Architectural and Engineering Specification

for:

Brivo ACS 4000 Control Panels and ACS Service

January 25, 2005

Brivo Systems, LLC
4350 East-West Highway
Suite 201
Bethesda, MD 20814

TABLE OF CONTENTS

1 General

The purpose of this document is to specify the Architectural/Engineering and Bid criteria for a Wide Area Network (WAN) based Access Control System (ACS).

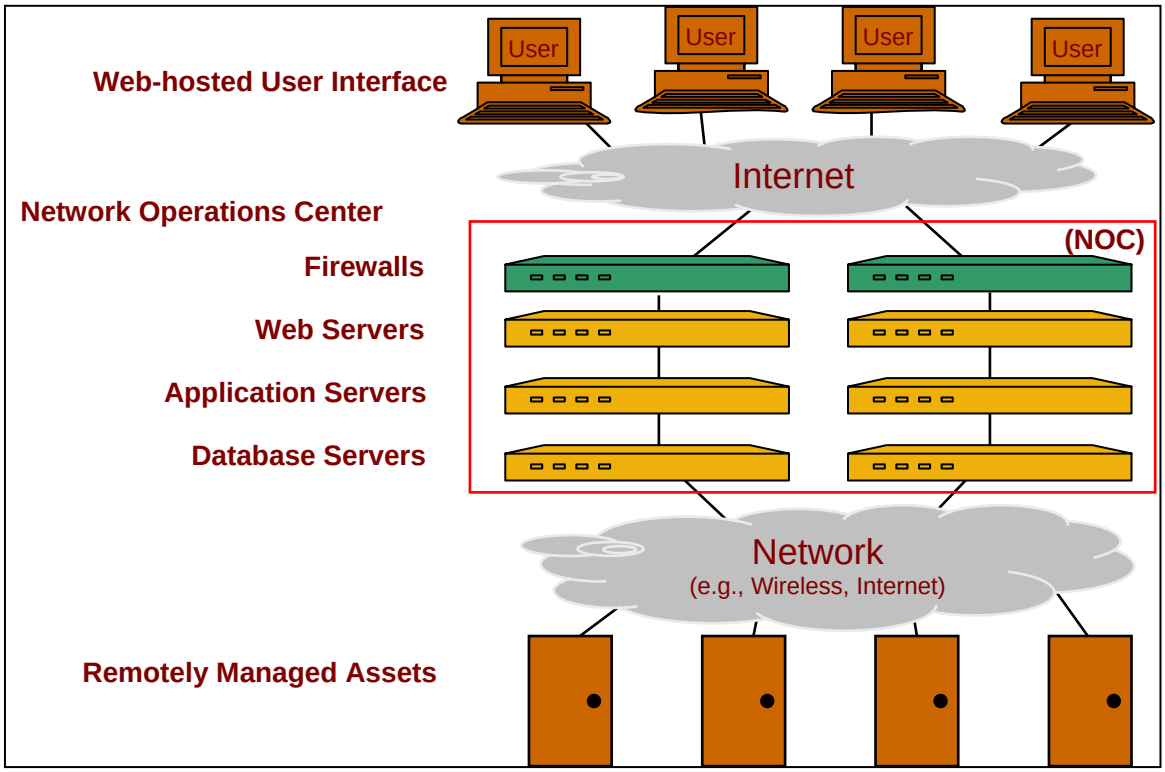
1.1 System Description

The WAN-based ACS allows companies to network access control systems across the nation and manage them all via a Web-based interface. This ACS architecture — with the system provider responsible for all required network connections — eliminates the time, cost and complexity custom cabling or internal IT setup and the provisioning of telecom networks to the remote facilities. It also removes the need to set up and maintain local networks and dedicated PCs or servers.

The WAN-based ACS control panels installed at customer facilities are networked with a central data center where the ACS application is hosted. The application is made available via the Web to customers for administration and management control of facilities, users, credentials, access logs, auxiliary devices, etc.

The core components of the ACS service platform are the centrally hosted and managed applications operated at secure hosting facilities. These applications integrate wide area networking technology with Web-based application services to provide specific products within vertical markets.

A reference diagram for the system is provided below.



