CCSD21 Security Camera and Door Access RFP Specifications

Video Management, IP Camera, and Card Access Specifications

- Please note building maps will outline detailed locations and specifications.
- CCSD21 school ceilings are mostly 2x4 suspended acoustical ceiling tiles on a grid and 2x2 in offices suites and limited other areas. Most ceilings are 8' on most second floors up to 9' on first floors and a limited number of 2nd floor spaces. Spaces such as gyms, libraries, multi-purpose, etc. are at various taller heights.

Minimum Required Specific Components:

- **Prime Contractor Requirements**: Illinois Licensed Alarm Agency, Current Genetec Unified Elite Partner, Located within 60 miles of the CCSD21

Base Bid: IP Camera System

- VMS: Provide Genetec Security Center 5.7, GSC Omnicast™ Enterprise Package, GSC Synergis™ Enterprise Package, Site License for Genetec Security Desk client connections, 10 1 Security Center Mobile app, Advanced Plan Manager for GIS Map, GSC-THREATLEVELS, Security Center Active Directory, Federation License, 13 Bosch B/G Series intrusion control panel connections, 2 1 RF Ideas USB enrollment reader.

- **Cameras:** Provide as listed on CCSD21 Site Drawings and Specifications as well as CCSD21 Component Inventory and Parts List. Mounting hardware as required.

- **Servers: Per school:** Provide 1 Streamvault Archiver SV-4001. Or 1 HP Proliant DL360HP Proliant DL380 Archiver. SATA Drives for archiving, solid state drive for OS.
    - For proper sizing the following parameters must be utilized: 30 days of storage, 15 Frames per second, 75 % motion, native resolution. (See attachment for exact part number and server sizing)

- **Directory Server at District MDF:** Provide HP Proliant DL360

- **POE + Switches:** Supplied by CCSD21. The District's network consists of 14 buildings/sites. All sites are connected via the District's fiber based WAN provided by AT&T. 1 Gbps WAN connections are in place between the Gill Administration Center and the other facilities. By the start of this project, there will be a 3 Gbps shared Internet connection for all 14 sites.

    - **Data Network - For Reference Only**

        A. Current network has extreme high reliability of above 99.99%.
        B. The network is primarily used for data, video, and other cloud-based web applications.
        C. Current routers - Cisco ISR 4431
        D. Current core switching - Redundant Cisco Catalyst 3850 switches
        E. Current access switching - Meraki 350x and Cisco 2960x PoE switches
            a. There are available switch ports in each building to accommodate cameras
        F. Current Access Points - Meraki MR-53 access points

- **Security Workstation and Monitor:** Provide one per school unless illustrated otherwise: Small

form factor HP ProDesk 400G4 with mounting sleeve, mounted to back of Monitor: Samsung 50" UN50NU7100F with wall mount

- **Racks & UPS:** Supplied by CCSD21
- **Patch panels and patch cables:** Provide 24 Port Empty Patch Panel - AX103114, 24 Port Cat6 Patch Panel - AX103253, 48 Port Empty Patch Panel - AX103115,2' patch cord- C601106002
- **Cabling -** Provide Cat 6 Plenum Belden 2413 Desired - District to provide color
- **Warranty and Maintenance -** Provide a five-year Software Maintenance Agreement from Genetec (Genetec Advantage) and one year warranty on all parts and labor.
- **Installation and Training –** Provide entire project planning and installation as well as 24 hours of administrator and end user training. Installation shall include entire scope including cabling, mounting and connectivity, configuration, and cutover/testing. Vendor must provide detailed documentation with drawings, configurations, manuals, and any credentials needed.

  ****As built drawings to be provided in CAD format**

Alternate Bid: Door Access Control:

- **Genetec Security Center Synergis Enterprise Package,** Site License for Genetec Security Desk client connections, 10 1 Security Center Mobile app, Advanced Plan Manager for GIS Map, GSC-THREATLEVELS, Security Center Active Directory, 13 Bosch B/G Serie intrusion control panel connections, 2 1 RF Ideas USB enrollment reader
- **Electronics Hardware:** Mercury based with CloudLink per school, Altronix Trove Cabinet and power supply with supply with individually fused power for strikes.
- **Readers, REX, and door contacts per drawings;**
- **Door hardware: Not in this scope of work!** Folger Adams is district standard. Strike or Mag Lock as required.
- **Card credentials:** Provide 3500 IClass dual sided, glossy, pre-punched
- **Access Control Server:** Provided by district.
- **Readers associated with ADA Access must be interfaced with ADA Door Operators for proper operation.**
- **Full integration with Intrusion panels is required, all door opening will be illustrated.**
- **Warranty -** Provide a five-year Software Maintenance Agreement from Genetec and one year warranty on all parts and labor.

  ****As build drawings to be provided in CAD format**

- **Badge printer:** 2 required: Fargo DTC4500E Dual SIDE PTR W/O LOCKING HOPPE. 4- Fargo 45210 MCKOK FULLCOLOR RIBBON FOR DTC4500E/5, 2 Cleaning Kits86177. Workstation, camera by owner.

- **Installation and Training –** Provide entire project planning and installation as well as 24 hours of administrator and end user training. Installation shall include entire scope including cabling, mounting and connectivity, configuration, and cutover/testing. Vendor must provide detailed documentation with drawings, configurations, manuals, and any credentials needed.

Visitor Management: Stand Alone

Provide 1 Per School, workstation by owner. PassagePoint Global with license and 1 year support. Dymo LabelWriter 450 Printer, ScanSel R2 License Scanner, 4-Adhesive Name Badge Label w/ Clip Hole - 2 1/4" X 4" Blank White (250 per roll) DYMO 30857 Compatible

Table of Contents

Section 28 13 00 – Access Control Software and Database Management

Part 1 - General

1.01 Related Work

A. Door Hardware- By this contract, door stikes or mag locks as required. District Standard is Folger Adams

B. Section 28 23 00 – Video Surveillance

1.02 Definitions

A. ACS – Access Control System

B. CSA – Client Software Application

C. DGM – Dynamic Graphical Maps

D. ALPR – Automatic License Plate Recognition

E. SDK – Software Development Kit

F. GLM – Genetec Lifecycle Management

G. SSM – Server Software Module

H. UI – User Interface

I. USP – Unified Security Platform

J. USW – Unified Web Client

K. VMS – Video Management System

1.03 Qualifications

A. The system programmer shall have attended manufacturer training and obtained certification in Genetec™ Security Center - Synergis™ Technical Certification.

B. Optionally, the system programmer shall have attended manufacturer training and obtained certification in Genetec Security Center - Enterprise Technical Certification.

C. The system programmer shall be a Genetec certified partner with the following level of qualification: No exceptions and proof of the certification shall be submitted with the bid.

a. Unified Elite Reseller

Part 2 - Products

2.01 Electronic Access Control System General Requirements

A. The ACS shall be an enterprise class IP access control software solution. It shall be fully embedded within a Unified Security Platform (USP). The USP shall allow the seamless unification of the ACS with an IP video management system (VMS).

B. The ACS shall be highly scalable to support configurations consisting of thousands of doors with facilities spanning multiple geographic areas.

C. The ACS shall support an unrestricted number of logs and historical transactions (events and alarms) with the maximum allowed being limited by the amount of hard disk space available.

D. The ACS shall support a variety of access control functionalities, including but not limited to:

1. Controller (Unit) management, door management, elevator management, and area management.
2. Cardholder and cardholder group management, credential management, and access rule management.
3. Badge printing and template creation.
4. Visitor Management shall be PassPoint Edu by Stopware
5. People counting, area presence tracking, and mustering.
6. Offering a framework for third party hardware integration such as card and signature scanner.

E. Manufacturer:

1. Genetec Security Center:
    a. Synergis Enterprise
    b. Site License for unlimited clients

F. Certification

1. The ACS shall be certified
    a. UL-294
    b. ULC-S319
    c. EN-60839-11-1

2.02 ACS Access Management

A. The ACS shall be based on an open architecture able to support multiple access control hardware manufacturers. The ACS shall be able to integrate with multiple non-proprietary interface modules and controllers, access readers, and other third party applications.

B. The ACS shall be an IP enabled solution. All communication between the ACS and hardware controllers shall be based on standard TCP/IP protocol.

C. Access Manager Role

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

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

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

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

D. The Access Server shall store all access events associated with the doors, areas, hardware zones (hardware input points), elevators, and controllers under its direct control.

2.03 ACS Hardware Compatibility List

A. The ACS shall have an open architecture that supports the integration of third party IP-based door controllers and I/O modules. The ACS shall simultaneously support mixed configurations of access control hardware from multiple vendors.

B. The ACS shall support multiple types of hardware devices: single-reader controllers, 2-reader controllers, 1- to 64-reader controllers, integrated readers and door controllers, and Power-over-Ethernet (PoE) enabled door controllers.

C. The ACS shall support most industry standard card readers that output card data using the Wiegand protocol and Clock-and-Data.

D. The ACS shall support the following IP-enabled controllers. For a description of the capabilities of the controller, refer to the specific controller's A&E specifications and design:

1. Synergis Master Controller
2. Synergis Cloud Link
3. SharpV
4. HID VertX
5. HID VertX EVO
6. HID Edge
7. HID Edge EVO
8. Mercury controllers and SIO modules
9. Mercury M5 Bridge
10. Mercury MS Bridge
11. Assa Abloy Aperio RS485 8 to 1 hub
12. Assa Abloy IP Locks (no DSR required)
    a. Corbin Russwin
    b. Sargent Passport
    c. Sargent Profile
    d. IN220
13. Salto Sallis RS485 and PoE routers
14. Schlage AD-300 and AD-400 electronic locks
15. Axis A1001
16. STid RS485 readers
17. DDS AS34/TPL4
18. SimonsVoss Smart Intego

E. The following USB enrollment readers shall be supported: 2 Provided

1. RF Ideas pcProx HID USB reader for enrolling proximity cards
2. RF Ideas AIR ID Enroll iCLASS ID# USB reader for enrolling HID iCLASS cards

3. RF Ideas AIR ID Enroll 14443/15693 CSN USB reader for enrolling a MIFARE card using the CSN (card serial number)
4. RF Idea AIR ID Enroll pcProx Plus w/iCLASS reader for enrolling proximity and iCLASS cards
5. STid STR-W35-E/PH5-5AA
6. HID Omnikey 5x2x USB readers

2.04 Seamless Unification with VMS

A. Through the USP, the ACS shall support integration with an IP Video Surveillance System or MVS. Integration with an IP video surveillance system shall permit the user to view live and recorded video.

B. Users shall be able to associate one or more video cameras to the following entity types: doors, elevator, and hardware zone (input points) and more.

C. The Monitoring UI shall present a true Unified Security Interface for access control and video surveillance. Advanced live video viewing and playback of archived video shall be available through the Monitoring UI.

D. It shall be possible to view video associated with access control events when viewing a report.

2.05 ACS Controller (Unit) Management

A. The ACS shall support the discovery, configuration, and management of IP enabled controllers and I/O modules (hardware units). A user shall be permitted to add, delete, or modify a controller if he or she has the appropriate privileges.

B. The ACS shall support automatic unit discovery. The user shall establish the settings for discovery ports and for the types of unit discovery and the ACS shall automatically detect all connected devices.

C. The ACS shall support a unit swap utility for swapping out an existing controller with a new controller. The unit swap utility shall avoid the reprogramming of the system whenever a unit is replaced. All logs and events from the old unit shall be maintained.

D. The ACS shall support pre-configuration of the system prior to the physical hardware installation.

E. The ACS shall support Firmware upgrade in bulk from the application.

2.06 ACS Cardholder and Cardholder Group Management

A. The ACS shall support the configuration and management of cardholders and cardholder groups. A user shall be able to add, delete, or modify a cardholder or cardholder group if he or she has the appropriate privileges.

B. Custom fields shall be supported for both cardholders and cardholder groups.

C. The ACS shall permit the following activation/expiration options for a cardholder's profile: delayed activation of a cardholder's profile, expiration based on the date of first use of credentials, or expiration on a user-defined date.

D. It shall be possible to set a start date and expiration date for the association of a cardholder and an access rule for temporary access.

E. It shall be possible to associate a picture to a cardholder's profile. The picture shall be imported from a file, captured with a digital camera, or captured from a video surveillance camera. When a cardholder event occurs, the picture of the cardholder shall be displayed in the Monitoring UI. The ACS shall support multiple standard picture formats.

F. Cardholder groups shall enable the grouping of cardholders to facilitate mass changes to system settings. It shall be possible to assign cardholder groups to access rules, thus avoiding the assignment of one cardholder at a time.

G. It shall be possible to search by picture association, custom fields, names and credential codes.

H. It shall be possible to select multiple cardholders for immediate deactivation or reactivation.

I. The ACS shall support the synchronization of cardholders and cardholders group through Active Directory including the credentials and pictures of the cardholders. (Specifier, Active Directory integration requires a license and available in Professional and up).

J. It shall support the ability to track unused credentials for x days.

2.07 ACS Credential Management

A. The ACS shall support the configuration and management of credentials, e.g. access cards and keypad PIN numbers. A user shall be able to add, delete, or modify a credential if the user has the appropriate privileges.

B. Users shall be able to add Custom Fields (user-defined fields) to credentials. Creating a new credential shall be accomplished either manually or automatically.

C. Automatic creation shall allow the user to create a credential entity by presenting a credential to a selected reader. The ACS shall read the card data and associate it to the credential entity. It shall be possible to automatically enroll any card format (128 bits or less).

D. The ACS shall support multiple credentials per cardholder without necessitating duplicate cardholder information. The ACS shall automatically detect and prevent attempts to register an already-registered credential.

E. Batch enrollment of credentials shall be supported.

F. The ACS shall provide a workflow for badge issuance and card requests.

G. The ACS shall support the use of license plates as a credential.

H. The ACS shall natively support the creation and management of mobile IDs in the same way as other credentials.

2.10 ACS Custom Card Formats

A. A custom card format feature shall allow the administrator to add additional custom card formats using an intuitive tool within the Configuration UI. The custom card format tool shall be flexible in the following ways:

1. Once enrolled, new custom card formats shall appear in the card format lists for manual card enrollment.
2. An unrestricted number of additional custom card formats can be added.
3. Shall support credential with up to 256 bits.
4. The administrator shall be able to set the following options when defining a new format:
    a. The order in which card fields appear in the user interface or CSA.
    b. Whether a field is hidden from or visible to an operator.
    c. Whether a field is read only or modifiable by an operator.
    d. Complex parity checking schemes.
    e. The order and location of a field's data. Location can be defined on a bit-by-bit basis.
    f. Application ID and keys for Desfire EV1 credentials.

2.11 ACS Badge Designer: 2 Fargo DTC1250e Dual Sided Card Printers shall be provided; Workstation by end user

A. The badge designer shall allow the creation of badge templates that define the content and presentation format of a cardholder badge to be printed.

B. Badge production shall consist of selecting the credential, the badge template, and clicking print.

C. Batch printing of cards shall be available.

D. The contents of a badge template can include: cardholder's first and last name, picture, custom fields, bitmap graphics, lines, ovals, rectangles, dynamic text labels linked to custom fields and static text labels, and barcodes (Interleaved 2 of 5, Extended Code 39).

E. Copy and paste of badge template objects shall be available.

F. It shall be possible to set the border thickness, and color, the fill color of badge objects (content), and the color of text labels.

G. Settings, such as object transparency, text orientation, and auto-sizing of text shall be available or transparent to the user.

H. Supported badge formats shall be (portrait and landscape): CR70 (2.875" x 2.125"), CR80 (3.37" x 2.125"), CR90 (3.63" x 2.37"), CR100 (3.88" x 2.63"), and custom card sizes.

