Keri Systems *Doors.NET* Architectural Bid Specification

This document has been prepared to assist design professionals in the preparation of project or office master specifications including Proximity access control systems. Modify this document as necessary and delete items that are not applicable.

2305 Bering Drive • San Jose CA 95131
800 260-5265 • 408 435-8400 • Fax 408 577-1792
www.kerisys.com

P/N 01778-001 Rev. A

Computer, Operating System, and Database Requirements

a. Any computer running the designated operating systems will be capable of running both the Client and Server Software. The computer shall have a standard 10/100 Ethernet Card.

b. It is recommended the computer have Internet access for online software registration and software license authentication. An offline registration and license authentication process must also be available.

c. The operating system software for Servers shall be one of the following in either 32 or 64 bit configurations:
- Microsoft ® Windows ® XP Professional with Service Pack 2 or 3
- Microsoft ® Windows ® Vista Business or Ultimate
- Microsoft ® Windows ® 7 Professional or Ultimate
- Microsoft ® Windows ® Server 2003 or 2008

d. The operating system software for Clients shall be one of the following in either 32 or 64 bit configurations:
- Microsoft ® Windows ® XP Professional with Service Pack 2 or 3
- Microsoft ® Windows ® Vista Business or Ultimate
- Microsoft ® Windows ® 7 Professional or Ultimate

e. The system software shall use the Microsoft® SQL Server 2000/2005 or Microsoft® SQL Server 2005 Express. The software installation application shall allow the user/installer to install the appropriate database if it is not already installed on the system computer or network. The appropriate drivers shall be automatically installed as part of the installation.

f. The system software shall use the Microsoft ® .Net Framework; version 3.5 or greater. The most recent version of the .Net Framework shall be installed, if required, as part of the software installation.

2. Network Requirements and Communication
The system shall be deployed on a network; it shall be based upon a TCP/IP 10/100 architecture.

The software shall enable PC communication to system controllers over a LAN and/or WAN using Ethernet protocol. The software shall allow the user to perform all system functions in a LAN/WAN environment as are possible when controllers are communicating with the server PC.

3. Access Control Field Hardware
The access control hardware shall have the capability to control and monitor all doors, exit devices, locking hardware, Readers and security detectors.

a. Scope of Control
There shall be several types of control devices

i. Controllers
The system shall consist of either 2 or 4 reader Controllers, or a combination thereof. The Controllers will operate in a 'stand-alone' mode or within a network of other like Controllers. All decisions regarding the user access, alarms, and automatic timed functions are made at the Controller, independent of any computer. It shall also have RS-485 communication buses to provide additional system functionality to expansion boards or modules and high security proximity readers.

ii. Expansion Modules
There shall be modules that allow a Controller to expand the number of I/O points it can monitor and control. The number and type are described in the next section.

iii. Input Types and Number
Inputs shall be user definable to accept 2, 3 or 4 state supervision. The 4 Reader Controller shall be expandable to at least 144 additional inputs. The 2 Reader Controller shall be expandable to at least 72 additional inputs. Inputs on the main Controller shall default to a standard door configuration but shall be re-assignable to monitor devices such as (but not limited to) a Door Contact Switch, Request to Exit, Bond Sensor, PIR, Glass Break Detector or any other general purpose dry contact device.

iv. Tamper Input
All Controllers and Expansion Modules shall have dedicated tamper inputs.

v. Output Types and Number
Outputs shall be 1.0 amp, (24VDC max.) dry circuit, single pole, double throw relays for application of power to an electric locking device, automatic gate, door operator, annunciator, shunting an alarm or other general purpose function triggered by a relay. The 4 Reader Controller shall be expandable to at least 144 additional outputs. The 2 Reader Controller shall be expandable to at least 72 additional outputs.

b. Communication

i. Communication to Server
All communication from the Controllers to the Server shall be via a TCP/IP 10/100 bus.

ii. Communication between Controllers

1. Supported Network Type
The Controllers shall have Ethernet hardware and TCP/IP protocols embedded built in, without requiring additional boards or converters. There shall be no single point of failure within the Access Control hardware where communication or decision-making is compromised. There shall be no master-slave architecture.

iii. Response Time
1. On a dedicated TCP/IP network without other network traffic, the response time between inputs and outputs on different Controllers shall not exceed 1 second communication between other Controllers and the Server.

iv. Communication to Expansion Modules and High Security Proximity Readers
1. Supported Network Type
All communication between a host Controller and its Expansion Modules used for a variety of functions, and the high security Proximity Readers shall be via a supervised, encrypted, 9 bit RS-485 bus. The Expansion modules can be placed up to 500 feet (150m) away from the Controller.