1.2 Related Documentation

The following documentation is incorporated into this specification by reference:

1. Brivo ACS3000 Installation Manual, Document Number - 114A2581, Revision 1.13
2. Brivo ACS4000 Installation Manual - 114A2687- G4, Revision 1.3
3. Brivo Administrator's Manual, Updated February 14, 2003.
4. Brivo ACS Information Security, March 5, 2003

2 System Architecture

The following subsections specify the system architecture and related services for the ACS application.

2.1 Managed Service Provider

1. The ACS service shall be provided under the Managed Service Provider (MSP) model, with the characteristics listed in this section. MSPs provide software and system functionality on a centralized, hosted basis, rather than as an installed application that resides at an end-user site.

2. The MSP shall host the ACS applications in a secure data facility.

3. The secure data facility shall have 24x7x365 staffing, including security and operational personnel.

4. The secure data facility shall have redundant main AC power supplies, including diesel generator backup.

5. The MSP shall perform all system and application maintenance on behalf of the end user.

6. The MSP facility shall provide secure archival data storage, including periodic offline tape backups.

7. The MSP shall provide "automatic" software upgrades by updating central server software that will be available to the end user upon the next login to the system after the upgrade has been performed.

8. The MSP shall provide on-call customer support services for the application and control panel.

2.2 Web Hosted

1. The ACS application shall be hosted on Web servers which are accessible via the Internet.

2. The ACS application shall be interoperable with common firewall and proxy server settings.

2.3 Internet Browser Accessible

1. The ACS application shall be accessible via a standard Web browser over the Internet.

2. The ACS application shall not require any special “client” hardware or software other than a standard Web browser (e.g., Internet Explorer 4.0 or above).

3. All end-user control over the application shall be possible via a standard Web browser, including Internet Explorer 5.0 or higher, AOL 5.0 or higher, Netscape 6.0 or higher, or Opera 5.0 or higher.

4. The ACS application shall not require the end user to install any server software whatsoever.

2.4 Encryption & Authentication

1. Sessions between the end-user browser and the Web-based ACS application shall be encrypted using 128-bit Secure Sockets Layer (SSL) encryption.

2. Communications between the control panel and the ACS application servers shall be encrypted using 128-bit Secure Sockets Layer (SSL) encryption.

3. The MSP servers shall validated the identity of any control panel attempting to communicate with the servers through the use of X509 digital certificates.

4. When attempting to communicate with the MSP, the control panel shall validate the identity of the MSP servers via the use of X509 digital certificates.

2.5 Wide Area Network

1. Control panels shall communicate with the central ACS application servers via either the Internet or a wide area wireless network.

2. The wide area network connectivity shall be provided by the MSP as integral to the ACS service.

3. In the case of wide are wireless connectivity, the ACS system shall not require the end user to install any serial communications, or network wiring to connect to the end-user’s LAN/WAN infrastructure.

4. In the case of Internet connectivity, the ACS system shall provide an integral RJ45 connector for Category 5 Ethernet cabling to connect to the end-user’s LAN/WAN infrastructure.

2.6 Central Data Storage

1. All customer and system data shall be centrally stored at the MSP’s hosting facility.

2. All data stored at the MSP facility shall be backed up to a secondary site or to off-site storage.

2.7 Redundancy

1. All servers that are essential to providing the ACS service shall be redundant.

2. All communications channels between the MSP and the wide area network shall be redundant.

3. The MSP shall have a secondary set of servers that can provide the ACS service in the event of a catastrophic disruption at the primary facility.

3 ACS Application

The ACS application resides at the centrally hosted facility and supplies data storage, user interface, and all other server-side functions.

The ACS application shall support the functionality described in this section.

3.1 General

1. Provide storage of all data in a centrally hosted database which is managed by the service provider.

2. Time stamp all access and system events.

3. Provide ability for the end user to make ACS configuration changes such as, but not limited to: door open time, door contact shunt time, site and door names, schedules for credential validity, restricted holiday access, auxiliary device control and card databases.

4. Provide a means for the MSP to backup and restore of any archival data.

5. Provide a robust communications protocol to the control panels so that all commands and updates to the panels are verified and will be retried if communications have failed.

6. Provide the ability for the end-user to define custom schedules to control credential validity.

7. Provide integrated, Web-based biometric support such that users can be registered to the system at the same time their biometric data is being captured.