I. Dual-sided badges shall be supported.

J. A badge template import and export function shall be available to allow the sharing of badge templates between distinct or independent ACS.

K. Chromakey shall be supported.

2.12 ACS Door Management

A. The ACS shall support the configuration and management of doors. A user shall be able to add, delete, or modify a door if he or she has the appropriate privileges.

B. The ACS shall permit multiple access rules to be associated to a door.

C. The ACS shall support the following forms of authentication: Card Only, Card or Keypad (PIN), or Card and Keypad (PIN). It shall be possible to define a schedule for when Card Only or Card and Keypad authentication modes shall be required.

D. It shall be possible to set an extended grant time on a per-door basis (in addition to the standard grant time). Cardholder properties shall include the option of using the extended grant time. When flagged cardholders are granted access, the door shall be unlocked for the duration of the extended grant time instead of the standard grant time.

E. The ACS shall allow the configuration of the relocking mode on doors such as on door open, after a definite time, or on door close.

F. The ACS shall support the ability to enforce the use of two valid reads from different cardholders to grant access to an area.

G. The ACS shall support the ability to enable access rules for other cardholders once a supervisor has accessed an area.

H. The ACS shall support the ability to enable unlocking schedule on a door once an employee has entered the facility.

I. Readerless doors.

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

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

3. Unlocking schedules shall be programmable for readerless doors.

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

J. Unlocking schedules and exceptions to unlocking schedules shall be associated with a door. An unlocking schedule shall determine when a door should be automatically unlocked. The ACS shall also support the use of a specific offline unlocking schedule. Exceptions to unlocking schedules shall be used to define time periods during which unlocking schedules shall not be applied, such as during statutory holidays.

K. The ACS shall support one or more cameras per door. Video shall then be associated to door access events, such as access grant or access denied.

2.13 ACS Visitor Management *Passage Point EDU by Stop ware 1 per building; PC by owner*

2.14 ACS People Counting & Area Presence Tracking (Mustering)

A. The ACS shall support people counting (or area presence tracking). The ACS shall be able to monitor and report the number of cardholders in an area in real-time and for all areas. Monitoring shall be based on the entire access control infrastructure, for both local areas and those in remote geographic locations. People counting can also be used to perform mustering.

B. The ACS shall report area presence counts in the UI. Area presence tracks shall dynamically track the total number of cardholders in an area. Displayed data shall be updated dynamically.

C. The ACS shall be able to generate an area presence report listing the cardholders located in one or more areas, accessible through the Monitoring UI. It shall be possible to filter the report by area and time period. The report shall also include activity from sub-areas (nested areas).

D. Through people counting, the ACS shall be able to generate First Person In and Last Person Out events. The First Person In event shall detect when the first cardholder enters an empty area. The Last Person Out event shall detect when the last cardholder leaves an area. It shall be possible to trigger actions from both events such as sending a message or triggering an alarm.

E. The ACS shall be able to determine the entry of a cardholder based on a dedicated sensor.

2.15 ACS Custom Fields (User-Defined Fields)

A. The ACS shall permit the creation of custom fields. Up to 1,000 custom fields shall be supported.

B. Custom fields shall be supported for the following entities: cardholders, cardholder groups, credentials, and visitors.

C. Supported custom fields shall include: text, integers, decimal numbers, dates, Boolean, and images (graphics).

D. Users shall be able to define a default value for a custom field.

E. The creation of new custom field types shall be possible. New custom field types shall be based on the standard custom fields supported. They shall support user- defined values from which an operator must make a selection.

F. Administrators have the ability to define which users can view and modify specific custom fields. This shall limit the access to custom field data to users with pre-defined privileges. The ACS shall support querying and report generation using custom fields.

G. Custom fields can be grouped and ordered within these groups as defined by the user.

H. Values for custom fields can be imported using the Import Tool.

I. The ACS shall support an integrated Import Tool to facilitate the import of existing cardholder and credential data. The import of data shall be through the use the CSV file format. The tool shall be available from the Configuration UI.

J. The Import Tool shall also support the ability to manually import data that has been exported from a third party database if it is in CSV format.

K. The import tool shall permit the import of the following data:

1. Cardholder name, descriptions, picture, email, and status.
2. Cardholder group information.
3. Credential name, status, format, and card number (including credentials with custom formats).
4. Partition information.
5. Custom fields.

L. Full flexibility in selecting the fields to be imported during an import session shall be available.

M. The option to use a custom and unique cardholder key shall be specified during the import process to ensure that cardholders with duplicate names will not have their data overwritten. Cardholder key generation shall be automated. The end user shall have the option to select which fields will be used to create this unique key, e.g. credential number, custom fields, cardholder name.

N. The ACS shall also support re-importing a CSV file containing new information to update existing information in the ACS database. Re-importing shall enable bulk amendments to existing access control data.

2.16 General Client Software Requirements

A. 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.

B. 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).

C. The CSA for monitoring shall support running in 64-bit mode.

D. 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.

E. The CSA shall seamlessly merge access control, license plate recognition (ALPR), and video functionalities within the same user application.

F. 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.

G. 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.

H. Logging on to a CSA shall be done either through locally stored USP user accounts and passwords or using the operators Windows credentials when Active Directory integration is enabled.

I. When integrated with Microsoft's Active Directory (Included), 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.

J. 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.

K. To enhance usability and operator efficiency, the Configuration UI and Monitoring UI shall support many of the latest UI such as:

1. A customizable Home Page that includes favorite and recently used tasks.
2. Task-oriented approach for administrator/operator activities where each type of activity (surveillance, visitor management, individual reports, and more) is an operator task.
3. Consolidated and consistent workflows for video, ALPR, and access control.
4. 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.

L. Configuration UI and Monitoring UI Home Page and Tasks

1. The Configuration UI and Monitoring UI shall be task-oriented.
2. 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.
3. Tasks shall be accessible via the Home Page of either the Configuration or the Surveillance CSA.
4. Newly created tasks shall be accessible via the Configuration UI or the Monitoring UI taskbar.
5. Similar tasks shall be grouped into the following categories:
    a. Operation: Access control management, LRP management, and more.

b. Investigation: access control activity reports, visitor activity reports, alarm reports, and more.

c. Maintenance: Access control and, troubleshooters, audit trails, health-related reports, and more.

6. An operator shall be able to launch a specific task only if he or she has the appropriate privileges.

7. 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.

M. The Contractor shall provide unlimited Simultaneous Clients via site license.

2.17 Configuration User Interface (UI)

A. General

1. 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.

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

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

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

5. The Configuration UI shall include a static reporting interface to:

a. 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.

b. View audit trails that show a history of user/administrator changes to an entity.

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

2.18 ACS Client User Interface (UI)

A. 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.

B. 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.

C. To enhance usability and operator efficiency, the Monitoring UI shall support the following UI concepts:

1. Dynamically adaptive interface that adjusts in real-time to what the operator is doing.
2. A dynamic dashboard loaded with entity-specific widgets (e.g. door and camera widgets).
3. Use of transparent overlays that can display multiple types of data in a seamless fashion.
4. Display tile menus and quick commands.
5. Consolidated and consistent workflows.
6. Tile menus and quick commands easily accessible within every display tile of the user workspace.
7. 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.

D. Monitoring UI Home Page and Tasks

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

E. Dynamically Adaptive UI, Dashboard, and Widgets

1. 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 dashboard.
2. Widgets shall be mini-applications or mini-groupings in the Monitoring UI dashboard that let the operator perform common tasks and provide them with fast access to information and actions.
3. With a single click on an entity (e.g. 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.

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

F. Operator Workflows

1. 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.

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

3. 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.

G. Each task within the Monitoring UI shall consist of one or more of the following items:

1. Event list.
2. Logical tree. Doors, cameras, zones, ALPR units, and elevators shall be grouped under Areas in a hierarchical fashion.
3. Entities list of all entities being tracked.
4. Display tiles with various patterns (1 x 1, 2 x 2, and more).
5. Display tile menu with various commands related to cameras, doors, PTZ, and tile controls.
6. Dashboard with widgets.

H. The Monitoring UI shall support multiple event lists and display tile patterns, including:

1. Event/alarm list layout only
2. Display tile layout only
3. Display tile and alarm/event list combination
4. ALPR map and alarm/event list combination

I. User workspace customization

1. 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.
2. Once customized, the user shall be able to save his or her workspace.
3. The user workspace shall be accessible by a specific user from any client application on the network.
4. Display tile patterns shall be customizable.
5. 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.
6. The Monitoring UI shall support multiple display tile patterns (e.g. 1 display tile (1x1 matrix), 16 tiles (8x8 matrix), and multiple additional variations).
7. The Monitoring UI shall support as many monitors as the PC video adapters and Windows Operating System are capable of accepting.

8. 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.

J. The Monitoring UI shall provide an interface to support the following tasks and activities common to access control, ALPR, and video:

    1. Monitoring the events from a live security system (ACS and/or VMS and/or ALPR).
    2. Generating reports, including custom reports.
    3. Monitoring and acknowledging alarms.
    4. Creating and editing incidents and generating incident reports.
    5. Displaying dynamic graphical maps and floor plans as well as executing actions from dynamic graphical maps and floor plans.
    6. Management and execution of hot actions and macros.

K. The Monitoring UI shall be able to monitor the activity of the following entities in real-time: areas, ALPR entities, doors, elevators, cameras, cardholders, cardholder groups, zones (input points), and more. The Monitoring UI shall provide an interface to support the following access control tasks and capabilities:

    1. Monitoring and management of access events and alarms.
    2. Viewing of cardholder picture or badge IDs.
    3. Verification of cardholder picture IDs against live video.
    4. Visitor management.
    5. People counting or mustering, including resetting the people count in an area.
    6. Door control, including remotely unlocking doors, overriding a door's unlocking schedules, and enabling door maintenance mode.
    7. Forgiving antipassback.
    8. Generation of ACS configuration and activity reports.
    9. Viewing of HTML files including alarm instructions.

L. Entity Monitoring

    1. 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.
    2. The Monitoring UI shall provide the option to filter which events shall be displayed in the display tile layout and/or event list layout.
    3. 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).

4. 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.

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

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

M. Display Tile Packing and Unpacking

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

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

3. 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.

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

N. The following additional tools or utilities shall be available from the Monitoring UI: create credentials, create cardholders, and access control troubleshooter.

2.19 Server Administrator User Interface Requirements

A. 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.

B. 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.

C. Access to the Server Administrator shall be protected via login name, password, and encrypted communications.

D. The Server Administrator shall allow the administrator (user) to perform the following functions:

1. Manage the system license.

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

3. Activate/Deactivate the Directory Role.

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

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

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

2.20 Unified Web Client (UWC) General Requirements: Provide Unlimited Site License

A. The USP shall support a unified web client (UWC) for access control and video.

B. The UWC shall be a truly thin client with no download required other than an internet web browser or standard web browser plugins.

C. The UWC shall be platform independent and run within Microsoft Internet Explorer, Firefox, Safari, and Google Chrome.

D. The UWC shall be designed as an HTML5 application.

E. The UWC will support native H.264 video in the web client.

F. 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.

G. 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.

H. The UWC shall provide the ability to configure, save, and reload camera layouts.

I. The UWC shall provide the ability to control PTZ cameras.

J. Functionalities:

1. Login using name and password or Active Directory support shall be available.

2. Encrypted communications for all transactions.

3. Print reports and export to CSV file.

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

5. Access Control

a. Cardholder and group (add/modify/delete).

b. Credential management (modify/delete).

c. Visitor management (check-in/modify/check-out).

d. Unlock door.

e. Door Activities report.

6. Alarms

a. Alarm report.

2.21 Smartphone and Tablet App General Requirements

A. The USP shall support mobile apps for various off-the-shelf smartphones and tablets. The mobile apps shall communicate with the Mobile Server of the USP over any WiFi or mobile network connection.

B. Mobile apps shall communicate with the USP via a Mobile Server (same as the Unified Web Client or UWC). Communication between the mobile device and the Mobile Server shall support optional encryption.

C. Supported device manufacturers shall include (refer to Mobile App specifications for latest compatibility list):

1. Apple iPod Touch, iPhone, and iPad.
2. Android-compatible smartphones and tablets.
3. Windows and Windows Phone 8.1.

D. It shall be possible to download the mobile apps from the Central application store (Apple iTunes App Store, Google Play, Windows Store).

E. Functionalities

1. Live monitoring and command and control of the USP.
2. Control of camera PTZ.
3. Receive alarm push notifications from the Apple Push Notification Server or from the Google Android push server.
4. Alarm management (view and acknowledge alarms, video tied to alarms).
5. View USP hierarchy and search for entities.
6. Digital zoom on cameras.
7. Support for adaptive resolution scaling.
8. Save camera layouts.
9. Picture-in-picture to view live video when doing playback.
10. View up to 20 cameras simultaneously on iPads.

F. Access Control

a. View cardholder picture with access-related events.
b. Monitor door status.
c. Unlock door.
d. Override unlocking or locking schedule.
e. Set door in maintenance mode.

2.22 Health Monitor

A. The USP shall monitor the health of the system, log health-related events, and calculate statistics.

B. USP services, roles, agents, units, and client apps will trigger health events.

C. The USP shall populate the Windows Event Log with health events related to USP roles, services, and client apps.

D. A dedicated role, the Health Monitoring Role, shall perform the following actions:

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

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

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

E. A Health Monitoring task and Health History reporting task shall be available for live and historical reporting.

F. A web-based, centralized health dashboard shall be available to remotely view unit and role health events of the USP.

G. 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.

H. Health events shall be accessible via the SDK (can be used to create SNMP traps).

2.23 USP General Requirements

A. The Unified Security Platform (USP) shall be an enterprise class IP-enabled security and safety software solution.

B. 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.

C. Functionalities available with the USP shall include:

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

2. Live event monitoring.

3. Live video monitoring and playback of archived video.

4. Alarm management.

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

6. Microsoft Active Directory integration for synchronizing USP user accounts and ACS cardholder accounts.
7. Intrusion device and panel integration (live monitoring, reporting, and arming/disarming). *Must include data integration with existing Bosch Intrusion Panels.*
8. SIP Intercom device integration for bi-directional communication. *(.*
9. Integration with third party systems and databases via plug-ins (access control, video analytics, point of sale, and more). .
10. Dynamic graphical map viewing.
11. Asset management system integration.

D. The USP shall be deployed in one or more of the following types of installations:

1. Unified access, ALPR, video platform, and any combination thereof.
2. Standalone access control, video, or ALPR platform.
3. Unified access and video platform that federates multiple remote ACS, VMS, and ALPR.
4. Standalone access control that federates multiple independent remote ACS.

E. Licensing

1. A single central license shall be applied centrally on the configuration server.
2. There shall be no requirement to apply a license at every server computer or client workstation.
3. Based on selected options, one or more embedded systems shall be enabled or disabled.

F. Hardware and Software Requirements

1. 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.

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

3. 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.

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

5. 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.

2.24 USP Architecture

A. 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).

B. 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.

C. 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.

D. 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.

E. The USP shall protect against potential database server failure and continue to run through standard off-the-shelf solutions.

