ACCESS CONTROL SYSTEM (ACS) OVERVIEW

Vendor will provide and install an integrated door access system with **9** doors. System shall integrate with BadgePass Server software to provide a platform for integrated card issuance, access control and visitor management. If vendor wishes to quote another manufacturer, it should be approved by the IT department at least 5 business days prior to bid opening.

SCOPE OF WORK

The contractor shall furnish all equipment, material and labor required in accordance with this specification and applicable drawings for a fully operational Access Control System to the complete satisfaction of the customer. Pulling and Installation of all wire/cable will be performed by Mt. Pleasant Fire Dept.

It is the intent of this specification to provide a complete and operational system ready for use. All equipment, accessories and/or materials necessary for the proper operation of the System as specified shall be deemed part of the specifications and shall be provided by the Contractor.

The contractor shall set up all initial door and user groups and provide training for the user on the programming and operation of the system

SUBSTITUTIONS

References to brand names are to establish minimal standard requirements. They are not intended to limit competition.

Bids on items or materials by other manufacturers will be considered. Substitutions **MUST** be of equal or higher quality, performance, and durability. Customer reserves the right to request demonstration of similar equipment to determine whether substitution is equal or better.

Any substitution or deviation from specified items MUST be fully documented to be considered. Substitutions not fully noted and documented may result in an invalid bid.

UNIFIED SECURITY PLATFORM (USP)

The Access Control System (ACS) shall be fully embedded within a Unified Security Platform (USP). The USP shall be an enterprise class software-based security platform.

Available functionality with the USP shall include:

- ACS live and real-time event monitoring.
- ACS web-based reporting (including custom reports and report templates).
- ACS alarm management.
- Microsoft Active Directory integration for synchronizing USP users and cardholders.
- Data-Sync utility for integration with existing employee database information.
- ACS system incident reports.

- Through the appropriate licensing options, the ACS shall be enabled as sub-system within the USP.
- ID badge design module.
- Credentialing module for employee, contractor, visitor, etc.
- Visitor management module.

GENERAL

The ACS shall be an enterprise class access control software solution. It shall be fully embedded within a Unified Security Platform (USP).

The ACS shall be capable of performing and integrating multiple security functions including the configuration, management and monitoring of cardholder access, hardware units (controllers), events, alarms, as well as real-time tracking and reporting.
The ACS shall be highly scalable and include provisions for future growth.

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

SYSTEM ARCHITECTURE

The ACS shall be based on a client/server model. The ACS shall consist of Server Software Modules (SSM) and Client Software Applications (CSA). The ACS shall be both a multi-user and a multi-tasking environment.

The ACS shall support the installation of SSM and CSA on the same machine. Conversely, the ACS shall support a distributed environment where the SSM and CSA can be installed across unlimited PCs over an IP network.

CSA's shall ping the SSM and check for updates. If updates are available, the CSA shall install the update without action from the user. Upon installation, the USP will publish CSA's as an available installation program over the network. No CD shall be required to install a CSA at a remote PC connected to the network.

The ACS shall be an IP enabled solution. All communication between the SSM, CSA, and hardware controllers shall be based on standard TCP/IP protocol. The ACS shall support the creation of security partitions. Security partitions shall allow the system administrator to logically segment the configuration database and group multiple entities within a security partition.

SYSTEM DESIGN GUIDELINES

The ACS shall be designed to run on a standard PC-based Windows server platform.

The ACS interface shall be easy-to-use and minimize the number of external applications required to configure and monitor the system. The user interface shall consist of a single configuration client interface and a single live monitoring client interface.

The ACS server modules shall be compatible with multiple 32-bit and 64-bit operating systems including any of the following Windows Server 2003, Windows Server 2008, Windows Server 2008 R2 and future Windows Server releases. ACS management modules shall also be compatible with list of compatible Operating Systems for the ACS client modules.

The ACS client modules shall be able to run on all of the following platforms: 32 and 64 bit versions of Windows XP, Windows Vista, and Windows 7.