8. Provide detailed activity reports of failed access events in the following cases; users attempting access to restricted doors, users attempting to access outside of their approved schedule, users attempted access with a revoked credential, users attempted to access with deleted or expired credentials, attempted access by cards not yet assigned, attempted access by unknown card types

3.2 Application User Authentication and Journaling

1. The ACS application shall be protected by requiring users to supply a logon ID and a password in order to gain entry to an account and its associated control panels and databases.

2. The ACS shall support multiple administrators per account, each with a unique logon ID and password.

3. The ACS system shall create and display a non-editable journal of all administrative actions performed on the account for the purpose of generating an unalterable audit trail.

3.3 Browser Based Controls

The ACS application shall support the following system control and editing functions from any Internet-connected browser, after a user has logged in:

Browser Based ACS Functions
1. Create Group of Users
2. Edit Access Privileges for Users
3. Turn Keypad Unlock-Hold Privilege ON
4. Turn Keypad Unlock-Hold Privilege OFF
5. Delete Group of Users
6. Create User
7. Assign PIN to User (4 to 8 digits)
8. Change PIN for User
9. Erase PIN
10. Assign Card to User
11. Change Card for User
12. Revoke Card from User
13. Edit User Start Date
14. Insert User Expiration Date
15. Edit User Expiration Date
16. Erase User Expiration Date
17. Add User to a Group
18. Remove User from a Group
19. Delete User
20. Create Schedule
21. Edit Schedule
22. Delete Schedule
23. Create Holiday
24. Edit Holiday time range
25. Edit Holiday doors
26. Delete Holiday
27. Create a Site
28. Create Door
29. Create an Auxiliary Device
30. Edit and Auxilury Device
31. Edit Door Timer schedule
32. Turn Door Timer ON / OFF
33. Turn door_ajar_checkbox ON / OFF
34. Edit door_ajar_seconds
35. Edit freeze_keypad_after_x_invalid_pins
36. Edit freeze_keypad_for_x_seconds
37. Edit user_has_x_seconds_to_enter_door_after_authentication
38. Edit deactivate_alarm_shunt_after_x_seconds
39. Edit auxiliary_relay_duration_seconds
40. Display Activity Log – All Activities
41. Display Activity Log with individual User filter
42. Display Activity Log with individual Site filter
43. Display Activity Log with individual Door/Device filter

Browser Based ACS Functions
44. Allow User to view Activity Log by 20, 30 or 40 events per page
45. Activity Log Reports – search user by absolute date and relative days
46. Activity Log Reports – search exception events, user events, control panel events and device events by absolute date and relative days
47. Activity Log Reports – search by site door/device specific events.
48. Activity Log Reports – search by site door specific user.
49. Turn on/off Email Notifications
50. Turn on/off Daily Email Activity Summary Reports
51. Preferences – Change/Override time zone.
52. Preferences – Create Assistant Administrators.
53. Preferences – Edit Assistant Administrators.
54. Preferences – Delete Assistant Administrators
55. Preferences – Change Password
56. Add Cards to Card Bank.
57. Add Cards of various Bit lengths to card bank (26, 34, 35, 37 with FC, 37 without FC, 40)

3.4 Email Notifications

The ACS application shall provide the ability to send email notifications to standard email accounts, pagers, and cell phones in response to various system events as described below.

1. The ACS application shall allow user to create an arbitrary number of Email Notification Rules which specify the events types that shall produce email notifications, as well as the addresses of the recipients.

2. The ACS application shall allow user to specify an arbitrary number of email addresses for each rule.

3. The application shall allow user to select from the following event types for email notifications:

   - Door Ajar/Door Ajar Cleared
   - Door Forced Open
   - Too many invalid PIN entries
   - Door unlocked by keypad
   - Door locked by keypad
   - Failed Access Attempt by Known Person
   - Failed Access Attempt by Unknown Person
   - Access by individual user
   - Access by any user within a group
   - Auxiliary Device Engaged/Disengaged
   - Control Panel Unit Opened/Closed
   - AC Power Loss/Restoral and Battery Status

3.5 Email Reports

The central ACS application shall support a configurable utility for sending reports to end users.

1. The ACS application shall email Daily summary reports to the end user.
2. The Daily reports shall include a summary of all access and exception events for the day, by site, user and time.