2. Capacity
Different module types (input/output boards, or other products that may be developed) can be connected to an RS-485 bus on each controller.

3. Response Time
The response time when linking inputs and outputs within any specific Controller shall not exceed 1 second.

c. Reader Interface
i. Reader Types and Formats
The Controller will directly support a high security 64 Bit Encrypted format that also provides for Reader supervision. It will also support via a Reader Interface Module, the following Reader types or formats:
1. Up to 64 bit Wiegand
2. Magnetic Stripe with Wiegand output
3. Bar Code with Wiegand output
4. Keypad with Wiegand output
5. Biometric with Wiegand output
6. Electronic Discharge or Touch Memory Devices with Wiegand output
7. Keri Systems MS Series Proximity Reader

Wiegand Interface Reader devices must output data per the Security Industry Association's (SIA) Wiegand Reader Interface Standard (SIA document number AC-01D-96).

ii. Mounting Options
The Reader Interface Board will mount on any Controller or optionally on any Expansion Module to maximize wiring flexibility and decrease installation cost.

d. Memory

i. Memory Type
The Controller's memory shall be non-volatile (supported by a lithium battery) with an expected life of 5 years. The Controller will send a notification to the Server Software when the lithium battery power approaches a state where it can no longer back up the memory.

ii. Cardholders
The Controllers must have the capacity to store up to 48,000 individual Credentials/PINs.

iii. Events
The Controller shall store up to 10,000 events should communication fail between it and the Server. The system will automatically send events to the Server during normal communication. The Controller shall be configurable such that only events designated by a system administrator are stored. Should the event buffer become full, each Controller will delete events only as needed on a first in, first out basis. Each Controller's memory shall operate independently of all other Controllers.

e. Surge Protection

i. Power Protection
The Controller and Expansion modules shall be protected by a self-resetting, thermal fuse as well as diode protection. The Reader shall have reverse voltage diode protection.

ii. Network Protection
The RS-485 network shall be protected by diodes and gas discharge tubes on all communication ports.

iii. Input Protection
All inputs shall be protected against power surges by diodes.

iv. Output Protection
All outputs shall be protected against power surges by MOVs and resistor snubber circuits.

f. Power Requirements

i. Main Controller
The main Controller shall be powered from 12VDC and draw no more than 650 mA at 12VDC when all outputs LEDs and communication buses are fully active.

ii. Expansion Board
The 4 input/4 output Expansion board shall normally draw its power from the main Controller at 12 VDC and shall draw no more than 250 mA when all outputs LEDs and communication buses are fully active. It can optionally be powered locally.

iii. Readers
The primary High Security Reader types' current draw shall not exceed 120 mA at 12VDC and shall be powered from the Controller. They can optionally be powered locally.

g. Indicators
i. Communication Buses
1. There shall be LED indicators for RS-485 network activity
2. All TCP/IP networking lines shall have LEDs to indicate network speed and activity (10 or 100 mb).

ii. There shall be a power fault LED for over voltage and reverse voltage.

iii. There shall be a reset LED to indicate when the Controller memory is in the process of being cleared that turns off when the process is complete.

iv. All relays shall have status LEDs indicating when they are energized.

h. Operating Temperature
The operating temperature range of the Controller shall be no less than 32º F to 150º F (0º C to 65º C) at 0% to 90% Relative Humidity, non-condensing.

i. Connections
i. Power, I/O and RS-485 Connections
These shall be made via quick disconnect connectors. TCP/IP connections shall be made with an RJ-45 connector or optionally with the quick disconnect connector also provided on the Controller.

ii. Earth Ground
A ground lug shall be provided for earth ground that meets all appropriate UL specifications for security and control equipment.