F. 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.

G. 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.

H. Roles-Based Architecture

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

2. 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:
    a. Deploy one or several SSM across the network prior to activating roles.
    b. Activate and deactivate roles as needed on each and every SSM.
    c. Centralize role configuration and management.
    d. Support remote configuration.
    e. Move roles over from one SSM to another.
3. Each role, where needed, shall have its own database to store events and role-specific configuration information.
4. 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.
5. Directory Role
    a. The Directory Role shall manage the central database that contains all the system information and component configuration of the USP.
    b. The Directory Role shall authenticate users and give access to the USP based on predefined user access rights or privileges, and security partition settings.
    c. The Directory Role shall support the configuration/management of the following components common to the ACS, ALPR, and VMS sub-systems:
        i. Security Partitions, users and user groups.
        ii. Areas.
        iii. Zones, input/output (IO) linking rules, and custom output behavior.
        iv. Alarms. Schedules, and scheduled tasks.
        v. Custom events.
        vi. Macros or custom scripts.
    d. The Directory Role shall support the configuration/management of the following components specific to VMS:
        vii. Video servers and their peripherals (e.g. audio, IOs, and serial ports).
        viii. PTZ.
        ix. Camera sequences.
        x. Recording and archiving schedules.
    e. The Directory Role shall support the configuration/management of the following components specific to ACS:

i. Door controllers, and input and output (IO) modules.

ii. Doors, Elevators, and Access rules.

iii. Cardholders and cardholder groups, credentials, and badge templates.

f. The Directory Role shall support the configuration/management of the following components specific to ALPR:

i. ALPR units and cameras.

ii. Hotlists, permit lists, and overtime rules.

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

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

4. 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.

5. 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.

6. 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.

7. 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.

8. Optional Roles

a. The Active Directory Role shall be responsible for synchronizing user accounts and cardholder accounts with a Microsoft Active Directory server.

b. The Intrusion Manager Role shall be responsible for managing third party intrusion devices such as alarm panels and perimeter detection devices. This role shall also be responsible for logging all intrusion events in a database. *Existing Bosch Intrusion must integrate.*

c. The Asset Manager Role shall be responsible for integrating and synchronizing with third party asset management systems and logging asset related events. This role shall also be responsible for supporting the execution of asset-related reports such as inventory reports and asset activity reports.

d. The Plug-in Manager Role shall be responsible for the communication between the USP and third party systems such as video analytics, access control, video, ALPR, and building management systems.

e. 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.

f. The Communication Management Role shall be responsible for registering the SIP communication endpoints and for managing the call routing.

B. Server Monitoring Service (Watchdog)

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

2. 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.

3. 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.

2.25 USP Access Control, Video, and ALPR Unification

A. 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.

B. The Configuration UI shall present a true Unified Security Interface for the configuration and management of the ACS, VMS, and ALPR.

C. 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.

D. It shall be possible to view video associated to access control events when viewing a report.

E. It shall be possible to view video associated to intrusion panel events when viewing a report.

F. It shall be possible to view video associated to ALPR events when viewing a report.

2.26 USP Alarm Management

A. The USP shall support the following Alarm Management functionality:

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

2. 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.

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

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

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

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

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

8. 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.

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

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

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

B. The workflows to create, modify, add instructions and procedures, and acknowledge an alarm shall be consistent for access control, ALPR, and video alarms.

C. Alarms shall be federated, allowing global alarm management across multiple independent USP, ACS, and VMS systems.

D. The USP shall also support alarm notification to an email address or any device using the SMTP protocol.

E. 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.

F. 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.

G. The user shall have the ability to acknowledge alarms, create an incident upon alarm acknowledgement, and put an alarm to snooze.

H. The user shall be able to spontaneously trigger alarms based on something he or she sees in the system.

I. An alarm shall be configured in such a way that it remains visible until the source condition has been acknowledged.

J. The user shall be able to investigate an alarm without acknowledging it.

2.27 USP Threat Levels

A. The USP shall support Threat Levels to dynamically change the system behavior to respond to critical events.

B. Threat Levels shall be activated and deactivated by the CSA operator with the right privilege.

C. Threat Levels shall be set on an area or on the entire system.

D. 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.

E. The following specific actions shall be available with Threat Level:

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

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

3. Set reader mode to change how the doors are accessed (e.g. card and PIN, or card or PIN).

F. A visible notification shall be displayed in all operator CSA when a Threat Level is activated.

2.28 USP Advanced Task Management

A. USP shall support an infrastructure for managing Monitoring UI tasks used for live monitoring, day to day activities, and reporting.

B. 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.

C. 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.

D. 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.

2.29 USP Reporting

A. The USP shall support report generation (database reporting) for access control, ALPR, video, and intrusion.

B. 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 he or she has the appropriate privilege.

C. The workflows to create, modify, and run a report shall be consistent for access control, ALPR, and video reports.

D. Reports shall be federated, allowing global consolidated reporting across multiple independent USP, ACS, VMS, and ALPR systems.

E. Access control and ALPR reports shall support cardholder pictures and license plate pictures, respectively.

F. The USP shall support the following types of reports:

1. Alarm reports.
2. Video-specific reports (archive, bookmark, motion, and more).
3. Configuration reports (cardholders, credentials, units, access rules, readers/inputs/outputs, and more).
4. Activity reports (cardholder, cardholder group, visitor, credential, door, unit, area, zone, elevator, and more).
5. ALPR-specific reports (mobile ALPR playback, hits, plate reads, reads/hits per day, reads/hits per ALPR zone, and more).
6. Health activity and health statistics reports.
7. Other types of reports, including visitor reports, audit trail reports, incident reports, and time and attendance reports.

G. Generic Reports, Custom Reports and Report Templates

1. 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.
2. 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).

3. All report templates shall be created within the Monitoring UI.
4. These templates can be used to generate reports on a schedule in PDF or Excel formats.
5. An unrestricted number of custom reports and templates shall be supported.

H. 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.

I. The USP shall support comprehensive data filtering for most reports based on entity type, event type, event timestamp, custom fields, and more.

J. The reporting task shall have the ability to display results through graphics such as pie charts and bar graphs.

K. The user shall be able to click on an entity within an existing report to generate additional reports from the Monitoring UI.

L. The USP shall support the following actions on a report: print report, export report to a PDF/Microsoft Excel/CSV file, and automatically email a report based on a schedule and a list of one or more recipients.

2.30 USP Zone Management

A. 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 he or she has the appropriate privileges.

B. 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.

C. 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.

D. A schedule shall be defined for a zone, indicating when the zone will be monitored.

E. 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.

F. The ACS shall support one or more cameras per zone. Video shall then be associated to zone state changes.

G. Input/Output (IO) Linking

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

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

3. 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.

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

2.31 USP User and User Group Security, Partitions, and Privileges Management

A. 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 he or she has the appropriate privileges.

B. The USP shall support user authentication with claims-based authentication using external providers. External providers shall include:

    1. ADFS (Active Directory Federation Services)

C. 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.

D. User privileges shall be extensive in the USP. All configurable entities for the USP, including access control, video, and ALPR, shall have associated privileges.

E. 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.

F. Partitions

    1. 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.

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

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

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

G. It shall be possible to specify user and user group privileges on a per partition basis.

H. Advanced logon options shall be available such as dual logon and more.

I. 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.

2.32 USP Event/Action Management

A. 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.

B. 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.

C. The USP shall receive and log the following events:

    1. System-wide events

2. Application events (clients and servers)
3. Area, camera, door, elevator, and ALPR events (reads and hits)
4. Cardholder and credential events
5. Unit events
6. Zone events
7. Alarm events
8. ALPR events
9. First Person In and Last Person Out events and antipassback events
10. Intrusion events
11. Asset management events

D. The USP shall allow the creation of custom events.

E. The USP shall have the capability to execute an action in response to an access control, video, and ALPR event.

F. 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.

2.33 USP Schedules and Scheduled Tasks

A. Schedules

1. The USP shall support the configuration and management of complex schedules. A user shall be able to add, delete, or modify a schedule if he or she has the appropriate privileges.
2. 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.
3. Daily, weekly, ordinal, and specific schedules shall be supported.

B. Scheduled Tasks

1. The USP shall support scheduled tasks for access control, video, and ALPR.
2. 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.
3. Scheduled tasks shall support all standard actions available within the USP, such as sending an email or emailing a report.

2.34 USP Macros and Custom Scripts

A. 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.

B. Custom macros shall be created with the USP Software Development Kit (SDK).

C. A macro shall be executed either automatically or manually.

D. In the Monitoring UI, a macro shall be launched through hot actions.

2.35 USP Dynamic Graphical Maps (DGM)

A. The USP shall support mapping functionality for access control, video surveillance, intrusion detection, ALPR, and external applications.

B. 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.

C. 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 screen must provide the same command and control capabilities than in a single screen display.

D. The DGM shall support the following file format and protocol for importing map background:

1. PDF
2. JPG
3. PNG
4. Web Tile Map Service (WMTS) and Web Map Service (WMS) defined by the Open Geospatial Consortium (OGC)
5. BeNomad

E. 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:

1. Google Map, aerial, terrain (Licensed)
2. Bing Map, aerial, satellite, hybrid (Licensed)
3. ESRI ArcGIS (Licensed)
4. OpenStreet Map aerial
5. OVI hybrid

F. It shall be possible to configure a mixed set of maps made of GIS, online providers and private imported files and link them together.

G. The DGM shall provide the ability to display all native entities of the USP including:

1. Cameras, fix, and PTZ
2. Doors

3. Camera sequences
4. Areas
5. Intrusion areas
6. Intrusion zones
7. License Plate Recognition cameras
8. Digital inputs
9. Digital outputs
10. Intercoms
11. Alarms
12. Macros
13. Police Car Patrollers

H. The DGM shall provide the ability to draw and display information over the map in the form of:

1. Vectoriel shapes: line, rectangles, polygones, ellipse
2. Pictures
3. Text

I. The DGM shall provide the ability to display any type of third party entities integrated through an SDK.

J. The DGM shall provide the ability to display layer of information in Keyhole Markup Language (KML) format.

K. 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.

L. The DGM shall provide the ability to import data layers from one or more ESRI ArcGIS servers.

M. 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.

N. The DGM shall offer built-in map data backup and restore for both map backgrounds and layers of entities.

O. The DGM shall offer failover capabilities.

P. The DGM shall scale up to several thousands of entities on a single map and hundreds of maps.

Q. The DGM shall provide a means to update a map background without affecting the map object configuration.

R. The DGM shall offer a user friendly graphical map designer to configure the maps.

S. The DGM shall provide a user friendly and intuitive navigation that includes:

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

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

    3. 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.

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

    5. A history log of positions.

T. 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.

U. The DGM shall offer the ability to optionally set a graphical display notification of the motion detection.

V. The DGM shall offer a smart selection tool to access the video. By clicking the location the user wants to see, the DGM will automatically select the cameras that can see this location and move the PTZ towards that location. This smart selection tool shall take obstacles into consideration and not display cameras that cannot see the location because of a wall.

W. It shall be possible to select a location by drawing a zone of interest on the DGM, and to display all the entities that are part of that zone of interest at once.

X. The user shall be able to select and display the content of multiple USP entities on the map in pop-up windows.

Y. The user shall be able to move, resize, and pin the USP entity pop-up windows to the map.

Z. It shall be possible to access live and playback video from the map.

AA. 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.

BB. The DGM shall offer the ability to fully operate alarm monitoring. It shall be possible to:

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

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

    3. Trigger and receive alarms.

4. Act on the alarm from the DGM, including acknowledgements, forwarding, and investigation.
5. Visualize that an alarm occurred in an underlying linked map.

CC. The DGM shall provide the following search capabilities:

1. Search and center by entity name.
2. 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.

DD. Any update of map content by an administrator shall be immediately and dynamically pushed to all DGM users.

EE. The DGM shall support the use of GIS maps or private maps or a combination of both for map background.

FF. 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.

GG. 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.

HH. It shall be possible to edit and configure multiple map objects at once.

II. All map design modifications shall be logged in an audit trail.

JJ. 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.

KK. Through the following functionality, the DGM shall allow the management of USP alarms from the map: Locate on the map entities related to the alarm.

1. Display entities of the alarm with a specific icon, color, transparency level, and blinking rate.
2. List, select, and locate alarms.
3. Auto center the map on the highest priority alarm.
4. Handle the alarm from the map, including acknowledgement, forwarding and investigation.
5. All map containers, such as hotspots or map links shall reflect the alarm status of the contained entities.

LL. It shall be possible to add advanced functionality to maps object using the SDK. Any functionality available through the USP SDK shall be available within maps.

MM. The DGM shall offer lasso tools for:

1. Displaying entities at one location through a single action.
2. Triggering an action on all entities at one a location in a single click.
3. Editing multiple entities at one location simultaneously.

NN. The DGM shall allow the display of USP entities selected from the map on a remote monitor (video wall)

OO. The DGM shall provide the following search capabilities:

1. Search within the map by entity name, street name, or point of interest.

PP. The DGM shall allow the use of KML overlay map information for both GIS and private maps. Movable objects shall be supported through the use of KML.

QQ. Any updating of map content by an administrator shall be immediately and dynamically pushed to all operators displaying the map.

RR. The Contractor shall provide licenses for each entity that is required to be shown on the graphical maps. USP Audit and User Activity Trails (Logs)

AA. The USP shall support the generation of audit trails. Audit trails shall consist of logs of operator/administrator additions, deletions, and modifications.

BB. 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.

CC. For entity configuration changes, the audit trail report shall include detailed information of the value before and after the changes.

DD. 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.

EE. 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.

2.36 USP Incident Reports

A. 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.

B. The operator shall be able to create standalone incident reports or incident reports tied to alarms.

C. 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.

D. 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.

E. Incident reports shall allow the creation of a custom form on which to input information on an incident.

F. Incident reports shall allow entities, events, and alarms to be added to support at the report's conclusions.

2.37 USP Third Party Integration

A. Microsoft Active Directory Integration

1. 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.

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

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

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

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

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

7. It shall be possible to synchronize the following USP entities and their information from Active Directory with the USP:

    a. Users (username, first and last names, email address, and more).

    b. User groups (user group name, description, and group email address).

    c. Cardholders (first and last names, description, email, picture and more).

d. Cardholder groups (cardholder group name, description, and group email address).

e. Active Directory attributes to USP custom fields.

8. 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.

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

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

11. The USP shall support user connections across independent organizations by connecting to an external ADFS (Active Directory Federation Services) service using claims-based authentication.

B. Intrusion Detection Integration: *Data integration with existing Bosch intrusion*

1. The USP shall integrate with third party intrusion panels and devices via an Intrusion SDK. The Intrusion Manager Role shall manage communications with the intrusion panels. Communications with intrusion devices shall be over serial communications and/or an IP network.

2. Integration with intrusion panels shall be possible outside the release cycle of the USP. It shall be possible to add new integrations at any point in time.

3. Functionality available via the integration of intrusion devices with the USP shall include the following (where supported by the intrusion panel):

   a. Arm and disarm intrusion devices (manually, on schedule, or following a USP event).

   b. Activate or trigger intrusion device outputs.

   c. View intrusion events and alarms.

   d. Monitor the status, including arming status, of the intrusion devices.

   e. Video verification of intrusion events and alarms with video panels.

   f. Create USP zones using intrusion device inputs.

4. Currently supported intrusion panels include:

   a. Bosch G Series panels.

C. Third Party Access Control Systems

1. The USP shall integrate with third party access control software via the SDK. Communications with access control software shall be over an IP network, and should not support administrative tasks such as cardholder management.

