Brivo OnAir®

Architecture & Engineering Specifications

Brivo OnAir®
Legal Disclaimers

Canada-Underwriters Laboratories (C-UL) Compliancy
For C-UL Listed applications, the unit shall be installed in accordance with Part 1 of the Canadian Electrical Code.

Document Disclaimer and Restrictions
Information in this document is subject to change without notice and does not represent a commitment on the part of Brivo Inc. For the most up-to-date information, visit http://www.brivo.com. This document and the data herein shall not be duplicated, used or disclosed to others for procurement or manufacturing, except as authorized with the written permission of Brivo Inc. The information contained within this document or within the product itself is considered the exclusive property of Brivo Inc. All information in this document or within the hardware and software product themselves is protected by the copyright and/or other intellectual property laws of the United States.

Product Support
All support for this product is provided by the third-party dealer. Please contact the dealer who installed the product with questions and support requests.

© 2015 Brivo Inc. All rights reserved.
The Brivo logo is a registered trademark of Brivo Inc.

Brivo Inc.
7700 Old Georgetown Road
Suite 300
Bethesda, MD 20814
Phone: (301) 664-5242
Fax: (301) 664-5264
www.brivo.com

This Architectural and Engineering Specification document utilizes the Construction Specifications Institute (CSI) Project Resource Manual (PRM), including MasterFormat™, SectionFormat™ and PageFormat™. The purpose of this document is to specify the Architectural/Engineering and Bid criteria for a Web-based, IP (Internet Protocol) based Access Control Appliance using such technologies as the Internet, private corporate networks, or wireless cellular networks.

This Architectural and Engineering Specification document specifies access control equipment and services. Equipment specifications include control panels, expansion chassis, I/O boards, door/reader control boards and power supplies. Services include Web-based monitoring and control services to manage control panels. These products and services are manufactured and/or provided by Brivo Inc.
SECTION 28 13 00
ACCESS CONTROL

PART 1 GENERAL

1.0 SUMMARY
A. This section includes
   1. A description of Web-based access control devices, intrusion detection devices, security access devices, relay control, alarm monitoring controllers, credential creation and credential holder database and management.
B. Related Sections
   1. Section 08 74 00 – Access Control Door Hardware.
   2. Section 28 13 33 – Access Control Interfaces.
   4. Section 28 23 00 – Video Surveillance.
   5. Section 27 05 33 – Pathways for Communications.
   6. Section 27 10 00 – Structured Cabling.
   7. Section 27 15 00 – Access Control Communications Horizontal Cabling.

2.0 DEFINITIONS
A. AES: Advanced Encryption Standard
B. DHCP: Dynamic Host Configuration Protocol
C. DNS: Domain Name System
D. HSMS: Hosted Security Management System (SaaS PACS Application)
E. IEC: Independent Edge Controller
F. IP: Internet Protocol
G. ISO: International Standards Organization
H. LAN: Local Area Network
I. PACS: Physical Access Control System
J. PoE: Power over Ethernet
K. SaaS: Software as a Service
L. SDC: Security Door Controller
M. SIA: Security Industry Association
N. SSH: Secure Shell
O. SSL: Secure Socket Layer
P. UI: User Interface
Q. RPC: Remote Procedure Call
R. XML: Extensive Markup Language
S. API: Application Programming Interface
T. PII: Personally Identifiable Information
U. WAN: Wide Area Network
3.0 REFERENCES
A. Underwriters Laboratories, Inc. (UL) (www.ul.com)
   1. UL294 – Underwriters Laboratory Safety Standard 294 for Access Control System Units.

4.0 QUALITY ASSURANCE
A. Manufacturer shall be capable of providing field service representation during construction and approving application method

5.0 WARRANTY
A. Refer to conditions of the contract for project warranty provisions
B. The manufacturer shall warrant that the hardware product(s) are free from defect in materials and/or workmanship for a period of three (3) years from the date of shipment

6.0 MAINTENANCE
A. The HSMS manufacturer shall provide periodic software upgrades
   1. Updates will be available to the customer via the manufacturer’s website.