The ACS database server(s) shall be built on Microsoft's SQL Server 2005, SQL Server 2008, including SQL Express Editions.

SYSTEM SCALABILITY AND CAPACITY

The ACS shall be capable of supporting a wide range of configurations. The ACS shall be capable of supporting access control configurations that consist of a single door and one reader to a configuration consisting of a multitude of doors with facilities spanning multiple geographic areas.

The ACS shall be upgradeable one entity at a time, for example: 1 credential at a time, 1 door at a time, 1 cardholder at a time, etc.

The ACS shall support an unrestricted number of controllers and interface cards.

The ACS shall permit multiple instances of Client Software Applications (CSA) to run simultaneously on the network. The number of instances of CSA shall only be limited by the number of available application licenses. Only one CSA application type can be simultaneously active on a single workstation.

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

SYSTEM SECURITY AND ENCRYPTION

Communication between the SSM and CSA (sever-to-server and client-to-server) shall be encrypted. The ACS client applications (CSA) shall be password protected. Passwords shall be stored in the Configuration Server database in an encrypted manner.

The ACS shall limit what users can view in the configuration database via security partitions (database segments). The administrator, who has all rights and privileges, shall be allowed to segment a database into multiple security partitions. Users who are given access to a specific partition shall only be able to view entities (components) within the partition they have been assigned.

The system shall use smart card contactless cards. Card numbers shall be encrypted within the system. Communication between the card reader and the ACS controllers shall be encrypted.

SERVER SOFTWARE MODULES (SSM) OVERVIEW

The ACS SSM shall be fully embedded within the USP.

The SSM shall be responsible for receiving, processing and responding to requests from the CSA. The SSM shall consist of a Configuration Server, an Access Server, and an Integration Server. Several Access Servers and Integration Servers modules shall be supported per Configuration Server.

A dedicated SSM module shall be used as an Integration Server allowing the ACS to connect to multiple external systems such as a Microsoft Active Directory server and an external video surveillance system.

The SSM shall offer the capability to be installed on either the same server, or on several servers to enable distributed operation in a LAN or WAN environment. The SSM shall not limit the number of servers which can be networked together to form a distributed server system.

The SSM shall automatically launch at computer start up, irrespective of whether a user is logged onto the machine or not.

CONFIGURATION SERVER

The Configuration Server shall be the central database that contains all the system information and component configuration.

The Configuration Server shall support the configuration/management of the following components:

- Door Controllers (hardware units)
- Input and Output (IO) modules (hardware units)
- Doors
- Door Groupings
- Schedules (Including Holiday Schedules)
- Access rules
- Cardholder Groups
- Event Notification Service
- Alarms Conditions
- Users & User Groups
- Security Partitions
- Scheduled Tasks

- Custom Events
- Custom Output Behavior
- Input – Output (IO) Linking Rules
- Custom Fields

At system start up, the Configuration Server shall download all the configuration information to each Access Server under its control.

The Configuration Server shall authenticate users and give access to the ACS based on predefined user access rights or privileges.

The Configuration Server shall continuously monitor Server application connections and Client application connections.

ACCESS SERVER

The Access Server shall be the server that synchronizes all hardware units under its control. The Access Server shall also be able to validate and log all access activities and events when the controllers are online.

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

Synchronization of hardware units shall be transparent to users and shall occur in the background.

If communication is lost between the controller and the server, the system shall continue to function at its last downloaded capability and store a minimum of 250,000 transactions in the buffer. Once communication is restored, the records shall be uploaded to the server so that no transactions are lost.

The Access Server shall support doors and controllers located within one or more facilities.

At system start up, the Access Server shall load all the configuration information that is applicable to the units under its direct control.

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

INTEGRATION SERVER

The Integration Server shall enable the connection and data synchronization of the ACS to the following types of external systems:

- Microsoft Active Directory
- Any ODBC database

CLIENT SOFTWARE APPLICATIONS (CSA) OVERVIEW

The Client Software Applications (CSA) shall provide the user interface for ACS configuration and monitoring. The CSA shall consist of the Configuration UI for system configuration and the Surveillance UI for monitoring. The Server Administrator shall be used to configure the server database(s). The CSA shall be Windows based and provide an easy-to-use graphical user interface (GUI).