j. Mechanical Spec.
i. Main Controller
The maximum dimensions for the Controller's enclosure shall be 13.125" high by 10.625" wide by 3.06" deep (33.34 cm high x 26.99 cm wide x 7.77 cm deep), with "knock-outs" to accept both USA and metric conduit. The enclosure shall be metal and equipped with a locking mechanism. The enclosure shall have provisions for an optional tamper switch assembly.

ii. Expansion Board
The maximum dimensions for the Expansion Board's enclosure shall be 9.50" high by 8.00" wide by 4.00" deep (24.13 cm high x 20.32 cm wide x 10.16 cm deep), with "knock-outs" to accept both USA and metric conduit. The enclosure shall be metal and equipped with a locking mechanism. The enclosure shall have provisions for an optional tamper switch assembly.

4. Reader Types
   The primary type of Reader shall be a High Security Proximity Reader. The Proximity Reader shall read a unique identification number from each Card or Tag when the Card or Tag is presented to the surface of the Reader, without a need for the Card or Tag to touch the Reader.

   a. General Reader Characteristics
      All Proximity Readers shall be of a weatherproof, potted, rugged design.

   b. Operating Temperature
      The operating temperature of all Readers shall be at least -40ºF to 150ºF (-40ºC to 65ºC).

   c. Encryption, Security and Supervision
      Accidental or intentional transmission of radio frequency signals into the Reader shall not compromise the security of the access control system. The Readers shall read encrypted Proximity Cards. The Reader shall be supervised by the Controller with a regular "heartbeat" capable of responding within 1 second if the Reader goes offline.

   d. Connections
      The interface to the Controller will be on the supervised, encrypted, 9 bit RS-485 bus and shall require only a 4 conductor cable for all Reader functionality including dual color LED control and beeper control.

   e. Reader Function
      When connected to the Controller, presentation of a card or tag will produce an audible beep from the Reader and will change the color of the Reader LED.

      - An Amber LED shall indicate power is on and the Reader is in its ready state.
      - A Green LED shall indicate access is granted.
      - A Red LED shall indicate access is denied.

   f. Primary Reader Styles
      i. Mullion Reader
         1. Size
            A doorframe Reader (mullion Reader) that can be mounted directly on a standard metal mullion doorframe. The dimensions of the Reader shall be 3.75" high by 1.60" wide by 0.625" deep (9.5 cm high x 4.1 cm wide x 1.6 cm deep).

         2. Power
            The Reader shall be powered directly from the Controller and shall not exceed 120 mA. The Reader may optionally be powered independently from the controller.

3. Read Range
   The read range using a standard Proximity Card shall be up to 4" (10 cm).

4. Indicators
   The Reader shall provide a multi-color LED and a sound alert for status annunciation.

ii. Euro Reader

1. Size
   A single gang mount, wall switch Reader that can be mounted onto a metal or plastic European electrical junction box or on a non-metallic flat surface. The dimensions of the Reader shall be 3.25" high by 3.25" wide by 0.625" deep (8.3 cm high x 8.3 cm wide x 1.6 cm deep).

2. Power
   The Reader shall be powered directly from the Controller and shall not exceed 120 mA. The Reader may optionally be powered independently from the controller.
3. Read Range
   The read range using a standard Proximity Card shall be up to 5" (12.5 cm).

4. Indicators
   The Reader shall provide a multi-color LED and a sound alert for status annunciation.

iii. Wall Switch Reader

1. Size
   A single gang mount, wall switch Reader that can be mounted onto a metal or plastic USA electrical junction box or on a non-metallic flat surface. The dimensions of the Reader shall be 4.18" high by 2.95" wide by 0.625" deep (10.6 cm high x 7.5 cm wide x 1.6 cm deep).

2. Power
   The Reader shall be powered directly from the Controller and shall not exceed 120 mA. The Reader may optionally be powered independently from the controller.

3. Read Range
   The read range using a standard Proximity Card shall be up to6" (15 cm).

4. Indicators
   The Reader shall provide a multi-color LED and a sound alert for status annunciation.

iv. Other Reader Types
As needed, the system shall also have the capability of accepting inputs from Readers such as Biometric Readers, Vehicle Readers, other Proximity devices, Swipe, Optical or Contact Readers as described in Section 2.d.