7.0 SUPPORT
A. On-site support shall be provided by the local authorized installation company
B. Installing company shall provide evidence that it is an authorized dealer in good standing for the manufacturer of the HSMS, and that it meets the manufacturer’s technical certification requirements

8.0 SYSTEM DESCRIPTION
A. Application Functions
   1. The HSMS shall be a multi-tenant hosted application delivered via “Software as a Service” (SaaS) model. The HSMS system shall feature a centrally hosted “cloud” data center which is accessible to both on-premise equipment and system administrators via a variety of private and public networks.
   2. The HSMS application shall offer integrated access control, ID badging and support for web-hosted and recorded video and integration with a variety of on-site video recording platforms.
   3. The HSMS application shall offer immediate provisioning of new devices on demand by the end user.
   4. All access control data shall be managed and maintained through a Web-based interface to the cloud data center.
      a. Reference Section 28 13 49 – Access Control Web Interface for specifications regarding Web-based UI.
   5. The system shall provide firmware installation capabilities to all connected Security Door Controller (SDC) panels.

B. System Architecture
   1. The HSMS solution shall be delivered as a multi-tenant, Software as a Service platform supporting tens of thousands of remote access control points in single, geographically redundant multi-tenant application architecture. The HSMS service shall allow access from any standard browser by authenticated users with proper credentials.
   2. The HSMS solution must have a demonstrated up time in excess of 99.95% or greater over the past five years of service.
   3. The HSMS must be internally redundant so that there is no single point of failure within the system.
   4. The HSMS architecture must also contain a geographically remote Disaster Recovery facility with a full copy of all applications, synchronized databases, and the ability to take over data processing operations in the event of a system failure at the primary facility.

© 2015 Brivo Inc. All rights reserved.
5. The HSMS platform shall have been awarded a SAS-70 Type II and/or SSAE-16 information security audit rating as well as TRUSTe certification and Safe Harbor from the Department of Commerce.
6. The HSMS application shall protect PII through the use of 128-bit AES encryption for all communications.
7. New features for the HSMS platform shall be released automatically on a quarterly basis at no incremental cost to customers.
8. Pricing shall conform to an on-demand model, with no up-front licensing expense.
9. Encryption & Authentication:
   a. Communications between Security Door Controller (SDC) panels and the HSMS shall be encrypted using 128-bit SSL encryption.
   b. The HSMS shall validate the identity of any SDC panel attempting to communicate with it through the exchange of X.509 digital certificates.
10. Network Communications:
    a. The HSMS shall utilize Ethernet communications as its primary communications medium and shall conform to IEEE 802.3 industry standards for typical computer based network connectivity:
       1) Ethernet connections shall use industry standard 8P8C modular connectors and shall conform to TIA/EIA-568-B wiring standards.
11. Security Door Controller (SDC):
    a. SDCs shall represent multiple door controller devices including, but not limited to:
       1) Multi-Door Controller Hub.
    b. SDCs multi-door controller hubs shall be fully expandable from 1 to 30 readers.
    c. SDCs shall include a UL-listed chassis and power supply designed to accommodate a variety of expansion options.
    d. SDCs shall include the ability to maintain a maximum of 25,000 cardholders.
    e. The HSMS shall provide a seamless programming environment and shall fully integrate IECs and SDCs as integral components of the system.
    f. Communications options shall include:
       1) 10/100Mbs Ethernet.
       2) CAN Bus - capable of using CAT5 or higher cable up to 1500 feet.
12. Independent Edge Controller (IEC):
    a. Each IEC shall have the ability to maintain a maximum of 25,000 card holders and a minimum of 6,000 off-line events.
    b. IECs shall include Power-over-Ethernet (PoE) capabilities, with the ability to supply up to 750mA of auxiliary power for external locks and/or REX devices and/or card readers.
    c. IEC PoE shall conform to the IEEE 802.3af standard.
    d. Communications options shall include:
       1) 10/100Mbs Ethernet.
C. Schedules and Holidays
1. The HSMS shall provide the ability to define custom schedules for the purpose of managing facility access and operating auxiliary devices with the following options:
   a. Create and edit a schedule. The HSMS shall permit up to 32 time periods per day.
   b. Associate a schedule with groups, floors, doors and/or devices.
   c. Terminate a schedule’s association with one or more groups, floors, doors or devices.
   d. Delete a schedule.
   e. Create and edit a Holiday.
   f. Edit a Holiday’s start and end date.
   g. Delete a Holiday.
D. Doors and Devices
1. Doors:
   a. Each site may have one or more doors associated with it.
   b. Administrators shall be allowed permission to manage doors, including permission to create the door, edit its name and manage its security settings.