2. Integration with access control software shall be possible outside the release cycle of the USP. It shall be possible to add new integrations at any point in time.
3. Functionality available via the integration of access control software with the USP shall include the following (where supported by the access control solution):
    a. Synchronize access control entities and receive associated events and states within the USP, including:
        i. Cardholders and access rights
        ii. Visitors
        iii. Readers and doors
        iv. Alarms
    b. Monitor access control events
    c. Monitor and acknowledge access control alarms
    d. Trigger actions and outputs in the access control software using hot actions and event-to-actions
    e. Lock and unlock doors in the access control software
    f. Configure event-to-actions using the access control events and alarms
    g. Generate Security Center reports using the access control data
    h. View and monitor states of door entities in the USP maps

D. Asset Management Integration

1. The USP shall integrate with third party asset management systems via the Asset Management Role.
2. Communications with asset management solutions shall be over an IP network (via software communications).
3. Functionality available via the integration of asset management systems with the USP shall include the following (where supported by the asset management systems):
    a. Synchronize asset management system assets with USP asset entities.

b. Live monitoring of asset-related activity events, health events, and activity (asset online, asset offline, asset moves, or low battery).

c. Synchronization of asset management alarms with Security Center alarms.

d. Viewing video tied to asset-related activity and alerts within monitoring and reporting tasks.

e. Acknowledging alarms in Security Center which acknowledges alerts in the asset management system and vice versa.

f. Real-time tracking of asset locations on a per area basis.

g. Asset Management Inventory reporting task that details the current location (area) of an asset.

h. Asset Activity reporting task that provides a historical review of asset-related events and activity.

4. Currently supported asset management systems include:

a. RF Code Asset Manager

E. Additional Third Party Integrations

1. 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.

2. The USP architecture shall support the addition of new connectors to integrate to third party system integration, such as:

a. Third party video systems.

b. Third party access control systems.

c. ALPR integrations with pay stations, permit vendors, pay-by-phone vendors, and ticketing vendors.

d. Building management systems.

e. Human resource management systems (HRMS).

2.38 USP Software Development Kit (SDK)

A. A USP SDK shall be available to support custom development for the platform.

B. The SDK shall include functionalities specific to the embedded automatic license plate recognition (ALPR), access control (ACS), and video (VMS) systems.

C. Integration with external applications and databases shall be possible with the SDK.

D. 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.

E. The SDK shall be based on the .NET framework.

F. The SDK shall support dynamic or transactional updates to the USP configuration. It shall also support change notification of USP entity configuration.

G. 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.

H. The SDK shall provide an extensive list of programming functions to view and configure ACS, VMS, and ALPR.

I. 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.

J. 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.

K. 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.

L. The SDK shall support the following alarm functions: view alarms in real time, acknowledge alarms, change priority, and change recipient.

Part 3 - Execution

3.01 Warranty

A. 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.

B. 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:

1. Access to phone support and online chat for technical assistance
2. Online case management
3. Online system availability monitor
4. Access to Major and Minor Release Upgrades
5. 24/7 pager support and dedicated support specialist *(Specifier, additional cost)*

3.02 Deployment Services and System Commissioning

A. General Requirements

1. 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:

    a. Multiple contractors or subcontractors that will be responsible for deploying the USP at multiple client sites in different geographical regions.

    b. Complex enterprise installations involving advanced functionality (e.g. The Federation feature, failover, plugins) and/or multiple systems (e.g. access control, video, ALPR) and/or third party integrations.

    c. Extensive use of customized solutions/plugins developed by the vendor that will be integrated into the USP.

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

B. Deployment Management Service

1. 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:

    a. Conducting a Risk Assessment of the impact of potential risk factors on the operation of the vendor's USP.

    b. Providing a project plan for the deployment of the vendor's USP.

    c. Managing the development and deployment of the custom solution components that will be integrated into the vendor's USP (if applicable).

    d. Providing a scope of work detailing the services to be provided by the vendor to assist in the deployment of the vendor’s USP.

    e. Coordinating and scheduling the vendor field services with the contractor to assist with the deployment of the vendor’s USP.

    f. Providing regular project status updates to the contractor regarding the development of custom solutions (if applicable) and the deployment of the vendor’s USP.

C. Solution Architect Service

1. 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:

    a. Assisting the contractor/subcontractor with the design and architecture of the vendor’s USP.

b. 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.

c. Conducting a system assessment and ensuring best practices of the vendor's USP are followed.

d. Providing upgrade and migration strategy for the vendor's USP where applicable.

e. 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.

D. System Configuration and Commissioning Service

1. The System Configuration and Commissioning service from the vendor shall include a Field Engineer who will be responsible for:

a. Assisting the contractor's or subcontractor's onsite/remote technicians with the configuration and commissioning of the vendor's USP at the client site.

b. Conducting a test of the USP following the deployment of the system using real-world operator scenarios to ensure optimal system performance.

c. 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.

d. Providing a knowledge transfer of the vendor's USP to the contractor following the deployment of the USP at the client site.

3.03 Manufacturer End User Operator Training

A. 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. Include 24 hours of End User Training: 16 of which shall be done upon completion of system and 8 hours to be done 3 months later.

End of Section

Section 28 23 00 – Video Management System

Part 1 - General

1.01 Related Work

A. Section 28 13 00 – Electronic Access Control System

1.02 Definitions

A. ACS – Access Control System

B. CSA – Client Software Application

C. DGM – Dynamic Graphical Maps

D. DVS – Digital Video Server

E. ALPR – Automatic License Plate Recognition

F. SDK – Software Development Kit

G. GLM – Genetec Lifecycle Management

H. SSM – Server Software Module

I. UI – User Interface

J. USP – Unified Security Platform

K. USW – Unified Web Client

L. VMS – Video Management System

1.03 Qualifications

A. The system programmer shall have attended manufacturer training and obtained certification in Genetec Security Center - Omnicast™ Technical Certification

B. The prime contractor shall be a Genetec certified partner with the following level of qualification:

1. Unified Elite Reseller
2. Illinois Licensed Agency Alarm Contractor

C. The system programmer shall submit proof of certifications.

Part 2 - Products

2.01 VMS General Requirements

A. 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.

B. The VMS shall offer a complete and scalable video surveillance solution that shall allow cameras to be added on a unit-by-unit basis.

C. 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.

D. The VMS shall integrate DVS using the DVS native SDK or using the following industry standards to interface to the DVS:

1. ONVIF

E. 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.

F. 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.

G. 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.

H. 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).

I. The VMS shall be able to retrieve and set the current position of PTZ cameras using XYZ coordinates.

J. The VMS shall support PTZ camera protocols from multiple manufacturers, including analog and IP protocols.

K. The VMS shall arbitrate the user conflict on PTZ usage based on user levels per camera.

L. The VMS shall support the following list of CCTV keyboard protocols:

1. American Dynamics 2078 ASCII, and American Dynamics 2088 ASCII
2. Bosch Autodome, Bosch Intuikey
3. DVTel

4. GE ImpactNet

5. Panasonic, Pelco ASCII, Pelco KBD-300, and Pelco P.
6. Radionics
7. Samsung SSC-1000 and SPC-600
8. Videoalarm
9. Sony RM-NS1000
10. Panasonic WV-CU161C

M. The VMS shall support the following list of joysticks and control keyboards:
   1. Axis 295.
   2. Axis T8310 Video Surveillance Control Board.
   3. Panasonic WV-CU950 Ethernet keyboard.
   4. Any USB joystick detected as a Windows Game Controller.

N. 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:
   1. Local time of the camera
   2. Local time of the SSM
   3. Local time of user's workstation
   4. GMT Time
   5. Other time zone

O. Audio and Video storage configuration for the SSM shall either be:
   1. Internal or external IDE/SATA/SAS organized or not in a RAID configuration.
   2. Internal or external SCSI/iSCSI/Fiber Channel organized or not in a RAID configuration.
   3. Within the overall storage system, it shall be possible to include disks located on:
      a. External PCs on a LAN or WAN
      b. Network Attached Servers (NAS) on a LAN or WAN
      c. Storage Area Networks (SAN)

P. The SSM shall not limit the actual storage capacity configured per server.

Q. Manufacturer:
   1. Genetec Security Center:
      a. Omnicast Enterprise

2.02 Cyber Security Requirements

A. 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.

B. The USP shall support user authentication with claims-based authentication using external providers. External providers shall include:

    1. ADFS (Active Directory Federation Services)

C. The USP shall limit the IP ports in use and shall provide the Administrator with the ability to configure these ports.

D. 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.

E. 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:

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

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

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

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

    5. Use a random encryption key and change periodically.

    6. Allow encrypted streams to be exported.

F. The VMS shall support end to end encrypted streams with cameras supporting Secure RTP (SRTP) both in unicast and multicast from the camera.

2.03 Failover and Standby Requirements

A. The USP shall support native and off-the-shelf failover options.

2.04 Archiving

A. The Archiver (role) shall use an event and timestamp database for the advanced search of audio/video archives. This database shall use Microsoft SQL.

B. The Archiver shall protect archived audio/video files and the system database against network access and non-administrative user access.

C. The Archiver shall digitally sign recorded video using 248-bit RSA public/private key cryptography.

D. The Archiver shall offer a plug and play type hardware discovery service with the following functionalities:

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

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

E. The Archiver shall have the capacity to configure the key frame interval (I-frame) in seconds or number of frames.

F. 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.

G. The Archiver shall provide the functionality of storing of video and audio streams based on triggering events, such as:

    1. Digital motion detection.

    2. Digital input activation.

    3. Macros.

    4. Through SDK application recording.

H. 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:

    1. 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.

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

    3. 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.

    4. 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.

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

I. The Archiver shall be able to detect motion in video within 200 milliseconds and not only on key frames.

J. The Archiver shall allow for multiple recording schedules to be assigned to a single camera. Each schedule shall be created with the following parameters:

    1. Recording mode:

        a. Continuous.

        b. On Motion/Manual.

        c. Manual.

        d. Disabled.

    2. Recurrence pattern:

        a. Once on specific days.

        b. Specific days on a yearly basis.

        c. Specific days on a monthly basis.

        d. Specific days on a weekly basis.

        e. Daily.

K. Time coverage:

        a. All day.

        b. Specific time range(s).

        c. 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.

L. 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.

M. 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:

    1. Live.

    2. Recording.

    3. Remote.

    4. Low resolution.

    5. High resolution.

N. 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:

1. Maximum bit rate.
2. Maximum frame rate.
3. Image quality.
4. Key frame interval.

O. The Archiver shall have the ability to dynamically boost the quality of the "recording stream" (see previous bullet) based on specific events:
    1. When recording is started manually by a user.
    2. When recording is triggered by a macro, an alarm or detected motion.

P. The Archiver shall have the capacity to communicate with the DVS using 128 bits SSL encryption.

Q. The Archiver shall have the capacity to communicate with the DVS using HTTPS secure protocol.

R. The Archiver shall have the capacity to receive multicast UDP streams directly from the DVS.

S. 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.

T. The Archiver shall have the capacity to redirect audio/video streams to active viewing clients on the network using unicast UDP or TCP.

U. The Archiver shall empower the administrator with a full range of disk management options:
    1. The Archiver shall allow the administrator to choose which disks to use for archiving and to set a maximum quota for each.
    2. 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.
    3. 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.

V. The Archiver shall offer the following options to clean up old archives, on a camera by camera basis:
    1. After a preset number of days.
    2. Deleting oldest archives first when disks run out of space.
    3. Stop archiving when disks are full.

W. The Archiver shall allow important video sequences to be protected against normal disk cleanup routines.

X. Users shall have the following options when protecting a video sequence:

    1. Until a specified date.
    2. For a specified number of days.
    3. Indefinitely (until the protection is explicitly removed).

Y. The Archiver shall allow the administrator to put a cap on the percentage of storage space occupied by protected video.

Z. The Archiver shall keep a log and compile statistics on disk space usage.

    1. The statistics shall be available by disk group or for the whole Archiver.
    2. The statistics shall show the percentage of protected video over the total used disk space.

AA. The Archiver shall have the capacity to down-sample video streams for storage saving purposes. The down-sampling options available are the following:

    1. 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.
    2. 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.

BB. The Archiver shall support DVS with edge recording capabilities and offer the following capacity:

    1. The ability to playback the video recorded on the DVS at different speeds.
    2. The ability to offload (video trickling) the video recorded on the DVS on schedule, on event, or manually to store it on the Archiver.
    3. It shall be possible to filter the video that is being offloaded using one or multiple of the following filters:
        a. Time interval
        b. Playback request
        c. Video analytic events
        d. Motion events
        e. Bookmarks
        f. Alarms
        g. Input pin events
        h. Unit offline events

CC. The Archiver shall be provided with proven performance and scalability figures: HP Series

1. 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.
2. 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.

.

DD. The Archiver shall provide the ability to encrypt the media stream coming from the DVS including the video, audio and metadata Media encryption shall be optional and can be activated on a per DVS basis.

1. Media encryption shall be performed with AES 128-bits.
2. 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.
3. It shall be possible to export the encrypted media into a non-encrypted ASF file.

2.05 Auxiliary Archiver

A. 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.

B. The Auxiliary Archiver shall have the ability to record a camera on a different schedule than the Archiver.

C. 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.

D. The Auxiliary archiver shall have the capacity to move video archives to the Azure Cloud.

.

2.06 VMS Media Streaming

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

B. The Media Router Role shall support multiple transport protocols, such as unicast TCP, unicast UDP, and multicast UDP.

C. The Media Router shall support IGMP (Internet Group Management Protocol) to establish multicast group memberships:

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

D. The Media Router Role using Redirector Agents shall be responsible for redirecting a stream from a source IP endpoint to a destination IP endpoint.

E. The Redirector Agents shall be capable of converting a stream from and to any supported transport protocols:

    1. Multicast UDP to Unicast TCP.
    2. Multicast UDP to Unicast UDP.
    3. Unicast TCP to Multicast UDP.
    4. Unicast UDP to Multicast UDP.

F. 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.

G. 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.

H. 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.

I. Multiple Redirector Agents shall be used on a large VMS installation to increase the service availability and to provide automatic load balancing.

2.07 VMS Video Archives Transfer capabilities

A. Archive transfer shall provide the ability to:

1. Transfer video from a server to another server in the same system.
2. Transfer video from a federated server to another server.
3. Transfer video from camera storage to a server.

B. It shall be possible to program video transfers either on a recurrent schedule, or to trigger them manually or upon connection.

C. It shall be possible to filter the video of interest for a transfer. The video of interest shall be defined with the following filters:

1. All archives when the camera was offline.
2. Alarms.
3. Playback request from the edge.
4. Video analytics events.
5. Motion events.
6. Bookmarks.
7. Input triggers.
8. Time range.

D. 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.

E. 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.

2.10 VMS Analytics

A. Perimeter Protection

1. The analytics shall automatically detect the intrusion of persons or vehicles in critical areas.
2. The analytics shall be completely unified with the Video Management System.
3. Configuration shall natively be performed in the configuration interface of the Video Management System.
4. The analytics shall feature rain and haze filters to filter out disturbances.
5. The analytics shall feature two different detection variants:
    a. Trigger an alarm if a motion pattern moves from zone A (source) through zone B into zone C (sink).
    b. Trigger an alarm if a motion pattern moves anywhere inside a specified zone.
6. The analytics shall support an unlimited number of detection areas (each with its own zones and settings).
7. The analytics shall employ feature-point-based tracking algorithms to detect and analyze motion.
8. The analytics shall not employ pixel-based object tracking but shall employ grid-based analysis (using cues at multiple scales for analytics).
9. The analytics shall offer the possibility to configure object movement paths.
10. The analytics shall not employ tripwires or cross-lines.
11. Areas and the scenes perspective (near & far object size) shall be configured on-screen using a point-and-click interface.
12. The analytics shall feature filters for movement speed, distance, and direction to detect events.
13. The analytics shall be fully server-based, with no calculation on cameras necessary.
14. The analytics shall operate with color, thermal, and infrared cameras.

2.11 Privacy Protector

A. Description:

1. Automatically obscures all movement in surveillance videos in real-time.
2. Live privacy masking of moving objects (such as people and vehicles).
3. Completely unified with the video management system.
4. Native configuration in the configuration interface of the video management system.