5. Cards and Tags
The system will have the option of using any of the following Proximity Credentials. Cards and Tags shall be uniquely encoded and not sensitive to facility code matching or other limiting factors. Several Card/Tag options shall be available, including a standard "clamshell" Proximity Card in the shape of a credit Card and shall fit comfortably in a wallet, pocket, or purse. The manufacturer guarantees there will be no functioning duplicate cards or tags in existence.

a. Clamshell Card
The color shall be white with the encoded number and a date code printed on its surface.

The dimensions shall be 3.38" long by 2.13" wide by 0.065" thick (8.6 cm H x 5.4 cm W x 178 mm D).

The card shall have a slot punch for attachment to a badge clip.

b. ISO Card
The Card shall be capable of accepting a direct print of photo and other graphics from a dye-sublimation printer.

The dimensions shall be 3.38" long by 2.13" wide x 0.031" thick (86 mm x 54 mm x 0.08mm).

The color shall be white with the encoded number and a date code printed on its surface.

The Card shall be optionally available with a standard high coercivity three track magnetic stripe.

The card shall have an available area for a slot punch for attachment to a badge clip.

c. Key Tag
A standard Proximity Key Tag shall be in the shape of a teardrop. It will have an eyelet, allowing the Tag to be attached to a key ring.

The dimensions shall be 1.57" long by 0.98" wide (at its widest area) by 0.157" thick (40 mm H x 25 mm W x 4 mm D).

The color shall be light gray with the encoded number and a date code printed on its surface.

6. System Software Infrastructure
    a. The software shall enable secure, encrypted connections from remote locations over the Internet without the use of a Web Browser or VPN connections. Web Browser user interfaces are unacceptable.

    b. The software shall provide a multitasking-type environment that allows other Windows®-compatible programs to run on Client and Server computers without interrupting or disturbing communications with the network of NXT Controllers or operation of the software. The system software shall always be capable of alerting a user to security events as required while other programs are running.

    c. The system software shall be a native Windows .NET Framework-designed application and shall run on a Windows® compatible personal computers using one of the following operating systems in either 32 or 64 bit formats: Microsoft® Windows® XP Professional (SP-2 or 3), Windows Server 2003, Windows Server 2008, or Microsoft Windows Vista Business or Ultimate, or Windows 7 Professional or Ultimate.

    d. The Application Server shall be the only component of the software that communicates with the SQL database; Client PCs shall not communicate with the SQL database directly.

    e. All interaction with the SQL database from the software must be performed using Stored Procedures for increased efficiency.

    f. System shall support the use of DHCP addressing for all gateways and all clients.

7. System Software Features
    a. The system shall be capable of accepting future activation or expiration dates for users. The system operator shall have the capability to enroll such time periods down to the minute on any calendar day. These dates shall be kept in the Controller rather than downloaded from the PC.

    b. The Software shall automatically find and configure in its database all Controllers, Expansion boards, Interface boards, and Readers attached to the system.

    c. The Software will automatically assign Static IP addresses to the Controllers based on starting IP address provided to the Software.

    d. There shall be an unlimited number of operators capable of configuring, monitoring, and operating the system.

    e. The integrated security management software shall be Keri Doors.NET®.

    f. The software shall be licensed without the use of hardware dongles.

    g. The software shall not be accessible via web browsers.

h. The software shall support multiple concurrent client licenses.

i. The software shall not require more than 1 SQL client user license to operate.

j. The software installation application shall allow the user/installer to select between a Microsoft® SQL Server Express or Microsoft® SQL Server database structure.

k. The system software shall record all transactions with a GMT timestamp, Local time zone timestamp of the primary controller that generated the transaction, and the SQL server timestamp when the transaction was inserted into the database.

l. All timestamps must be in the ISO 8601 format.

m. User logins that incorporate passwords and other administrative controls available in the system shall protect the system software, database, and data distributed to the controller panels from unauthorized access.
    i. User Rights
        1. The software shall permit assignment of rights to system features on a feature-by-feature basis to any and all system users, whether individually or as members of a defined user group. It shall be possible to add, remove, and edit any user and user group rights.