2. Devices:
   a. Bulk Device Management via Device Profiles:
      1) The HSMS shall permit authorized administrators the ability to assign “profiles” such as schedules and permissions to doors, inputs, and credentials.
   b. A device may have logical or physical inputs and outputs.
   c. A logical input may be a schedule input to a timer.
   d. A physical input is any physical input point on a SDC board.
   e. A site can have one or more devices associated with it.
   f. Administrators shall be allowed permission to manage devices, including permission to create the device, edit its name and manage its security settings.

E. Elevators and Floors
1. Authorized administrators shall have permission to manage elevators and floors including, but not limited to:
   a. Creating the elevator or floor.
   b. Editing its name.
   c. Managing its settings.

F. Credentials: Credential Database and Cards
1. Credential Database:
   a. The HSMS shall support multiple credentials per user.
   b. The HSMS software interface shall maintain a database of all credentials associated with the account or sub-account, and the user to whom each is assigned.
   c. Operations to be performed by the interface shall include, but not be limited to:
      1) Validate that card numbers are unique, numeric and value is appropriate for the credential in use.
      2) Support the creation of PIN credentials that are unique, 4 to 8 digits long, and either randomly generated by the system or selected by the user.
      3) Automatically send updated credential information to the appropriate access control panels with no other user intervention.
      4) Provide up to 64 customized fields per account for data storage pertaining to individual credential holders (users) registered in the system.
   d. The HSMS shall support a variety of credential types including proximity cards, magnetic stripe cards and smart cards.
   e. The HSMS shall support a variety of Wiegand bit patterns.

2. Cards:
   a. May be assigned, revoked or deleted.
   b. Authorized operators shall have the capability to see all cards associated with an account.
   c. Sub-account administrators shall be capable of viewing only those cards assigned to users affiliated with their account.
   d. Sub-account administrators shall have the ability to view currently unassigned cards.
   e. The HSMS software interface shall provide the capability to display the card format in addition to the name of the user to whom the card is currently assigned.
   f. The ACS shall provide the capability to add cards using a local card reader.
   g. The HSMS shall provide the ability to support an unlimited number of standard and custom formats.
G. ID Badging
1. The HSMS shall provide the necessary capabilities to allow authorized operators the ability to create fully customizable badge templates.
2. The HSMS shall provide all necessary functionality to display images and print badges directly from the operator’s screen.
3. The HSMS shall provide for the support of two-sided badge printing.
4. The HSMS shall provide the ability of bulk badge printing.

H. Antipassback
1. Antipassback zones shall be constrained to a single SDC.
2. Each SDC shall support two Antipassback zones, Ingress and Egress.
3. Antipassback capabilities shall allow administrators the ability to enforce policies which control how individual users and groups of users are permitted to enter or exit physically controlled areas.
4. Antipassback shall incorporate the following features:
   a. Hard Antipassback:
      1) Hard Antipassback shall prevent individual users from exiting or entering a zone if the system detects an incorrect current zone state.
   b. Soft Antipassback:
      1) Soft Antipassback design shall allow administrators to specify controls for both individuals and groups.
      2) Antipassback Reset Interval:
         i) Soft Antipassback shall incorporate a Reset Interval providing the ability to determine a time period for Antipassback enforcement. Once the time period has elapsed, the system shall effectively reset the users’ Antipassback status to allow re-entry into the same zone.
      3) Antipassback Reset Time:
         i) Soft Antipassback shall incorporate an Antipassback Reset Time parameter which shall reset a group’s status as inside or outside the Antipassback zone at a specific time of day, and shall permit the ability to enter the time on a 24-hour clock with minute-by-minute detail.
   c. All doors controlling access to a designated Antipassback Zone shall be configured for Antipassback.
   d. Administrators shall not have the ability to delete a door once it has been configured for Antipassback.
   e. Users who enter through a door in a zone configured with Antipassback without presenting a credential shall not be authorized to exit when presenting a credential until the Antipassback Reset Interval has elapsed if enabled, or until their Antipassback status has been reset.
   f. Users who exit a door without presenting a credential shall not be allowed to reenter until the Antipassback Reset Interval has elapsed if enabled, or until their Antipassback status has been reset.
   g. Antipassback Immunity:
      1) Antipassback immunity shall permit users the ability to enter and exit Antipassback areas without restrictions. Immunity shall function as if Antipassback controls are not enabled.
      2) Antipassback immunity shall function on User Groups only.
      3) User Group configuration shall include a check box to enable Antipassback Immunity for the entire group.
      4) Groups that are immune to Antipassback controls do not follow the same Antipassback controls as groups that are not immune. These users are free to enter or exit a door even if the Antipassback Reset Interval has not elapsed.
I. Video Integration
   1. The system shall be able to associate video camera clips with access events.
   2. The HSMS shall provide authorized administrators the ability to retrieve a video segment related to a specific event.
   3. The HSMS shall use the time stamp of the event and camera identifier to query the DVR for event clips.
   4. Video integration shall be available via on-line video recording incorporated within the HSMS Service as well as with third party video recording devices installed on the customer’s premise.
   5. The HSMS shall provide email notifications for online video camera motion events, allowing designated recipients to get an email alert.