B. Details:

1. Certified with a valid certification seal.
2. Indoor / outdoor modes using flexible background modeling:
    a. 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.
    b. 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.
3. Detects movements using an absolute difference image, calculated by subtracting the current frame from a calculated background model.
4. Masks movements using blocks, thus obscuring the outline of an object or person.
5. Eight different scrambling methods: Average, Average Ghost, Colorize, Colorize Difference, Colorize Ghost, Icon, Image, and Blur.
6. Masking grids can be configured in a point-and-click interface.
7. Option to set analysis resolution to optimize performance.
8. No calculation on the camera necessary, completely server-based.

2.12 General Client Software Requirements

A. 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.

B. 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).

C. The CSA for monitoring shall support running in 64-bit mode.

D. 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.

E. The CSA shall seamlessly merge access control, license plate recognition (ALPR), and video functionalities within the same user application.

F. 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.

G. 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.

H. Logging on to a CSA shall be done either through locally stored USP user accounts and passwords or using the operators Windows credentials when Active Directory integration is enabled.

I. 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.

J. 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.

K. To enhance usability and operator efficiency, the Configuration UI and Monitoring UI shall support many of the latest UI such as:

1. A customizable Home Page that includes favorite and recently used tasks.
2. Task-oriented approach for administrator/operator activities where each type of activity (surveillance, visitor management, individual reports, and more) is an operator task.
3. Consolidated and consistent workflows for video, ALPR, and access control.
4. 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.

L. Configuration UI and Monitoring UI Home Page and Tasks

1. The Configuration UI and Monitoring UI shall be task-oriented.
2. 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.
3. Tasks shall be accessible via the Home Page of either the Configuration or the Surveillance CSA.
4. Newly created tasks shall be accessible via the Configuration UI or the Monitoring UI taskbar.
5. Similar tasks shall be grouped into the following categories:
    a. Operation: Access control management, LRP management, and more.
    b. Investigation: Video bookmark/motion/archive reports, access control activity reports, visitor activity reports, alarm reports, ALPR activity reports, and more.
    c. Maintenance: Access control and video configuration reports, troubleshooters, audit trails, health-related reports, and more.
6. An operator shall be able to launch a specific task only if he or she has the appropriate privileges.

7. 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.

M. The Contractor shall provide unlimited simultaneous Clients.

2.13 Configuration User Interface (UI)

A. General

1. 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.

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

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

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

5. The Configuration UI shall include a static reporting interface to:

   a. 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.

   b. View audit trails that show a history of user/administrator changes to an entity.

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

B. Video management system

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

2. 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.

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

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

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

6. The Configuration UI shall provide the ability to change the audio parameters, serial port and I/O configuration of individual DVS units.
7. The Configuration UI shall provide the capability to rename all DVS units based on system topology and to add descriptive information to each DVS.
8. The Configuration UI shall provide the ability to set recording schedules and modes for each individual camera. The recording mode can be:
    a. Continuous.
    b. On motion and Manual.
    c. Manual only.
    d. Disabled.
9. The Configuration UI shall support the creation of schedules to which any of the following functional aspects can be attached:
    a. Video quality (for each video stream per camera).
    b. Recording (for each camera).
    c. Motion detection (for each detection zone per camera).
    d. Brightness, Contrast, and Hue (for each camera)
    e. Camera sequence execution
10. The Configuration UI shall support the creation of unlimited recording schedules and the assigning of any camera to any schedule.
11. The Configuration UI shall detect and warn user of any conflict within assigned schedules.
12. 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.
13. 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.

2.14 VMS Client User Interface (UI)

A. 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.

B. 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.

C. To enhance usability and operator efficiency, the Monitoring UI shall support the following UI concepts:

1. Dynamically adaptive interface that adjusts in real-time to what the operator is doing.
2. A dynamic dashboard loaded with entity-specific widgets (e.g. door and camera widgets).
3. Use of transparent overlays that can display multiple types of data in a seamless fashion.
4. Display tile menus and quick commands.
5. Consolidated and consistent workflows.
6. Tile menus and quick commands easily accessible within every display tile of the user workspace.
7. 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.

D. Monitoring UI Home Page and Tasks

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

E. Dynamically Adaptive UI, Dashboard, and Widgets

1. 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 dashboard.
2. Widgets shall be mini-applications or mini-groupings in the Monitoring UI dashboard that let the operator perform common tasks and provide them with fast access to information and actions.
3. With a single click on an entity (e.g. 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.
4. Specific widgets include those for a door, camera, alarm, zone, display tile, video stream (statistics), PTZ camera, and more.

F. Operator Workflows

1. 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.
2. The Monitoring UI shall be equipped with consistent workflows for the ALPR, video, and access control systems that it unifies.
3. 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.

G. Each task within the Monitoring UI shall consist of one or more of the following items:
   1. Event list.
   2. Logical tree. Doors, cameras, zones, ALPR units, and elevators shall be grouped under Areas in a hierarchical fashion.
   3. Entities list of all entities being tracked.
   4. Display tiles with various patterns (1 x 1, 2 x 2, and more).
   5. Display tile menu with various commands related to cameras, doors, PTZ, and tile controls.
   6. Dashboard with widgets.

H. The Monitoring UI shall support multiple event lists and display tile patterns, including:
   1. Event/alarm list layout only
   2. Display tile layout only
   3. Display tile and alarm/event list combination
   4. ALPR map and alarm/event list combination

I. User workspace customization
   1. 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.
   2. Once customized, the user shall be able to save his or her workspace.
   3. The user workspace shall be accessible by a specific user from any client application on the network.
   4. Display tile patterns shall be customizable.
   5. 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.

6. The Monitoring UI shall support multiple display tile patterns (e.g. 1 display tile (1x1 matrix), 16 tiles (8x8 matrix), and multiple additional variations).
7. The Monitoring UI shall support as many monitors as the PC video adapters and Windows Operating System are capable of accepting.
8. 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.

J. The Monitoring UI shall provide an interface to support the following tasks and activities common to access control, ALPR, and video:

1. Monitoring the events from a live security system (ACS and/or VMS and/or ALPR).
2. Generating reports, including custom reports.
3. Monitoring and acknowledging alarms.
4. Creating and editing incidents and generating incident reports.
5. Displaying dynamic graphical maps and floor plans as well as executing actions from dynamic graphical maps and floor plans.
6. Management and execution of hot actions and macros.

K. 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.

L. The Monitoring UI shall include advanced video capabilities, including:

1. Advanced live video viewing functionality.
2. Advanced archive playing and video playback functionality.
3. Monitoring and management of video system events and alarms.
4. Intercom or duplex audio.
5. Generation of video reports.
6. Control of PTZ cameras.
7. Creating and monitoring archive transfer requests.
8. Display metadata overlaid on live or playback video.

M. The Monitoring UI shall leverage the Graphical Processing Unit (GPU) for video decoding.

1. The following GPU technologies shall be supported:
    a. NVidia CUDA
    b. Intel Quick Sync

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

N. The live video viewing capabilities of the Monitoring UI shall include:

1. The ability to display all cameras attached to the USP and all cameras attached to federated systems.
2. Support for live video monitoring on each and every display tile within a task in the user's workspace.
3. 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.
4. The ability to drag and drop a camera into a display tile for live viewing.
5. 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).
6. The ability to drag and drop a camera from a map into a display tile for live viewing.
7. Support for digital zoom on live camera video streams.
8. The ability for audio communication with video units with audio input and output.
9. The ability to control pan-tilt-zoom, iris, focus, and presets.
10. 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.
11. 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.
12. The ability to activate or de-activate viewing of all system events as they occur.
13. The ability to switch to instant replay of the video for any archiving camera with the simple click of button.
14. The ability to take snapshots of live video and be able to save or print the snapshots.
15. The ability to view the same camera multiple times in different tiles.

O. The video playback (archive playing) capabilities of the Monitoring UI shall include:

1. Support for audio and video playback for any time span.
2. Support for video playback on each and every display tile.
3. The ability to instantly replay the video for any archiving camera with the simple click of a button.

4. 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.
5. The ability to simultaneously view the same camera in multiple tiles at different time intervals.
6. The ability to control playback with:
    a. Pause.
    b. Lock Speed.
    c. Forward and Reverse Playback at: 1x, 2x, 4x, 6x, 8x, 10x, 20x, 40x, 100x.
    d. Forward and Reverse Playback frame by frame.
    e. Slow Forward and Reverse Playback at: 1/8x, 1/4x, 1/3x, 1/2x.
    f. Loop playback between two time markers.
7. 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.
8. The ability to display the level of motion at any point on a timeline.
9. The ability to clearly display bookmarked events on the timeline(s).
10. The ability to query archived video using various search criteria, including, but not limited to, time, date, camera, and area.
11. The tool necessary for searching video and associated audio based on user-defined events or motion parameters.
12. 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.
13. The ability to browse through a list of all bookmarks created on the system and select any bookmarked event for viewing.
14. The ability to add bookmarks to previously archived video for easier searching and retrieval.
15. Support for digital zoom on playback video streams.
16. Still image export to PNG, JPEG, GIF, and BMP format with Date and Time stamp, and Camera Name on the image (snapshot).
17. 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.

18. Tools for exporting video sequences in standard video formats, such as ASF or MP4.
19. The ability to encrypt exported video files.
20. The ability for an operator to load previously exported video files from their computer or network.
21. The ability for queries to be saved upon closing the CSA and reappear when the application is reopened.
22. 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.
23. 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.
24. The ability to store the video export and still image export at a pre-defined storage location.
25. An interface with the ability to list, search, and manipulate previously generated video exports.
26. The ability to export sequences of video in open standards including ASF and MP4.

P. The Monitoring UI shall provide an interface to support the following ALPR tasks and capabilities:

1. Monitoring and management of ALPR events and alarms.
2. Viewing of license plate picture(s) and context images.
3. Viewing of license plate data (e.g. license plate reads)
4. Verification of ALPR data against live and recorded video.

Q. Entity Monitoring

1. 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.
2. The Monitoring UI shall provide the option to filter which events shall be displayed in the display tile layout and/or event list layout.
3. 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).
4. 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.
5. Event, alarm, monitoring/tracking, and report lists shall contain cardholder pictures where applicable.
6. The user shall be permitted to start or pause the viewing of events within

each display tile.

R. Display Tile Packing and Unpacking

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

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

3. 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.

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

S. Visual Tracking

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

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

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

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

2.15 Server Administrator User Interface Requirements

A. 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.

B. 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.

C. Access to the Server Administrator shall be protected via login name, password, and encrypted communications.

D. The Server Administrator shall allow the administrator (user) to perform the following functions:

1. Manage the system license.

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

3. Activate/Deactivate the Directory Role.

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

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

6. Configure the network communications hardware, including connection addresses and ports.
7. Configure system SMTP settings (mail server and port).
8. Configure event and alarm history storage options.

2.16 Unified Web Client (UWC) General Requirements

A. The USP shall support a unified web client (UWC) for access control and video.

B. The UWC shall be a truly thin client with no download required other than an internet web browser or standard web browser plugins.

C. The UWC shall be platform independent and run within Microsoft Edge, Internet Explorer, Firefox, Safari, and Google Chrome.

D. 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.

E. Video Stream shall be redirected to the Web Client with no stream transformation or re-encoding for all streams in H264.

F. The Contractor shall provide unlimited simultaneous Web Clients.

G. Functionalities:

1. Login using name and password or Active Directory support shall be available.
2. Encrypted communications for all transactions.
3. Print reports and export to CSV file.
4. Customer logo customization shall be available for multi-tenant and hosted services applications.
5. Video
    a. Live and playback video at 320 x 240, 640 x 480 or 1280 x 1024 @ 15 fps.
    b. Video export.
    c. 1, 4, 6 or 9 tiles.
    d. Basic PTZ Controls (Pan/Tilt, Zoom, go to presets, start pattern).
    e. Start / Stop recording.
    f. Sample web page for customers to see how to view video for their own development.
    g. Add bookmarks.
6. Alarms

a. Alarm report.

2.17 Smartphone and Tablet App General Requirements

A. The USP shall support mobile apps for various off-the-shelf smartphones and tablets. The mobile apps shall communicate with the Mobile Server of the USP over any WiFi or mobile network connection.

B. Mobile apps shall communicate with the USP via a Mobile Server (same as the Unified Web Client or UWC). Communication between the mobile device and the Mobile Server shall support optional encryption.

C. Supported device manufacturers shall include (refer to Mobile App specifications for latest compatibility list):

1. Apple iPod Touch, iPhone, and iPad.
2. Android-compatible smartphones and tablets.
3. Windows and Windows Phone 8.1.

D. It shall be possible to download the mobile apps from the Central application store (Apple iTunes App Store, Google Play, Windows Store).

E. Functionalities

1. Live monitoring and command and control of the USP.
2. Receive alarm push notifications from the Apple Push Notification Server or from the Google Android push server.
3. Alarm management (view and acknowledge alarms, video tied to alarms).
4. View USP hierarchy and search for entities.
5. Stream video from the mobile device using the built-in camera.
    a. Video streams from mobile devices shall be available in the USP to be viewed in live and recorded on the Archiver.
6. Video
    a. View live and playback video at 320 x 240, 640 x 480 or 1280 x 1024 @ 15 fps.
    b. Monitor camera status.
    c. View up to 6 video feeds.
    d. Control PTZ functionality of a camera, including access to PTZ presets.
    e. Save snapshots locally on the device.
    f. View video tied to access control events, and alarms.

2.18 Health Monitor

A. The USP shall monitor the health of the system, log health-related events, and calculate statistics.

B. USP services, roles, agents, units, and client apps will trigger health events.

C. The USP shall populate the Windows Event Log with health events related to USP roles, services, and client apps.

D. A dedicated role, the Health Monitoring Role, shall perform the following actions:

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

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

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

E. A Health Monitoring task and Health History reporting task shall be available for live and historical reporting.

F. A web-based, centralized health dashboard shall be available to remotely view unit and role health events of the USP.

G. 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.

H. Health events shall be accessible via the SDK (can be used to create SNMP traps).

2.19 Session Initiation Protocol (SIP) Communication Management (CM)

A. 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.

B. The USP shall support CM between the USP client User Interface and SIP endpoint devices.

C. SIP endpoints shall be able to register to the USP using a standard SIP protocol.

D. The USP shall support CM between two SIP endpoint devices.

E. The USP shall allow the configuration of SIP trunk connections to multiple SIP Servers supporting SIP Trunks.

F. The CM shall support the management of calls to and from other SIP Servers connected though SIP Trunks.

G. The CM is a service of the USP and shall not require the addition of any third party software.

H. The CM shall support the following video codecs:

1. H.264
2. H.263
3. H.263+ (1998)

I. The CM shall support the following audio codecs:
   1. PCMA (G.711 aLaw)
   2. PCMU (G.711 uLaw) 3. G.722
   4. G.729
   5. iLBC
   6. GSM
   7. telephone event
   8. Speex (Narrowband)
   9. Speex (Wideband)
   10. Speex (Ultrawideband) 11. L.16
   12. L.16-44-1
   13. G.728
   14. G.726-16
   15. G.726-24
   16. G.726-32
   17. G.726-40

J. The CM shall certify SIP devices from the following manufacturers:
   1. 2N Telekomunikace
   2. Axis
   3. Cisco
   4. Code Blue
   5. Commend
   6. EMCOM
   7. Jacques
   8. Siedle
   9. TalkaPhone

10. TOA Corporation
11. Vingtor-Stentofon
12. Zenitel

K. The CM shall allow bidirectional audio and video recording of call sessions. The USP shall offer the following recording capabilities:

1. Automatic cleanup of call session files after a programmable number of days
2. Deactivation of call recording between operators
3. Deactivation of call recording with specific operators
4. Deactivation of call recording with specific voice devices
5. Selection of the storage path for call session recordings

L. The CM shall provide the flexibility for the administrator to define the network ports used to communicate between the USP servers and the following:

1. USP Operator Client User Interfaces
2. SIP devices
3. SIP servers

M. 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.

N. 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:

1. Match a phone number with regular expression.
2. Route calls based on matching the phone numbers from which calls are made.
3. Route calls based on matching the destination phone numbers to which calls are made.
4. Change the phone extension from which calls are received.
5. Change the phone extensions to which calls are sent.
6. A combination of any of the above capabilities in a configured priority and based on a schedule.