The ACS CSA shall be fully embedded within the USP.

The CSA shall perform functions without interfering with any of the SSM operations (for example, responding to access requests, logging ACS events, etc.).

The CSA shall support multiple forms of IP network connectivity, including LAN, WAN, VPN, and Internet technologies. The CSA shall be able to log into the ACS from a remote site.

All applications shall provide an authentication mechanism, which verifies the validity of the user. As such, the administrator (who has all rights and privileges) can define specific access rights and privileges for each user in the system.

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

CONFIGURATION USER INTERFACE (UI)

The ACS Configuration UI application shall be the same Configuration UI application for the USP.

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

The Configuration UI shall provide decentralized configuration and administration of the entire access control system from anywhere on the IP network.

The Configuration UI shall allow the system administrator to configure the ACS entities. An entity shall be defined as a system component used to create an access control system.

The user shall easily navigate between this application and the other CSA (if he has access rights) by single point and click functionality.

The Configuration UI shall facilitate the creation of entities through the use of installation wizards. Installation wizards shall guide the user through a step by step installation process.

The Configuration UI shall provide a static reporting interface to:

- View historical events based on entity activity. This reporting interface shall be in addition to the monitoring and reporting interface provided by the Surveillance UI. The user shall be able to perform actions such as printing a report and troubleshooting a specific access event from the reporting view.

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

The Configuration UI shall include an integrated import utility.

SURVEILLANCE USER INTERFACE (UI)

The ACS Surveillance UI application shall be the same Surveillance UI application for the USP.

The Surveillance UI shall provide a graphical user interface to control and monitor the ACS.

The Surveillance UI shall be based on and use the latest UI design tools and usability concepts such as:

- Task-oriented approach
- Dynamically adaptive
- Widgets

The Surveillance UI shall provide decentralized monitoring of the entire system from anywhere on the IP network.

The Surveillance UI, part of the USP, shall provide an interface to support the following access control capabilities:

- Monitoring and management of access events and alarms
- Viewing of cardholder picture or badge IDs
- Generation of configuration and activity reports
- Viewing of HTML files including alarm instructions
- Management and execution of hot actions

The Surveillance UI shall be able to monitor the activity of the following entities in real-time:

- Cardholders
- Cardholder groups
- Doors
- Event, alarm, monitoring/tracking

The Surveillance UI shall be customizable to user preferences. The Surveillance UI shall provide several visual cues when the system status has changed. The user shall easily navigate between this application and the other CSA (if he has access rights) by single point and click functionality.

The ACS shall permit the user to select multiple entities to monitor from the Surveillance UI by adding the entities one by one to the monitored list. From the monitored list, the user shall be allowed to trigger individual entity tracking and report generation functions. While monitoring an area, the user can also trigger a report to list all cardholders within the area.

SERVER ADMINISTRATOR

The Server Administrator shall be used to configure all the SSM (Configuration Server, Integration Server, Access Server, and Server Monitoring Service), associated licenses, as well as the services available on each local machine. The Server Administrator shall be accessible through a graphical user interface (UI) and shall be installed on all machines that run one or more SSM.

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

- Configure the databases and database servers.
- Start/Stop a database server.
- Define the client-to-server communications security settings.
- Configure the network communications hardware, including connection addresses and ports.
- Add and configure hardware extensions and discovery options.
- Configure system SMTP settings (mail server and port)
- Configure the Server Monitoring Service automatic email settings.
- Configure event and alarm history storage options.
- Manually back up databases and/or restore the server databases, as well as configure scheduled backups of the databases.

HARDWARE COMPATIBILITY LIST (HCL) OVERVIEW

The ACS shall interface with IP-enabled hardware access controllers, interface modules, and IO modules.

The ACS shall have an open architecture that supports the integration of third party IP-based door controllers. Through these door controllers, the ACS shall interface with industry standard access control readers.