J. System Administrators
   1. Full tier-based Administrative Security Module:
      a. The HSMS shall permit multiple administrative tiers.
      b. The HSMS shall provide multiple capabilities per tier.

K. Two-Factor Authentication
   1. The HSMS shall be capable of two-factor login authentication using the following:
      a. Login/password.
      b. Temporary token sent to administrators email valid for a limited time.

L. Email and Text Message Notifications
   1. The HSMS shall have the ability to dispatch email and text message notifications to select administrators when one of the following predetermined events occur:
      a. Door Ajar/Door Ajar Cleared.
      b. Door Forced Open.
      c. Too Many Invalid PINs.
      d. Unlock Schedule Restored/Door Locked by Keypad.
      e. Unlock Schedule Overridden by Keypad/Door Unlocked by Keypad.
      f. Door Locked by Timer.
      g. Door Unlocked by Timer.
      h. Failed Access by Unknown Person.
      i. Failed access by unknown person due to invalid credential type (card required).
      j. Failed Access by Known Person.
      k. Failed Access by a User within a Group.
      l. Successful access by a user within a Group.
      m. Successful access by a specific user.
      n. Device Engaged/Disengaged.
      o. Unit Opened/Closed.
      p. Control Panel/Control Board Unit Opened/Closed.
      q. AC Power Loss/Restoration and Battery Status.
      r. Control Panel Communication Failure.
      s. Camera Connected.
      t. Camera Disconnect.
      u. Camera Motion Event.
      v. Account administrators shall have the ability to manage email or text message notifications according to functionality listed below:
         1) Create and edit notification rules specifying which administrator will receive email or text message notification of which system events.
         2) Associate a schedule with each notification rule.
         3) Specify the language to be used in notification emails.
         4) Delete notification rules.
M. Activity Logs
1. The HSMS shall include an Activity Report tool that tracks all attempts to access the sites associated with an account, including both successful and failed attempts, with the following options:
   a. Display the Activity Report unfiltered, so that all activities are listed.
   b. Display the Activity Report filtered by user, so that only those actions performed by a specific user are displayed.
   c. Display the Activity Report filtered by site, so that only those actions performed at a specific site are listed.
   d. Display the Activity Report filtered by door or device, so that only those actions performed on a specific door or device are listed.
2. Allow administrators to search the Activity Report for exception events, user events, control panel events and device events, searching by absolute date or relative days.
3. Allow administrators to search the Activity Report for events related to a specific door or device.
4. Allow administrators to search the Activity Report for actions performed by a specific user on a specific door.

N. Reports
1. User Report:
   a. The system, shall permit top level Administrators the ability to create customized reports of user properties, including:
      1) The date on which a user record was created or updated.
      2) Any custom field data maintained for one or more users.
2. Schedule Report:
   a. The system shall permit authorized administrators the ability to print Schedule configuration reports.
   b. Schedule configuration reports shall include the following attributes:
      1) Schedule Name.
      2) Day of Week Name.
      3) Time of Day.
   c. Schedule reports shall be grouped by schedule name.
   d. Schedule reports shall be formatted to fit a standard letter 8.5” width paper.
   e. Print execution shall be performed through the Browsers Print function.
3. Scheduled Reports should allow either predefined or new reports to be run on a define schedule.

O. Licensing
1. No licensing shall be required for the HSMS system.

P. API Interface
1. The HSMS shall provide API support for XML-RPC integration with third party products providing capabilities such as:
   a. Automatically adding, modifying and deleting users from external sources.
   b. Exporting user data and system events to 3rd party systems.