O. Dial Plans shall be applicable to calls between SIP entities registered to the USP as well as to and from external SIP servers.

P. 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.

Q. The USP shall support video and audio calls:

1. Between USP Client User Interfaces.
2. To and from USP Client User Interfaces and SIP devices.
3. Between SIP devices.

R. The USP shall provide an advanced and friendly call management user interface that allows operators to:

1. 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.
2. Display the video associated with the call and switch between multiple video sources.
3. Receive incoming call notifications directly through a notification tray.
4. Initiate, answer, forward, place on hold, or cancel calls from a dedicated call dialog box.
5. Control cameras, doors, zones, and device outputs during a call.
6. 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.
7. Dial a phone number to make a call.
8. Dial a DTMF sequence during a call.
9. Monitor the availability status of a user and set its own availability status.
10. 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.

S. 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.

T. The USP shall offer a call window. It shall be possible within the call windows to:

1. Switch between cameras associated with the call participant.
2. Open and lock doors associated with the call participant.
3. Arm and Disarm zones associated with the call participant.
4. Trigger outputs associated with the call participant.
5. Put on hold, resume, forward, and end a call.
6. Mute the microphone.
7. Hide the webcam video feed.

U. 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:

    1. Call a contact by simply double-clicking the contact name.
    2. See the availability status of their contacts (users and SIP Devices).
    3. Quickly display a contact's information, such as photo, name, and number.
    4. Filter their contacts by type (SIP Device or User).
    5. Create a list of favorites by adding and removing contacts.
    6. Search for and call numbers that appear in the contact list.

V. The USP shall provide a graphical dial pad to allow the operator to make calls and dial DTMF tones during a call.

W. 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:

    1. Date and time.
    2. Call session duration.
    3. Involved users and call stations.
    4. Call events and actions.
    5. Actions taken by a user on doors, intrusion zones and outputs during the call session.

X. The USP shall give the capability to export a call session, including bidirectional audio, associated video, and log journal of the call session.

Y. 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:

    1. Answer or reject an incoming call.
    2. Initiate a call to the device.
    3. Put on hold and resume a call with the device.

Z. 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.

2.20 USP General Requirements

A. The Unified Security Platform (USP) shall be an enterprise class IP-enabled security and safety software solution.

B. 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.

C. Functionalities available with the USP shall include:

1. Configuration of embedded systems, such as ACS, ALPR, and VMS systems.
2. Live event monitoring.
3. Live video monitoring and playback of archived video.
4. Alarm management.
5. Reporting, including creating custom report templates and incident reports.
6. Global cardholder management across multiple facilities and geographic areas each with their own independent ACS system.
7. Microsoft Active Directory integration for synchronizing USP user accounts and ACS cardholder accounts.
8. Intrusion device and panel integration (live monitoring, reporting, and arming/disarming).
9. SIP Intercom device integration for bi-directional communication.
10. Integration with third party systems and databases via plug-ins (access control, video analytics, point of sale, and more).
11. Dynamic graphical map viewing.

D. The USP shall be deployed in one or more of the following types of installations:

1. Unified access, ALPR, video platform, and any combination thereof.
2. Standalone access control, ALPR, or video platform.
3. Unified access and video platform that federates multiple remote ACS, VMS, ALPR.
4. Standalone video platform that federates multiple independent remote VMS.
5. Standalone access control that federates multiple independent remote ACS.
6. Standalone access control that federates multiple independent remote ALPR.

E. Licensing

1. A single central license shall be applied centrally on the configuration server.
2. There shall be no requirement to apply a license at every server computer or client workstation.
3. Based on selected options, one or more embedded systems shall be enabled or

disabled.

F. Hardware and Software Requirements

1. 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.

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

3. 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.

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

5. 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.

2.21 USP Architecture

A. 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).

B. 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.

C. 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.

D. 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.

E. 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.

F. The USP shall protect against potential database server failure and continue to run through standard off-the-shelf solutions.

G. 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.

H. 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.

I. 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.

J. Roles-Based Architecture

1. The USP shall consist of a role-based architecture, with each SSM hosting one or more roles.
2. 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:
    a. Deploy one or several SSM across the network prior to activating roles.
    b. Activate and deactivate roles as needed on each and every SSM.
    c. Centralize role configuration and management.
    d. Support remote configuration.
    e. Move roles over from one SSM to another.
3. Each role, where needed, shall have its own database to store events and role-specific configuration information.
4. 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.
5. Directory Role
    a. The Directory Role shall manage the central database that contains all the system information and component configuration of the USP.
    b. The Directory Role shall authenticate users and give access to the USP based on predefined user access rights or privileges, and security partition settings.
    c. The Directory Role shall support the configuration/management of the following components common to the ACS, ALPR, and VMS sub-systems:
        i. Security Partitions, users and user groups.
        ii. Areas.
        iii. Zones, input/output (IO) linking rules, and custom output behavior.
        iv. Alarms. Schedules, and scheduled tasks.
        v. Custom events.
        vi. Macros or custom scripts.
    d. The Directory Role shall support the configuration/management of the following components specific to VMS:

i. Video servers and their peripherals (e.g. audio, IOs, and serial ports).
ii. PTZ.
iii. Camera sequences.
iv. Recording and archiving schedules.

e. The Directory Role shall support the configuration/management of the following components specific to ACS:

i. Door controllers, and input and output (IO) modules.
ii. Doors, Elevators, and Access rules.
iii. Cardholders and cardholder groups, credentials, and badge templates.

f. The Directory Role shall support the configuration/management of the following components specific to ALPR:

i. ALPR units and cameras.
ii. Hotlists, permit lists, and overtime rules.

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

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

8. 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.

9. 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.

10. 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.

11. 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.

12. Optional Roles

a. 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.

b. The Global Cardholder Synchronizer Role shall be responsible for synchronizing cardholder and credential data between the local site and a

central site. Synchronization between remote sites shall also be supported.

c. The Active Directory Role shall be responsible for synchronizing user accounts and cardholder accounts with a Microsoft Active Directory server.

d. The Intrusion Manager Role shall be responsible for managing third party intrusion devices such as alarm panels and perimeter detection devices. This role shall also be responsible for logging all intrusion events in a database.

e. The Asset Manager Role shall be responsible for integrating and synchronizing with third party asset management systems and logging asset related events. This role shall also be responsible for supporting the execution of asset-related reports such as inventory reports and asset activity reports

f. 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.

g. 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. The Communication Management Role shall be responsible for registering the SIP communication endpoints and for managing the call routing.

h. 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.

i. The Media Gateway Role shall be responsible for connecting any video stream to a third party system using standard RTSP protocol. This role shall provide access to live video.

K. Server Monitoring Service (Watchdog)

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

2. 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.

3. 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.

2.22 USP Access Control, Video, and ALPR Unification

A. 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.

B. The Configuration UI shall present a true Unified Security Interface for the configuration and management of the ACS, VMS, and ALPR.

C. 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.

D. It shall be possible to view video associated to access control events when viewing a report.

E. It shall be possible to view video associated to intrusion panel events when viewing a report.

F. It shall be possible to view video associated to ALPR events when viewing a report.

G. The USP shall support the following Alarm Management functionality:

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

2. 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.
3. Set the priority level of an alarm and its reactivation threshold.
4. Define whether to display live or recorded video, still frames or a mix once the alarm is triggered.
5. Provide the ability to display live and recorded video within the same video tile using picture-in-picture (PiP) mode.
6. Provide the ability to group alarms by source and by type.
7. Define the time period after which the alarm is automatically acknowledged.
8. 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.
9. Define the alarm broadcast mode. Alarm notifications shall be sent using either a sequential or an all-at-once broadcast mode.
10. Define whether to display the source of the alarm, one or more entities, or an HTML page.
11. Specify whether an incident report is mandatory during acknowledgment.

H. The workflows to create, modify, add instructions and procedures, and acknowledge an alarm shall be consistent for access control, ALPR, and video alarms.

I. Alarms shall be federated, allowing global alarm management across multiple independent USP, ACS, VMS, and ALPR systems.

J. The USP shall also support alarm notification to an email address or any device using the SMTP protocol.

K. 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.

L. 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.

M. The user shall have the ability to acknowledge alarms, create an incident upon alarm acknowledgement, and put an alarm to snooze.

N. The user shall be able to spontaneously trigger alarms based on something he or she sees in the system.

O. An alarm shall be configured in such a way that it remains visible until the source condition has been acknowledged.

P. The user shall be able to investigate an alarm without acknowledging it.

2.23 USP Threat Levels

A. The USP shall support Threat Levels to dynamically change the system behavior to respond to critical events.

B. Threat Levels shall be activated and deactivated by the CSA operator with the right privilege.

C. Threat Levels shall be set on an area or on the entire system.

D. 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.

E. The following specific actions shall be available with Threat Level:

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

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

   3. Set reader mode to change how the doors are accessed (e.g. card and PIN, or card or PIN).

F. A visible notification shall be displayed in all operator CSA when a Threat Level is activated.

2.24 USP Remote Task

A. 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.

B. The USP shall support video wall applications by connecting and controlling multiple workstations and monitors simultaneously.

C. The Remote Task shall be a graphical interface showing a replication of the remote workstation running the CSA (Monitoring UI).

D. The Remote Task shall allow the connection to other workstations using a low bandwidth mode to receive only snapshots of video viewed remotely.

E. The Remote Task shall allow the connection to other workstations using a spy mode to remain invisible to the remotely connected workstation.

F. The functionality provided by the remote monitoring and control capability shall include:

   1. Remote monitoring and control of the monitoring and alarm monitoring tasks.

   2. Ability to remotely switch cameras, doors and zones into display tiles.

   3. Ability to remotely control live and playback video.

   4. Ability to remotely change the tile pattern.

5. Ability to remotely create and delete tasks.
6. Ability to remotely start/stop task cycling.
7. Ability to remotely go into full screen mode.
8. Ability to remotely save and reload the workspace.

2.25 USP Advanced Task Management

A. USP shall support an infrastructure for managing Monitoring UI tasks used for live monitoring, day to day activities, and reporting.

B. 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.

C. 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.

D. 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.

2.26 USP Reporting

A. The USP shall support report generation (database reporting) for access control, ALPR, video, and intrusion.

B. 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 he or she has the appropriate privilege.

C. The workflows to create, modify, and run a report shall be consistent for access control, ALPR, and video reports.

D. Reports shall be federated, allowing global consolidated reporting across multiple independent USP, ACS, VMS, and ALPR systems.

E. Access control and ALPR reports shall support cardholder pictures and license plate pictures, respectively.

F. The USP shall support the following types of reports:

1. Alarm reports.
2. Video-specific reports (archive, bookmark, motion, and more).
3. Configuration reports (cardholders, credentials, units, access rules, readers/inputs/outputs, and more).
4. Activity reports (cardholder, cardholder group, visitor, credential, door, unit, area, zone, elevator, and more).
5. ALPR-specific reports (mobile ALPR playback, hits, plate reads, reads/hits per day, reads/hits per ALPR zone, and more).

6. Health activity and health statistics reports.

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

G. Generic Reports, Custom Reports and Report Templates

1. 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.

2. 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).

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

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

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

H. 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.

I. The USP shall support comprehensive data filtering for most reports based on entity type, event type, event timestamp, custom fields, and more.

J. The user shall be able to click on an entity within an existing report to generate additional reports from the Monitoring UI.

K. The USP shall support the following actions on a report: print report, export report to a PDF/Microsoft Excel/CSV file, and automatically email a report based on a schedule and a list of one or more recipients.

2.27 USP Federation feature: Monitoring of Remote Systems

A. The USP shall support the concept of a Federation feature for access control, video, and ALPR.

B. 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.

C. The Federation feature shall support the unification of multiple independent video surveillance systems or VMS.

D. 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).

E. 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.

F. The Federation feature shall support Global Alarm Management from the Monitoring UI for access control, video, and ALPR.

G. The Federation feature shall support Global Report Generation from the Monitoring UI for access control, video, and ALPR.

H. The Federation feature shall support dozens of operator actions on remote (federated) entities from the Monitoring UI (e.g. generating a global report taking into account events from multiple independent sites or acknowledging remote alarms).

2.28 USP Zone Management

A. 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 he or she has the appropriate privileges.

B. 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.

C. 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.

D. A schedule shall be defined for a zone, indicating when the zone will be monitored.

E. 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.

F. The ACS shall support one or more cameras per zone. Video shall then be associated to zone state changes.

G. Input/Output (IO) Linking

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

2. IO Linking shall be available in offline mode when communication between the server and hardware is not available.

3. 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.

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

2.29 USP User and User Group Security, Partitions, and Privileges Management

A. 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 he or she has the appropriate privileges.

B. The USP shall support user authentication with claims-based authentication using external providers. External providers shall include:

1. ADFS (Active Directory Federation Services)

C. 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.

D. User privileges shall be extensive in the USP. All configurable entities for the USP, including access control, video, and ALPR, shall have associated privileges.

E. 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.

F. Partitions

1. 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.

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

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

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

G. It shall be possible to specify user and user group privileges on a per partition basis.

H. Advanced logon options shall be available such as dual logon and more.

I. 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.

2.30 USP Event/Action Management

A. 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.

B. 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.

C. The USP shall receive and log the following events:

    1. System-wide events
    2. Application events (clients and servers)
    3. Area, camera, door, elevator, and ALPR events (reads and hits)
    4. Unit events
    5. Zone events
    6. Alarm events
    7. ALPR events

D. The USP shall allow the creation of custom events.

E. 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:

    1. Add bookmark
    2. Block and unblock video
    3. Display a camera on an analog monitor
    4. Display an entity in the CSA
    5. Email a report
    6. Email a snapshot
    7. Export report
    8. Go home
    9. Go to preset
    10. Override recording quality
    11. Play a sound
    12. Reboot unit
    13. Run a macro
    14. Run a pattern
    15. Send a message
    16. Send an email
    17. Set threat level

18. Start/Stop applying video protection
19. Start/Stop recording
20. Start/Stop transfer
21. Trigger alarm
22. Trigger output

F. 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.

2.31 USP Schedules and Scheduled Tasks

A. Schedules

1. The USP shall support the configuration and management of complex schedules. A user shall be able to add, delete, or modify a schedule if he or she has the appropriate privileges.
2. 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.
3. Daily, weekly, ordinal, and specific schedules shall be supported.

B. Scheduled Tasks

1. The USP shall support scheduled tasks for video, and ALPR.
2. 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.
3. Scheduled tasks shall support all standard actions available within the USP, such as sending an email or emailing a report.

2.32 USP Macros and Custom Scripts

A. 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.

B. Custom macros shall be created with the USP Software Development Kit (SDK).

C. A macro shall be executed either automatically or manually.

D. In the Monitoring UI, a macro shall be launched through hot actions.

2.33 USP Dynamic Graphical Maps (DGM)

A. The USP shall support mapping functionality for access control, video surveillance, intrusion detection, ALPR, and external applications.

B. 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.

C. 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 screen must provide the same command and control capabilities than in a single screen display The DGM shall support the following file format and protocol for importing map background:

1. PDF
2. JPG
3. PNG
4. Web Map Service (WMS) defined by the Open Geospatial Consortium (OGC)
5. BeNomad

D. 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

1. Google Map, aerial, terrain (Licensed)
2. Bing Map, aerial, satellite, hybrid (Licensed)

E. It shall be possible to configure a mixed set of maps made of GIS, online providers and private imported files and link them together.