The ACS shall have an open architecture that supports the integration of third party IP-based IO hardware modules. Through IO modules, the ACS shall interface with multiple input points and connect to multiple output relays.

The ACS shall simultaneously support mixed configurations of access control hardware from multiple vendors.

The ACS shall support multiple types of hardware devices:

- Single-reader controllers

- 2-reader controllers
- to 64-reader controllers
- Integrated readers and door controllers
- Power-over-Ethernet (PoE) enabled door controllers
- Wireless Door Controllers
- Keyed Fire Pulls

INTEGRATION WITH MICROSOFT ACTIVE DIRECTORY

The ACS shall support a direct connection to a Microsoft Active Directory server. Active Directory integration shall enable the synchronization of information from the Active Directory server to the USP.

Active Directory integration shall permit the central management of the USP users, user groups, cardholders, and cardholder groups. When enabled, Active Directory shall manage user log on to the USP client applications through the user's Windows credentials. Log on to the USP shall utilize native Active Directory password management and authentication features.

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

- Users (user-name, first and last names, email address, and more)
- User groups (user group name, description, and group email address)
- Cardholders (first and last names, description, email, and more)
- Cardholder groups (cardholder group name, description, and group email address)
- When enabled, the addition, removal, or suspension of a user's account in Active Directory shall result in the creation, modification, or disabling of the equivalent user account in the USP.
- When enabled, the addition, removal, or suspension of a user's account in Active Directory shall result in the creation or disabling of the equivalent cardholder account in the USP.
- System Supported synchronization methods for additions, modification, and disabling of synchronized entities shall include:
- Manual synchronization
- Scheduled synchronization

CONTROLLER (UNIT) MANAGEMENT

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

The ACS shall support the configuration of units from the Configuration UI.

The ACS shall support remote firmware upgrades, if supported by the hardware. Upgrades shall be executed on edge devices connected to the network.

The ACS shall support multiple reader types, including card or keypad readers. It shall be possible to define controller settings on a controller-by-controller basis. This shall permit full customization of the access control infrastructure by customizing controller settings based on card and reader specifications.

Inputs detected by the controller or IO modules shall trigger appropriate events in the ACS.

IO module inputs and outputs shall support both user-defined and physical names. It shall be possible to modify user-defined names.

Maintenance mode

The ACS shall support Maintenance Mode operation during controller installation or maintenance.

While in maintenance mode, the ACS shall force a door to be unlocked (lock schedules are overridden).

Unit Swap Utility

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

USER AND USER GROUP MANAGEMENT

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

Common access rights and privileges shared by multiple users shall be defined as User Groups. Individual group members shall inherit the rights and privileges from their parent user groups.

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

CARDHOLDER AND CARDHOLDER GROUP MANAGEMENT

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

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

It shall be possible to associate a picture to the cardholder’s profile. The picture shall be imported from a file or captured with a digital camera.

It shall be possible to create a cardholder without requiring the immediate assignment of a credential. Credential assignment can occur at a later time.

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

CREDENTIAL MANAGEMENT

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

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

Automatic creation shall allow the user to create a credential entity by presenting a credential to a selected reader. The ACS shall read the card data and associate it to the credential entity. It shall be possible to automatically enroll any industry standard card format.

Manual creation shall allow the user to select the type of credential to create and to enter the data manually.

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

- Once enrolled, new custom card formats shall appear in the card format lists for manual card enrollment.

- An unrestricted number of additional custom card formats can be added.

- The administrator shall be able to set the following options when defining a new format:
    - The order in which card fields appear in the user interface or CSA
    - Whether a field is hidden from, or visible to an operator
    - Whether a field is read only or modifiable by an operator

- The order and location of a field's data/ Location can be defined on a bit-by-bit basis

The ACS shall permit the creation of one or more credentials in advance, without requiring the assignment of the credential(s) to a cardholder. A credential in this state shall be designated as an "unassigned credential".

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

The ACS must be capable of scanning a driver's license, PDF417 barcode, magstripe, & EPIC barcode and populating the system.

Batch enrollment of credentials shall be supported.