PART 2 PRODUCTS

1.0 MANUFACTURER

A. Brivo Inc.
   1. 7700 Old Georgetown Road, Suite 300, Bethesda, MD 20814.
      a. Telephone: (301) 664-5242.
      b. Fax: (301) 664-5264.
      c. Website: www.brivo.com.
2.0 PRODUCT SUBSTITUTIONS

A. No substitutions permitted

3.0 SYSTEM COMPONENTS

A. Hosted Security Management System (HSMS)
   1. Brivo OnAir®
      b. System requires no user-installed software.
      c. System requires no dedicated on-site PC hardware.
      d. System software requires no software maintenance.

B. Security Door Controllers (SDC)
   1. Brivo ACS5000-E/ACS5008-E Door Control Panels:
      a. Expandable modular design.
      b. Individually fused interface boards, locks, and REX devices.
      c. Door tamper switch.
      d. Power loss detection and automatic battery backup.
   2. IP Door Controller (Brivo ACS-IPDC-E models):
      a. Built-in 802.3af Power over Ethernet (PoE):
         1) IPDC - 750mA available for external field devices including readers.
      b. Compatible reader protocols utilizing common Wiegand formats.
      c. Authentication and encryption of X.509 Digital Certificates and 128-bit SSL.

C. Ancillary Components
   1. Card Readers – Wiegand Interface:
      a. HID
      b. XceedID
      c. Farpoint.
   2. Biometric Readers – Wiegand Interface:
      a. Suprema
   3. Wireless Locksets
      a. The HSMS shall have the capability to integrate with wireless locksets from two manufacturers:
         1) IP Locksets:
            i. Salto Sallis
         2) Wiegand Locksets:
            i. Schlage IR AD400
   4. Telephone Entry
      a. Liftmaster IPAC
   5. Video – Local Storage
      a. Smartvue

4.0 BRIVO ACS5000-E/ACS5008-E CONTROL PANEL

A. Capacities
   1. Supports up to 14 expansion boards for up to 30 readers per panel.
   2. Support for up to 25,000 credential holders per panel.
   3. Elevator control:
      a. 118 floors.
   4. Inputs: 4:
      a. Maximum 120 using Brivo ACS5000-IO expansion modules.
      b. Optional 4-state, dual end-of-line supervision.
   5. Outputs: 4:
a. Form C (SPST) 3A @24VDC.

b. Maximum 118 outputs using Brivo ACS5000-IO expansion modules.

6. Communications:
   a. Ethernet connection using port 443 outbound.

7. Authentication and encryption:
   a. X.509 Digital Certificates and 128-bit SSL.

8. Event history:
   a. 6,000 events (FIFO) offline from host.

9. Expansion Boards:
   a. Maximum 14 per Brivo ACS5000-E/ACS5008-E.

10. Power consumption:
    a. 12VDC @ 500mA peak with all relays engaged (board only).

11. Communication bus wiring:
    a. CAN Bus: Use CAT5 (or higher) UTP cable up to 1,500 feet.

12. Temperature and humidity range:
    a. Operating Temp: 32° to 125° F, (0° to 49° C) Humidity: Max 85% non-condensing.

13. Control chassis dimensions:
    a. Brivo ACS5000-E: 15"h x 15"w x 3.75"d.
    b. Brivo ACS5008-E: 23.5"h x 15"w x 3.75"d.

14. Enclosure:
    a. NEMA type 1.
    b. Tamper switch.
    c. Key locks.
    d. Knockouts.

15. Compliance:
    a. Listed 33HR.
    b. Access Control UL294 ULC Listed.
    c. CE Certified.

B. Expansion Modules

1. Brivo ACS5000-DB – ACS5000 Door expansion board:
   a. Wiegand reader ports (2).
   b. Inputs points (4):
      1) Optional 4 state supervision.
   c. Output relays (4):
      1) Form C (SPST) 3A @24VDC.
   d. Power consumption:
      1) 12VDC @ 90mA idle / 400mA peak with all relays engaged.
   e. Communication bus wiring:
      1) CAN Bus: Use CAT5E (or higher) UTP cable up to 1500 feet.
   f. Temperature and humidity range:
      1) Operating Temp: 32° to 125° F (0° to 49° C).
      2) Humidity: Max 85% non-condensing.
   g. Compliance:
      1) UL294/ULC Listed.
      2) CE Certified.
   h. Dimensions:
      1) 3.5"h x 11.5"w.

