Keri Systems *Doors NetXtreme*™ 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.

Keri Systems *Doors NetXtreme*™ Architectural Bid Specification

System Architecture
a. Operating Systems
    The System shall function under Windows versions of:
    i.   Vista Enterprise
    ii.   Vista Ultimate
    iii. Vista Business
    iv.   XP Pro
    v.   Windows 2003 Server

b. Computer Requirements
    Any computer running operating systems listed in 1a above will be capable
    of running both the Client and Server Software. The computer shall have a
    standard 10/100 Ethernet Card.

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

d. System Structure
    The System shall consist of 3 sections
    i. Server Software
       The Server Software shall consist of the database, communications
       protocol to the access control hardware, communications protocol to the
       Thin Clients and a GUI for Server administration. Because of security
       concerns, the sole method for accessing the Server shall be the Thin Client.
       There shall be no browser access into the Server. The complete Software
       database shall reside solely on the PC housing the Server to take
       advantage of network back up tools. The complete Server Software and
       Database shall not reside solely on the access control hardware. The
       database shall be SQL compliant. There shall be no 3rd party license fees
       associated with the SQL database.

    ii. Thin Client Software
        The Thin Client (defined here as the application/Client by which users
        interface to the system: it has no processing or database storage
        functionality) shall provide the sole means of controlling the access control
        hardware via the Server or making changes to the Server database or
        reporting on system activities. There shall be no browser interface to the
        system to minimize security risks. The thin Client may be installed either on
        the same PC as the Server Software or a different PC. The thin client shall
        be easily transportable on a 50-megabyte "thumb" drive or other transport
        device.

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

2. Hardware
   a. Scope of Control
      There shall be several types of control devices
      i. Controllers
         The system shall consist of either 2 or 4 door 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 via expansion boards or modules.

      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 24 inputs. The 2 Reader Controller shall be expandable up to 12 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 relay 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 up to 20 outputs.   The 2 Reader Controller shall be expandable up to 10 outputs.

   b. Capacity
      The limit on the number of doors shall be solely constrained by Ethernet and TCP/IP standards

c. Communication
    i. Communication to Server
        All communication 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. All communications between Controllers shall be via a TCP/IP 10/100 bus. The Controllers shall operate on a true Peer-To-Peer protocol with each Controller being able to communicate directly to other Controllers and to the Server. 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
        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
        1. Supported Network Type
            All communication between a host Controller and its Expansion modules shall be via a supervised, encrypted, 9 bit RS-485 bus. The Expansion modules can be placed up to 1,000 feet away from the Controller.

        2. Capacity
            Different module types can be located on a single RS-485 bus.

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

d. 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
        3. Bar Code
        4. Keypad
        5. Biometric
        6. Electronic Discharge or Touch Memory Devices
        7. Keri Systems MS Series 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 cost.

e. 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 longer back up the memory.

ii. Cardholders
The Controllers must have the capacity to store up to 50,000 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.

f. 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.

g. Power Requirements
   i. Main Controller
   The main Controller shall be powered from 12VDC and draw no more than 650mA 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 Reader types' current draw shall not exceed 120 mA at 12VDC and shall be powered from the Controller. They can optionally be powered locally.

h. 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 backwards voltage.

   iii. There shall be a reset LED to indicate when the Controller memory is cleared.

   iv. All relays shall have status LEDs indicating their programmed logical status.

i. Operating Temperature
   The operating temperature range of the Controller shall be no less than -40º F to 140º F (-40º C to 60º C) at 0% to 90% Relative Humidity, non-condensing.

j. 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.

  k. Mechanical Spec.
    i. Main Controller
    The maximum dimensions for the Controller within the enclosure shall be 13.125 inches high by 10.625 inches wide by 3.06 inches 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 within the enclosure shall be 9.50 inches high by 8.00 inches wide by 4.00 inches 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.

3. 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 -22°F to 150°F (-30°C to 65°C).