        2. Passwords assigned to system users shall allow a user to log onto any Client interface without affecting system control of current users logged onto other client interfaces.

n. Capacities
    i. The system software shall be capable of controlling/monitoring of at least 256 doors, and 1,024 four state supervised inputs and 1,024 auxiliary relay outputs.

    ii. There shall be an unlimited number of operators capable of configuring, monitoring, and operating the system.

    iii. The system shall allow for at least 48,000 cardholders (users), each with the ability to have multiple credentials and be assigned to multiple access groups.

    iv. The Software shall have the ability to manage up to 64 distinct time schedules with each time zone subdivided into the 7 days of the week divided into 4 start/stop time intervals and 8 holiday types, with 32 holidays per type.

o. The system shall support the use of PIN digits in a PIN only mode, Card or PIN mode, or Card and PIN mode at selected readers. The PIN digit assigned to a cardholder shall be capable of different lengths for each cardholder with a range of 0 to 6 digits. Leading zero PIN digits shall be supported.

8. Door Configuration
    a. The system software shall support configuration of a wide variety of doors and support for most industry standard reader types and peripheral hardware, as well as Keri NXT Series and MS Series Proximity Readers.

    b. The system software shall provide for configuration and setup of door position switches, request to exit (REX) devices, and all associated door hardware.

    c. The system software shall provide for the configuration of door strike times, help open times, and ADA timing by allowing the operator to type in the exact time in hours, minutes, and seconds.

    d. Through the door configuration interface, the user shall be able to set up, monitor, and control the security hardware components in the software for any door or access-control point in the system. The interface shall also allow the user to see doors that have been configured, edit existing door configurations, and delete door configurations from the system.

    e. It shall be possible to individually assign input points and relays through the software to readers to permit door monitoring and door-lock control. "Autolock" shall be software-selectable on a per-reader basis, and when activated shall cause the pulse time of the corresponding relay and the shunt time for the door-position input to reset when the door closes, overriding the programmed relay pulse time and input point shunt time and re-securing the door. Systems that are not capable of "autolock" shall be unacceptable.

    f. The software shall allow access to designated listings of alarms, readers, relays, schedules, and access levels. Authorized operators shall be able to view, edit, add, or delete any or all alarms, readers, relays and/or schedules and access levels as their designated privilege level allows.

    g. Operators shall also have the capability, within their authorized privilege parameters, to use the same display screen to mask, unmask any alarm point; turn on, turn off, or pulse any relay; or lock, unlock, momentary release or set modes including card only, card or pin, card and pin, or pin only for any card reader.

    h. It shall be possible through the software's User Interface to add, edit, activate, deactivate, and/or delete individual card or cardholder records.

    i. A cardholder entry screen shall provide tabbed pages to allow a system user to:
        i. Capture a photo using a digital camera or retrieve a stored photo file for inclusion in individual new or existing card or cardholder records. Photos shall be displayable in the cardholder record and printable on a photo ID badge, and they shall be made part of the card and cardholder record.

        ii. Digitally store the photo in over 39 different formats including BMP, GIF, JPG, and TIF and export the selected image to any of the 39 formats.

iii. Configure and assign virtually unlimited access groups, which consist of a time schedule and a reader group.

iv. Provide separate drop-down calendar controls for use in assigning card-activation and card-expiration dates.

v. Enter cardholder names, user group membership, access level information, a personal identification number (PIN), company information, and user defined custom data fields.

vi. Set cardholder ADA information.

vii. View data concerning the recent transaction for the cardholder in the system.

viii. Enable PIN Exempt override.

9. User Interface
   a. The User Interface shall incorporate a menu bar with drop-down menus and display icons for full system setup and operation. This menu and these icons shall offer to system users' complete access on one screen to all system functions and system setup parameters to which the users have rights.

   b. The background and text colors for all transaction-display screens shall be customizable for each user, and it shall be possible to apply filters to display only selected transactions on a transaction-display screen, as described in this specification.

   c. The screen layouts shall provide for viewing system cardholder activity; monitoring and acknowledging alarms; and monitoring and controlling input points, relays, and door configurations.

   d. Capability to include a site tree per connected hardware gateway for displaying system setup and configuring system parameters shall be provided.