2. Brivo ACS5000-IO – ACS5000 Input/output expansion board:
   a. 8 - Inputs points:
      1) Optional 4 state supervision.
b. 8 - Output relays:
   1) Form C (SPST) relays 3A @24VDC.

c. Power consumption:
   1) 12VDC @ 90mA idle / 400mA peak with all relays engaged.

d. Communication bus wiring:
   1) CAN Bus: Use CAT5E (or higher) UTP cable up to 1500 feet.

e. Temperature and humidity range:
   1) Operating Temp: 32° to 125° F, (0° to 49° C).
   2) Humidity: Max 85% non-condensing.

f. Compliance:
   1) UL294/ULC Listed.
   2) CE Certified.

g. Dimensions:
   1) 3.5”h x 11.5”w.

3. Brivo ACS5000-EXP – Small Expansion Enclosure:
   a. 2 - Expansion Board Capacity.
   b. Enclosure Dimensions:
      1) 15”h x 15”w x 3.75”d.

4. Brivo ACS5008-EXP – Large Expansion Enclosure:
   a. 4 - Expansion Board Capacity.
   b. Enclosure Dimensions:
      1) 23.5”h x 15”w x 3.75”d.

5.0 BRIVO IPDC

A. Brivo IP Door Controller
   2. Dimensions: 3.3” w x 4.8” h x 1.5” d (83.8 mm W x 121.9 mm H x 36.3 mm D).
   3. Compliance: UL 294 Listed Component, CSA 205 for Canada (Pending), FCC Class A Verification (Pending), ICES-003 Class A Canada (Pending), EU (CE Marking) (Pending), Australia (C-Tick Mark, New Zealand (Pending).
   4. Card format: Supports any card data format up to 128 bit.
   5. 25,000 cardholder memory.
   6. 6,000 event history (FIFO) offline from host.
   7. Power Supply Requirements: 1.5A @ 12 VDC maximum:
      a. Recommended: Power is supplied using the Power over the Ethernet technology available with PoE (802.3af) enabled network devices. Alternate: Supervised 12 VDC linear power supply with battery backup, input surge protection, and AC Fail and battery low contact outputs. Relays can be configured to supply power as follow:
         1) Available Power: The IPDC is capable of supplying a total of 700mA to field devices. Unpowered, relay contacts are rated for 2 A @ 30VDC.
         2) Use of a Listed Access Control / Burglary power-limited power supply is required for all listed installations.
   8. The IPDC is intended for use in indoor environment that comply with the following specifications:
      a. Operating Temperature: 32° to 125° F (0° to 50° C).
      b. Operating Humidity: 5% to 95% relative, noncondensing.
   9. Communication Ports:
      a. Ethernet 10/100 Mbps.
      b. USB to Ethernet.

6.0 HARDWARE SUPPORT

A. Salto Sallis Wireless Locksets with IP Router
1. The Salto node communicates the following data in series with the Brivo ACS5000 panel to the HSMS:
   a. Open with card.
   b. Open with metallic key.
   c. Open with PPD (Portable Programming Device).
   d. Open from Host.
   e. Door Forced.
   f. Door Forced Cleared.
   g. Door Ajar.
   h. Door Ajar Cleared.
   i. Communication has been established.
2. Any combination of up to 30 card readers and Salto locks may be used per Brivo ACS5000-W/G, ACS5008-W/G, ACS5000-E or ACS5008-E panel.
3. 1 router may be used per Brivo ACS5000 panel mentioned in A.2.
4. Up to 16 locks per node.

B. Schlage IR AD400
1. The Schlage controller communicates via Wiegand transmission to the Brivo ACS5000 panels.
2. Any combination of up to 30 card reader and Schlage locks may be used per Brivo ACS5000-W/G, ACS5008-W/G, ACS5000-E or ACS5008-E panel.
3. Up to 2 locks per controller or panel interface module.

C. Suprema Biometric Readers
1. The Suprema readers shall communicate via Wiegand transmission to an ACS control panel.
2. Any combination of up to 30 supported biometric readers may be used per Brivo ACS5000-W/G, ACS5008-W/G, ACS5000-E or ACS5008-E panel.
3. Any combination of up to 2 supported biometric readers may be used per Brivo ACS-IPDC.