Although multiple industry standard cards must be supported in the ACS, the only acceptable format for this project is a smart card contactless card, such as MOCA or Mifare.

Lower security formats such as 26-bit Wiegand must be supported in the event the end user wishes to utilize contactless prox technology, other than door access, which has not incorporated smart card technology. In this situation the ACS should be able to interface with third party software through exported event manager csv, html, and other file formats utilizing needed features such as name, card number, groups, etc.

BADGE DESIGNER

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

Badge template shall be related to entity type.

Badges production shall be capable of printing to one or more printers located locally or on the network and printing shall occur automatically based on rules defined within the USP.

Badge production shall consist of selecting the credential or entity type, the badge template (when applicable), and clicking print.

Batch printing of cards shall be available.

Badge designer software shall be capable of designing badges for all entity types (card users, employees, contractors, visitors, etc.) within the same location.

The contents of a badge template must include:

- The cardholder's first name
- The cardholder's last name
- The cardholder's picture
- Custom fields
- Bitmap graphics
- The name of the cardholder's credential
- Lines and rectangles

- Dynamic text labels linked to custom fields
- Static text labels
- Barcodes (Code 39, Code 128, PDF417, EPIC, QR and others)

Copy and paste of badge template objects shall be available from one design to another.

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

It shall be possible to set the color of text labels.

It shall be possible to easily reorder the layer levels (bring forward, send to back, etc.)

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

Standard portrait and landscape badge formats, custom card sizes and dual-sided badges shall be supported.

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

Fields must be interchangeable between static and dynamic.

Fields (including custom fields) and information must be automatically pulled from the USP database.

DOOR MANAGEMENT

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

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

The ACS shall support the following forms of authentication:

- Card Only
- Card or Keypad (PIN)
- Card and Keypad (PIN)

AREA MANAGEMENT

The ACS shall support the configuration and management of areas. A user shall be able to add, delete, or modify an area if he has the appropriate privileges.

The ACS shall support areas within areas (nested areas).

The ACS shall permit multiple access rules to be associated to an area. To facilitate the assignment of access rules, the ACS shall support associating rules to areas in lieu of doors. All perimeter doors shall then inherit the access rules assigned to the area.

The ACS shall have the option to give visitors cards which will work on designated doors at the time of check in. The cards shall not work until a visitor is checked in and assigned the appropriate access areas. When a visitor leaves and checks out, or if a visitor leaves campus with the card and is manually checked out, the card shall be inactive. This process of turning a card on/off shall be automatically controlled through the Visitor Manager CSA.

In/Out

The ACS shall support in/out functionality. When an "out" situation is detected, an associated "out" event shall be triggered in the ACS.

The ACS shall have reporting capability of an "onsite list". In the event of an emergency, the onsite list shall be easily printable or emailed for the purpose of verifying who may still be left inside the building.

The ACS shall track people using the card readers within the building to actively show the last location a person passed through. The ACS shall track visitors who are issued credentials in the same manner.

SCHEDULE MANAGEMENT

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

The ACS shall provide full flexibility and granularity in creating a schedule. Daily schedules shall define a schedule applicable on a daily basis. Weekly schedules shall define specific schedules for each day of the week. The ACS shall support multiple blocks of schedule per day.

It shall be possible to associate schedules to the following entities:

- Access rules
- Scheduled tasks
- Alarms
- Events/actions

ACCESS RULE MANAGEMENT

The ACS shall support the configuration and management of access rules. A user shall be able to add, delete, or modify an access rule if he has the appropriate privileges.

An access rule shall be associated to a door side (entry or exit reader) or door (both entry and readers), area. It shall be possible to create and unlimited number of access rules per door, area, or elevator floor.

Access rules shall determine whether a cardholder or cardholder group shall be granted or denied access based on a schedule. Once an access rule is created, the user shall associate the access rule to a door side, door, area, or floor.

It shall be possible to program an access rule throughout the entire system.

An access rule shall be assignable to multiple door controllers. Separate access rules shall not be required if the same rule applies to several independent controllers.