3.6 Credential Data Base

1. Card credential information shall include unique card number up to 16.
2. Allow multiple credentials per user.
3. The ACS system shall allow the creation of PIN credentials of between 4 to 8 digits, user selectable.
4. The ACS system shall be capable of assigning Random or User designated PIN codes of between 4-8 digits, with guaranteed uniqueness across the account.
5. Provide 10 user definable fields associated with user in the user database.
6. Upon editing credential information, the updated information shall be sent automatically to the appropriate access control panels with no other user intervention

3.7 Access Control

1. The ACS application shall provide the ability to define specific schedules for access, and be able to associate these schedules with groups of users and doors within the system.
2. The ACS application shall provide the ability to define specific reader points of access Groups of users.
3. The ACS application shall provide the ability to define groups of doors and users.

3.8 Tiered Administration

The ACS application shall support Tiered Administration to enable accounts to establish different logon IDs for different administrators with different permissions for viewing and editing account data.

1. The Master Administrator of an Account shall be able to create, edit and delete Assistant Administrators; Assistant Admins shall have the following properties:
    a. First Name
    b. Last Name
    c. Role
    d. Phone
    e. E-mail Address
    f. Time Zone
    g. Admin ID
    h. Password
    i. Secret Question
    j. Secret Answer

2. The Master Administrator shall be able to define a set of permissions for each Assistant Administrator.

3. The Master Administrator shall be able to view a list of all Assistant Administrator, in alphabetical order by last name, along with their Admin IDs, created dates and updated dates; view or edit an Assistant Admin by clicking on the name; and delete an Assistant Admin via the list screen.

4. The Master Administrator shall have the maximum set of permissions. Additionally, the following Account level actions *shall be restricted to the Master Administrator:*

    a. Creating and Deleting Groups
    b. Creating and Deleting Cards
    c. Creating, Editing and Deleting Schedules
    d. Creating, Editing and Deleting Holidays
    e. Creating Sites and Deleting empty Sites
    f. Editing Custom Field Labels
    g. Creating, Editing and Deleting Assistant Administrator
    h. Creating, Editing and Deleting Roles
    i. Editing Summary Recipient List
    j. Editing Company Information

5. The Master Administrator shall be able to edit the above properties A-E at any time; The Assistant Admin shall be able to edit the above properties F, H, I and J.

6. The ACS application shall support multiple Senior Administrators with the same privileges to modify access control data as the Master Administrator.

4 Control Panels

The following subsections specify required control panel characteristics.

4.1 Supported Readers

Control panels shall support multiple card reader technology via standard Weigand interfaces, including:

Weigand effect readers
Proximity readers
Biometric readers
Keypads (PIN)

4.2 Power Requirements

1. The control panel shall be powered from a standard 120VAC, 60Hz. outlet.

2. The control panel shall be supplied with internal battery backup, and include the following functionality related to power source:

   - The control panel shall indicate whether it is on main or battery backup power;
   - The control panel shall send an alarm to the central ACS application when it switches between main and battery power;
   - The control panel shall send low battery alarms each time the remaining battery capacity declines by 10%.

3. The control panel shall provide a notification to the central ACS application upon Power Up / Start-up / Reboot.

4.3 Door Control Boards and I/O

1. The control panel shall support up to four Door Control boards.

2. Each Door Control board shall support the following output relays:

   - Door Latch Relay
   - Alarm Shunt relay
   - Auxiliary Relay

3. Each Door Control Board shall support the following inputs:

   - Reader Interface
   - Door Closure Sensor Input
   - Request to Exit Switch Input
   - Auxiliary Switch Input

4. The Reader interface shall support the following (Weigand) lines:

Circuit / State
Weigand DATA 0
Weigand DATA1
RED Led Control Output (8 wire option)
12VDC thru 1amp fuse (F2)
Ground
Shield
GREEN Led Control Output
BEEPER Output Control (8 wire option)
Keypad Hold Control

4.4 Access Control Functions

1. The control panel shall support a “Request to Exit” input which energizes an associated relay in order to open a door.

2. The control panel shall support an “Auxiliary” input which energizes an associated relay.

3. The control panel shall perform local credential-based User Authentication against a local database stored in FLASH memory.

4. The control panel shall perform local credential-based User Authorization against a local database stored in FLASH memory.

5. The control panel shall provide for door latch activation / deactivation via a relay output.

6. The control panel shall provide Door Ajar Notification with a configurable timer to define the length of time before a door is considered to be “ajar”.