D. Liftmaster Internet Protocol Access Control (IPAC):
1. The Liftmaster IPAC shall communicate directly to the HSMS via Ethernet communication.
2. Up to 50,000 residents per IPAC unit.
3. The Liftmaster IPAC utilizes VoIP communication to perform calls to residents.

E. Smartvue Video Gateway:
1. The Smartvue Video Gateway shall communicate directly to the HSMS.
2. The Video Gateway shall allow the use of short cut routing to log directly into the gateway.

PART 3 EXECUTION

1.0 MANUFACTURER’S INSTRUCTIONS

A. Compliance
   1. Comply with manufacturer’s written data, including product technical bulletins, product catalog installation instructions and product carton installation instructions.

2.0 EXAMINATION

A. Site Verification of Conditions
   1. Verify that substrate conditions, which have either been previously installed under other sections, or that existing site conditions, are acceptable for product installation in accordance with manufacturer’s instructions.
   2. Verify that building doors, frames, walls, wire runs, related items, and conditions are ready to receive work of this Section.

3.0 PROTECTION

A. Other Trades
   1. Protect installed work of other trades.
4.0 PREPARATION
A. Manufacturer Forms
   1. Obtain and complete project planning forms from manufacturer of surveillance system; customize forms to be project specific.

B. Final Setup
   1. Review, adjust, and prepare final documents to establish system software setup.

C. Record Setup Data
   1. Electrical Preparation:
      a. Coordinate with trade where applicable.
   2. Elevators:
      a. Coordinate with trade where applicable.
   3. Information Services:
      a. Coordinate with trade where applicable.
   4. Fire Alarm:
      a. Coordinate with trade where applicable.

5.0 INSTALLATION
A. Installation
   1. The installer shall show evidence of factory certification from the HACS manufacturer.
   2. The installer shall install all system components and appurtenances in accordance with the manufacturer’s specifications, referenced practices, guidelines and applicable codes. Furnish all necessary interconnections, services, and adjustments required for a complete and operable system as specified. Control signal, communications, and data transmission line grounding shall be installed as necessary to preclude ground loops, noise and surges from adversely affecting system operation.

B. Wiring
   1. All wiring is to be installed in dedicated conduit throughout. Cable shall not be pulled into conduits or placed in raceways, compartments, outlet boxes, junction boxes or similar fittings with other building wiring.
   2. All low voltage wiring outside the control console, cabinets, boxes and similar enclosures, shall be plenum rated where required by code.
   3. All wiring conductors connected to terminal strips shall be individually numbered and each cable or wiring group being extended from a panel or cabinet to a building mounted device shall be identified with the name and number of the particular device as identified and shown on building drawings.
   4. All exposed wiring inside and outside the control console, cabinets, boxes and similar enclosures, shall be dressed down neatly and secured with wiring cleats or wire ties.

C. Containers
   1. All exposed metallic flexible conduit and armored cable shall be dressed down neatly and secured with low profile, metal fasteners.
   2. All cabinets, boxes, and similar enclosures containing security system components and/or cabling, which may easily be accessible to employees or to the public, shall be provided with a lock. Boxes above ceiling level in occupied areas of the building shall not be considered to be accessible.
   3. All junction boxes and small device enclosures below ceiling level, and easily accessible to employees or the public, shall be covered with a suitable cover plate and secured with tamper proof screws.
   4. End-of-Line resistors shall be installed at the field device location and not at the controller panel location.

D. Drawings and Diagrams
   1. System devices identified on building drawings are intended to generally indicate areas where such devices are to be located. Installers shall be responsible for determining final location of these devices in accordance with Owner’s requirements.
2. Riser diagrams are schematic and do not show every conduit, wire box, fitting, or other accessories. Provide such materials as necessary for a complete and functioning installation. Install in accordance with referenced codes and these specifications. Use weatherproof equipment or covers where installed in areas exposed to weather.

6.0 POST-INSTALLATION
A. Software updates to the HSMS application are to be delivered automatically without dealer intervention
B. Firmware updates to SDCs are to be delivered with dealer intervention

7.0 FIELD QUALITY CONTROL
A. Written Reports
   1. Contractor must note any variants at the site and notify owner’s representative within three business days of anything that might affect the delivery date of the system or any trades associated with the functioning of the system.
B. Manufacturer’s Field Services
   1. When applicable, contractor is to coordinate a specific number of visits with the manufacturer’s engineering support team for the system design, insulation, commissioning, final testing, or training.