   e. It shall be possible to create tabbed windows in the screen layout to conserve desktop space in the viewing area without in any way restricting the availability of information that can be displayed for the user.

   f. The user interface will provide a hardware configuration tree and display grids to display information to the user.

   g. The hardware configuration tree shall display all Gateways at a time for configuration while actively monitoring all system gateways.
      i. The user interface shall store the screen layout on a per login basis to include the following: docking positions and state of all dockable controls, group sort categories and direction of all status views, displayed/hidden columns in all status views.

h. The system shall provide for multiple concurrent users. The system shall allow via a license process for one user with the software, with optional unlimited additional licenses.

i. The system shall provide an open architecture event video recording (EVR) solution for video management. The EVR must employ seamless integration and be built on a Microsoft.NET framework. EVR must be user friendly with the complexity and sophistication hidden from the user to provide a uniform, simple look and feel. EVR shall be an advanced Open IP-Surveillance module. It shall simultaneously enable digital video recording from network, mega-pixel and analog devices, and remote access to live and recorded images from any networked computer.

10. Card Design

a. It shall be possible to create and save an unlimited number of card template designs.

b. Systems that do not permit users to create and save multiple custom card designs shall be unacceptable. The system shall allow any or all of the following elements to be employed together in card design that can be used to create individual, cardholder-specific cards or identification badges:

i. Captured or retrieved cardholders' photos that are part of the cardholder database.

ii. Graphics, logos, or other images.

iii. Static data that is duplicated on each card printed.

1. Variable data from the cardholder database that is specific to each card printed.
2. Bar codes.

c. It shall be possible for users to create card designs that employ:

i. A choice of vertical orientation or horizontal orientation with optional card rotation.

ii. Dual-sided printing.

iii. Predefined or custom dimensions.

iv. Cardholder photos with optional borders. It shall be possible to rotate the image, select border color and width, and adjust the image brightness.

v. Bitmaps or JPEGs of logos, designs, pictures, and other graphics, including a card background color or graphic, all with definable dimensions.

vi. Text using the font selections available in Windows®. It shall be possible to vary the formatting of this text.

vii. Slots for insertion of clips, lanyards, etc.

viii. Bar codes associated with database fields that shall be selected from a drop-down list that includes not only the database fields but also a constant or separator. The user shall have the capability to select the field length, use of padding, padding characters, position, rotation, ratio, height, size, and readability of text appearing with the bar code.

ix. The system software shall be capable of allowing unlimited individual badge designs to be designed and created. It shall be possible to preview the design before saving. The software shall allow for on-screen printer selection from a drop-down list that displays all installed print drivers within Windows®.

x. The user shall be able to define logical arguments based on selected database information that may vary from card record to card record. It shall be possible to define different bitmap images to appear on the printed card as a result of the application this logic, which uses the specific data from the database as the criterion for displaying or not displaying the image. In this way, logos or color-coding can be used to identify cardholders having, for example, the same department assignments, shifts, job assignments, or the like.

xi. The software shall provide a page in the cardholder database module to permit template definitions that can be assigned to new cardholders.

d. Card Printing
The software shall permit the printing of identification cards using selected designs as described in this specification.

e. Custom Pages and Fields
The software shall provide pages in the cardholder database module to allow custom fields to be saved to the cardholder database. These fields shall be displayed in the software on a custom tabbed page that can be added for display in the cardholder database interface in the software. It shall be possible for users to:
i. Rename each field and its accompanying label.

ii. Enter and save existing data into the custom field, or delete the data from the field.

f. Define standard Card Templates

11. Peripherals
The system shall allow the use of commercial, off-the-shelf printers and digital cameras for the capture of identification photos and printing of identification badges and system activity reports.

12. Warranties
    a. The product warranty to the user warrants the equipment to be free from defects in material and workmanship for the following time period from the date of purchase.

    b. A two-year no questions asked warranty for the replacement of product only for the Controller, I/O Expansion Boards, and Reader Interface Modules.

    c. A limited lifetime warranty for the Mullion, Euro, and Wall Switch Readers.

    d. A limited lifetime warranty for standard “Clamshell” Proximity Cards and Key Tags.

    e. A one-year warranty for the ISO Card.

13. Acceptable manufacturers of access-control systems include: Keri Systems Inc.