  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 inches high by 1.60 inches wide by 0.625 inches 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 120mA. 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 inches (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 inches high by 3.25 inches wide by 0.625 inches 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 120mA. 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 inches (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 inches high by 2.95 inches wide by 0.625 inches 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 120mA. 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 inches (12.5 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.

4. 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 inches long by 2.13 inches wide by 0.065 inches thick (8.6 cm H x 5.4 cm W x 178 mm D).

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

  The dimension shall be 3.38" x 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.

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 inches long by 0.98 inches wide (at its widest area) by 0.157 inches 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.

5. Software
   a. Configuration
   All configuration, programming, and monitoring of the access control system must be done through a Thin Client Software program that makes these tasks easy to perform and is supported by an optional two hour on-line training course. For security purposes, no browser-based software configuration shall be acceptable.

   b. Features
      i. The Software shall be a Client/Server architecture with no browser access into the system to minimize security concerns.

      ii. Multiple Operators shall have the ability to concurrently connect to the access control Server.

      iii. The system shall have the ability to be divided into an unlimited number of sites up to the number of readers in the system.

      iv. The system will allow system operators to be assigned different privilege levels at different sites.

      v. The system will allow the user to create an unlimited number of user definable fields in the cardholder record.

      vi. The system will allow for different daylight savings time schedules based upon a Controller's location.

      vii. All relay points must be optionally programmable to either follow the state of an associated input point, to be latched to a state based on an input point or formed a specific time period after being triggered by an input state.

viii. The operation of all Form C, output relay points must be assignable to time zones, such that the output relay points can have time periods when they are active/operational, and time periods when they are inactive/idle.

ix. All input monitoring points must be linkable to output relay points, allowing input events to initiate output relay responses.

x. For each Controller and its associated I/O Expansion Boards, all input monitoring points and output relay points on that Controller must be able to be used in multiple links on that Controller, allowing any combination of Controller inputs to trigger any combination of Controller outputs.

xi. An unlimited number of access groups (combinations of access/egress points and time zones) shall be available for creation and assignment of Cardholders access privileges.

xii. Cardholders can be assigned to an unlimited number of access groups.

xiii. The Software shall contain a utility to automatically store archived event data in weekly, monthly or yearly files.

xiv. The Software shall have the ability to optionally configure up to three, separately configurable, event monitoring windows, with each window capable of displaying operator-selectable event information.

xv. It shall have the ability to automatically unlock and relock specific doors at specified times of the day and day of the week, with user-defined overrides on user defined dates.

xvi. It shall have the ability to implement a "First Person In" feature such that an auto-unlock schedule is not activated until an authorized person has entered the premises. This feature should allow early entrance in fifteen minute increments up to one hour in advance of the specified unlock time.

xvii. The Software shall have the ability to disable the reporting of specified events that do not need to be tracked, to save event storage space on the Controller.

xviii. The Software shall have the ability to poll the access control network and retrieve network hardware status information that the program uses to automatically setup and configure itself without manual data entry.

xix. It shall allow the assignment of future activation and expiration dates and times to individual Cardholders, which are stored at the Controller level. The operator shall be able to set the time frame for activation or deactivation in 1 minute increments.

xx. It will allow multiple Access Groups per Card user.

xxi. The Software will allow multiple Credentials per user.

xxii. Controllers may be assigned to local geographic time zones so the system can accurately report local times for events.

xxiii. The system will allow the customer to design various action sequences using the Controller's inputs and outputs to allow for user defined needs.

xxiv. The system shall allow manual or automatic assigning of static Ethernet addresses.

xxv. 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.

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

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

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

   ii. The Software shall have the ability to manage up to 64 distinct time zones with each time zone subdivided into the 7 days of the week divided into 4 start/stop time intervals and 6 holiday schedules.

d. Reporting
The Software shall have a library of pre-defined, commonly used reports, and will also allow for the use of 3rd party reporting tools for user-generated custom reports.

6. Warranties
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.

a. A two-year no questions asked warranty for the Controller and Expansion and Reader Interface Modules.

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

c. A limited lifetime warranty for standard "Clamshell" Proximity Cards and Key Tags.

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