F. The DGM shall provide the ability to display all native entities of the USP including:

1. Cameras, fix, and PTZ
2. Doors
3. Camera sequences
4. Areas
5. Intrusion areas
6. Intrusion zones
7. License Plate Recognition cameras
8. Digital inputs
9. Digital outputs
10. Intercoms
11. Alarms
12. Macros
13. Police Car Patrollers

G. The DGM shall provide the ability to draw and display information over the map in the form of:

    1. Vectoriel shapes: line, rectangles, polygones, ellipse
    2. Pictures
    3. Text

H. The DGM shall provide the ability to display any type of third party entities integrated through an SDK.

I. The DGM shall provide the ability to display layer of information in Keyhole Markup Language (KML) format.

J. The DGM shall provide the ability to the operator to manage layers of entities display over the map, being able to turn them on and off and changing the superposition order.

K. The DGM shall offer built-in map data backup and restore for both map background and layers of entities.

L. The DGM shall offer failover capabilities.

M. The DGM shall scale up to several thousands of entities on a single map and hundreds of maps.

N. The DGM shall provide a means to update a map background without affecting the map object configuration.

O. The DGM shall offer a user friendly graphical map designer to configure the maps.

P. The DGM shall provide a user friendly and intuitive navigation that includes:

    1. The ability to create hierarchies of maps to facilitate navigation within and between various sites and buildings.
    2. The ability to define favorites for recurrent position recall.
    3. 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.
    4. A common user experience regarding navigation into the map for both GIS and private maps.
    5. A history log of positions.

Q. 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.

R. The DGM shall display the actual video Field of View of camera. It shall be possible to configure the FOV of a camera by entering the specification of the camera installation or graphically by moving the boundaries of the Field of View.

S. For PTZ cameras offering position feedback capability, the DGM shall

   1. Dynamically represent the accurate Field of View of the camera.

   2. Allow the user to act on the PTZ by moving its field of view.

T. The DGM shall offer the ability to optionally set a graphical display notification of the motion detection.

U. The DGM shall offer a smart selection tool to access the video simply by clicking the location the user wants to see, the DGM will automatically select the cameras that can see this location and move the PTZ towards that location. This smart selection tool shall take into consideration the obstacle and not display cameras that cannot see the location because of a wall.

V. It shall be possible to select a location by drawing a zone of interest on the DGM and display all the entities that are part of that zone of interest at once.

W. The user shall be able to select and display the content of multiple USP entities on the map in popup windows.

X. It shall be possible to access live and playback video from the map.

Y. It shall be possible to monitor from the DGM all entities event notification. User shall be able to turn on and off the notification per entity.

AA. The DGM shall offer the ability to fully operate alarm monitoring. It shall be possible to:

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

   2. Visualize the Alarms notification on the map access the related video from the map.

   3. Trigger and receive alarms.

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

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

BB. The DGM shall provide the following search capabilities:

   1. Search and center by entity name.

   2. 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.

CC. Any update of map content by an administrator shall be immediately and dynamically pushed to all DGM users.

2.34 USP Audit and User Activity Trails (Logs)

A. The USP shall support the generation of audit trails. Audit trails shall consist of logs of operator/administrator additions, deletions, and modifications.

B. 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.

C. For entity configuration changes, the audit trail report shall include detailed information of the value before and after the changes.

D. 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.

E. 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.

2.35 USP Incident Reports

A. 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.

B. The operator shall be able to create standalone incident reports or incident reports tied to alarms.

C. 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.

D. 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.

E. Incident reports shall allow the creation of a custom form on which to input information on an incident.

F. Incident reports shall allow entities, events, and alarms to be added to support at the report's conclusions.

2.36 USP Third Party Integration

A. Microsoft Active Directory Integration

1. 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.

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

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

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

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

6. When enabled, Active Directory shall manage user logon to the USP client applications through the user's Windows credentials. Logging to the USP shall utilize native Active Directory password management and authentication features.
7. It shall be possible to synchronize the following USP entities and their information from Active Directory with the USP:
    a. Users (username, first and last names, email address, and more).
    b. User groups (user group name, description, and group email address).
    c. Active Directory attributes to USP custom fields.
8. 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.
9. Supported synchronization methods for additions, modification, and deletions of synchronized entities shall include: on first logon (users only), manual synchronization, and scheduled synchronization.
10. The USP shall support user connections across independent organizations by connecting to an external ADFS (Active Directory Federation Services) service using claims-based authentication.

B. Intrusion Detection Integration

1. The USP shall integrate with third party intrusion panels and devices via an Intrusion SDK. The Intrusion Manager Role shall manage communications with the intrusion panels. Communications with intrusion devices shall be over serial communications and/or an IP network.
2. Integration with intrusion panels shall be possible outside the release cycle of the USP. It shall be possible to add new integrations at any point in time.
3. Functionality available via the integration of intrusion devices with the USP shall include the following (where supported by the intrusion panel):
    a. Arm and disarm intrusion devices (manually, on schedule, or following a USP event).
    b. Activate or trigger intrusion device outputs.
    c. View intrusion events and alarms.
    d. Monitor the status, including arming status, of the intrusion devices.
    e. Video verification of intrusion events and alarms with video panels.
    f. Create USP zones using intrusion device inputs.
4. Currently supported intrusion panels include:
    a. Bosch G Series panels.

b. DSC Power Series panels.

c. DMP XR Series panels.

d. Honeywell Galaxy Dimension panels.

C. Third Party Access Control Systems

1. The USP shall integrate with third party access control software via the SDK. Communications with access control software shall be over an IP network, and should not support administrative tasks such as cardholder management.

2. Integration with access control software shall be possible outside the release cycle of the USP. It shall be possible to add new integrations at any point in time.

3. Functionality available via the integration of access control software with the USP shall include the following (where supported by the access control solution):

   a. Synchronize access control entities and receive associated events and states within the USP, including:

      i. Cardholders and access rights

      ii. Visitors

      iii. Readers and doors

      iv. Alarms

   b. Monitor access control events

   c. Monitor and Acknowledge access control alarms

   d. Trigger actions and outputs in the access control software using hot actions and event-to-actions

   e. Lock and unlock doors in the access control software

   f. Configure event-to-actions using the access control events and alarms

   g. Generate Security Center reports using from the in the access control data

   h. View and monitor states of door entities in the USP maps

D. Asset Management Integration

1. The USP shall integrate with third party asset management systems via the Asset Management Role.

2. Communications with asset management solutions shall be over an IP network (via software communications).

3. Functionality available via the integration of asset management systems with the USP shall include the following (where supported by the asset management systems):

a. Synchronize asset management system assets with USP asset entities.

b. Live monitoring of asset-related activity events, health events, and activity (asset online, asset offline, asset moves, or low battery).

c. Synchronization of asset management alarms with Security Center alarms.

d. Viewing video tied to asset-related activity and alerts within monitoring and reporting tasks.

e. Acknowledging alarms in Security Center which acknowledges alerts in the asset management system and vice versa.

f. Real-time tracking of asset locations on a per area basis.

g. Asset Management Inventory reporting task that details the current location (area) of an asset.

h. Asset Activity reporting task that provides a historical review of asset-related events and activity.

4. Currently supported asset management systems include:

a. RF Code Asset Manager.

E. Additional Third Party Integrations

1. 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.

2. The USP architecture shall support the addition of new connectors to integrate to third party system integration, such as:

a. Video analytics.

b. Third party video systems.

c. Third party access control systems.

d. ALPR integrations with pay stations, permit vendors, pay-by-phone vendors, and ticketing vendors.

e. Point-of-sale (POS) systems.

f. Building management systems.

g. Human resource management systems (HRMS).

2.37 USP Software Development Kit (SDK)

A. A USP SDK shall be available to support custom development for the platform.

B. The SDK shall include functionalities specific to the embedded automatic license plate recognition (ALPR), access control (ACS), and video (VMS) systems.

C. Integration with external applications and databases shall be possible with the SDK.

D. 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.

E. The SDK shall be based on the .NET framework.

F. The SDK shall support dynamic or transactional updates to the USP configuration. It shall also support change notification of USP entity configuration.

G. 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.

H. The SDK shall provide an extensive list of programming functions to view and configure ACS, VMS, and ALPR.

I. 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.

J. 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.

K. 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.

L. The SDK shall support the following alarm functions: view alarms in real time, acknowledge alarms, change priority, and change recipient.

Part 3 - Execution

3.01 Warranty

A. 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.

B. 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:

1. Access to phone support and online chat for technical assistance.

2. Online case management.

3. Online system availability monitor.

4. Access to Major and Minor Release Upgrades.

5. 24/7 pager support and dedicated support specialist. *(Specifier, additional cost)*

3.02 Deployment Services and System Commissioning

A. General Requirements

1. 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:

   a. Multiple contractors or subcontractors that will be responsible for deploying the USP at multiple client sites in different geographical regions.

   b. Complex enterprise installations involving advanced functionality (e.g. The Federation feature, failover, plugins) and/or multiple systems (e.g. access control, video, ALPR) and/or third party integrations.

   c. Extensive use of customized solutions/plugins developed by the vendor that will be integrated into the USP.

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

B. Deployment Management Service

1. 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:

   a. Conducting a Risk Assessment of the impact of potential risk factors on the operation of the vendor's USP.

   b. Providing a project plan for the deployment of the vendor's USP.

   c. Managing the development and deployment of the custom solution components that will be integrated into the vendor's USP (if applicable).

   d. Providing a scope of work detailing the services to be provided by the vendor to assist in the deployment of the vendor’s USP.

   e. Coordinating and scheduling the vendor field services with the contractor to assist with the deployment of the vendor’s USP.

   f. Providing regular project status updates to the contractor regarding the development of custom solutions (if applicable) and the deployment of the vendor’s USP.

C. Solution Architect Service

1. 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:

a. Assisting the contractor/subcontractor with the design and architecture of the vendor's USP.

b. 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.

c. Conducting a system assessment and ensuring best practices of the vendor's USP are followed.

d. Providing upgrade and migration strategy for the vendor's USP where applicable.

e. 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.

D. System Configuration and Commissioning Service

1. The System Configuration and Commissioning service from the vendor shall include a Field Engineer who will be responsible for:

a. Assisting the contractor's or subcontractor's onsite/remote technicians with the configuration and commissioning of the vendor's USP at the client site.

b. Conducting a test of the USP following the deployment of the system using real-world operator scenarios to ensure optimal system performance.

c. 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.

d. Providing a knowledge transfer of the vendor's USP to the contractor following the deployment of the USP at the client site.

3.03 Manufacturer End User Operator Training

A. 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

a. n/management of the following components specific to ACS:

   i. Door controllers, and input and output (IO) modules.

   ii. Doors, Elevators, and Access rules.

   iii. Cardholders and cardholder groups, credentials, and badge templates.

b. The Directory Role shall support the configuration/management of the following components specific to ALPR:

   i. ALPR units and cameras.

   ii. Hotlists, permit lists, and overtime rules.

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

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

4. 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.

5. 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.

6. 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.

7. 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.

8. Optional Roles

    a. The Global Cardholder Synchronizer Role shall be responsible for synchronizing cardholder and credential data between the local site and a central site. Synchronization between remote sites shall also be supported.

    b. The Active Directory Role shall be responsible for synchronizing user accounts and cardholder accounts with a Microsoft Active Directory server.

    c. The Intrusion Manager Role shall be responsible for managing third party intrusion devices such as alarm panels and perimeter detection devices. This role shall also be responsible for logging all intrusion events in a database.

    d. The Asset Manager Role shall be responsible for integrating and synchronizing with third party asset management systems and logging asset related events. This role shall also be responsible for supporting the execution of asset-related reports such as inventory reports and asset activity reports.

    e. The Plug-in Manager Role shall be responsible for the communication between the USP and third party systems such as video analytics, ALPR, access control, video, and building management systems.

    f. The Point of Sale (POS) Manager Role shall be responsible for integrating the USP with third party POS systems and for logging transactions.

    g. 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.

    h. The Communication Management Role shall be responsible for registering the SIP communication endpoints and for managing the call routing.

i. The Video Redirector Role shall be responsible for connecting any video stream to a third party system using standard RTSP protocol. This role shall provide access to live video.

B. Server Monitoring Service (Watchdog)

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

2. 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.

3. 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.

2.11 USP Access Control, Video, and ALPR Unification

A. 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.

B. The Configuration UI shall present a true Unified Security Interface for the configuration and management of the ACS, VMS, and ALPR.

C. 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.

D. It shall be possible to view video associated to access control events when viewing a report.

E. It shall be possible to view video associated to intrusion panel events when viewing a report.

F. It shall be possible to view video associated to ALPR events when viewing a report.

G. The USP shall support the following Alarm Management functionality:

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

2. 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.

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

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

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

6. Provide the ability to group alarms by source and by type.
7. Define the time period after which the alarm is automatically acknowledged.
8. 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.
9. Define the alarm broadcast mode. Alarm notifications shall be sent using either a sequential or an all-at-once broadcast mode.
10. Define whether to display the source of the alarm, one or more entities, or an HTML page.
11. Specify whether an incident report is mandatory during acknowledgment.

H. The workflows to create, modify, add instructions and procedures, and acknowledge an alarm shall be consistent for access control, ALPR, and video alarms.

I. Alarms shall be federated, allowing global alarm management across multiple independent USP, ACS, VMS, and ALPR systems.

J. The USP shall also support alarm notification to an email address or any device using the SMTP protocol.

K. 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.

L. 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.

M. The user shall have the ability to acknowledge alarms, create an incident upon alarm acknowledgement, and put an alarm to snooze.

N. The user shall be able to spontaneously trigger alarms based on something he or she sees in the system.

O. An alarm shall be configured in such a way that it remains visible until the source condition has been acknowledged.

P. The user shall be able to investigate an alarm without acknowledging it.

2.12 USP Threat Levels

A. The USP shall support Threat Levels to dynamically change the system behavior to respond to critical events.

B. Threat Levels shall be activated and deactivated by the CSA operator with the right privilege.

C. Threat Levels shall be set on an area or on the entire system.

D. 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.

E. The following specific actions shall be available with Threat Level:

1. Set minimum security clearance to restrict or permit access to cardholders on specific areas on top of the restrictions imposed by the access rules.
2. Set minimum user level to automatically log out user from the USP.
3. Set reader mode to change how the doors are accessed (e.g. card and PIN, or card or PIN).

F. A visible notification shall be displayed in all operator CSA when a Threat Level is activated.

2.13 USP Remote Task

A. 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.

B. The USP shall support video wall applications by connecting and controlling multiple workstations and monitors simultaneously.

C. The Remote Task shall be a graphical interface showing a replication of the remote workstation running the CSA (Monitoring UI).

D. The Remote Task shall allow the connection to other workstations using a low bandwidth mode to receive only snapshots of video viewed remotely.

E. The Remote Task shall allow the connection to other workstations using a spy mode to remain invisible to the remotely connected workstation.

F. The functionality provided by the remote monitoring and control capability shall include:

1. Remote monitoring and control of the monitoring and alarm monitoring tasks.
2. Ability to remotely switch cameras, doors and zones into display tiles.
3. Ability to remotely control live and playback video.
4. Ability to remotely change the tile pattern.
5. Ability to remotely create and delete tasks.
6. Ability to remotely start/stop task cycling.
7. Ability to remotely go into full screen mode.
8. Ability to remotely save and reload the workspace.

2.14 USP Advanced Task Management

A. USP shall support an infrastructure for managing Monitoring UI tasks used for live monitoring, day to day activities, and reporting.

