
S. Override with event recording quality
T. Override with manual recording quality
U. Play a sound
V. Postpone intrusion detection area arming
W. Reboot unit
X. Recording quality as standard configuration
Y. Rest area people count
Z. Reset parking zone inventory
AA. Run a macro
BB. Run a pattern
CC. Send a message
DD. Send a task
EE. Send an email
FF. Set parking zone occupancy
GG. Set reader mode
HH. Set the door maintenance mode
II. Set threat level
JJ. Start/Stop applying video protection
KK. Start/Stop recording
LL. Start/Stop transfer
MM. Synchronize role
NN. Temporary override elevator schedules
OO. Trigger intrusion alarm
PP. Trigger alarm
QQ. Trigger output
RR. Trigger read
SS. Unlock door explicitly

39.06 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

40.01 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.

40.02 SCHEDULED TASKS

A. The USP shall support scheduled tasks for 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 or emailing a report.

USP MACROS AND CUSTOM SCRIPTS

41.01 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.

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

41.03 A MACRO SHALL BE EXECUTED EITHER AUTOMATICALLY OR MANUALLY.

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

USP DYNAMIC GRAPHICAL MAPS (DGM)

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

42.02 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.

42.03 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.

42.04 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 (WTMS) and Web Map Service (WMS) defined by the Open Geospatial Consortium (OGC)

E. BeNomad

F. AutoCAD (DWG & DXF)

42.05 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

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

42.07 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

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

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

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

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

42.11 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.

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

42.13 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.

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

42.15 THE DGM SHALL PROVIDE THE ABILITY TO IMPORT CONFIGURATION FROM AN ETERNAL FILE SUCH AS:

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

42.16 THE DGM SHALL OFFER FAILOVER CAPABILITIES.

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

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

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

42.20 THE DGM SHALL PROVIDE A 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 zoom level of the map.

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

42.21 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.

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

42.23 THE DGM SHALL OFFER A SMART SELECTION TOO 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 TOO SHALL TAKE OBSTACLES INTO CONSIDERATION AND NOT DISPLAY CAMERAS THAT CANNOT SEE THE LOCATION BECAUSE OF A WALL.

42.24 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 OR INTEREST AT ONCE.

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

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

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

42.28 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.

42.29 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.

42.30 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 provider)

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

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

42.33 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.

42.34 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.

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

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

42.37 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.

42.38 THROUGH THE FOLLOWING FUNCTIONALITIES, 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.

42.39 IT SHALL BE POSSIBLE TO ADD ADVANCED FUNCTIONALITY TO MAP OBJECTS USING THE SDK. ANY FUNCTIONALITY AVAILABLE THROUGH THE USP SDK SHALL BE AVAILABLE WITHIN MAPS.

42.40 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 location in a single click.

C. Editing multiple entities at one location simultaneously.

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

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

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

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

USP DIGITAL EVIDENCE MANAGEMENT SYSTEM (DEMS) SEPARATE SUBSCRIPTION TO GENETEC CLEARANCE REQUIRED.

43.01 THE USP SHALL SUPPORT THE ABILITY TO ELECTRONICALLY SHARE VIDEO EXPORTS WITH THIRD PARTIES.

43.02 THE USP SHALL ALLOW RECIPIENTS TO NATIVELY REVIEW EXPORTED VIDEO FROM A WEB BROWSER, WITHOUT THE NEED TO INSTALL SOFTWARE OR BROWSER PLUGINS.

43.03 VIDEO EXPORTED FROM THE UPS WILL INCLUDE THE ORIGINAL FILE AND TIMESTAMP INFORMATION, AS WELL AS THE SYSTEM, WORKSTATION, AND CAMERA SOURCE METADATA THAT CAN BE VIEWED FROM THE DEMS.

43.04 THE USP SHALL SUPPORT THE ABILITY TO CREATE A CASE WITHIN THE DEMS, AND ASSIGN ASSOCIATED INCIDENT DETAILS, WHEN EXPORTING VIDEO.

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.

USP DATA INGESTION

46.01 THE 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 DEFINED BY A SET OF FIELDS AND FIELD TYPES THAT DESCRIBE THE DATA SOURCE. FIELD TYPES SHALL BE:

A. String

B. 32 bit & 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 SHALL BE:

A. Which fields are displayed or hidden

B. What order are the fields displayed

C. A label to specify the name of the field (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 / DENY ACCESS TO SPECIFIC USER & 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 be able to connect to and synchronize data from multiple Active Directory servers (up to 10).

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

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

F. 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.

G. 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. Active Directory attributes to USP custom fields

H. 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.

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

J. The USP shall support user connections across independent organizations by connecting to an 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:
   1. Video analytics
   2. Third-party video systems
   3. ALPR integrations with pay stations, permit vendors, pay-by-phone vendors, and ticketing vendors
   4. Access Control ecosystem (such as ID scanner, card synchronization, Guardtour, Morpho Biometrics, Advanced Enrollment)
   5. Industrial IoT: Data ingestion from external devices through standard communication protocols (Modbus, BACnet, OPC, SNMP, HTTP Server, MQTT Client, TCP Server)
   6. Industrial Protocol Interface: Data exposure from GSC to external protocol interfaces using standard communication protocols (BACnet, SNMP)
   7. Videowall (Barco, Eizo)
   8. Intelligent Keys (Salto SVN, Medeco XT, CLIQ, ILOQ (future))
   9. Gunshot Detection (Shot Spotter, Guardian GunShot)
   10. Dynamic Logbook: Customizable forms with reporting capabilities

USP SOFTWARE DEVELOPMENT KIT (SDK)

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 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.

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

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

48.07 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.

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

48.09 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.

48.10 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.

48.11 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.

48.12 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 23 00