8.0 TESTING & VERIFICATION
A. Perform tests recommended and required by manufacturer to verify required performance of Brivo Inc. products
B. The Installer is required to place entire system into full and proper operation as designed and specified
C. Verify that all hardware components are properly installed, connected, communicating and operating correctly
D. Verify that all system software is installed, configured, and complies with specified functional requirements

9.0 COMPLETION & CLEANUP
A. Upon completion and verification of performance of installation, remove surplus materials, excess materials, rubbish, tools and equipment
B. The Installer shall perform final acceptance testing in the presence of Owner’s representative, executing a point by point inspection against a documented test plan that demonstrates compliance with system requirements as designed and specified
   1. Submit documented test plan to Owner at least (14) days in advance of acceptance test, inspection and check-off.
   2. Conduct final acceptance tests in presence of Owner’s representative, verifying that each device point and sequence is operating correctly and properly reporting back to control panel and control center.
   3. Acceptance by Owner is contingent on successful completion of check-off; if check-off is not completed due to additional work required, re-schedule and perform complete check-off until complete in one pass, unless portions of system can be verified as not adversely affected by additional work.
   4. The system shall not be considered accepted until all acceptance test items have been successfully checked-off. Beneficial use of part or all of the system shall not be considered as acceptance.
C. The Installer shall provide system operations, administration, and maintenance training by factory trained personnel qualified to instruct in the following areas
   1. Owner will designate personnel to be trained.
   2. Provide printed training materials for each trainee including product manuals, course outline, workbook or student guides, and written examinations for certification.
   3. Provide hands-on training with operational equipment.
PART 1 GENERAL
1.0 SUMMARY
   A. This section provides the specifications necessary for managing the entire Access Control System (ACS) over a Web-based Interface
   B. The interface shall be intuitive, and shall follow industry standards for providing cross-platform compatibility with multiple Internet browser technologies such as: Internet Explorer, Mozilla Firefox, Google Chrome or Safari and shall not require a separate native application for any system configuration

2.0 DEFINITIONS
   A. HSMS – Hosted Security Management System
   B. X.509 – ITU-T standard for a Public Key Infrastructure for Single Sign-On and Privilege Management Infrastructure
   C. ITU-T – International Telecommunication Union, Telecommunications Standards Sector
   D. SSL – Secure Socket Layer
   E. SDC – Security Door Controller

3.0 SYSTEM DESCRIPTION
   A. The HSMS Web-based Interface shall provide authorized operators the ability to manage the access control system over secured connections using any standard Web browser
   B. Encryption & Authentication
      1. All sessions between the browser and the HSMS shall be encrypted using 128-bit Secure Sockets Layer (SSL) encryption.
   C. Browser requirements shall include, but not be limited to
      1. The use of cookies must be enabled to preserve session information and allow the interface to function properly.
      2. JavaScript to validate form data, control navigation, and display images.
      3. The use of pop-up windows for functional elements.

4.0 WEB-BASED ARCHITECTURE
   A. The HSMS Web-based Interface shall follow a structured layout allowing access to all major system categories
      1. The main display shall consist of a home page that shall allow the user log-in access using a pre-determined user name and password.
      2. Access to all major categories of the system shall be through the use of a horizontal navigation bar.
      3. The navigation bar shall be accessible from all category and sub-category views.
      4. Upon log-in, the user shall be redirected to a Dashboard view, which shall provide dynamic activity lists and device status logs displaying the most recent events in reverse chronological order.
      5. All page views shall also include:
a. An icon which shall link the user to Help supported topics.
b. An icon which shall permit the user to Logout of the system in a secure manner.

5.0 OTHER PROGRAMMABLE FEATURES

A. The Interface shall also include category views for the creation and management of
   1. System activity logs and activity reporting.
   2. System devices and hardware.
   3. User cards, including editing, deleting and formatting.
   4. Users and user groups.
   5. Schedules and holidays.
   6. Account details, email notifications and the creation of custom fields.
   7. Configuration and networking details of the ACS.

PART 2 PRODUCTS

1.0 MANUFACTURERS

A. Reference Section 28 13 00 – Access Control, Part 2, Article 2.01

SECTION END