B. 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.

C. 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.

D. 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.

2.15 USP Reporting

A. The USP shall support report generation (database reporting) for access control, ALPR, video, and intrusion.

B. 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 he or she has the appropriate privilege.

C. The workflows to create, modify, and run a report shall be consistent for access control, ALPR, and video reports.

D. Reports shall be federated, allowing global consolidated reporting across multiple independent USP, ACS, VMS, and ALPR systems.

E. Access control and ALPR reports shall support cardholder pictures and license plate pictures, respectively.

F. The USP shall support the following types of reports:

1. Alarm reports.
2. Video-specific reports (archive, bookmark, motion, and more).
3. Configuration reports (cardholders, credentials, units, access rules, readers/inputs/outputs, and more).
4. Activity reports (cardholder, cardholder group, visitor, credential, door, unit, area, zone, elevator, and more).
5. ALPR-specific reports (mobile ALPR playback, hits, plate reads, reads/hits per day, reads/hits per ALPR zone, and more).
6. Health activity and health statistics reports.
7. Other types of reports, including visitor reports, audit trail reports, incident reports, and time and attendance reports.

G. Generic Reports, Custom Reports and Report Templates

1. 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.
2. 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).
3. All report templates shall be created within the Monitoring UI.
4. These templates can be used to generate reports on a schedule in PDF or Excel formats.
5. An unrestricted number of custom reports and templates shall be supported.

H. 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.

I. The USP shall support comprehensive data filtering for most reports based on entity type, event type, event timestamp, custom fields, and more.

J. The user shall be able to click on an entity within an existing report to generate additional reports from the Monitoring UI.

K. The USP shall support the following actions on a report: print report, export report to a PDF/Microsoft Excel/CSV file, and automatically email a report based on a schedule and a list of one or more recipients.

2.16 USP Federation feature: Monitoring of Remote Systems

A. The USP shall support the concept of a Federation feature for access control, video, and ALPR.

B. 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.

C. The Federation feature shall support the unification of multiple independent video surveillance systems or VMS.

D. 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).

E. 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.

F. The Federation feature shall support Global Alarm Management from the Monitoring UI for access control, video, and ALPR.

G. The Federation feature shall support Global Report Generation from the Monitoring UI for access control, video, and ALPR.

H. The Federation feature shall support dozens of operator actions on remote (federated) entities from the Monitoring UI (e.g. generating a global report taking into account events from multiple independent sites or acknowledging remote alarms).

2.17 USP Zone Management

A. 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 he or she has the appropriate privileges.

B. 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.

C. 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.

D. A schedule shall be defined for a zone, indicating when the zone will be monitored.

E. 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.

F. The ACS shall support one or more cameras per zone. Video shall then be associated to zone state changes.

G. Input/Output (IO) Linking

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

2. IO Linking shall be available in offline mode when communication between the server and hardware is not available.

3. 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.

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

2.18 USP User and User Group Security, Partitions, and Privileges Management

A. 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 he or she has the appropriate privileges.

B. The USP shall support user authentication with claims-based authentication using external providers. External providers shall include:

    1. ADFS (Active Directory Federation Services)

C. 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.

D. User privileges shall be extensive in the USP. All configurable entities for the USP, including access control, video, and ALPR, shall have associated privileges.

E. 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.

F. Partitions

    1. 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.

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

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

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

G. It shall be possible to specify user and user group privileges on a per partition basis.

H. Advanced logon options shall be available such as dual logon and more.

I. 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.

2.19 USP Event/Action Management

A. 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.

B. The USP shall receive all incoming events from one or more ACS, VMS, and ALPR. The USP shall take the appropriate actions based on user-define event/action relationships.

C. The USP shall receive and log the following events:

1. System-wide events
2. Application events (clients and servers)
3. Area, camera, door, elevator, and ALPR events (reads and hits)
4. Unit events
5. Zone events
6. Alarm events
7. ALPR events

D. The USP shall allow the creation of custom events.

E. 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:

1. Add bookmark
2. Block and unblock video
3. Display a camera on an analog monitor
4. Display an entity in the CSA
5. Email a report
6. Email a snapshot
7. Export report
8. Go home
9. Go to preset
10. Override recording quality
11. Play a sound
12. Reboot unit
13. Run a macro
14. Run a pattern
15. Send a message
16. Send an email
17. Set threat level
18. Start/Stop applying video protection
19. Start/Stop recording

20. Start/Stop transfer
21. Trigger alarm
22. Trigger output

F. 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.

2.20 USP Schedules and Scheduled Tasks

A. Schedules

1. The USP shall support the configuration and management of complex schedules. A user shall be able to add, delete, or modify a schedule if he or she has the appropriate privileges.
2. 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.
3. Daily, weekly, ordinal, and specific schedules shall be supported.

B. Scheduled Tasks

1. The USP shall support scheduled tasks for video, and ALPR.
2. 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.
3. Scheduled tasks shall support all standard actions available within the USP, such as sending an email or emailing a report.

2.21 USP Macros and Custom Scripts

A. 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.

B. Custom macros shall be created with the USP Software Development Kit (SDK).

C. A macro shall be executed either automatically or manually.

D. In the Monitoring UI, a macro shall be launched through hot actions.

2.22 USP Dynamic Graphical Maps (DGM)

A. The USP shall support mapping functionality for access control, video surveillance, intrusion detection, ALPR, and external applications.

B. 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.

C. 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 screen

must provide the same command and control capabilities than in a single screen display The DGM shall support the following file format and protocol for importing map background:

1. PDF
2. JPG
3. PNG
4. Web Map Service (WMS) defined by the Open Geospatial Consortium (OGC)
5. BeNomad

D. 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

1. Google Map, aerial, terrain (Licensed)
2. Bing Map, aerial, satellite, hybrid (Licensed)

E. It shall be possible to configure a mixed set of maps made of GIS, online providers and private imported files and link them together.

F. The DGM shall provide the ability to display all native entities of the USP including:

1. Cameras, fix, and PTZ
2. Doors
3. Camera sequences
4. Areas
5. Intrusion areas
6. Intrusion zones
7. License Plate Recognition cameras
8. Digital inputs
9. Digital outputs
10. Intercoms
11. Alarms
12. Macros
13. Police Car Patrollers

G. The DGM shall provide the ability to draw and display information over the map in the form of:

1. Vectoriel shapes: line, rectangles, polygones, ellipse
2. Pictures
3. Text

H. The DGM shall provide the ability to display any type of third party entities integrated through an SDK.

I. The DGM shall provide the ability to display layer of information in Keyhole Markup Language (KML) format.

J. The DGM shall provide the ability to the operator to manage layers of entities display over the map, being able to turn them on and off and changing the superposition order.

K. The DGM shall offer built-in map data backup and restore for both map background and layers of entities.

L. The DGM shall offer failover capabilities.

M. The DGM shall scale up to several thousands of entities on a single map and hundreds of maps.

N. The DGM shall provide a means to update a map background without affecting the map object configuration.

O. The DGM shall offer a user friendly graphical map designer to configure the maps.

P. The DGM shall provide a user friendly and intuitive navigation that includes:

1. The ability to create hierarchies of maps to facilitate navigation within and between various sites and buildings.
2. The ability to define favorites for recurrent position recall.
3. 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.
4. A common user experience regarding navigation into the map for both GIS and private maps.
5. A history log of positions.

Q. 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.

R. The DGM shall display the actual video Field of View of camera. It shall be possible to configure the FOV of a camera by entering the specification of the camera installation or graphically by moving the boundaries of the Field of View.

S. For PTZ cameras offering position feedback capability, the DGM shall

1. Dynamically represent the accurate Field of View of the camera.
2. Allow the user to act on the PTZ by moving its field of view.

T. The DGM shall offer the ability to optionally set a graphical display notification of the motion detection.

U. The DGM shall offer a smart selection tool to access the video simply by clicking the location the user wants to see, the DGM will automatically select the cameras that can see this location and move the PTZ towards that location. This smart selection tool shall take into consideration the obstacle and not display cameras that cannot see the location because of a wall.

V. It shall be possible to select a location by drawing a zone of interest on the DGM and display all the entities that are part of that zone of interest at once.

W. The user shall be able to select and display the content of multiple USP entities on the map in popup windows.

X. It shall be possible to access live and playback video from the map.

Y. It shall be possible to monitor from the DGM all entities event notification. User shall be able to turn on and off the notification per entity.

AA. The DGM shall offer the ability to fully operate alarm monitoring. It shall be possible to:

1. Center the map on entities related to the alarm.
2. Visualize the Alarms notification on the map access the related video from the map.
3. Trigger and receive alarms.
4. Act on the alarm from the DGM, including acknowledgements, forwarding, and investigation.
5. Visualize that an alarm occurred in an underlying linked map.

BB. The DGM shall provide the following search capabilities:

1. Search and center by entity name.
2. 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.

CC. Any update of map content by an administrator shall be immediately and dynamically pushed to all DGM users.

2.23 USP Audit and User Activity Trails (Logs)

A. The USP shall support the generation of audit trails. Audit trails shall consist of logs of operator/administrator additions, deletions, and modifications.

B. 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.

C. For entity configuration changes, the audit trail report shall include detailed information of the value before and after the changes.

D. 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.

E. 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.

2.24 USP Incident Reports

A. 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.

B. The operator shall be able to create standalone incident reports or incident reports tied to alarms.

C. 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.

D. 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.

E. Incident reports shall allow the creation of a custom form on which to input information on an incident.

F. Incident reports shall allow entities, events, and alarms to be added to support at the report's conclusions.

2.25 USP Third Party Integration

A. Microsoft Active Directory Integration

1. 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.

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

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

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

5. The USP shall support Microsoft Active Directory encryption using LDAP SSL.
6. When enabled, Active Directory shall manage user logon to the USP client applications through the user's Windows credentials. Logging to the USP shall utilize native Active Directory password management and authentication features.
7. It shall be possible to synchronize the following USP entities and their information from Active Directory with the USP:
    a. Users (username, first and last names, email address, and more).
    b. User groups (user group name, description, and group email address).
    c. Active Directory attributes to USP custom fields.
8. 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.
9. Supported synchronization methods for additions, modification, and deletions of synchronized entities shall include: on first logon (users only), manual synchronization, and scheduled synchronization.
10. The USP shall support user connections across independent organizations by connecting to an external ADFS (Active Directory Federation Services) service using claims-based authentication.

B. Intrusion Detection Integration

1. The USP shall integrate with third party intrusion panels and devices via an Intrusion SDK. The Intrusion Manager Role shall manage communications with the intrusion panels. Communications with intrusion devices shall be over serial communications and/or an IP network.
2. Integration with intrusion panels shall be possible outside the release cycle of the USP. It shall be possible to add new integrations at any point in time.
3. Functionality available via the integration of intrusion devices with the USP shall include the following (where supported by the intrusion panel):
    a. Arm and disarm intrusion devices (manually, on schedule, or following a USP event).
    b. Activate or trigger intrusion device outputs.
    c. View intrusion events and alarms.
    d. Monitor the status, including arming status, of the intrusion devices.
    e. Video verification of intrusion events and alarms with video panels.
    f. Create USP zones using intrusion device inputs.
4. Currently supported intrusion panels include:

a. Bosch G Series panels.

b. DSC Power Series panels.

c. DMP XR Series panels.

d. Honeywell Galaxy Dimension panels.

C. Third Party Access Control Systems

1. The USP shall integrate with third party access control software via the SDK. Communications with access control software shall be over an IP network, and should not support administrative tasks such as cardholder management.

2. Integration with access control software shall be possible outside the release cycle of the USP. It shall be possible to add new integrations at any point in time.

3. Functionality available via the integration of access control software with the USP shall include the following (where supported by the access control solution):

    a. Synchronize access control entities and receive associated events and states within the USP, including:

        i. Cardholders and access rights

        ii. Visitors

        iii. Readers and doors

        iv. Alarms

    b. Monitor access control events

    c. Monitor and Acknowledge access control alarms

    d. Trigger actions and outputs in the access control software using hot actions and event-to-actions

    e. Lock and unlock doors in the access control software

    f. Configure event-to-actions using the access control events and alarms

    g. Generate Security Center reports using from the in the access control data

    h. View and monitor states of door entities in the USP maps

D. Additional Third Party Integrations

1. 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.

2. The USP architecture shall support the addition of new connectors to integrate to third party system integration, such as:

    a. Video analytics.

    b. Third party video systems.

c. Third party access control systems.

d. ALPR integrations with pay stations, permit vendors, pay-by-phone vendors, and ticketing vendors.

e. Point-of-sale (POS) systems.

f. Building management systems.

g. Human resource management systems (HRMS).

2.26 USP Software Development Kit (SDK)

A. A USP SDK shall be available to support custom development for the platform.

B. The SDK shall include functionalities specific to the embedded automatic license plate recognition (ALPR), access control (ACS), and video (VMS) systems.

C. Integration with external applications and databases shall be possible with the SDK.

D. 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.

E. The SDK shall be based on the .NET framework.

F. The SDK shall support dynamic or transactional updates to the USP configuration. It shall also support change notification of USP entity configuration.

G. 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.

H. The SDK shall provide an extensive list of programming functions to view and configure ACS, VMS, and ALPR.

I. 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.

J. 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.

K. 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.

L. The SDK shall support the following alarm functions: view alarms in real time, acknowledge alarms, change priority, and change recipient.

Part 3 - Execution

3.01 Warranty

A. 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.

B. Extended warranty, up to 5 years, shall be available through the purchase of a software maintenance agreement (SMA) which includes the following additional services over the standard warranty:

1. Access to phone support and online chat for technical assistance.
2. Online case management.
3. Online system availability monitor.
4. Access to Major and Minor Release Upgrades.
5. 24/7 pager support and dedicated support specialist. *(Specifier, additional cost)*

3.02 Deployment Services and System Commissioning

A. General Requirements

1. 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:

   a. Multiple contractors or subcontractors that will be responsible for deploying the USP at multiple client sites in different geographical regions.

   b. Complex enterprise installations involving advanced functionality (e.g. The Federation feature, failover, plugins) and/or multiple systems (e.g. access control, video, ALPR) and/or third party integrations.

   c. Extensive use of customized solutions/plugins developed by the vendor that will be integrated into the USP.

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

B. Deployment Management Service

1. 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:

   a. Conducting a Risk Assessment of the impact of potential risk factors on the operation of the vendor's USP.

   b. Providing a project plan for the deployment of the vendor's USP.

   c. Managing the development and deployment of the custom solution components that will be integrated into the vendor's USP (if applicable).

d. Providing a scope of work detailing the services to be provided by the vendor to assist in the deployment of the vendor's USP.

e. Coordinating and scheduling the vendor field services with the contractor to assist with the deployment of the vendor's USP.

f. Providing regular project status updates to the contractor regarding the development of custom solutions (if applicable) and the deployment of the vendor's USP.

C. Solution Architect Service

1. 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:

a. Assisting the contractor/subcontractor with the design and architecture of the vendor's USP.

b. 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.

c. Conducting a system assessment and ensuring best practices of the vendor's USP are followed.

d. Providing upgrade and migration strategy for the vendor's USP where applicable.

e. 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.

D. System Configuration and Commissioning Service

1. The System Configuration and Commissioning service from the vendor shall include a Field Engineer who will be responsible for:

a. Assisting the contractor's or subcontractor's onsite/remote technicians with the configuration and commissioning of the vendor's USP at the client site.

b. Conducting a test of the USP following the deployment of the system using real-world operator scenarios to ensure optimal system performance.

c. 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.

d. Providing a knowledge transfer of the vendor's USP to the contractor following the deployment of the USP at the client site.

3.03 Manufacturer End User Operator Training 24 Hours

A. 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