The ACS shall support the viewing and/or configuration of the following properties for an access rule:

- Access rule name
- Access rule description
- Schedule when the rule is active
- Permissions when rule is active (grant or deny access)
- Cardholders and cardholder groups affected by the rule

EVENT/ACTION MANAGEMENT

The ACS shall support the configuration and management of events. A user shall be able to add, delete, or modify an action to an event if he has the appropriate privileges.

The ACS shall receive all incoming events in the system. The ACS shall take the appropriate actions based on user-define event/action relationships.

The ACS shall be able to view events from multiple video systems.

The ACS shall support IO linking; one or more inputs shall trigger one or more outputs.

The ACS shall receive and log the following events:

- Alarm events
- Application events (clients and servers)
- Area events
- Cardholder events
- Credential events
- Entity about to expire events
- Door events
- Unit events
- User events
- System-wide events
- Hardware tamper events
- The ACS shall allow the creation of custom events.

The ACS shall have the capability to execute an action in response to an event. Possible actions include, but are not limited to the following:

- Send an email
- Email a report
- Send a message
- Trigger an alarm
- Trigger an output
- Trigger a macro
- Sound or silence a buzzer
- Play a sound

The ACS shall allow a schedule to be associated with an action. The action shall be executed only if it is an appropriate action for the current time period.

REPORT GENERATION

The ACS shall support report generation (database reporting).

The ACS shall support both static and custom reports. Report generation shall not result in any degradation of system performance.

Reports are fully configurable. A user has the option of generating static reports from an existing list, generating reports from a list of user-defined templates, or creating a new report or report template. Each report can be customized to the current context.

The ACS shall support the following types of reports:

- Configuration reports (cardholders, credentials, units, access rules, readers/inputs/outputs, and more)
- Activity reports (Cardholder, visitor, credential, door, unit, area, zone, and more)
- Audit trail reports
- Incident reports
- Time and attendance reports
- Alarm report

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

SCHEDULED TASKS

The ACS shall support scheduled tasks. Scheduled tasks shall be executed on a user-defined schedule at a specific day and time. Recurring or periodic scheduled tasks shall also be supported.

Scheduled tasks shall support standard actions available within the ACS such as sending an email or emailing a report.

CUSTOM FIELDS (USER-DEFINED FIELDS)

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

Custom fields shall be supported for the following entities: Cardholders, Cardholder groups, and Credentials.

Supported custom fields include: Text, Integers, Decimal Numbers, Dates, Boolean, and Images (graphics).

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

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

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

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

CARD READERS

Multi-technology card readers are required. Supported card formats should include MOCA, Schlage, XceedID, MIFARE, HID Proximity protocols, HID iClass, GE/CASI
ProxLite, AWID Proximity, LenelProx, etc.

Reader must have

- A read range of up to 4.5" or better
- Environmental protection for indoor or outdoor placement
- Security Key Management
- UL Listing
- Mullion mount available
- Mini-mullion sizes (smaller read range), where approved for install

Readers must be PIV compliant.

GENERAL CODES AND STANDARDS

All work shall comply with the applicable codes and standards as issued by NEC, ANSI/EIA/TIA, BISCI, IEEE, UL, IFC, NFPA and the Michigan Construction Code.

The complete system as installed shall meet all applicable Fire Codes.

REFERENCES

Provide a list of current references.

MANADATORY WALK-THROUGH OF PROJECT

A mandatory walk-through of the project site will be held on Thursday July 19, 2012 at 9:00AM at the Mt. Pleasant Department of Public Safety, 804 East High Street, Mount Pleasant, MI 48858. **Attendance at the walk-through is required to have bid considered.**

BID DUE DATE

Sealed bids must be received in the office of the Mount Pleasant City Clerk, 320 W. Broadway, Mount Pleasant, MI 48858 by 1:30PM on Tuesday July 31, 2012 to be considered. Bids will be opened at that time.

Questions related to this bid should be directed to: Gregory L. Walterhouse, Fire Chief (989) 779-5152, or gwalterhouse@mt-pleasant.org