7. The control panel shall provide Door Open Notification to the central ACS application via a contact closure input.

8. The control panel shall provide Door Close Notification to the central ACS application via a contact closure input.

9. The control panel shall provide Auto Unlock Notification to the central ACS application.

10. The control panel shall provide for local buffering and replay of events in case of a communications failure between the control panel and the central ACS application.

11. The control panel shall provide a centrally configurable Holiday override feature.

12. The control panel shall provide centrally configurable Door Unlock by Schedule feature.

13. The control panel shall provide centrally configurable Door Unlock by Keypad feature.

14. The control panel shall send Device Status to the central ACS application at least once per hour.

15. The control panel shall send a notification to the ACS of unauthorized door opening.

5 Brivo ACS Product Specifications

5.1 General Features

1. The ACS4100 is designed for single door/gate reader installations.
2. The ACS4400 is designed for multi-door installations up to 4 readers per control panel.
3. Centralized control and management of all sites, readers, doors, and access privileges via any PC, Mac or Web-enabled device.
4. Wiegand reader compatible.
5. Automatic event buffer.
6. Up-to-the-minute online updates of event transactions.
7. User-specified event notifications to e-mail, pager and cell phone.
8. 1,000 users/credentials per control panel.

5.2 Hardware Components

1. Brivo ACS Control and Communications Panel
2. Power supply, transformer, battery and antenna kit (wireless version only).

5.3 Recommended Readers

- Essex ThinLine 2x6 Stainless Steel Keypad
- Essex 12 Pad 3x4 Stainless Steel
- HID ThinLine II Switch Plate Proximity Reader.
- HID Prox-Point Plus Proximity Reader
- HID Mini-Prox Proximity Reader
- HID Prox-Pro Proximity Reader with Integrated Keypad
- HID Prox-Pro Proximity Reader
- BioScrypt V-Smart™ Biometric Reader
- Additional Readers Supported on Custom Basis

5.4 Online Service for Account Administration

1. Web-based user interface, including online activity log.
2. Multiple administrative account passwords, with journal.
3. Immediate notification of events to e-mail, pager, or cell phone.
4. Templates and customized time schedules, time zones and group management.
5. Cards and PINs supported, including card bank management features.
6. Archive history online.

5.5 Service & Support

1. User manual, help, installation manual and quick-start user guide available online.
2. 24/7 unlimited use of Brivo's access control service.
3. One Year Warranty.
4. Toll-free telephone and e-mail customer support.

6 Brivo ACS Technical Specifications

Number of readers:	1 for ACS-3100; 4 for ACS-3400
Secure Wireless Network Connection:	Yes
Wiegand Reader Compatibility:	37 Bit, HID Corporate 1000, 26 Bit, 33 bit
Wiegand Keypad Compatibility:	8 Bit (Word) / 4 Bit (Nibble)
Wiegand Biometric Capability:	26 Bit
Real-time reporting at www.brivo.com:	Yes
Archived Data:	Yes
E-mail notifications & activity reports:	Yes
Inputs:	3 for ACS-4100; 12 for ACS-4400
Relay Outputs:	ACS-3100: 1 SPDT Form C 16A Contacts, 2 DPDT Form C5A Contacts ACS-3400: 4 SPDT Form C 16A Contacts, 8 DPDT Form C5A Contacts
Alarm Shunting:	Yes
Control Panel Power Requirements:	16.5 Volt, 40 VA
Battery Backup:	12 Volt DC 4 Ah
Enclosure:	NEMA Type 1, Tamper Switch, Key Locks
Dimensions:	6.25" (d) x 14.25" (h) x 16.25" (w)
Panel to Panel Wiring Distance:	Unlimited due to long-range wireless networking
	Not applicable for Ethernet version of panel
Temperature & Humidity Range:	Operating Temp: 35-110° F (2-43° C) Humidity: Max 85% Non-Condensing
Panel/Reader Limit Per Account:	Unlimited/Unlimited
Card Memory:	8,000 Users/credentials per panel.
Antenna Included (wireless only):	Yes, w/ 16 ft. of coaxial cable & mounting bracket
Warranty:	One year, parts.
Smart Cards Supported:	Yes, HID 1430 & 1431 Contactless Smart Cards